UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL INGENIERIA DE SISTEMAS
CARRERA PROFESIONAL INGENIERIA DE SISTEMAS

POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS

LÍNEA DE INVESTIGACIÓN: Ingeniería y Tecnología.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

TESISTA:
Bach. Villa Sanchez, Luis Arnold

ASESOR:
Mg. Flores Vidal, Jimmy Grover

HUÁNUCO – PERÚ
2024

DEDICATORIA

Agradezco a Dios por concederme la existencia y por permanecer a mi lado, especialmente en este crucial período de mi desarrollo académico.

A mis padres, quienes me han brindado amor incondicional y han sido mi mayor motivación para alcanzar mis metas. Su sacrificio y dedicación son la luz que ilumina cada paso de mi trayectoria educativa.

A mis profesores y mentores, cuya guía experta ha sido fundamental en mi formación académica. Agradezco sinceramente su paciencia, sabiduría y compromiso con mi crecimiento intelectual.

Este trabajo no solo es el resultado de mi esfuerzo individual, sino también de la contribución invaluable de todos aquellos que han creído en mí.

A todos ustedes, les dedico este logro con profundo agradecimiento y gratitud. Este proyecto de tesis es también suyo, y celebro cada paso con la certeza de que lo hemos alcanzado juntos.

AGRADECIMIENTO

Expresamos nuestra gratitud, primero, a Dios por otorgarme la fortaleza y coraje necesaria para finalizar exitosamente este proyecto de tesis.

Agradezco al Ingeniero Jimmy Flores Vidal, asesor, cuya orientación experta y dedicación han sido esenciales para dar forma y dirección a este trabajo. Su apoyo constante y valiosos aportes han sido un faro que ha iluminado cada paso de esta investigación.

A mi familia, agradezco su inquebrantable respaldo y comprensión a lo largo de este arduo proceso. Su amor y apoyo moral han sido la fuerza motivadora que me ha impulsado a alcanzar este logro académico.

RESUMEN

Este proyecto parte de la problemática de la Municipalidad Distrital de Amarilis que es la falta de políticas de seguridad y esto pone en riesgo la confidencialidad, integridad y disponibilidad de la información que se evidencia por muchos factores como los accesos no autorizados, evidencias de malware, fallos en la seguridad, errores humanos, desastres naturales y fallas tecnológicas, fallas en los sistemas de respaldo, acciones maliciosas internas y brechas de seguridad de terceros; todos estos factores nos pueden llevar a la perdida de información, mala reputación, riesgos legales y cumplimiento normativa de acuerdo a las políticas que maneja la municipalidad distrital de amarilis, interrupción de operación, costos financieros y vulnera a toda la entidad. Este proyecto tiene como objetivo implementar Políticas de seguridad para mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

Para el desarrollo de este proyecto se inició con el diagnóstico de la situación actual de la Municipalidad Distrital de Amarilis con el propósito de analizar las actitudes, perspectivas y la situación esencial de la efectividad del resguardo de la información.

Luego se identificó los escenarios de riesgo de Tecnología de información para posteriormente valorizarlos y poder realizar su respectivo tratamiento de estos escenarios de riesgos bajo la metodología MAGERIT versión 3, con los resultados de esta metodología se procedió a la auditoría de procesos bajo la metodología COBIT 4.1 para identificar los niveles de cada modelo de madurez en la que se encuentra la Municipalidad Distrital de Amarilis con estos resultados nos proporciona una visión integral del resguardo de la información en la entidad, permitiendo tener un enfoque para el diseño de las políticas de seguridad de la información.

Una vez diseñado las políticas de seguridad se procedió a su respectiva implementación previa coordinación con la Municipalidad Distrital de Amarilis para su aprobación, disposición, implementación y publicación.

En un periodo de dos meses se realizó una segunda auditoria de procesos bajo la metodología COBIT 4.1 para ver si las políticas de seguridad mejoran la efectividad del resguardo de la información.

Los resultados evidencian que realmente las políticas de seguridad mejoran la efectividad del resguardo de la información porque hubo un incremento significativo en las dos auditorías realizadas, en la primera obtuvo un resultado de NIVEL BAJO con un promedio de 15.82% y en la segunda auditoría obtuvo un resultado de NIVEL MEDIO con un promedio de 52.83%.

Con estos resultados podemos concluir que las políticas de seguridad desempeñan un papel fundamental en el fortalecimiento integral de la seguridad de la información en la Municipalidad Distrital de Amarilis. Estos hallazgos proporcionan una base sólida para recomendaciones prácticas y futuras iniciativas destinadas a optimizar la seguridad de la información en el ámbito municipal y han logrado cumplir con éxito los objetivos planteados.

Palabras Clave: Políticas de seguridad de la información, metodología MAGERIT versión 3, confidencialidad, integridad, disponibilidad, riesgo, metodología COBIT 4.1, modelos de madurez, efectividad, resguardo de la información.

SUMMARY

This project is based on the problem of the District Municipality of Amarilis, which is the lack of security policies and this puts the confidentiality, integrity and availability of the information at risk, which is evidenced by many factors such as unauthorized access, evidence of malware, security failures, human errors, natural disasters and technological failures, failures of backup systems, malicious internal actions and third party security breaches; All of these factors can lead to loss of information, bad reputation, legal risks and regulatory compliance in accordance with the policies managed by the Amaryllis District Municipality, interruption of operations, financial costs and harm to the entire entity. This project aims to implement security policies to improve the effectiveness of information protection in the District Municipality of Amarilis.

For the development of this project, it began with the diagnosis of the current situation of the District Municipality of Amarilis with the purpose of analyzing the attitudes, perspectives and the essential situation of the effectiveness of information protection.

Then, the Information Technology risk scenarios were identified to subsequently assess them and be able to carry out their respective treatment of these risk scenarios under the MAGERIT version 3 methodology. With the results of this methodology, the process audit was carried out under the COBIT 4.1 methodology. to identify the levels of each maturity model in which the District Municipality of Amarilis is located. With these results, it provides us with a comprehensive vision of the protection of information in the entity, allowing us to have an approach for the design of the security policies of the entity. information.

Once the security policies were designed, their respective implementation was carried out after coordination with the District Municipality of Amarilis for their approval, provision, implementation and publication.

In a period of two months, a second process audit was carried out under the COBIT 4.1 methodology to see if the security policies improve the effectiveness of information protection.

The results show that security policies actually improve the effectiveness of information protection because there was a significant increase in the two audits carried out, in the first one it obtained a LOW LEVEL result with an average of 15.82% and in the second audit it obtained a result of MEDIUM LEVEL with an average of 52.83%.

With these results we can conclude that security policies play a fundamental role in the comprehensive strengthening of information security in the District Municipality of Amarilis. These findings provide a solid basis for practical recommendations and future initiatives aimed at optimizing information security at the municipal level and have successfully met the stated objectives.

Keywords: Information security policies, MAGERIT version 3 methodology, confidentiality, integrity, availability, risk, COBIT 4.1 methodology, maturity models, effectiveness, information protection.

INTRODUCCIÓN

La seguridad de la información es un componente esencial en el entorno digital actual, especialmente para entidades gubernamentales encargadas de gestionar datos sensibles y críticos para el funcionamiento de la sociedad. En este contexto, el presente proyecto de tesis, titulado "Políticas de Seguridad para la Efectividad del Resguardo de la Información en la Municipalidad Distrital de Amarilis", aborda la problemática sustancial que enfrenta dicha municipalidad respecto a la falta de políticas de seguridad.

En este proyecto se implementó políticas de seguridad de la información en la Municipalidad Distrital de Amarilis mediante la metodología MAGERIT versión 3 y la metodología COBIT 4.1 con el propósito de proteger, salvaguardar y conservar la información producida por los procesos que se realiza, evitando su posible pérdida mediante exposición a amenazas latentes en el entorno, como acceso no autorizado, manipulación o deterioro de la información en forma accidental o deliberada.

La estructura de la investigación se organiza de la siguiente manera para presentar dicho modelo:

En el CAPÍTULO I, se inicia la investigación abordando la problemática, objetivos, justificación, limitaciones y variables involucradas.

En el CAPÍTULO II, en el marco teórico, ofrece una revisión bibliográfica del tema principal y hace referencia a investigaciones previas relacionadas con el mismo.

En el CAPÍTULO III detalla la metodología que servirá como guía para la implementación de las políticas de seguridad de la información en la Municipalidad Distrital de Amarilis (MDA). También, se describe el diseño de la investigación y se presenta la muestra de la población.

En el CAPÍTULO IV, se desarrolla la identificación de activos de TI para el análisis y valorización de riesgos y con esos resultados realizar la auditoria de procesos para el diseño de las políticas de seguridad de la información propuestas para la Municipalidad Distrital de Amarilis.

En el CAPÍTULO V, concluye la investigación describiendo la discusión y presentando las conclusiones. Al finalizar, se enumeran las recomendaciones que serán de gran utilidad para la implementación de las políticas de seguridad de la información.

CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

CAPITULO I
PROBLEMA DE INVESTIGACIÓN

1.1. Fundamentación del Problema de Investigación

En la municipalidad distrital de amarilis, se ha identificado una realidad problemática que es la falta de políticas de seguridad y esto pone en riesgo la confidencialidad, integridad y disponibilidad de la información que se evidencia por muchos factores como los accesos no autorizados, evidencias de malware, fallos en la seguridad, errores humanos, desastres naturales y fallas tecnológicas, fallas en los sistemas de respaldo, acciones maliciosas internas y brechas de seguridad de terceros; todos estos factores nos pueden llevar a la perdida de información, mala reputación, riesgos legales y cumplimiento normativa de acuerdo a las políticas que maneja la municipalidad distrital de amarilis, interrupción de operación, costos financieros y vulnera a toda la entidad.

Por la falta políticas de seguridad en la municipalidad distrital de amarilis no se puede proteger la información y los activos de la organización contra posibles amenazas y riesgos, ya sean internos o externos.

1.2. Formulación del Problema de Investigación General y Específicos

1.2.1. Problema General:

- ¿De qué manera la implementación de las políticas de seguridad va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?

1.2.2. Problema Específico:

- ¿De qué manera la identificación de los activos de sistemas de información va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?
- ¿De qué manera la evaluación de las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?

- ¿De qué manera la evaluación de los modelos de madurez de los procesos de los sistemas de información va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?
- ¿De qué manera el Diseño de las políticas de seguridad va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?

1.3. Formulación del Objetivo General y Específicos

1.3.1. Objetivo General:

- Implementar Políticas de seguridad para mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis

1.3.2. Objetivos Específicos:

- Identificar los activos de sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis distrital de amarilis basado en la metodología MAGERIT V.3.
- Evaluar las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de Amarilis basado en la metodología MAGERIT V.3.
- Evaluar los modelos de madurez para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de AMARILIS basado en la metodología COBIT 4.1.
- Diseñar políticas de seguridad para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis basado en la metodología COBIT 4.1.

1.4. Justificación

La presente investigación se justifica debido a la creciente preocupación por parte del alcalde y el personal administrativo de la Municipalidad Distrital de Amarilis en torno a la falta de políticas de seguridad que esto conlleva a la perdida y fuga de la información sensible, Esto es un problema que puede tener consecuencias graves y perjudiciales para el funcionamiento y el rendimiento de dicha entidad. La información es un activo invaluable en cualquier organización, ya que respalda la toma de decisiones, facilita la realización de tareas y contribuye al logro de los objetivos establecidos. Sin embargo, debido a diversos factores, como errores humanos, fallos tecnológicos o desastres naturales, la información puede perderse o dañarse, lo que puede generar pérdidas financieras, retrasos en las operaciones, insatisfacción de los clientes y daños a la reputación de la entidad. Por lo tanto, resulta imprescindible abordar este problema y desarrollar políticas de seguridad para prevenir, mitigar y resguardar la pérdida de información.

La importancia de resolver el problema de perdida de información en la Municipalidad Distrital de Amarilis es para resguardar toda la información para así proteger los activos de la entidad, cumplir con la normativa y legal de la entidad y mejorar la eficiencia y la productividad de los procesos que opera en la entidad.

1.5. Limitaciones

Una de las principales limitaciones de este proyecto es que en la Municipalidad Distrital de Amarilis se cuenta con una gestión entrante y todos sus procesos funcionales y herramientas de gestión se encuentran en modificaciones basándose a las políticas de gobierno de la nueva gestión.

1.6. Formulación de Hipótesis

1.6.1. Hipótesis General

- **Ho:** Las políticas de seguridad mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

- **Ha:** Las políticas de seguridad no mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

1.6.2. Hipótesis Especifica:

- **H1:** La identificación de los activos de sistemas de información mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.
- **H2:** La evaluación de las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.
- **H3:** La evaluación de los modelos de madurez de los procesos de los sistemas de información mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.
- **H4:** El diseño de las políticas de seguridad mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

1.7. Variables

(HAIR JR., BLACK, BABIN, & ANDERSON, 2010) nos dice que, *"Al utilizar variables dependientes e independientes, se busca establecer una relación causal entre los fenómenos o eventos que se están estudiando. Las variables independientes son aquellas que se manipulan o controlan en el estudio, mientras que las variables dependientes son aquellas que se miden o registran para determinar el efecto o la influencia de las variables independientes."*

- **Variable Dependiente VD:** Efectividad del resguardo de la información.

  Esta variable es la que queremos estudiar y medir, y su valor dependerá de las políticas de seguridad implementadas en la Municipalidad Distrital de Amarilis.

- **Variable Independiente VI:** Políticas de seguridad.

  Esta variable es el factor que influirán en la efectividad del resguardo de la información.

1.8. Definición teórica y operacionalización de variables

1.8.1. Dimensiones

- **Variable dependiente:** Disponibilidad, integridad, confidencialidad, autenticidad y Trazabilidad.
- **Variable independiente:** Modelos de Madurez.

1.8.2. Indicadores

- **Variable dependiente:** % de resguardo de la información en la disponibilidad, % de resguardo de la información en la integridad, % de resguardo de la información en la confidencialidad, % de resguardo de la información en la autenticidad y % de resguardo de la información en el Trazabilidad.
- **Variable independiente:** % del impacto de los modelos de madurez en el criterio de información efectividad, % del impacto de los modelos de madurez en el criterio de información eficiencia % del impacto de los modelos de madurez en el criterio de información disponibilidad, % del impacto de los modelos de madurez en el criterio de información integridad, % del impacto de los modelos de madurez en el criterio de información disponibilidad, % del impacto de los modelos de madurez en el criterio de información cumplimiento, % del impacto de los modelos de madurez en el criterio de información confiabilidad.

1.8.3. Operacionalización de las variables

Tabla 1: Operacionalización de la variable dependiente

VARIABLE	DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES
Efectividad del resguardo de la información	(Martinez, 2022) Nos dice que la efectividad del resguardo de la información Hace referencia a la habilidad para salvaguardar los datos e información sensible de amenazas y riesgos, como accesos no autorizados, pérdida de datos, manipulación o robo de información.	Disponibilidad	% de resguardo de la información en la disponibilidad.
		Integridad	% de resguardo de la información en la integridad.
		Confidencialidad	% de resguardo de la información en la confidencialidad
		Autenticidad	% de resguardo de la información en la autenticidad.
		Trazabilidad	% de resguardo de la información en el Trazabilidad.

Tabla 2: Operacionalización de la variable independiente.

VARIABLE	DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES
Políticas de seguridad	Según (ISO 27001, 2013) Una política de seguridad, es una declaración formal de las reglas, directivas y prácticas que rigen la forma de gestión de los activos de tecnología e información dentro de una organización. Las políticas proporcionan una guía más detallada de cómo poner en práctica los principios y cómo éstos influirán en la toma de decisiones.	Modelos de Madurez	% del impacto de los modelos de madurez en el criterio de información efectividad
			% del impacto de los modelos de madurez en el criterio de información eficiencia
			% del impacto de los modelos de madurez en el criterio de información disponibilidad.
			% del impacto de los modelos de madurez en el criterio de información integridad.
			% del impacto de los modelos de madurez en el criterio de información disponibilidad.
			% del impacto de los modelos de madurez en el criterio de información cumplimiento.
			% del impacto de los modelos de madurez en el criterio de información confiabilidad.

CAPITULO II
MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes Internacionales

(Avilés Arjimos & Uyaguari Guartatanga, 2012), en su investigación el principal objetivo fue *"Disminuir el riesgo y mantener las dimensiones de seguridad tomando en cuenta las recomendaciones de las normas ISO definidas."* En la estructura de esta investigación primero empezaron estableciendo su metodología, lo cual trabajaron con la metodología y el enfoque MAGERIT versión 3.0 para el análisis, desarrollo y gestión de riesgos utilizando las ISO y también se hizo el uso de su Software PILAR para que simulen la situación real, luego empezaron con el diseño de las políticas de seguridad par que de esa forma identifiquen las salvaguardas de acuerdo a su grado de riesgo e impacto con la finalidad de mitigar cualquier tipo de amenazas que pudieran poner en peligro la función del negocio, y para terminar con todos sus datos obtenidos en la investigación finalizaron con la última de etapa de la gestión y administración de riesgos donde se considera el diseño de nuevas políticas de seguridad basándose a las necesidades generados mediante el estudio.

(Pilla Yanzapanta, 2019), la tesis tuvo como objetivo "*Diseñar una política de seguridad de la información para el área de Tecnología de Información (TI) de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., en base a la norma ISO/IEC 27002:2013, que garantice la disponibilidad, integridad y confidencialidad de los datos de la organización."* En la estructura de esta investigación se llevó a cabo un análisis de la norma internacional ISO 27002:2013, para identificar controles aplicables y así poder mitigar los eventos de alto riesgo; y como último paso, se diseñó la política de seguridad de información para el área de Tecnología de Información. Finalmente, se recomienda que esta política sea aprobada por el Consejo de Administración, dando paso a su posterior implementación y difusión a todos los empleados

de la Cooperativa. En sus conclusiones el autor mencionó, que en su investigación obtuvo una política de seguridad de la información que están siguiendo los controle de la norma ISO-27002-2013, la cual están basados en lineamientos y controles de seguridad de información que debe cumplir todas las áreas involucradas de la cooperativa.

(Torres Núñez, 2015) en su investigación el principal objetivo fue *"Elaborar políticas de seguridad de la información en base a parámetros de la norma ISO/IEC 27002:2013 en la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato y como objetivos específicos tenemos; "Analizar la protección de la información actual contra acceso no autorizado, Establecer lineamientos de seguridad de la información mediante parámetros de la norma ISO/IEC 27002:2013 y Elaborar un plan de evaluación continua de seguridad de la información mediante responsabilidades y procedimientos"*

(Enríquez Miranda, 2011) en su investigación tiene como objetivo general *"Reflexionar sobre las políticas de seguridad que las empresas privadas deben implementar para precautelar su información confidencial de ataques externos.*

La Norma ISO 27001 hace una clara referencia a la seguridad de la información, donde se muestran los parámetros que se deben seguir para conseguir que el activo más importante de las organizaciones sea debidamente protegido. La Seguridad como lo determina la norma no solo se enfoca a una Seguridad lógica de la información donde se enfatiza la creación de usuarios, protección de acceso a Servidores, etc, sino también hace referencia al área física donde reside la misma.

La Tesis que pongo en consideración ha reflejado la propuesta de implementación de Seguridad Física en la infraestructura del Área de Servidores de la empresa Turbotech, también esquematiza los parámetros de Seguridad Lógica del Servidor Web que almacena los aplicativos Web de la organización, así como las diferentes"

(Oñate Arboleda, 2021) En este proyecto nos dice que, *"Dentro del diseño de las políticas de seguridad de la información se define un aspecto fundamental en seguridad informática en donde se evalúan las herramientas tecnológicas para asegurar, aplicar, monitorear algunos componentes establecidos en la política de seguridad para evitar ataques a los sistemas de información y que sea de uso obligatorio de los usuarios en las organizaciones. La política debe ser fácil de comprender, concisa para los usuarios, deben enmarcar las guías y las actividades de una organización, se deben aplicar según las directrices en donde se especifica el estándar y/o norma a utilizar como la ISO 27001:2013 protegiendo la información de cualquier amenaza. Se debe tener Comprensión y entendimiento de los requerimientos de seguridad y la Identificación de aspectos legales, comerciales y regulatorios relacionados con seguridad de la información"* y el autor concluye *"que las organizaciones al no tener un modelo a seguir de políticas de seguridad definidas es muy importante aplicarlas en una de las reglas definidas por el administrador o gestor de la seguridad de tecnologías de información escogido al interior de la entidad para evitar robos o fugas de información."*

2.1.2. Antecedentes Nacionales

(Vilcarromero Zubiate & Vilchez Linares, 2018) la tesis tuvo como objetivo principal "P*roveer al área del SOC un marco de ciberseguridad para generar una solución que le permita implantar, operar, monitorear, revisar y mejorar los controles de Ciberseguridad, con el fin de ser un SOC de referencia y llegar a ser competitivo en el mercado."* En sus conclusiones el autor menciona que todo el análisis de su investigación dio como resultado y concluye que "*La viabilidad de la ciberseguridad para la empresa, obtuvo un VPN positivo de s/. 392,905.16, esto conlleva beneficios a la empresa, con un TIR que supera a lo que actualmente usaba la empresa del 10% a 11.74%, para esta implementación se tomó un tiempo de 36 meses, lo cual el autor considera que es bastante razonable dentro del marco de seguridad del área."* En resumen,

esta investigación considera la ciberseguridad en la gestión del área para tomar y promover a otra empresa, entidad y organización y al mismo tiempo que tomen conciencia los trabajadores de la forma en la que utilizan las tecnologías en su día a día.

(Sanchez Herrera, 2022) La presente investigación tuvo como objetivo *"Determinar la relación que existe entre políticas de seguridad y riesgos de la información en la Facultad de Ciencias de la UNASAM en el año 2022."* La investigación fue de tipo aplicada, el diseño tuvo un enfoque cuantitativo, de diseño no experimental y correlacional, la técnica que se empleará para la recolección de datos fue la encuesta, para la investigación se aplicó dos instrumentos, el primer instrumento enfocado a medir la variable políticas de seguridad y el según instrumento para medir la variable riesgos de la información , cuyos ítems estuvieron basados en el escala de Likert, estudiándose la muestra de 48 empleados (Docentes y administrativos) de la Facultad de Ciencias de la UNASAM. De manera complementaria se analizó la validez como la confiabilidad, mediante Alpha de Cronbach para ambos instrumentos. Se concluyó que *"Las Políticas de Seguridad y Riesgos de la Información tienen una relación inversamente proporcional, debido a que el Rho de Spearman arrojo un valor de (-0.422**) y la significancia p=0.003 (p<5), con la cual se determinó la relación significativa"*

(Aguilar, 2006) En esta investigación toma en cuenta el estado actual *"En la actualidad, las empresas están canalizando una proporción decreciente de sus inversiones en seguridad hacia la adquisición de productos, prefiriendo asignar una parte considerable del marco presupuestal a la administración de la seguridad de la información. Se ha observado un cambio en el concepto y definición de la seguridad, para dar inicio a un nuevo surgimiento denominado "seguridad gestionada", que gradualmente reemplaza al término "seguridad informática". Las estrategias adoptadas por las empresas ahora se centran en el nuevo enfoque de gestión de la seguridad de la información, que abarca tres dimensiones: tecnicista, legal, normativa y organizativa. Esto implica un planteamiento coherente de directrices, procedimientos y*

criterios que permiten a las empresas asegurar el desarrollo eficiente de la seguridad de los sistemas de información, así como de la entidad y sus espacios físicos asociadas. Al gestionar la seguridad de la información de una entidad, es esencial partir de la premisa fundamental de que la seguridad absoluta no es alcanzable. A partir de esta premisa, una entidad puede adoptar y enfocarse en normativas existentes en el mercado que establecen reglas, directrices o estándares como guía para la gestión de la seguridad de la información. La presente investigación se enfocó en examinar las normas y estándares que están ganando prominencia en el mercado peruano, especialmente en el sector financiero. Se han identificado los aspectos más destacados de cada norma y estándar, a partir de los cuales se propone un marco de gestión de la seguridad de la información que podría ser implementado por una institución financiera a nivel nacional - Perú. Esto facilitaría el cumplimiento de las normativas vigentes relacionadas con la seguridad de la información."

(Riveros Paraguay, 2019) Este proyecto, *"busca primero conocer el negocio y tener un panorama general de la red buscando fallas y requisitos, para después proponer una solución viable implementando un rediseño de red logrando satisfacer las necesidades que tiene a empresa. En la elaboración del proyecto se hace uso de la metodología Top Down de Cisco que cuenta con cuatro fases. Siendo la primera fase el análisis de requerimientos que caracteriza el estado actual de la empresa brindando información también de la labor de cada usuario el rubro, características y el fin de la empresa, nos genera una perspectiva presente de la empresa centrándonos en su red actual. Contando con la primera fase se puede implementar el diseño lógico que es la fase II de la metodología, el cual busca guiándose de la fase anterior solucionar los defectos de la red actual con un rediseño de la infraestructura de red para resolver las necesidades que requiere la red de área local en la institución, para el desarrollo del diseño lógico se optó por el Sistema PfSense ya que brinda una gran gama de sistemas integrados siendo Open Source no se tiene ningún costo en su uso además de eso es compatible con Sistemas Windows, Linux y Unix para la integración de Sistemas ya implementados, haciendo*

que la nueva red sea altamente escalable y adaptable. Para el diseño lógico se selecciona los dispositivos de red a implementar. Finalmente, en la última fase de probar y optimizar la red se hace pruebas de lo implementado en bloqueo de páginas, creación de perfiles, logeo en usuarios, las reglas establecidas y testeo de la conexión a internet dándole mejoras si es necesario. La implementación del sistema integrado Pfsense y la correcta aplicación de la metodología de Cisco permite determinar políticas de seguridad donde se mejora el acceso a la red por la instalación del directorio activo y administración de tráfico y la seguridad lógica por medio creación de reglas, perfiles y listas de control de acceso mejorando la latencia y el tráfico generado en la red."

(Williams, 2019) El autor nos dice que, *"El presente estudio está enfocado en la apreciación y análisis de un factor riesgos que provienen desde el interior de la institución, asegurar sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información, conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa. Es importante diferenciar entre seguridad informática y seguridad de la información. La primera, la seguridad informática, se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestro negocio. Con el fin de proporcionar un marco de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización se ha creado un conjunto de estándares bajo el nombre de ISO/IEC 27000. Esta implementación de SGSI permitió un gran aumento en la seguridad de los activos de información de la comisaria región Huancavelica., que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías."*

(Camapaza Quispe, 2019) . En esta investigación *"El objetivo es desarrollar un Plan de Seguridad Informática basado en la NTP ISO/IEC 27001:2014, en el cual inicialmente se realizará un diagnóstico situacional de la Municipalidad del Centro Poblado de Salcedo Puno para poder identificar las debilidades y amenazas en temas de seguridad de la información. Luego se preparará el plan de seguridad informática con el propósito de definir el alcance del plan, identificar los requisitos legales, elaborar políticas de seguridad y proponer un plan a la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno. Por último, se terminará el plan de seguridad informática evaluando los riegos de seguridad informática para elaborar los controles respectivos que permitan mitigarlos."*

2.1.3. Antecedentes Locales

(Villadeza Romero & Condor Simon, 2022) En esta investigación nos dice que, *"La principal problemática de la Municipalidad Distrital de Huácar relacionado a la exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2014 en las instituciones del estado, por esta razón se hace necesario realizar una evaluación a dicha entidad, desarrollando un Sistema de Gestión de Seguridad de la Información (SGSI) para evaluar qué tan seguros son nuestros sistemas, cuantificando los activos y sus características de mayor valor, para así más adelante cuando se lleve a una implementación disminuir o eliminar los riesgos e incrementar la productividad y efectividad en el mismo, con el objetivo principal de Proponer el diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2014, para mejorar la seguridad de la información de la Municipalidad Distrital de Huácar 2022"*

(Arguezo Ramirez, 2019) La presente investigación *"tiene como objetivo principal el desarrollo de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 para la protección de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco. Donde se utilizó la metodología de Deming o PDCA sugerida por la norma ISO 27001, se dividió la investigación en cinco etapas: En la primera se*

estableció el contexto, en la segunda se identificó y clasificación de los activos de información; en la tercera se siguió la metodología de análisis de riesgos, en la cuarta se siguió la metodología de evaluación de riesgo y en la quinta etapa el tratamiento de riesgo identificando los controles teniendo en cuenta el ISO 27002:2013. Por otro lado, el presente trabajo nos permitió concluir en la importancia de contar con un Sistema de Gestión de la Seguridad de la Información para el área de informática de la Municipalidad Provincial de Huánuco, el sistema permite la protección de los activos de información garantizando la integración, disponibilidad y confidencialidad de estos.”

2.2. Bases Teóricas

2.2.1. Metodología Magerit v.3

(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica;, 2012)Siguiendo la terminología establecida por la normativa ISO-31000, MAGERIT en su versión 3.0. corresponde a lo que se conoce como el "*Proceso de Gestión de Riesgos*". En otras palabras, MAGERIT en su versión 3.0 ejecuta y aplica el Proceso de Gestión de Riesgos enmarcado dentro de un contexto operativo, con el objetivo principal de que los órganos y unidades de gobierno tomen decisiones considerando y dirigiéndose a los riesgos asociados al uso de tecnologías de la información.

MAGERIT en su versión 3.0 examina los riesgos inherentes a un sistema de información y su entorno relacionado, definiendo riesgo como la posibilidad de sufrir un daño o perjuicio. Proporciona recomendaciones sobre las medidas adecuadas que deberían implementarse para comprender, prevenir, evitar, reducir o controlar los riesgos identificados.

En la perspectiva de MAGERIT en su versión 3.0, las tareas relacionadas a esta metodología de análisis y tratamiento de riesgos no constituyen un fin en sí mismas, sino que también se integran en la en la continuidad de la actividad de gestión de la seguridad. El análisis de estos posibles riesgos permite evaluar la situación real actual de la entidad, el valor y el nivel de protección del sistema. En coordinación directa con los objetivos, estrategia,

metas y política de la organización o institución, las actividades de tratamiento o mitigación de riesgos contribuyen a desarrollar un plan de seguridad que, una vez implementado y operado, cumple con los objetivos propuestos, manteniendo el nivel de riesgo aceptado por la Dirección. Este conjunto la suma de actividades se denomina el Proceso de Gestión de Riesgos.

Para llevar a cabo este proceso, MAGERIT en su versión 3.0 propone un catálogo, sujeto a expansiones, que establece directrices para:

- Tipificación de los activos y recursos de TI.
- Dimensiones para la valoración de los activos y recursos de TI.
- Criterios para la valoración de los activos y recursos de TI.
- Amenazas típicas y usuales sobre los sistemas de TI.
- Salvaguardas a considerar y tener en cuenta para proteger los sistemas de TI.

MAGERIT en su versión 3.0 persigue dos objetivos fundamentales:

- Facilitar la labor de los profesionales involucrados en el proyecto, proporcionándoles componentes y elementos estándar a los que puedan adherirse rápidamente, enfocándose en lo específico y lo más mínimo del sistema analizado.
- Homogeneizar y homologar los resultados obtenidos de los análisis, promoviendo una terminología y criterios uniformes que nos permitan comparar e incluso integrar análisis realizados por distintos equipos de trabajo.

MAGERIT en su versión 3.0 identifica dos tareas principales:

- Análisis de riesgos, que determina los activos de la organización y/o entidad, su interrelación y su valor, evaluando el perjuicio y daño potencial asociado a su degradación.
- Tratamiento de riesgos, que organiza una defensa consciente y prudente para prevenir incidentes, así como para estar preparados para afrontar emergencias imprevistas, sobrevivir a los incidentes que se presentan y continuar operando en las mejores condiciones y sobre todo que sean

óptimas. Dado que la perfección no es posible, se postula que el riesgo se reduce a un nivel residual aceptado por la organización y/o entidad.

Ambas actividades, análisis y tratamiento, se combinan y conforman en el proceso denominado Gestión de Riesgos. En el análisis de riesgos, MAGERIT en su versión 3.0 propone los siguientes pasos:

- Determinar e identificar los recursos y activos relevantes para la Organización/Entidad, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar e identificar a qué posibles amenazas están expuestos aquellos recursos y activos de TI.
- Determinar e identificar qué salvaguardas hay dispuestas en la organización/Entidad y cuán eficaces son frente al riesgo que se presenta.
- Estimar el impacto, definido como el daño sobre el recurso y activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia; esto quiere decir que tan posible es que ocurra, o expectativa de materialización de la amenaza.

2.2.2. Metodología de Gestión de Riesgos de TI

En la elaboración del propuesto Modelo de Gestión de Riesgos de Tecnologías de la Información, se ha tomado como base las requisitorias de la Superintendencia de Banca y Seguros, conforme a sus regulaciones: la Resolución SBS 2116-2009 que regula el Sistema de Riesgo Operacional que las entidades financieras en el Perú deben implementar, y la Circular G-105-2002 que establece los lineamientos para la Gestión de Riesgos de Tecnologías de la Información para este tipo de empresas. Ambas normativas se incluyen como parte integrante

de este estudio de investigación. Para la evaluación de cada componente de la metodología propuesta, se han considerado las siguientes fuentes de consulta:

Tabla 3: Metodología para la gestión de TI

NOTA: Elaboración propia

ELEMENTO	REFERENCIA
Recursos de Tecnologías de la Información (Activos de TI)	Abordado en: - Enfoque de Magerit - Modelo de análisis de riesgos mediante tablas de la norma ISO 27005
Puntos débiles de seguridad (Vulnerabilidades)	Abordado en: - Normas ISO 27005
Posibles Amenazas	Abordado en: - Enfoque Magerit - Norma ISO 27005
Consecuencias de las amenazas (Impacto de las amenazas)	Tratado en: - Enfoque Magerit - Norma ISO 27005 en su modelo de análisis de riesgos mediante tablas (algunas fuentes lo describen como degradación)
Probabilidad de ocurrencia	Tratado en: - Enfoque de Magerit como probabilidad - Norma ISO 27005 en su modelo de análisis de riesgos mediante tablas (en algunos textos se menciona como degradación)
Medidas de control y protección (Controles y Salvaguardas)	Abordado en: - Enfoque Magerit - Norma ISO 27005 únicamente como controles
RI/RR (Riesgo intrínseco y Riesgo Residual)	Abordado en: - Enfoque Magerit únicamente como riesgo - Norma ISO 27005 únicamente como riesgo. - La clasificación ha sido establecida conforme al marco teórico de la gestión de riesgos.

Para la ejecución del propuesto Modelo de Gestión de Riesgos de Tecnologías de la Información, se ha concebido la siguiente metodología, compuesta por cuatro (03) etapas que engloban los procesos de (1) Identificación de los escenarios de riesgos de TI, (2) Valoración de los escenarios de riesgos de TI y (3) Tratamiento de los riesgos

Según, (MAGERIT, 2012). Las acciones contempladas en cada etapa se detallan a continuación:

1. Fase de Identificación de los escenarios de riesgos de TI. En esta fase se desarrollan las siguientes actividades:

- Identificación y clasificación de los activos de TI
- Valoración de la criticidad de los activos de TI 31
- Identificación de las amenazas por activo de TI
- Identificación de vulnerabilidades de cada activo de TI.

2. Fase de Valoración de los escenarios de riesgos de TI. En esta fase se desarrollan las siguientes actividades:

- Estimación del impacto de los escenarios de riesgo
- Estimación de la probabilidad de ocurrencia de los escenarios de riesgo
- Cálculo de los niveles de exposición a los riesgos
- Determinación del apetito y tolerancia al riesgo

3. Fase de Tratamiento de los riesgos. En esta fase se desarrollan las siguientes actividades:

- Definición de las políticas de seguridad
- Identificación de los controles/salvaguardas de seguridad
- Definición de la estrategia de implementación de controles/salvaguardas

2.2.3. Metodología COBIT 4.1

(ISACA, 2007) COBIT 4.1 es un marco referencia que permite el control de todos los aspectos técnicos y riesgos de negocios, habilitando el desarrollo de políticas claras y buenas prácticas para el control de TIC a lo largo de las organizaciones, estableciendo los criterios técnicos a implementar o controlar para el manejo de la seguridad informática, promoviendo la competitividad en las Empresas a partir de la implantación de una cultura de gestión, seguridad y calidad para afrontar las demandas de su sector, mejorando sus procesos con la garantía del aumento de la seguridad de sus sistemas de información y de las comunicaciones. Las actividades consideradas en la auditoría de procesos mediante la metodología COBIT 4,1 incluye las siguientes:

1. Fase de auditoría de procesos

- Determinar los procesos a auditar
- Determinar los niveles de madurez de los procesos

2. Fase de diseño de las políticas de seguridad
    - Políticas de seguridad y su respectivo manual
3. Fase de implementación de las políticas de seguridad
    - Aprobación, implementación y publicación
4. Fase de resultados obtenidos de la implementación de las políticas de seguridad

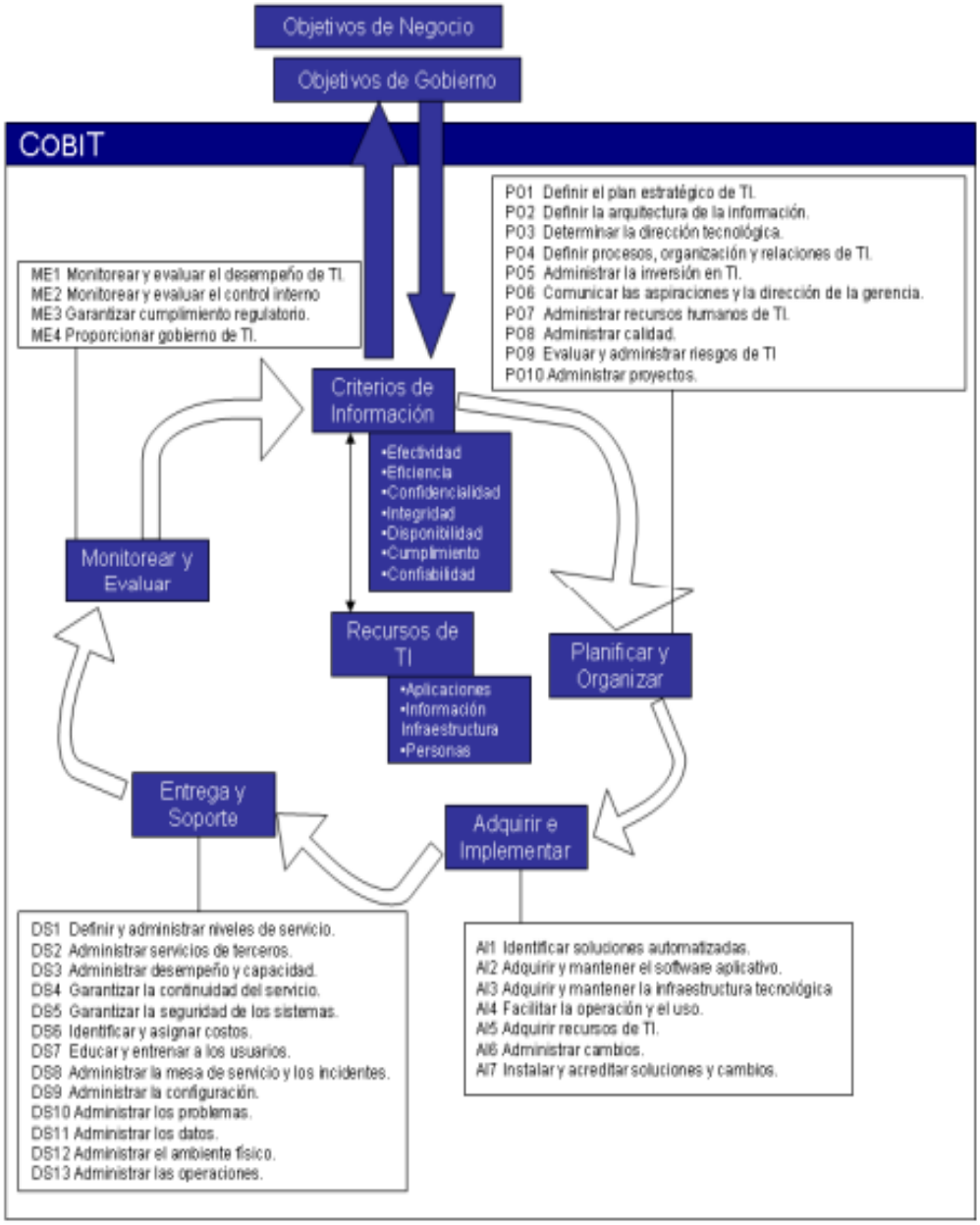


Ilustración 1: Objetivos de COBIT 4.1.
(COBIT 4.1., 2007)

Modelos de Madurez

En la actualidad, se insta a los líderes y ejecutivos de la organización a prestar especial atención a una gestión adecuada de las Tecnologías de la Información (TI). Para lograrlo, es necesario elaborar un plan de negocios que permita alcanzar un nivel óptimo de administración y control de las TI.

Los modelos de madurez se configuran como representaciones de perfiles de procesos de TI, que una organización podría reconocer como estados posiblemente actuales y futuros. Estos modelos no están concebidos como restrictivos, donde la transición a niveles superiores requiera necesariamente haber cumplido con los niveles anteriores. Al emplear los modelos de madurez para los 34 procesos de TI de COBIT 4.1, la dirección puede identificar:

- El desempeño real de la organización: su situación actual.
- El estado actual de la industria: comparación.
- El objetivo de mejora de la organización: su meta deseada.

Se ha establecido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición que va desde 0 (no existente) hasta 5 (optimizado). La ventaja radica en que es relativamente sencillo para la dirección situarse en la escala y, de esta manera, evaluar las acciones necesarias para mejorar.

A continuación, se presenta el modelo de madurez genérico a utilizar en esta auditoría:

Tabla 4: Niveles De Madurez de la Metodología COBIT 4.1.

FUENTE: (COBIT 4.1., 2007)

0 NO EXISTENTE	Total ausencia de cualquier proceso identificable. La organización no ha reconocido ni siquiera la existencia de un problema por resolver.
1 INICIAL	Existen señales de que la empresa ha identificado la existencia de problemas que necesitan solución. No obstante, no hay procesos estándar establecidos; en su lugar, se aplican enfoques ad hoc que tienden a ser utilizados de manera individual o caso por caso. La aproximación general hacia la gestión es desorganizada.
2 REPETIBLE	Los procesos han progresado al punto de seguir procedimientos similares en diversas áreas que realizan la misma tarea. No hay una formación o comunicación formal de los procedimientos estándar, y la responsabilidad recae en el individuo. Se confía considerablemente en el conocimiento individual, lo que aumenta la probabilidad de errores.

3 DEFINIDO	Los procedimientos han sido estandarizados y documentados, y se han divulgado mediante capacitación. No obstante, se permite que el individuo decida si utiliza estos procesos, y las desviaciones son poco probables de ser detectadas. Los procedimientos en sí mismos no son muy avanzados, pero formalizan las prácticas existentes.
4 ADMINISTRADO	Es posible supervisar y medir el cumplimiento de los procedimientos, tomando medidas cuando los procesos no están funcionando de manera efectiva. Los procesos están constantemente mejorándose y proporcionan prácticas sólidas. La automatización y las herramientas se utilizan de manera limitada o fragmentaria.
5 OPTIMIZADA	Los procesos se han perfeccionado hasta alcanzar el nivel de las mejores prácticas, basándose en los resultados de mejoras continuas y en un modelo de madurez compartido con otras empresas. Las Tecnologías de la Información se emplean de manera integrada para automatizar el flujo de trabajo, proporcionando herramientas que mejoran la calidad y la eficacia, permitiendo que la empresa se adapte rápidamente.

Modelos de Madurez a Nivel Cualitativo (COSO)

A continuación, se presenta en una tabla la influencia de los objetivos de control de COBIT 4.1 en los criterios y recursos de tecnología de la información. La codificación empleada para los criterios de información en esta tabla es la siguiente: (P) indica que el objetivo de control tiene un impacto directo en el requisito, (S) señala un impacto indirecto, es decir, no completo en el requisito, y finalmente, un espacio en blanco ( ) indica que el objetivo de control no afecta en absoluto al requisito. En cambio, cuando se encuentra con (X), significa que los objetivos de control afectan a los recursos, mientras que un espacio en blanco ( ) indica que los objetivos de control no tienen ningún impacto en los recursos.

Para obtener un porcentaje de los criterios de información, asignamos valores tanto para el impacto primario como para el secundario. Este porcentaje se establecerá siguiendo la metodología propuesta por COSO (Sponsoring Organizations of the Treadway) para la gestión de riesgos, tal como se presenta en la tabla.

Tabla 5: Calificación COSO (Sponsoring Organizations of the Treadway)

FUENTE:(COBIT 4.1., 2007)

CALIFICACION		IMPACTO	PROMEDIO
15%	50%	BAJO	32
51%	75%	MEDIO	63
76%	95%	ALTO	86

OBJETIVOS DE CONTROL DE COBIT		CRITERIOS DE INFORMACIÓN DE COBIT							RECURSOS DE TI DE COBIT			
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	PERSONAS	INFORMACIÓN	APLICACIÓN	INFRAESTRUCTURA
PLANEAR Y ORGANIZAR												
PO1	Definir un plan estratégico de TI.	P	S						X	X	X	X
PO2	Definir la arquitectura de la información	S	P	S	P					X	X	
PO3	Definir la dirección tecnológica.	P	P								X	X
PO4	Definir los procesos, organización y relaciones de TI.	P	P						X			
PO5	Administrar la inversión en TI.	P	P					S	X		X	X
PO6	Comunicar las metas y la dirección de la gerencia.	P					S		X	X		
PO7	Administrar los recursos humanos de TI.	P	P						X			
PO8	Administrar la calidad.	P	P		S			S	X	X	X	X
PO9	Evaluar y administrar los riegos de TI.	S	S	P	P	P	S	S	X	X	X	X
PO10	Administrar los proyectos.	P	P						X		X	X
ADQUIRIR E IMPLEMENTAR												
AI1	Identificar las soluciones automatizadas.	P	S								X	X
AI2	Adquirir y mantener software aplicativo.	P	P		S			S			X	
AI3	Adquirir y mantener la infraestructura tecnológica.	S	P		S	S						X
AI4	Facilitar la operación y el uso.	P	P		S	S	S	S	X		X	X
AI5	Procurar recursos de TI.	S	P				S		X	X	X	X
AI6	Administrar los cambios.	P	P		P	P		S	X	X	X	X
AI7	Instalar y acreditar soluciones y cambios.	P	S		S	S			X	X	X	X
ENTREGAR Y DAR SOPORTE												
DS1	Definir y administrar los niveles de servicio.	P	P	S	S	S	S	S	X	X	X	X
DS2	Administrar los servicios de terceros.	P	P	S	S	S	S	S	X	X	X	X
DS3	Administrar el desempeño y capacidad.	P	P			S					X	X
DS4	Asegurar el servicio continuo.	P	S			P			X	X	X	X
DS5	Garantizar la seguridad de los sistemas.			P	P	S	S	S	X	X	X	X
DS6	Identificar y asignar costos.		P					P	X	X	X	X
DS7	Educar y entrenar a los usuarios.	P	S						X			
DS8	Administrar la mesa de servicio y los incidentes.	P	P						X		X	
DS9	Administrar la configuración.	P	S			S		S		X	X	X
DS10	Administrar los problemas.	P	P			S			X	X	X	X
DS11	Administrar los datos.				P			P		X		
DS12	Administrar el ambiente físico.				P	P						X
DS13	Administrar las operaciones.	P	P		S	S			X	X	X	X
MONITOREAR Y EVALUAR												
ME1	Monitorear y evaluar el desempeño de TI.	P	P	S	S	S	S	S	X	X	X	X
ME2	Monitorear y evaluar el control interno.	P	P	S	S	S	S	S	X	X	X	X
ME3	Garantizar el cumplimiento regulatorio.						P	S	X	X	X	X
ME4	Proporcionar gobierno de TI.	P	P	S	S	S	S	S	X	X	X	X

Ilustración 2: COSO
(COBIT 4.1., 2007)

2.2.4. Comparación COBIT 4.1 vs COBIT 5

2.2.4.1. Características COBIT 4.1.

(ISACA, 2007) Para ayudar a las organizaciones, instituciones, entidades públicas o privadas a satisfacer con éxito los desafíos de los negocios, el IT Governance Institute® (ITGI) ha publicado la versión de COBIT® 4.1

- COBIT es un marco de trabajo de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de T.I. que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.
- COBIT hace posible el desarrollo de una política clara y las buenas prácticas para los controles de T.I. a través de las organizaciones.
- COBIT enfatiza en la conformidad a regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de la estructura COBIT.

La versión, COBIT® 4.1, enfatiza el cumplimiento normativo, ayuda a las organizaciones a incrementar el valor de T.I., apoya el alineamiento con el negocio y simplifica la implantación de COBIT. Esta versión no invalida el trabajo efectuado con las versiones anteriores del COBIT, sino que puede ser empleado para mejorar el trabajo previo.

2.2.4.2. Características COBIT 5.

(ISACA, 2007) Esta es la más recién versión de COBIT y está basada en procesos, se enfoca fuertemente en el control y menos en la ejecución, es decir, indica qué se debe conseguir sin focalizarse en el cómo.

La primera impresión es que ISACA ha orientado definitivamente COBIT hacia el Gobierno de las TI. En sus primeras versiones, COBIT se definía como un marco de control para auditores de TI. En la revisión del año 2000, COBIT 3, se incluía como

producto/documento aparte las Management Guide lines o guía de gestión para la dirección, con una orientación más cercana al concepto de Gobierno TI. La versión 4 de COBIT supuso la configuración definitiva de COBIT como un marco general de Gobierno TI, pero quedaba confusa la relación con otros marcos de ISACA con otra orientación como Val IT (valor de las TI) o RISK IT (riesgos) o con el nuevo estándar de Gobierno TI ISO/IEC38500.

La nueva versión tiene un carácter clarificador, integrando COBIT 4, Val IT y RISK IT en su modelo de referencia de procesos. Asimismo, COBIT 5 ha sido adaptado para alinearse con La norma ISO/IEC 38500 de Gobierno TI y con el marco GEIT del ITGI (IT Governance Institute).

2.2.4.3. ¿Por qué Se Escogió Trabajar con la Metodología COBIT 4.1?

En este trabajo se trabajará con la metodología COBIT 4.1. porque queremos centrarnos en el cumplimiento normativo ayudando a incrementar el valor de T.I. para el resguardo de la información, ya que se va a enfocar el proyecto en toda la municipalidad distrital de Amarilis y nos traerá beneficios como:

- Alineación optimizada, según la estrategia empresarial
- Una perspectiva comprensible para la dirección sobre las funciones de Tecnologías de la Información
- Definición precisa de roles y responsabilidades, en consonancia con la orientación hacia procesos
- Reconocimiento generalizado por parte de terceros y entidades reguladoras
- Consenso entre todas las partes interesadas mediante el uso de un lenguaje compartido
- Adherencia a los requisitos COSO para el control del entorno de Tecnologías de la Información

2.3. Bases Conceptuales o Definición de Términos Básicos

2.3.1. Vulnerabilidad

De acuerdo (MAGERIT – versión 3.0 Metodología de Análisis y Gestión, 2012) las vulnerabilidades se denominan a todo punto débil o debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Esto quiere decir que son todas las ausencias o ineficacias que salvaguardan el valor propio o acumulativo de un activo.

2.3.2. Amenaza

Según (UNE 71504 Metodología de análisis y gestión de riesgos para los sistemas de información, 2008) representa una fuente potencial de un suceso que podría ocasionar perjuicios a un sistema de información o a una entidad.

De acuerdo (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012) cuenta con un catálogo con su respectiva tipificación como:

- **De origen natural:** Se refiere a eventos naturales como terremotos e inundaciones. En tales circunstancias, el sistema de información actúa como una entidad pasiva, aunque es esencial considerar posibles escenarios.
- **Del entorno (de origen industrial):** Involucra desastres industriales como contaminación y fallos eléctricos, donde el sistema de información es afectado pasivamente. Sin embargo, la pasividad no implica indefensión, siendo necesario tomar medidas preventivas.
- **Defectos de las aplicaciones**: Se relaciona con problemas originados en el propio equipamiento debido a fallos en diseño o implementación, con

posibles consecuencias negativas para el sistema. A menudo denominados vulnerabilidades técnicas o simplemente vulnerabilidades.

- **Causadas por las personas de forma accidental:** Las personas con acceso al sistema pueden ser responsables de problemas no intencionados, generalmente debido a errores u omisiones.
- **Causadas por las personas de forma deliberada:** Aquí se aborda la posibilidad de que personas con acceso al sistema generen problemas intencionadamente, ya sea con el propósito de obtener beneficios indebidos o causar daños a los legítimos propietarios. Esos actos se consideran ataques deliberados.

No todas las amenazas afectan todos los activos; existe una relación específica entre el tipo de activo y las posibles eventualidades.

2.3.3. Riesgo

Según (ISACA, 2009) las Directrices para la Gestión de Seguridad de TI comunicadas, fomentadas y publicadas por la Organización Internacional de Estandarización (ISO) en su (ISO-IEC PDTR-13335 1), el riesgo implica la posibilidad de que una amenaza específica aproveche las vulnerabilidades de un activo o conjunto de activos, generando así pérdidas o daños para la organización.

En el análisis de (Medina, 2007), el riesgo se describe como la probabilidad de que las amenazas aprovechen las debilidades, ocasionando pérdidas o daños a los activos y afectando el negocio, es decir, impactando en la confidencialidad, integridad y disponibilidad de la información. El riesgo se define como:

- La condición en la que existe la posibilidad de que un evento ocurra y tenga un impacto negativo en los objetivos de la empresa.

- La posibilidad de un impacto negativo en los objetivos de la empresa.

El riesgo se considera una característica inherente a la vida empresarial, y dado que resulta impráctico y poco económico eliminar completamente los riesgos, cada organización establece un nivel de riesgo aceptable.

2.3.4. Políticas de Seguridad

Según (ISO 27001, 2013) Una política de seguridad, es una declaración formal de las reglas, directivas y prácticas que rigen la forma de gestión de los activos de tecnología e información dentro de una organización.

Las políticas proporcionan una guía más detallada de cómo poner en práctica los principios y cómo éstos influirán en la toma de decisiones. No todas las políticas relevantes están escritas y son propiedad de la función de seguridad de la información. Las políticas se estructuran en tres grupos:

- La política de seguridad de la información escrita por la función de seguridad de la información, pero dirigida por la Dirección Ejecutiva
- Las políticas específicas de seguridad de la información dirigidas por la función de seguridad de la información
- Otras políticas que puedan relacionarse con la seguridad de la información, pero que están dirigidas por otras funciones de la empresa. En estas políticas, la seguridad de la información debería influir en el desarrollo para asegurar el logro de los requisitos de seguridad de la información.

La siguiente lista de políticas relevantes es ilustrativa y no exhaustiva:

- Política de seguridad de la información
- Política de control de acceso
- Política de seguridad de la información del personal

- Política de seguridad física y ambiental
- Política de gestión de incidentes
- Política de continuidad de negocio y recuperación ante desastres
- Política de gestión de activos
- Reglas de comportamiento (uso aceptable)
- Política de adquisición, desarrollo de software y mantenimiento de sistemas de información
- Política de gestión de proveedores
- Política de gestión de comunicaciones y operaciones
- Política de cumplimiento
- Política de gestión de riesgos

2.4. Bases Epistemológicas, Bases Filosóficas y/o Bases Antropológicas

(Gómez Vieites, 2011) este libro nos dice, “La importancia de la seguridad de la información ya que todas las actividades de los países desarrollados dependen en todo nivel de los sistemas de información y sistemas informáticos Por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distinta Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad. De ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad informática en una organización. La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión”

CAPITULO III
METODOLOGÍA

3.1 Ámbito

El ámbito de esta investigación se centra en el análisis, diseño e implementación de las políticas de seguridad en la Municipalidad Distrital de Amarilis, con el objetivo de garantizar la efectividad del resguardo de la información. La investigación abarcará un periodo de tiempo de 4 meses. Cabe destacar que el ámbito de esta investigación se limitará al ámbito geográfico de la Municipalidad Distrital de Amarilis, en la región de Huánuco, Perú.

3.2 Población

La población objetivo sería el personal y los sistemas de información de la Municipalidad Distrital de Amarilis. Esto incluiría a los empleados de diferentes departamentos y áreas que tienen acceso a la información sensible, así como a los sistemas de información utilizados para almacenar y procesar dicha información.

3.3. Muestra:

Se tomará en cuenta la muestra de la investigación al igual que la población ya que son igual de importante no se puede dejar a ninguna de lado, que sería el personal y los sistemas de información de la Municipalidad Distrital de Amarilis. Esto incluiría a los empleados de diferentes departamentos y áreas que tienen acceso a la información sensible, así como a los sistemas de información utilizados para almacenar y procesar dicha información.

3.4 Nivel, tipo y diseño de estudio

3.4.1. Tipo de ESTUDIO

De acuerdo a diversos autores llegamos a la conclusión de nuestro nivel y tipo de estudio.

- **Según el Tipo de Investigación:**

Villa, Flores, (2023), “La presente investigación es aplicada, ya que tiene un alcance limitado de generalización y está destinada a resolver un problema específico.”

A través del diseño e implementación de políticas de seguridad para la mejor del resguardo de la información, se propone aplicar los conocimientos para resolver el problema cuya solución beneficiará a la municipalidad distrital de Amarilis.

3.5. Diseño de Investigación:

Sampieri, (2014), “Los diseños de investigación no experimentales son aquellos que no manipulan las variables de forma intencionada. Se basan fundamentalmente en la observación y el análisis de los acontecimientos tal y como se producen en su entorno natural.”

Para evitar la manipulación intencionada de las variables y estas no se vean involucradas, se utilizó una metodología no experimental transeccional descriptiva, que permitió la rápida recolección de datos en un solo momento. Para ello, se realizó una encuesta al personal de la municipalidad distrital de Amarilis.

3.6. Métodos, Técnicas e Instrumentos

Los métodos de recojo de datos utilizados para recopilar la información necesaria para el análisis de la investigación fueron los siguientes:

Tabla 6: Técnicas de recolección de datos

NOTA: Elaboración propia

Revisión de documentos de la entidad: Los documentos de la Municipalidad de Amarilis que fueron revisados son el inventario de activos, y documentos referentes a la organización proporcionados por el Sub Gerente de Patrimonio y Servicios Generales perteneciente a la Gerencia de Administración y Finanzas	- Documentos administrativos.
Observación: La observación se realizó para valorar los activos de información a criterio y juicio de los tesistas	- Fichas de observación.
Encuesta: Se realizó este instrumento para recolectar información inicial sobre	- Cuestionario

el estado situacional actual de la municipalidad distrital de Amarilis.	
Entrevista: El conversatorio con fines de investigación que se tendrá con los encargados de la municipalidad distrital de Amarilis.	- Apuntes

3.7. Validación y Confiabilidad del Instrumento

La validez y la confidencialidad del instrumento se realizará por tres expertos en el tema, lo que permitió valorar las diferentes opiniones y validar si el contenido del cuestionario se ajustó al contexto de los objetivos de la investigación, a la variable de estudios y a las dimensiones e indicadores de la misma, los resultados de la encuesta a nivel de confiabilidad se realizará el análisis con el alfa de Cronbach, para saber en qué nivel se encuentra la confiabilidad los expertos dieron su juicio a través de un documento creado con ese propósito que se encuentra en el Anexo 03.

3.8. Procedimiento

Una vez que se termine la recopilación de datos de las encuestas podremos el estado que se encuentra la entidad y posteriormente se identificará los activos de información, se llevará al Excel y se organizará por modelos según la metodología MAGERIT V3, para que nos ayude a hacer el análisis de los activos y para conocer la situación de la Municipalidad Distrital de Amarilis.

Con los resultados obtenidos podremos pasar a la auditoría de procesos con la metodología COBIT 4.1. para poder diseñar las políticas de seguridad de la información y posteriormente implementarse para ver los resultados y poder afirmar que las políticas de seguridad mejoran la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

3.9. Plan de tabulación y análisis de datos estadísticos

Se trasladarán los datos obtenidos por los formularios a una tabla de doble entrada conformada por filas y columnas, donde se calculará el porcentaje y poder diagnosticar la situación actual de la Municipalidad Distrital de Amarilis.

3.10. Consideraciones Éticas

Para la realización del trabajo de investigación se respetará la integridad, anonimato y privacidad de los trabajadores que participaron en las encuestas.

CAPITULO IV
RESULTADOS

4.1 Diagnostico de la Situación Actual de la Municipalidad Distrital de Amarilis

Se empleó una encuesta, detallado en el Anexo 02 de este proyecto, para recopilar información. Con el propósito de analizar las actitudes, perspectivas y la situación esencial de la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis, se llevó a cabo una encuesta que consta de 20 preguntas fundamentales. El objetivo era evaluar la situación actual de la municipalidad en relación con la efectividad del resguardo de la información y determinar si la implementación de las políticas de seguridad mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

Con los resultados obtenidos de las 274 encuestas realizadas al personal de la Municipalidad Distrital de Amarilis como se puede ver en el Anexo 4, se pasó a analizar y procesar dichos datos como se puede ver en el Anexo 05, con lo obtenido el personal de la Municipalidad Distrital de Amarilis tiene conocimiento nulo de las políticas de seguridad de información, no tiene conciencia plena sobre el resguardo de la información, no existe programas de formación con respecto a la seguridad a la información, las respuestas sobre las soluciones de incidentes son lentas.

Basado en el diagnostico inicial, se reconoce la necesidad de un enfoque más profundo y especializado en materia de seguridad de la información, por esa razón podemos continuar con nuestro proyecto de investigación

4.1.1. Contexto de la Entidad

4.1.1.1. Razón social, RUC, Actividad económica, Localización

- **Razón Social:** MUNICIPALIDAD DISTRITAL DE AMARILIS.
- **RUC:** 20146009060

- **Actividad económica**

  La municipalidad distrital de amarilis como institución prestadora de servicios públicos locales, fomentando el bienestar de los vecinos y el desarrollo integral y armónico de su localidad.

- **Localización**

  La municipalidad distrital de amarilis se ubica en el Jr. Huallaga N°300

Ilustración 3: Localización de la Municipalidad Distrital de Amarilis

4.1.1.2. Misión, Visión, Objetivos

- **Misión:** "La Municipalidad del Distrito de Amarilis tiene como visión como entidad de Gobierno Local que gestiona y promueve el desarrollo urbano y rural sostenible y la adecuada prestación de los servicios básicos, públicos, sociales y municipales. Concierta y coordina las iniciativas de participación del vecindario y de las instituciones públicas y privadas. Atrae recursos para el desarrollo e inversión para fortalecer la economía local".
- **Visión;** "Amarilis es un espacio integrado a nivel regional, nacional e internacional con desarrollo humano, social, económico y sostenible,

con instituciones y sociedad civil organizada y participativa con practica de valores".

- **Objetivos:**
    - Promover, realizar, y mantener en condiciones óptimas, los servicios sociales y comunales básicos de la Municipalidad.
    - Satisfacer la demanda del vecindario, respecto a los servicios de infraestructura urbana pública y rural, privado y e catastro.
    - Estimular e institucionalizar la participación de la población en la gestión municipal, fomentando el trabajo comunal, dando opción al ejercicio de libre iniciativa.
    - Administrar racionalmente las rentas de la Municipalidad.
    - Fomentar las actividades educativas, culturales y artísticas en todas sus expresiones, en coordinación con los organismos correspondientes, así como con la participación de la población.
    - Asumir las transferencias de funciones sectoriales de Educación, Salud y otros que irá dándose gradualmente en el proceso de descentralización.

4.1.1.3. Organigrama

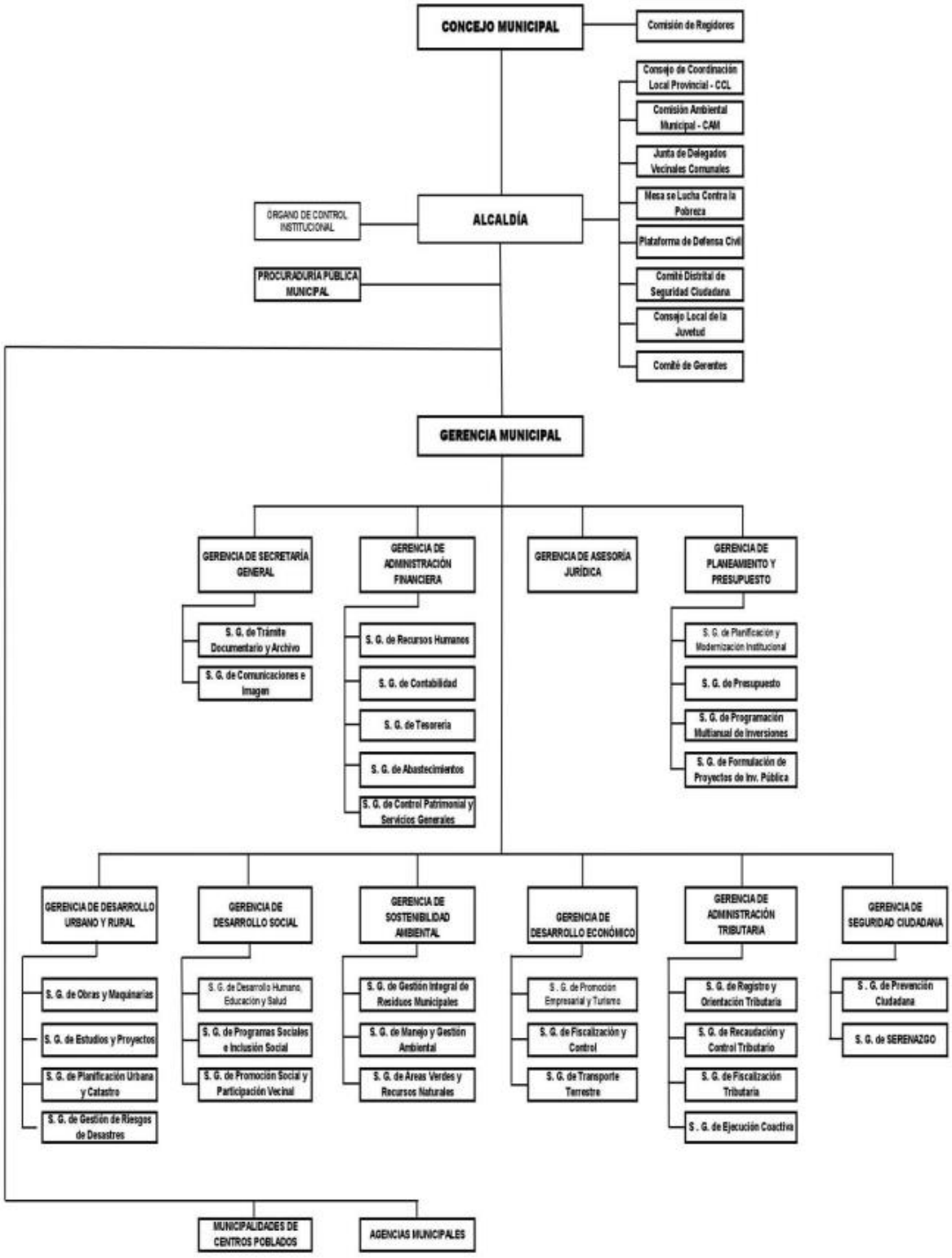


Ilustración 4: Organigrama de la Municipalidad Distrital de Amarilis

4.1.1.4. Política de la Municipalidad Distrital de Amarilis

Hacer de Amarilis un distrito seguro, sostenible, competitivo e inclusivo, en el cual los vecinos amarilenses mejoren su calidad de vida a través de la modernización de los servicios públicos, la generación de espacios de participación, promoción empresarial y concertación ciudadana, con la finalidad de promover el desarrollo integral local; teniendo como base una gestión municipal eficiente y acorde a las necesidades de nuestro distrito.

4.1.1.5. Servicios de la Municipalidad Distrital de Amarilis

- Brindar servicios de calidad en limpieza pública, serenazgo y áreas verdes
- Reducir las brechas de infraestructura vial
- Promover y fomentar el desarrollo económico local
- Gestionar con eficiencia, transparencia y de manera concertada
- Promover la inclusión social en poblaciones vulnerables
- Fortalecer la atención primaria de salud y educación
- Incrementar la generación de espacios públicos eco-amigables que mejore la calidad ambiental distrital
- Implementar una cultura de diálogo como parte de una gestión municipal eficiente, eficaz, democrática y participativa
- Promover una Cultura Tributaria en el distrito

4.1.1.6. Funciones de la Municipalidad distrital de Amarilis

Según la constitución Política del Perú son funciones generales de la Municipalidad distrital de Amarilis

- Aprobar su organización interna y su presupuesto
- Administrar sus bienes y rentas

- Crear, modificar y suprimir contribuciones, tasas, arbitrios, licencias y derechos municipales
- Organizar, reglamentar y administrar los servicios públicos locales de su responsabilidad
- Planificar el desarrollo urbano y rural de sus circunscripciones, y ejecutar los planes y programas correspondientes
- Participar en la gestión de las actividades y servicios inherentes al Estado, conforme a ley
- Lo demás que determine la ley

4.2 Fase de Identificación de los escenarios de riesgos de TI.

El objetivo de esta fase es identificar y comprender los posibles riesgos y amenazas que pueden afectar la seguridad y el funcionamiento de los sistemas de tecnología de la información en la Municipalidad Distrital de Amarilis. Durante esta fase, se busca analizar y documentar los riesgos potenciales relacionados con la infraestructura de TI, los datos, las aplicaciones y otros activos de tecnología. Se trabajó las siguientes actividades.

4.2.1. Identificación y clasificación de los activos de TI

Esta actividad nos permite identificar y categorizar todos los activos de tecnología de la información (TI) que la Municipalidad Distrital de Amarilis posee. Para categorizar los TI identificados, se empleó la taxonomía propuesta por el enfoque de la metodología Magerit versión 3.0.

Anexo 06

Los activos de TI críticos identificados en los procesos de la Municipalidad Distrital de Amarilis se muestran en la siguiente Tabla:

Tabla 7: Inventario de activos de TI de la Municipalidad Distrital de Amarilis de acuerdo a la clasificación propuesta por la metodología Magerit versión 3.0.

CLASIFICACIÓN DE LOS ACTIVOS DE TI IDENTIFICADOS		
N°	**TIPO DE ACTIVO**	**ACTIVO**
1	ACTIVOS ESENCIALES	Datos de Gestión interna
2	ACTIVOS ESENCIALES	Órdenes de Compra y de Servicio
3	ACTIVOS ESENCIALES	Documentos digitales
4	ACTIVOS ESENCIALES	Documentos físicos
5	ACTIVOS ESENCIALES	Información pública
6	SERVICIOS	Servidor principal de dominio
7	SERVICIOS	Servidor principal de base de datos INFO, SIAF Y SIGA
8	SERVICIOS	Servidor principal de base de datos SISRENTAS, ASTM Y SRTM
9	SERVICIOS	Correo electrónico institucional
10	DATOS/INFORMACIÓN	Base de datos
11	DATOS/INFORMACIÓN	Backups de base de datos
12	DATOS/INFORMACIÓN	Credenciales (usuario y contraseña)
13	EQUIPAMIENTO INFORMATICO	Equipos de cómputo y portátiles
14	EQUIPAMIENTO INFORMATICO	Fotocopiadora / Impresora
15	EQUIPAMIENTO INFORMATICO	Router
16	EQUIPAMIENTO INFORMATICO	Switch
17	SOTWARE - APLICACIONES INFORMÁTICAS	Software ofimático
18	SOTWARE - APLICACIONES INFORMÁTICAS	Sistema operativo
19	SOTWARE - APLICACIONES INFORMÁTICAS	Antivirus
20	SOTWARE - APLICACIONES INFORMÁTICAS	INFO
21	SOTWARE - APLICACIONES INFORMÁTICAS	SIAF
22	SOTWARE - APLICACIONES INFORMÁTICAS	SIGA
23	SOTWARE - APLICACIONES INFORMÁTICAS	RUB PVL
24	SOTWARE - APLICACIONES INFORMÁTICAS	SISMUN (SISTEMA MUNICIPAL)
25	SOTWARE - APLICACIONES INFORMÁTICAS	ASTM (APLICATIVOS DE SISTEMAS DE RECAUDACION TRIBUTARIA MUNICIPAL)
26	SOTWARE - APLICACIONES INFORMÁTICAS	SRTM (SISTEMA DE RECAUDACION TRIBUTARIA MUNICIPAL)
27	SOTWARE - APLICACIONES INFORMÁTICAS	SISRENTAS
28	REDES DE COMUNICACIÓN	Red Wifi
29	REDES DE COMUNICACIÓN	Red LAN
30	REDES DE COMUNICACIÓN	Internet
31	REDES DE COMUNICACIÓN	Telefonía
32	EQUIPAMIENTO AUXILIAR	Cableado
33	EQUIPAMIENTO AUXILIAR	UPS
34	EQUIPAMIENTO AUXILIAR	Estabilizador
35	EQUIPAMIENTO AUXILIAR	Mobiliario
36	SOPORTE DE INFORMACION	Disco Duro Externo
37	SOPORTE DE INFORMACION	Usb's

38	INSTALACIONES	Infraestructura
39	INSTALACIONES	Oficinas
40	PERSONAL	Titular de la entidad
41	PERSONAL	Responsables de las áreas
42	PERSONAL	Encargado de informática
43	PERSONAL	Usuarios

A continuación, se muestra un desglose de los activos de TI por cada unidad Orgánica de la Municipalidad Distrital de Amarilis. Ver en la siguiente Tabla.

Tabla 8: Inventario de activos de TI por Unidad Orgánica.

ALCALDIA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-i3-4160)**	**1**	**Malo**
2	**MONITOR LED (SAMSUNG-S19D300NY)**	**1**	**Regular**
3	**IMPRESORA A INYECCION DE TINTA (EPSON-L365)**	**1**	**Regular**
4	**ESTABILIZADOR (FORZA-FVR-1221B)**	**1**	**Regular**
5	**TECLADO - KEYBOARD (MICROSOFT-1576)**	**1**	**Malo**
ÓRGANO DE CONTROL INSTITUCIONAL (OCI)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**5**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**3**	
	MONITOR LED (SAMSUNG-S19D300NY)	1	Regular
	MONITOR PLANO (AOC-S/M)	1	Regular
	MONITOR PLANO (LG-W1943SI)	1	Bueno
3	**IMPRESORA**	**2**	
	IMPRESORA LASER (HP-M127fn)	1	Regular
	IMPRESORA LASER (HP-LASERJET 1020)	1	Regular
4	**SWITCH PARA RED (TP-LINK-TL-SF1008D)**	**1**	**Regular**
5	**SUPRESOR DE VOLTAJE TRANSITORIO**	**2**	
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (CDP-S/M)	1	Regular
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (ECOTREND-S/M)	1	Regular
6	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (PULSAR-PLI 1000)	1	Regular
	ESTABILIZADOR (ALTRON-S/M)	1	Regular
7	**TECLADO - KEYBOARD**	**4**	

	TECLADO - KEYBOARD (GENIUS-KG39)	1	Regular
	TECLADO - KEYBOARD (GENIUS-K645)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Bueno
	TECLADO - KEYBOARD (GENIUS-GK - 070006/U)	1	Regular
PROCURADURÍA PUBLICA MUNICIPAL			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-519D300NY)	1	Regular
2	**MONITOR**	**3**	
	MONITOR LED (SAMSUNG-S/M)	1	Regular
	MONITOR PLANO (AOC-195LM00008)	1	Regular
	MONITOR PLANO (LG-20M45A-B)	1	Regular
3	**COMPUTADORA PERSONAL PORTATIL (TOSHIBA-S/M)**	**1**	**Malo**
4	**IMPRESORA**	**2**	
	IMPRESORA LASER (HP-GM-070005)	1	Regular
	IMPRESORA LASER (HP-S/M)	1	Malo
5	**TECLADO - KEYBOARD**	**4**	
	TECLADO - KEYBOARD (GENIUS-C-313)	1	Bueno
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (SIN MARCA-KU-0138)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-S/M)	1	Regular
6	**SUPRESOR DE VOLTAJE TRANSITORIO - TVSS**	**3**	
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (PROFIELD-S/M)	1	Bueno
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (SIN MARCA-S/M)	1	Bueno
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (ECOTREND-S/M)	1	Regular
7	**SWITCH PARA RED SATRAS/M (SATRA-S/M)**	**1**	**Regular**
8	**TELEFONO (TELEFONICA-Amber)**	**1**	**Malo**
GERENCIA MUNICIPAL (GM)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCAS/M)**	**1**	**Regular**
2	**MONITOR LED (SAMSUNGS19D300NY)**	**1**	**Bueno**
3	**COMPUTADORA PERSONAL PORTATIL (TOSHIBALAPTOP)**	**1**	**Regular**
4	**IMPRESORA**	**2**	
	IMPRESORA A INYECCION DE TINTA (CANONS/M)	1	Malo
	IMPRESORA A INYECCION DE TINTA (CANONG2110)	1	Regular
5	**TECLADO - KEYBOARD (ECOTRENDKMS-01)**	**1**	**Regular**
6	**ESTABILIZADOR (OMEGA-PCG-1000)**	**1**	**Bueno**
GERENCIA DE SECRETARIA GENERAL (GSG)			

NRO	DESCRIPCION	CANTIDAD	ESTADO
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**COMPUTADORA PERSONAL PORTATIL (HP-BCM9431424)**	**1**	**Regular**
3	**MONITOR**	**3**	
	MONITOR LED (LG-19M37A)	1	Regular
	MONITOR LED (LG-19N435)	1	Regular
	MONITOR PLANO (BENQ-S/M)	1	Regular
4	**TECLADO - KEYBOARD**	**4**	
	TECLADO - KEYBOARD (BLANDBYTE-S/M)	1	Regular
	TECLADO - KEYBOARD (HALION-HA-188)	1	Malo
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
5	**ESTABILIZADOR**	**6**	
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-PC6-1200)	1	Regular
	ESTABILIZADOR (SIN MARCA-S/M)	1	Malo
	ESTABILIZADOR (HOLDING LEVEN-S/M)	1	Regular
	ESTABILIZADOR (PCG 1400-S/M)	1	Malo
	ESTABILIZADOR (OMEGA-PCG1200)	1	Regular
6	**ECUALIZADOR (BEHRINGER-S/M)**	**1**	**Regular**
7	**RUTEADOR DE RED - ROUTER (TP-LINK-TL-SF1008D)**	**1**	**Bueno**
8	**SWITCH PARA RED (POWER-TM 108 SK)**	**1**	**Regular**
GSG/SUB GERENCIA DE TRAMITE DOCUMENTARIO Y ARCHIVO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**2**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**5**	
	MONITOR LED (LG-S/M)	1	Regular
	MONITOR LED (SAMSUNG-733NW)	1	Regular
	MONITOR LED (SAMSUNG-L5190300NY/PE)	1	Regular
	MONITOR LED (SAMSUNG-732NPLUSW)	1	Malo
	MONITOR LED (SAMSUNG-592 V)	1	Malo
3	**IMPRESORA**	**2**	
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-CB411A)	1	Regular
4	**TECLADO - KEYBOARD**	**3**	
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Malo
	TECLADO - KEYBOARD (MICROSOFT-1406)	1	Regular
	TECLADO - KEYBOARD (VASTEC-S/M)	1	Bueno
5	**ESTABILIZADOR**	**2**	

	ESTABILIZADOR (MINI POWER-HP-1000A)	1	Malo
	ESTABILIZADOR (MINI POWER-S/M)	1	Malo
6	**SWITCH PARA RED (SIN MARCA-ADVANTEK)**	**1**	**Bueno**
GSG/SUG GERENCIA DE COMUNICACIONES E IMAGEN			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**4**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Bueno
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Bueno
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-CYBT108)	1	Bueno
2	**MONITOR**	**7**	
	MONITOR LED (ASUS-VH323)	1	Bueno
	MONITOR LED (LG-24MT47A)	1	Regular
	MONITOR LED (SAMSUNG-22335WPLUS)	1	Bueno
	MONITOR LED (SAMSUNG-524F350FHL)	1	Bueno
	MONITOR LED (SAMSUNG-9335NPLUS)	1	Regular
	MONITOR LED (TEROS-S/M)	1	Bueno
	MONITOR LED (SIN MARCA-S/M)	1	Bueno
3	**TECLADO - KEYBOARD**	**6**	
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-S/M)	1	Bueno
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Bueno
	TECLADO - KEYBOARD (VASTEC-S/M)	1	Bueno
	TECLADO - KEYBOARD (MICRONICS-MIC K701FX)	1	Bueno
	DISCO DURO EXTERNO (TOSHIBA-S/M)	1	Bueno
4	**ESTABILIZADOR**	**7**	
	ESTABILIZADOR (OMEGA-PCG-1000)	1	Bueno
	ESTABILIZADOR (ORION-S/M)	1	Bueno
	ESTABILIZADOR (QUASAR-S/M)	1	Regular
	ESTABILIZADOR (ORION-S/M)	1	Regular
	ESTABILIZADOR (QUASAR-POWER LITE)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Bueno
5	**RUTEADOR DE RED - ROUTER (SAGAMEGCON-S/M)**	**1**	**Malo**
6	**SWITCH PARA RED**	**2**	
	SWITCH PARA RED (SATRA-S/M)	1	Regular
	SWITCH PARA RED (SIN MARCA-S/M)	1	Regular
GERENCIA DE ADMINISTRACIÓN Y FINANZAS (GAF)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Regular**
2	**MONITOR PLANO (LG-20M45ASA)**	**1**	**Regular**
3	**COMPUTADORA PERSONAL PORTATIL (TOSHIBA-S/M)**	**1**	**Malo**

4	**IMPRESORA**	**2**	
	IMPRESORA LASER (HP-SHNGCC-1202-02)	1	Regular
	IMPRESORA LASER (HP-S/M)	1	Regular
5	**TECLADO - KEYBOARD**	**2**	
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Bueno
	TECLADO - KEYBOARD (GENIUS-SMARTKB- 100)	1	Regular
6	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (OMEGA-PCG 1400)	1	Regular
	ESTABILIZADOR (OMEGA-PLI 1200)	1	Regular
7	**SWITCH PARA RED (SATRA-S/M)**	**1**	**Regular**
GAF/SUB GERENCIA DE RECURSOS HUMANOS			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**7**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**10**	
	MONITOR LED (AOC-S/M)	1	Malo
	MONITOR LED (SAMSUNG-S19D300NY)	1	Bueno
	MONITOR LED (SAMSUNG-LS190300NY/PE)	1	Bueno
	MONITOR LED (SAMSUNG-733NW)	1	Regular
	MONITOR PLANO (ACER-V206HQL)	1	Bueno
	MONITOR PLANO (LG-19M37A)	1	Bueno
	MONITOR PLANO (ECOTREND-ET-M195)	1	Bueno
	MONITOR PLANO (LG-w1943SI)	1	Bueno
	MONITOR PLANO (LG-22MP57HQ)	1	Bueno
	MONITOR PLANO (ACER-X173W)	1	Regular
3	**IMPRESORA**	**4**	
	IMPRESORA A INYECCION DE TINTA (CANON-S/M)	1	Regular
	IMPRESORA LASER (HP-SHNGC-1202-02)	1	Malo
	IMPRESORA LASER (HP-CZ181A)	1	Bueno
	IMPRESORA LASER (HP-CE557A)	1	Regular
4	**TECLADO - KEYBOARD**	**6**	
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (ECOTREND-3 in 1)	1	Bueno
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Bueno
	TECLADO - KEYBOARD (ECOTREND-KM-01)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU- 0138)	1	Regular
5	**ESTABILIZADOR**	**9**	
	ESTABILIZADOR (FX EVOLUTION-S/M)	1	Regular

	ESTABILIZADOR (FORZA-FVR-1002)	1	Regular
	ESTABILIZADOR (POWER LINE-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-S/M)	1	Bueno
	ESTABILIZADOR (SOFTSERVICE-S/M)	1	Bueno
	ESTABILIZADOR (OMEGA-PCG1200)	1	Bueno
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Bueno
	ESTABILIZADOR (FX EVOLUTION-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-S/M)	1	Regular
6	**SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (SIN MARCA-S/M)**	**1**	**Malo**
7	**RELOJ MARCADOR FECHADOR ELECTRONICO**	**2**	
	RELOJ MARCADOR FECHADOR ELECTRONICO (SIN MARCA-BIO 3D)	1	Regular
	RELOJ MARCADOR FECHADOR ELECTRONICO (SIN MARCA-BIO 3D)	1	Regular
8	**SWITCH PARA RED**	**2**	
	SWITCH PARA RED (SATRA-S/M)	1	Regular
	SWITCH PARA RED (D-LINK-DES-1016A)	1	Regular
GAF/SUB GERENCIA DE CONTABILIDAD			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**4**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**5**	
	MONITOR LED (SAMSUNG-S19D300NY)	1	Regular
	MONITOR LED (SAMSUNG-LS19D300NY/PE)	1	Regular
	MONITOR PLANO (AOC-S/M)	1	Regular
	MONITOR PLANO (LG-20EN43SA)	1	Regular
	MONITOR PLANO (HP-L45523A)	1	Regular
3	**IMPRESORA**	**3**	
	IMPRESORA A INYECCION DE TINTA (CANON-Ip1800)	1	Malo
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Regular
4	**TECLADO - KEYBOARD**	**4**	
	TECLADO - KEYBOARD (MICRONICS-1366)	1	Regular
	TECLADO - KEYBOARD (GENIUS-K645)	1	Regular
	TECLADO - KEYBOARD (ENKORE-ENT-1500)	1	Regular
	TECLADO - KEYBOARD (ENKORE-ENT-1500)	1	Regular
5	**ESTABILIZADOR**	**6**	
	ESTABILIZADOR (OMEGA-PCG1400)	1	Regular
	ESTABILIZADOR (QUASAR-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular
	ESTABILIZADOR (SOFTSERVICE-S/M)	1	Regular

	ESTABILIZADOR (DIGICOM-AVR-1000)	1	Malo
	ESTABILIZADOR (ALTRON-S/M)	1	Regular
6	**SWITCH PARA RED (SATRA-S/M)**	**1**	**Malo**
GAF/SUB GERENCIA DE ABASTECIMIENTO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**13**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-E4600)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-i5 - 8500)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-i5 - 8500)	1	Regular
2	**MONITOR**	**11**	
	MONITOR LED (LG-E19515T)	1	Malo
	MONITOR LED (SAMSUNG-S19D300NY)	1	Regular
	MONITOR LED (ACER-S/M)	1	Regular
	MONITOR LED (ACER-S/M)	1	Malo
	MONITOR LED (AOC-195LM0003)	1	Regular
	MONITOR PLANO (HP-S/M)	1	Malo
	MONITOR PLANO (LG-20M47A)	1	Regular
	MONITOR PLANO (LG-20M47A)	1	Regular
	MONITOR PLANO (LG-20M47A)	1	Malo
	MONITOR PLANO (LG-E19151T)	1	Regular
	MONITOR PLANO (LG-E1940SI)	1	Regular
3	**TECLADO - KEYBOARD**	**10**	
	TECLADO - KEYBOARD (HALION-S/M)	1	Regular
	TECLADO - KEYBOARD (HALION-S/M)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (ECOTREND-KMS-01)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular

4	**FOTOCOPIADORA EN GENERAL (RICOH-S/M)**	**1**	**Malo**
5	**IMPRESORA LASER (HP-S/M)**	**1**	**Malo**
6	**ACUMULADOR DE ENERGIA - EQUIPO DE UPS (CDP-S/M)**	**1**	**Malo**
7	**ESTABILIZADOR**	**9**	
	ESTABILIZADOR (GTX-S/M)	1	Regular
	ESTABILIZADOR (HURRICANE-ADP-1000)	1	Malo
	ESTABILIZADOR (OMEGA-PCG1400)	1	Regular
	ESTABILIZADOR (QUASAR-S/M)	1	Regular
	ESTABILIZADOR (ALTRON-S/M)	1	Malo
	ESTABILIZADOR (CDP-RUAVR604i)	1	Malo
	ESTABILIZADOR (CDP-RUAVR604i)	1	Regular
	ESTABILIZADOR (CDP-RUAVR604i)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Malo
8	**REGULADOR DE VOLTAJE (SIN MARCA-EYF)**	**1**	**Regular**
9	**SWITCH PARA RED (D-LINK-S/M)**	**1**	**Malo**
GAF/SUB GERENCIA DE CONTROL PATRIMONIAL Y SERVICIOS GENERALES			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-V206HQL)	1	Malo
2	**MONITOR**	**3**	
	MONITOR LED (LG-19EN43SA)	1	Malo
	MONITOR LED (LG-E19515-BN)	1	Reular
	MONITOR PLANO (ACER-V206HQL)	1	Regular
3	**IMPRESORA**	**2**	
	IMPRESORA A INYECCION DE TINTA (CANON-S/M)	1	Regular
	IMPRESORA A INYECCION DE TINTA (EPSON-C462J)	1	Regular
4	**COMPUTADORA PERSONAL PORTATIL (TOSHIBA-S/M)**	**1**	**Malo**
5	**TECLADO - KEYBOARD**	**5**	
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Malo
	TECLADO - KEYBOARD (MICROSOFT-X823082-003)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Malo
6	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (ORION-PLI-1001)	1	Regular
	ESTABILIZADOR (ORION-S/M)	1	Regular
7	**SWITCH PARA RED (SATRA-S/M)**	**1**	**Regular**
GAF/SUB GERENCIA DE TESORERIA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**7**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular

	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-CBXC500BT)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**7**	
	MONITOR LED (SAMSUNG-S19A300N)	1	Bueno
	MONITOR LED (LG-E19515T)	1	Bueno
	MONITOR LED (LG-19M38A)	1	Regular
	MONITOR LED (SAMSUNG-S19A300N)	1	Bueno
	MONITOR LED (SAMSUNG-933SNPLUS)	1	Regular
	MONITOR PLANO (AOC-S/M)	1	Bueno
	MONITOR PLANO (HP-S/M)	1	Regular
3	**IMPRESORA**	**5**	
	IMPRESORA A INYECCION DE TINTA (EPSON-S/M)	1	Malo
	IMPRESORA A INYECCION DE TINTA (EPSON-S/M)	1	Regular
	IMPRESORA LASER (HP-SHNGC-1202-02)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-CZ181A)	1	Regular
4	**TECLADO - KEYBOARD**	**8**	
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KB0135)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KGQ-012)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (HALION-KITHA-52K3)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-K120)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Malo
	TECLADO - KEYBOARD (BTC-S/M)	1	Malo
5	**ACUMULADOR DE ENERGIA - EQUIPO DE UPS (SIN MARCA-S/M)**	**1**	**Regular**
6	**ESTABILIZADOR**	**7**	
	ESTABILIZADOR (OMEGA-PCG1200)	1	Regular
	ESTABILIZADOR (SKY LINK-S/M)	1	Malo
	ESTABILIZADOR (OMEGA-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular
	ESTABILIZADOR (CYBERTEL-CYBC223)	1	Malo
	ESTABILIZADOR (QUASAR-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-S/M)	1	Regular
7	**REGULADOR DE VOLTAJE (CDP-S/M)**	**1**	**Regular**
8	**SWITCH PARA RED (D-LINK-S/M)**	**1**	**Regular**
GERENCIA DE ASESORÍA JURÍDICA (GAJ)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**ESTABILIZADOR (OMEGA-493317)**	**1**	**Regular**

2	**IMPRESORA LASER (HP-SHNGC-1501-04)**	**1**	**Regular**
GERENCIA DE PLANEAMIENTO Y PRESUPUESTO (GPP)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**5**	
	MONITOR LED (AOC-195LM00003)	1	Bueno
	MONITOR LED (SAMSUNG-933BW)	1	Regular
	MONITOR LED (ACER-V206HQL)	1	Regular
	MONITOR LED (SAMSUNG-733 NW)	1	Regular
	MONITOR PLANO (SIN MARCA-S/M)	1	Malo
3	**TECLADO - KEYBOARD**	**4**	
	TECLADO - KEYBOARD (ENKORE-ENT 500)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Malo
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Bueno
4	**COMPUTADORA PERSONAL PORTATIL (LENOVO-80 EW)**	**1**	**Regular**
5	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (POWER-LITE)	1	Regular
	ESTABILIZADOR (QUASAR-PLI 1200)	1	Regular
6	**CAMARA DOMO A COLOR**	**5**	
	CAMARA DOMO A COLOR (LEVEL ONE-FCS-3101)	1	Malo
	CAMARA DOMO A COLOR (LEVEL ONE-FCS-3101)	1	Malo
	CAMARA DOMO A COLOR (ULTRAZIP-Z-20IP-2(IR))	1	Malo
	CAMARA DOMO A COLOR (ULTRAZIP-Z-20IP-2(IR))	1	Malo
	CAMARA DOMO A COLOR (ULTRAZIP-Z-20IP-2(IR))	1	Malo
7	**MANDO DE CONTROL DE CAMARAS DOMO**	**4**	
	MANDO DE CONTROL DE CAMARAS DOMO (LEVEL ONE-CAS-4300)	1	Malo
	MANDO DE CONTROL DE CAMARAS DOMO (LEVEL ONE-CAS-4300)	1	Regular
	MANDO DE CONTROL DE CAMARAS DOMO (LEVEL ONE-CAS-4300)	1	Malo
	MANDO DE CONTROL DE CAMARAS DOMO (LEVEL ONE-CAS-4300)	1	Regular
GPP/SUB GERENCIA DE PLANIFICACIÒN Y MODERNIZACIÒN INSTITUCIONAL			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**26**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo

	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**2**	
	MONITOR LED (LG-W22435V)	1	Bueno
	MONITOR PLANO (SAMSUNG-S/M)	1	Malo
3	**COMPUTADORA PERSONAL PORTATIL**	**5**	
	COMPUTADORA PERSONAL PORTATIL (HP-S/M)	1	Regular
	COMPUTADORA PERSONAL PORTATIL (LENOVO-20157)	1	Regular
	COMPUTADORA PERSONAL PORTATIL (HP-S/M)	1	Regular
	COMPUTADORA PERSONAL PORTATIL (LENOVO-20137)	1	Regular
	COMPUTADORA PERSONAL PORTATIL (DELL-GAMING G3 i5 3590)	1	Regular
4	**ESTABILIZADOR**	**5**	
	ESTABILIZADOR (SIN MARCA-S/M)	1	Malo
	ESTABILIZADOR (QUASAR-POWER)	1	Bueno
	ESTABILIZADOR (OUTPT-S/M)	1	Malo
	ESTABILIZADOR (OUTPT-S/M)	1	Malo
	ESTABILIZADOR (OUTPT-S/M)	1	Malo
5	**TECLADO - KEYBOARD**	**4**	
	TECLADO - KEYBOARD (AVATEC-GK-100015)	1	Malo
	TECLADO - KEYBOARD (GENIUS-K636)	1	Malo
	TECLADO - KEYBOARD (AVATEC-CKB3050BS)	1	Malo
	TECLADO - KEYBOARD (ADVANCE-5137AU)	1	Bueno
GPP/SGPMI/ÁREA FUNCIONAL DE TECNOLOGÍA DE LA INFORMACIÁN			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**

1	**COMPUTADORA SERVIDOR (SUPERMICRO 847-12)**	**1**	Regular
2	**UNIDAD CENTRAL DE PROCESO - CPU**	**6**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-OPTIPLEX)	1	Regular
3	**MONITOR**	**11**	
	MONITOR LED (SAMSUNG-S24D300H)	1	Malo
	MONITOR LED (SAMSUNG-S24D300H)	1	Malo
	MONITOR LED (SAMSUNG-S24D300H)	1	Regular
	MONITOR LED (SAMSUNG-S24D300H)	1	Malo
	MONITOR LED (SAMSUNG-S24D300H)	1	Malo
	MONITOR LED (SAMSUNG-S24D300H)	1	Regular
	MONITOR LED (SAMSUNG-S24D300H)	1	Malo
	MONITOR LED (SAMSUNG-LS19D300NY/PE)	1	Malo
	MONITOR LED (HP-L4S23A)	1	Regular
	MONITOR LED (LG-E1951ST)	1	Regular
	MONITOR LED (SAMSUNG-S19A 300N)	1	Regular
4	**IMPRESORA**	**3**	
	IMPRESORA A INYECCION DE TINTA (BROTHER-DCP-T300)	1	Malo
	IMPRESORA A INYECCION DE TINTA (EPSON-L210)	1	Malo
	IMPRESORA A INYECCION DE TINTA (CANON-MX391)	1	Malo
5	**TECLADO - KEYBOARD**	**8**	
	TECLADO - KEYBOARD (STARTEC-S/M)	1	Regular
	TECLADO - KEYBOARD (CYBERTEL-CYBK100)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100011)	1	Regular
	TECLADO - KEYBOARD (ENKORE-ENT503)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
	TECLADO - KEYBOARD (ADVANCE-5137AU)	1	Malo
	TECLADO - KEYBOARD (MICRONICS-MIC K580)	1	Malo
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Malo
6	**ACUMULADOR DE ENERGIA - EQUIPO DE UPS**	**11**	
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo

	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (ELISE-UMC-650)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (FORZA-NT-512U)	1	Regular
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (FORZA-NT-512U)	1	Regular
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (FORZA-NT-512U)	1	Regular
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (FORZA-NT-512U)	1	Regular
7	**EQUIPO DE ILUMINACION DE EMERGENCIA**	**4**	
	EQUIPO DE ILUMINACION DE EMERGENCIA (GALEAZZI-EMLG-24L)	1	Regular
	EQUIPO DE ILUMINACION DE EMERGENCIA (GALEAZZI-EMLG-24L)	1	Regular
	EQUIPO DE ILUMINACION DE EMERGENCIA (GALEAZZI-EMLG-24L)	1	Regular
	EQUIPO DE ILUMINACION DE EMERGENCIA (GALEAZZI-EMLG-24L)	1	Regular
8	**SWITCH PARA RED**	**2**	
	SWITCH PARA RED (MIKROTIK-RB1100AHX2)	1	Regular
	SWITCH PARA RED (TP-LINK-TL-WR8441HP)	1	Regular
9	**TELEFONO (SIN MARCA-S/M)**	**1**	**Malo**
10	**TELEVISOR A COLORES**	**8**	
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
	TELEVISOR A COLORES (SAMSUNG-UN5015500AGPE)	1	Bueno
GPP/SUB GERENCIA DE PRESUPUESTO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**2**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Bueno
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**2**	
	MONITOR LED (HP-V244H)	1	Bueno
	MONITOR LED (LG-20M47A)	1	Bueno
3	**IMPRESORA**	**3**	

	IMPRESORA A INYECCION DE TINTA (EPSON-14150)	1	Bueno
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-BOISB-0605-00)	1	Malo
4	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (CDP-S/M)	1	Bueno
	ESTABILIZADOR (FASE-FXE-1000)	1	Bueno
GPP/SUB GERENCIA DE PROGRAMACIÓN MULTIANUAL DE INVERSIONES			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Regular**
2	**MONITOR LED (LG-E19S15T)**	**1**	**Regular**
3	**ESTABILIZADOR (ALTRON-S/M)**	**1**	**Regular**
GPP/SUB GERENCIA DE FORMULACIÓN DE PROYECTOS DE INVERSIÓN PÚBLICA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Regular**
2	**MONITOR LED (SAMSUNG-5200300NH)**	**1**	**Regular**
3	**COMPUTADORA PERSONAL PORTATIL (TOSHIBA-S/M)**	**1**	**Regular**
4	**IMPRESORA LASER (HP-S/M)**	**1**	**Regular**
5	**ESTABILIZADOR**	**3**	
	ESTABILIZADOR (OMEGA-493317)	1	Regular
	ESTABILIZADOR (DUT PUT-S/M)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Regular
6	**SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (CDP-S/M)**	**1**	**Malo**
7	**EQUIPO DE POSICIONAMIENTO - GPS (GARMIN-S/M)**	**1**	**Malo**
8	**SWITCH PARA RED (D-LINK-S/M)**	**1**	**Regular**
GERENCIA DE DESARROLLO URBANO Y RURAL (GDUR)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Regular**
2	**MONITOR LED (LG-W2243TV)**	**1**	**Regular**
3	**TECLADO - KEYBOARD (MICROSOFT-S/M)**	**1**	**Regular**
4	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (OMEGA-S/M)	1	Bueno
	ESTABILIZADOR (PROTECTOR LINE-S/M)	1	Regular
5	**SUPRESOR DE VOLTAJE TRANSITORIO-TVSS (ORTEGA-S/M)**	**1**	**Regular**
6	**SWITCH PARA RED (TP-LINK-S/M)**	**1**	**Regular**
GDUR/SUB GERENCIA DE OBRAS Y MAQUINARIAS			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-POWER COULIN)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular

2	**MONITOR**	**4**	
	MONITOR LED (SAMSUNG-519D300 NY)	1	Bueno
	MONITOR LED (SAMSUNG-519D300 NY)	1	Regular
	MONITOR LED (HP-S/M)	1	Regular
	MONITOR LED (SAMSUNG-S190300NY/PE)	1	Regular
3	**IMPRESORA LASER (HP-CE658A)**	**1**	**Regular**
4	**TECLADO - KEYBOARD**	**3**	
	TECLADO - KEYBOARD (VASTEC-KEG-012)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEG-012)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK10015)	1	Regular
5	**ESTABILIZADOR**	**7**	
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Bueno
	ESTABILIZADOR (OMEGA-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-PCG-1200)	1	Bueno
	ESTABILIZADOR (AVATEC-S/M)	1	Bueno
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Regular
GDUR/SUB GERENCIA DE ESTUDIOS Y PROYECTOS			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Regular**
2	**MONITOR**	**3**	
	MONITOR LED (HP-L4523A)	1	Bueno
	MONITOR LED (LG-19M37A)	1	Malo
	MONITOR LED (LG-19M35A)	1	Malo
3	**IMPRESORA A INYECCION DE TINTA (EPSON-C462S)**	**1**	**Bueno**
4	**TECLADO - KEYBOARD (GENIUS-S/M)**	**1**	**Malo**
5	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (ORION-POWER LITE)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-S/M)	1	Regular
GDUR/SUB GERENCIA DE PLANIFICACIÓN URBANA Y CATASTRO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**8**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**11**	
	MONITOR LED (LG-W2243TV)	1	Regular
	MONITOR LED (SAMSUNG-519D300NY)	1	Regular

	MONITOR LED (LG-E2D51SR)	1	Malo
	MONITOR LED (ADVANCE-A-195 MS)	1	Regular
	MONITOR LED (SAMSUNG-519D300NY)	1	Regular
	MONITOR LED (HP-L4523A)	1	Malo
	MONITOR LED (LG-E19515T)	1	Regular
	MONITOR LED (LG-19M37A)	1	Regular
	MONITOR LED (ACER-X173W)	1	Malo
	MONITOR LED (LG-19M37A)	1	Malo
	MONITOR LED (LG-E1951ST)	1	Regular
3	**IMPRESORA**	**3**	
	IMPRESORA LASER (HP-S/M)	1	Regular
	IMPRESORA LASER (HP-S/M)	1	Regular
	IMPRESORA PARA PLANOS - PLOTTERS (HP-CM337A)	1	Regular
4	**ESTABILIZADOR**	**9**	
	ESTABILIZADOR (QUASAR-S/M)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-FXG-1000)	1	Bueno
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (POWER-S/M)	1	Regular
	ESTABILIZADOR (ORION-S/M)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-S/M)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Regular
	ESTABILIZADOR (POWER LITE-PLI1001)	1	Regular
5	**TECLADO - KEYBOARD**	**7**	
	TECLADO - KEYBOARD (VASTEC-KEG-012)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Bueno
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Bueno
	TECLADO - KEYBOARD (CYBERTEL-CYBT101)	1	Regular
	TECLADO - KEYBOARD (GENIUS-K639)	1	Regular
6	**SWITCH PARA RED (D-LINK-S/M)**	**1**	**Bueno**
GDUR/SUB GERENCIA DE GESTIÓN DE RIESGOS Y DESASTRES			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**2**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**2**	
	MONITOR LED (LG-E2351YRT)	1	Bueno
	MONITOR LED (AOC-19SLM00008)	1	Regular
3	**IMPRESORA**	**4**	
	IMPRESORA A INYECCION DE TINTA (EPSON-C463C)	1	Bueno
	IMPRESORA A INYECCION DE TINTA (EPSON-C462H)	1	Regular
	IMPRESORA LASER (HP-CE65A)	1	Malo
	IMPRESORA LASER (HP-S/M)	1	Bueno

4	**TECLADO - KEYBOARD (GENIUS-S/M)**	**1**	**Malo**
5	**FOTOCOPIADORA EN GENERAL (RICOH-S/M)**	**1**	**Regular**
6	**ESTABILIZADOR**	**4**	
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Malo
	ESTABILIZADOR (ENERGY-S/M)	1	Bueno
	ESTABILIZADOR (FORZA-FVR-1221B)	1	Regular
7	**VEHICULO AEREO NO TRIPULADO - DRONE (SIN MARCA-4RTK)**	**1**	**Bueno**
8	**EQUIPO DE POSICIONAMIENTO - GPS (GARMIN-S/M)**	**1**	**Regular**
GERENCIA DE DESARROLLO SOCIAL (GDS)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**COMPUTADORA PERSONAL PORTATIL (HP-S/M)**	**1**	**Regular**
2	**MONITOR**	**4**	
	MONITOR LED (HP-V1936)	1	Regular
	MONITOR LED (LG-E1991ST)	1	Malo
	MONITOR LED (AOC-S/M)	1	Regular
	MONITOR PLANO (AOC-18M1D4A6)	1	Malo
3	**TECLADO - KEYBOARD (GENIUS-KU-0138)**	**1**	**Regular**
4	**TABLETA PAD 1.30 GHZ 1 GB ALMACENAMIENTO 16 GB PANTALLA 7 in (SIN MARCA-S/M)**	**1**	**Bueno**
5	**IMPRESORA LASER (HP-CE658A)**	**1**	**Regular**
6	**LECTORA DE CODIGO DE BARRAS (ARGOX-AR-8000 URB)**	**1**	**Regular**
7	**ESTABILIZADOR**	**3**	
	ESTABILIZADOR (AVATEC-AVA-1200)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-S/M)	1	Malo
8	**SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (FORZA-S/M)**	**1**	**Regular**
GDS/SUB GERENCIA DE DESARROLLO HUMANO, EDUCACIÓN Y SALUD			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**2**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**2**	
	MONITOR LED (LG-E1941ST)	1	Regular
	MONITOR LED (LG-E1941ST)	1	Malo
3	**ESTABILIZADOR**	**3**	
	ESTABILIZADOR (POWER-LITE)	1	Regular
	ESTABILIZADOR (OMEGA-PCG 1200S)	1	Regular
	ESTABILIZADOR (ORION-S/M)	1	Regular
4	**IMPRESORA LASER (HP-CE658A)**	**1**	**Regular**
5	**TECLADO - KEYBOARD**	**3**	
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular

	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Malo
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
GDS/SUB GERENCIA DE PROGRAMAS SOCIALES E INCLUSION SOCIAL			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**25**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (2500-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (RHINOBOX)	1	Bueno
2	**MONITOR**	**27**	
	MONITOR LED (AOC-185LM00012)	1	Malo
	MONITOR LED (LG-19M35A)	1	Malo
	MONITOR LED (LG-E1951S)	1	Regular
	MONITOR LED (LG-19M35AA)	1	Regular
	MONITOR LED (SAMSUNG-S19D300NDY)	1	Regular
	MONITOR LED (LG-22M38H)	1	Regular
	MONITOR LED (LG-E1951S2)	1	Regular
	MONITOR LED (LG-W1943SI)	1	Malo
	MONITOR LED (SAMSUNG-LS19C1S0F)	1	Regular
	MONITOR LED (LG-20MK400H)	1	Malo
	MONITOR LED (SAMSUNG-S19A300N)	1	Regular
	MONITOR LED (BENQ-GL2030-TA)	1	Regular
	MONITOR LED (AOC-S/M)	1	Malo
	MONITOR LED (LG-E1951CR)	1	Regular

	MONITOR LED (SAMSUNG-S19C150F)	1	Regular
	MONITOR LED (HP-V193B)	1	Regular
	MONITOR LED (SAMSUNG-733 NW)	1	Malo
	MONITOR LED (AOC-S/M)	1	Regular
	MONITOR LED (LG-W194351)	1	Regular
	MONITOR LED 24 in (AOC-)	1	Bueno
	MONITOR PLANO (LG-E1951S)	1	Regular
	MONITOR PLANO (SAMSUNG-AN17L57L/PES)	1	Malo
	MONITOR PLANO (COMMODORE-70330)	1	Malo
	MONITOR PLANO (GOLDSTAR-S/M)	1	Malo
	MONITOR PLANO (DELL-S/M)	1	Malo
	MONITOR PLANO (SAMSUNG-753S)	1	Malo
	MONITOR PLANO (LG-19M35AA)	1	Regular
3	**IMPRESORA**	**9**	
	IMPRESORA A INYECCION DE TINTA (CANON-K10355)	1	Malo
	IMPRESORA A INYECCION DE TINTA (EPSON-C4624)	1	Regular
	IMPRESORA A INYECCION DE TINTA (EPSON-C42H)	1	Regular
	IMPRESORA A INYECCION DE TINTA (EPSON-L4260)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-Q5911A)	1	Malo
	IMPRESORA LASER (HP-C2181A)	1	Regular
	IMPRESORA LASER (HP-CE749A)	1	Regular
	IMPRESORA LASER (HP-C2127A)	1	Malo
4	**TECLADO - KEYBOARD**	**25**	
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Malo
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Malo
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Regular
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-K120)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-10001S)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-S/M)	1	Malo
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KB-125)	1	Regular
	TECLADO - KEYBOARD (AVATEC-CKB-3050BS)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1360)	1	Regular
	TECLADO - KEYBOARD (AVATEC-CKB-305089)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Malo
	TECLADO - KEYBOARD (ENKORE-ENK 300)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-400)	1	Regular
	TECLADO - KEYBOARD (GENIUS-K 645)	1	Malo
	TECLADO - KEYBOARD (GENIUS-GK-07000 BU)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-S/M)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-K 120)	1	Malo

	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KG39)	1	Regular
	TECLADO - KEYBOARD (LG-KCW3P)	1	Regular
	TECLADO - KEYBOARD (MICRONICS-MIC K580)	1	Malo
5	**FOTOCOPIADORA**	**2**	
	FOTOCOPIADORA EN GENERAL (KONICA MINOLTA-F5-530)	1	Regular
	FOTOCOPIADORA EN GENERAL (RICOH-LD220)	1	Malo
6	**ACUMULADOR DE ENERGIA - EQUIPO DE UPS (FORZA-SL-1012V)**	**1**	**Regular**
7	**ESTABILIZADOR**	**13**	
	ESTABILIZADOR (OMEGA-S/M)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Malo
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADOR (STABY LINE-S/M)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-S/M)	1	Malo
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADOR (CDP-AVR)	1	Malo
	ESTABILIZADOR (CDP-AVR)	1	Regular
	ESTABILIZADOR (FORZA-FPS-0058)	1	Bueno
	ESTABILIZADOR (ORION-PLI-1001)	1	Malo
	ESTABILIZADOR (POWER LITE-PLI 1100 USB)	1	Regular
8	**SWITCH PARA RED**	**4**	
	SWITCH PARA RED (MITRASTOR-DSL-2401HN-T1C)	1	Malo
	SWITCH PARA RED (D-LINK-S/M)	1	Regular
	SWITCH PARA RED (SATRA-S/M)	1	Malo
	SWITCH PARA RED (D-LINK-D65-1016)	1	Regular
9	**TELEFONO**	**2**	
	TELEFONO (SANDO-RZ251310)	1	Malo
	TELEFONO INALAMBRICO (SIN MARCA-T56EX)	1	Malo
GDS/SUB GERENCIA DE PROMOCIÓN SOCIAL Y PARTICIPACIÓN VECINAL			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Regular**
2	**MONITOR**	**2**	
	MONITOR LED (SAMSUNG-733NW)	1	Regular
	MONITOR LED (LG-E194AST)	1	Regular
3	**IMPRESORA LASER (HP-S/M)**	**1**	**Regular**
4	**TECLADO - KEYBOARD (HALION-K 5015)**	**1**	**Regular**
5	**SWITCH PARA RED (TP-LINK-TL-SF10080)**	**1**	**Regular**
GERENCIA DE SOSTENIBILIDAD AMBIENTAL (GSA)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	

	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**4**	
	MONITOR LED (SAMSUNG-S19B150N)	1	Bueno
	MONITOR LED (SAMSUNG-LS19D300NY/PE)	1	Malo
	MONITOR PLANO (LG-19M37A)	1	Regular
	MONITOR PLANO (LG-W1943SI)	1	Regular
3	**TECLADO - KEYBOARD**	**5**	
	TECLADO - KEYBOARD (ECOTREND-3IN1)	1	Bueno
	TECLADO - KEYBOARD (MICROSOFT-S/M)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Regular
	TECLADO - KEYBOARD (VASTEC-KEQ-012)	1	Malo
	TECLADO - KEYBOARD (CYBERTEL-S/M)	1	Malo
4	**IMPRESORA**	**2**	
	IMPRESORA A INYECCION DE TINTA (BROTHER-DCP-T300)	1	Regular
	IMPRESORA A INYECCION DE TINTA (EPSON-C463C)	1	Bueno
5	**ESTABILIZADOR**	**5**	
	ESTABILIZADOR (FORZA-S/M)	1	Bueno
	ESTABILIZADOR (FX EVOLUTION-S/M)	1	Regular
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (JKL-S/M)	1	Regular
	ESTABILIZADOR (ORION-S/M)	1	Regular
6	**SWITCH PARA RED (SATRA-S/M)**	**1**	**Regular**
GSA/SUB GERENCIA DE GESTIÓN INTEGRAL DE RESIDUOS MUNICIPALES			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**2**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**2**	
	MONITOR LED (SAMSUNG-S19D300NY)	1	Regular
	MONITOR PLANO (LG-E19515R)	1	Malo
3	**TECLADO - KEYBOARD**	**2**	
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
4	**IMPRESORA**	**2**	
	IMPRESORA A INYECCION DE TINTA (CANON-S/M)	1	Malo
	IMPRESORA LASER (HP-SHNGC-1202-02)	1	Regular
5	**ESTABILIZADOR**	**4**	
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Bueno
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
GSA/SUB GERENCIA DE MANEJO Y GESTION AMBIENTAL			

NRO	DESCRIPCION	CANTIDAD	ESTADO
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**4**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-ENC1021)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**4**	
	MONITOR PLANO (ACER-V206HQL)	1	Bueno
	MONITOR PLANO (LG-W19435I)	1	Regular
	MONITOR PLANO (LG-19M38A)	1	Regular
	MONITOR PLANO (LG-W19435I)	1	Bueno
3	**TECLADO - KEYBOARD**	**4**	
	TECLADO - KEYBOARD (GENIUS-K699)	1	Regular
	TECLADO - KEYBOARD (HALION-HA-K230)	1	Regular
	TECLADO - KEYBOARD (LOGITECH-Y-U0009)	1	Regular
	TECLADO - KEYBOARD (GENIUS-K-645)	1	Regular
4	**ESTABILIZADOR (SKY LINK-S/M)**	**1**	**Regular**
5	**SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (PROFIELD-S/M)**	**1**	**Malo**
6	**IMPRESORA A INYECCION DE TINTA (CANON-S/M)**	**1**	**Regular**
GSA/SGMGA/ÁREA TÉCNICA MUNICIPAL - ATM			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**COMPUTADORA PERSONAL PORTATIL (ASUS)**	**1**	**Bueno**
GSA/SUB GERENCIA DE ÁREAS VERDES Y RECURSOS NATURALES			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**IMPRESORA LASER (HP-CE657)**		**Regular**
2	**MONITOR PLANO (ACER-V206HQL)**		**Malo**
3	**TECLADO - KEYBOARD (LOGITECH-Y-U0009)**		**Malo**
4	**ESTABILIZADOR**		
	ESTABILIZADOR (FORZA-FVR-1O)		Bueno
	ESTABILIZADOR (OMEGA-PCG)		Regular
GERENCIA DE DESARROLLO ECONOMICO (GDE)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**COMPUTADORA PERSONAL PORTATIL (ASUS-X555L)**	**1**	**Bueno**
2	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
3	**MONITOR**	**3**	
	MONITOR LED (SAMSUNG-519D300NY)	1	Regular
	MONITOR LED (SAMSUNG-S19D300NY)	1	Regular
	MONITOR LED (AOC-S/M)	1	Regular
4	**IMPRESORA**	**5**	
	IMPRESORA A INYECCION DE TINTA (EPSON-C463C)	1	Regular

	IMPRESORA A INYECCION DE TINTA (EPSON-C463C)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-CZ181A)	1	Malo
	IMPRESORA LASER (HP-CE658A)	1	Regular
5	**TECLADO - KEYBOARD**	**2**	
	TECLADO - KEYBOARD (GENIUS-GK070008/LY)	1	Regular
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Regular
GDE/SUB GERENCIA DE PROMOCIÓN EMPRESARIAL Y TURISMO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**7**	
	MONITOR LED (LG-ELASIST)	1	Regular
	MONITOR LED (SAMSUNG-519D300NY)	1	Malo
	MONITOR LED (LG-W1943SI)	1	Malo
	MONITOR LED (LG-19H35A-B)	1	Regular
	MONITOR LED (SAMSUNG-S/M)	1	Malo
	MONITOR LED (LG-19M35AA)	1	Regular
	MONITOR PLANO (ACER-V206HQL)	1	Regular
3	**IMPRESORA**	**4**	
	IMPRESORA A INYECCION DE TINTA (EPSON-C462S)	1	Malo
	IMPRESORA LASER (CANON-S/M)	1	Malo
	IMPRESORA LASER (HP-CE658A)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Regular
4	**TECLADO - KEYBOARD**	**9**	
	TECLADO - KEYBOARD (BTC-5207)	1	Malo
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Bueno
	TECLADO - KEYBOARD (BTC-S/M)	1	Malo
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-100015)	1	Malo
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KB-0138)	1	Regular
5	**COMPUTADORA PERSONAL PORTATIL (LENOVO-LAPTOP)**	**1**	**Bueno**
6	**ESTABILIZADOR**	**7**	
	ESTABILIZADOR (QUASAR-S/M)	1	Regular
	ESTABILIZADOR (AVATEC-S/M)	1	Regular
	ESTABILIZADOR (AVATEC-S/M)	1	Bueno
	ESTABILIZADOR (FORZA-FVR-12218)	1	Bueno
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular

	ESTABILIZADOR (FORZA-S/M)	1	Regular
7	**SWITCH PARA RED (D-LINK-DGS 10160)**	**1**	**Regular**
GDE/SUB GERENCIA DE FISCALIZACIÓN Y CONTROL			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**5**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Malo
2	**MONITOR**	**2**	
	MONITOR LED (SIN MARCA-S/M)	1	Malo
	MONITOR LED (LG-19M37A)	1	Bueno
3	**IMPRESORA LASER (HP-S/M)**	**1**	**Regular**
4	**ESTABILIZADOR (HURRICANE-ADP-1001)**	**1**	**Bueno**
5	**TECLADO - KEYBOARD**	**5**	
	TECLADO - KEYBOARD (CYBERTEL-CYB-K102)	1	Regular
	TECLADO - KEYBOARD (SIN MARCA-S/M)	1	Malo
	TECLADO - KEYBOARD (SIN MARCA-S/M)	1	Malo
	TECLADO - KEYBOARD (MICRONICS-MICK 580)	1	Regular
	TECLADO - KEYBOARD (BLANDBYTE-SKB558+OPM353)	1	Malo
GERENCIA DE ADMINISTRACIÓN TRIBUTARIA (GAT)			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**SERVIDOR (HP-E5405)**	**1**	**Regular**
2	**COMPUTADORA PERSONAL PORTATIL (HP-PAVILION)**	**1**	**Regular**
3	**UNIDAD CENTRAL DE PROCESO - CPU**	**5**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-CBXC500STB)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-Core i7)	1	Regular
4	**MONITOR**	**6**	
	MONITOR LED (AOC-TFT17W80PS)	1	Regular
	MONITOR LED (LG-W1943SI)	1	Regular
	MONITOR LED (TEROS-TE-RE)	1	Regular
	MONITOR PLANO (TEROS-TE-R6)	1	Regular
	MONITOR PLANO (ACER-X173W)	1	Regular
	MONITOR PLANO (SIN MARCA-S/M)	1	Malo
5	**TECLADO - KEYBOARD**	**8**	
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Regular
	TECLADO - KEYBOARD (GENIUS-S/M)	1	Regular
	TECLADO - KEYBOARD (HALION-KIT HA-K233C)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular

	TECLADO - KEYBOARD (GENIUS-K 639)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KG45)	1	Regular
	TECLADO - KEYBOARD (ECOTREND-KM-02)	1	Regular
	TECLADO - KEYBOARD (GENIUS-GK-070006)	1	Malo
6	**IMPRESORA**	**2**	
	IMPRESORA LASER (HP-SHNGC-1202-02)	1	Malo
	IMPRESORA LASER (KYOCERA ECOSYS-M3655)	1	Regular
7	**FOTOCOPIADORA EN GENERAL**	**2**	
	FOTOCOPIADORA EN GENERAL (KONICA MINOLTA-BIZHUB)	1	Bueno
	FOTOCOPIADORA EN GENERAL (SIN MARCA-S/M)	1	Regular
8	**ACUMULADOR DE ENERGIA**	**4**	
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (SIN MARCA-CDP)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (CDP-S/M)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (CDP-S/M)	1	Malo
	ACUMULADOR DE ENERGIA - EQUIPO DE UPS (CDP-S/M)	1	Malo
9	**ESTABILIZADOR**	**8**	
	ESTABILIZADOR (SIN MARCA-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular
	ESTABILIZADOR (FORZA-S/M)	1	Regular
	ESTABILIZADOR (STABY LINE-S/M)	1	Regular
	ESTABILIZADOR (OMEGA-PC61400)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Regular
	ESTABILIZADOR (OMEGA-4A507)	1	Malo
	ESTABILIZADOR (UNITRON-4 PUERTOS)	1	Regular
10	**SWITCH PARA RED**	**3**	
	SWITCH PARA RED (TP-LINK-S/M)	1	Regular
	SWITCH PARA RED (D-LINK-S/M)	1	Regular
	SWITCH PARA RED (SATRA-S/M)	1	Regular
GAT/SUB GERENCIA DE REGISTRO Y ORIENTACIÓN TRIBUTARIA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-CBXC5005BT)	1	Regular
2	**MONITOR**	**4**	
	MONITOR LED (AOC-TFT17W80PS)	1	Regular
	MONITOR LED (LG-19M37A)	1	Regular
	MONITOR LED (LG-W1943SI)	1	Regular
	MONITOR LED 22 in (LG-)	1	Bueno

3	**TECLADO - KEYBOARD**	**3**	
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (HALION-KIT HA-K233C)	1	Regular
	IMPRESORA A INYECCION DE TINTA (EPSON-C462C)	1	Regular
4	**ESTABILIZADOR**	**4**	
	ESTABILIZADOR (SIN MARCA-S/M)	1	Malo
	ESTABILIZADOR (STABY-S/M)	1	Malo
	ESTABILIZADOR (OMEGA-PCG 1000)	1	Regular
	ESTABILIZADOR (OMEGA-493317)	1	Malo
GAT/SUB GERENCIA DE RECAUDACIÓN Y CONTROL TRIBUTARIO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**5**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**5**	
	MONITOR LED (LG-E19515T)	1	Regular
	MONITOR LED (LG-E1951ST)	1	Regular
	MONITOR LED 22 in (LG-)	1	Bueno
	MONITOR PLANO (ADVANCE-A-195MS)	1	Regular
	MONITOR PLANO (ADVANCE-A-195MB)	1	Regular
3	**TECLADO - KEYBOARD**	**8**	
	TECLADO - KEYBOARD (CYBERLINK-S/M)	1	Malo
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Malo
	TECLADO - KEYBOARD (GENIUS-SLIM STAR)	1	Malo
	TECLADO - KEYBOARD (CYBERTEL-CYB T108)	1	Malo
	TECLADO - KEYBOARD (GENIUS-KU-0138)	1	Regular
	TECLADO - KEYBOARD (DELL-SK-8115)	1	Regular
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
4	**IMPRESORA**	**3**	
	IMPRESORA A INYECCION DE TINTA (BROTHER-DCP-T510W)	1	Malo
	IMPRESORA LASER (HP-CE749A)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Regular
5	**ESTABILIZADOR**	**6**	
	ESTABILIZADOR (ALTRON-S/M)	1	Malo
	ESTABILIZADOR (SAKURA-POWER)	1	Regular
	ESTABILIZADOR (OMEGA-PCG 1200)	1	Regular
	ESTABILIZADOR (NEXOS-S/M)	1	Regular
	ESTABILIZADOR (FX EVOLUTION-FXE-1000)	1	Regular
	ESTABILIZADOR (ELISE-)	1	Bueno
GAT/SUB GERENCIA DE FISCALIZACIÓN TRIBUTARIA			

NRO	DESCRIPCION	CANTIDAD	ESTADO
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**2**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
2	**MONITOR**	**3**	
	MONITOR LED (SAMSUNG-519D300NV)	1	Regular
	MONITOR LED (LG-W1943SI)	1	Regular
	MONITOR LED 22 in (LG)	1	Bueno
3	**TECLADO - KEYBOARD**	**2**	
	TECLADO - KEYBOARD (MICROSOFT-1576)	1	Regular
	TECLADO - KEYBOARD (ECOTREND-S/M)	1	Regular
4	**ESTABILIZADOR (OMEGA-S/M)**	**1**	**Regular**
5	**IMPRESORA LASER (HP-BOISB-0405-00)**	**1**	**Malo**
6	**FOTOCOPIADORA EN GENERAL (RICOH-LD050)**	**1**	**Regular**
GAT/SUB GERENCIA DE EJECUCIÓN COACTIVA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**ESTABILIZADOR**	**2**	
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADORSTABY (TROMS/M)	1	Malo
2	**IMPRESORA**	**2**	
	IMPRESORA LASER (CANON-L11121E)	1	Regular
	IMPRESORA LASER (HP-CE658A)	1	Malo
3	**SWITCH PARA RED (D-LINKDGS-1016D)**	**1**	**Regular**
GERENCIA DE SEGURIDAD CIUDADANA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**UNIDAD CENTRAL DE PROCESO - CPU**	**3**	
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)	1	Regular
	UNIDAD CENTRAL DE PROCESO - CPU (TEXCOPER)	1	Regular
2	**MONITOR**	**2**	
	MONITOR LED (SAMSUNG-S24D300H)	1	Regular
	MONITOR LED (LG-E1951ST)	1	Regular
3	**TECLADO - KEYBOARD**	**5**	
	TECLADO - KEYBOARD (ENKORE-ENT500)	1	Bueno
	TECLADO - KEYBOARD (LOGITECH-K120)	1	Malo
	TECLADO - KEYBOARD (SEISA-DN-D221)	1	Bueno
	TECLADO - KEYBOARD (CYBERTEL-CYBK100)	1	Bueno
	TECLADO - KEYBOARD (GENIUS-KU- 0138)	1	Regular
4	**IMPRESORA**	**2**	
	IMPRESORA A INYECCION DE TINTA (HP-PAGEWIDE)	1	Bueno
	IMPRESORA LASER (HP-EC749A)	1	Regular
5	**ESTABILIZADOR**	**3**	
	ESTABILIZADOR (STABY LINE-S/M)	1	Regular
	ESTABILIZADOR (CDP-S/M)	1	Regular
	ESTABILIZADOR (ALTRON-S/M)	1	Regular

6	**REGULADOR DE VOLTAJE (SIN MARCA-S/M)**	**1**	**Bueno**
7	**SUPRESOR DE VOLTAJE TRANSITORIO - TVSS**	**2**	
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (OMEGA-6 PUERTOS)	1	Regular
	SUPRESOR DE VOLTAJE TRANSITORIO - TVSS (OMEGA-S/M)	1	Regular
GSC/SUB GERENCIA DE PREVENCION CIUDADANA			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**REGULADOR DE VOLTAJE(CDP-R2C-AVR1008i)**	**1**	**Regular**
2	**MONITOR LED(SAMSUNG-S19D300NY)**	**1**	**Regular**
GSC/SUB GERENCIA DE SERENAZGO			
NRO	**DESCRIPCION**	**CANTIDAD**	**ESTADO**
1	**MONITOR PLANO (IONIC-S/M)**	**1**	**Bueno**
2	**UNIDAD CENTRAL DE PROCESO - CPU (SIN MARCA-S/M)**	**1**	**Bueno**
3	**SWITCH PARA RED**	**2**	
	SWITCH PARA RED (SATRA-SA-SF1008D)	1	Regular
	SWITCH PARA RED (D-LINK-S/M)	1	Regular
4	**TELEFONO CELULAR INTELIGENTE - SMARTPHONE (SIN MARCA-HUAWEI Y8)**	**1**	**Bueno**

4.2.2. Valoración de la Criticidad de los Activos de TI

Una vez que se ha inventariado y clasificado los recursos de tecnología de la información (TI), se evalúa su importancia o criticidad en términos de seguridad. Esto implica determinar el grado en que cada dimensión de seguridad de la información (confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad) se vería afectada si se produjera un escenario de riesgo específico. La evaluación de la criticidad de los recursos de TI se lleva a cabo en colaboración con el personal responsable y con autoridad en seguridad de la información en la institución, ponderando cada dimensión de seguridad. Las escalas y criterios utilizados para valorar cada dimensión de seguridad de los recursos de TI se basan en la metodología Magerit (ver Anexo 07) y se presentan en la siguiente tabla:

Tabla 9: Escalas y criterios para la valoración de la criticidad de los activos de TI

ESCALAS Y CRITERIOS PARA LA VALORACIÓN DE LA CRITICIDAD DE LOS ACTIVOS		
DIMENSIÓN	**ESCALA**	**CRITERIO**
DISPONIBILIDAD (D)	1	No es relevante
	2	Disponible mínimo 10% del tiempo
	3	Disponible mínimo 50% del tiempo
	4	Disponible mínimo 75% del tiempo
	5	Disponible mínimo 95% del tiempo
INTEGRIDAD (I)	1	No es relevante
	2	Los errores o falta de información no afectan el funcionamiento del sistema

	3	La información debe estar correcta y completa al menos en un 50%
	4	La información debe estar correcta y completa al menos en un 70%
	5	La información debe estar correcta y completa al menos en un 95%
CONFIDENCIALIDAD (C)	1	No es relevante
	2	El incidente no repercute en los procesos ni en los sistemas
	3	El incidente repercute en los procesos o en los sistemas dentro del área afectada
	4	El incidente repercute en los procesos o en los sistemas fuera del área afectada
	5	El incidente repercute no solo en los procesos o en los sistemas, sino también en la reputación y la imagen de la institución se verían comprometidas
AUTENTICIDAD (A)	1	No es relevante
	2	Este incidente causa perjuicios de al menos 10%
	3	Este incidente causa perjuicios de al menos 50%
	4	Este incidente causa perjuicios de al menos 70%
	5	Este incidente causa perjuicios de al menos 95%
TRAZABILIDAD (T)	1	No es relevante
	2	Este incidente causa daños de al menos 10%
	3	Este incidente causa daños de al menos 50%
	4	Este incidente causa daños de al menos 70%
	5	Este incidente causa daños de al menos 95%

Los niveles de criticidad de los activos de tecnologías de información TI serán calculadas a partir del promedio de las valoraciones realizadas por cada dimensión de seguridad, y serán categorizadas de la siguiente forma:

Tabla 10: Niveles de criticidad de los activos de TI

NIVEL DE CRITICIDAD	DESCRIPCIÓN DE LA CRITICIDAD
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Los resultados que se obtuvieron en la evaluación de los criterios de seguridad para la determinación de los niveles de criticidad de los activos de Tecnologías de Información TI en la Municipalidad Distrital de Amarilis se muestra en la siguiente tabla.

Tabla 11: Valoración del nivel de criticidad de los activos de TI

TIPO DE ACTIVO	CODIGO	ACTIVO	DIMENSIONES DE SEGURIDAD					NIVEL DE CRITICIDAD	DESCRIPCION DE LA CRITICIDAD
			C	I	D	A	T		
ACTIVOS ESENCIALES	[AE1]	Datos de Gestión interna	5	5	5	5	5	5	MUY ALTO
	[AE2]	Órdenes de Compra y de Servicio	5	5	5	5	5	5	MUY ALTO
	[AE3]	Documentos digitales	5	5	5	5	5	5	MUY ALTO
	[AE4]	Documentos físicos	5	5	5	5	5	5	MUY ALTO
	[AE5]	Información pública	1	5	5	5	1	3	MEDIO
SERVICIOS	[S1]	Servidor principal de dominio	5	5	5	5	5	5	MUY ALTO
	[S2]	Servidor principal de base de datos INFO, SIAF Y SIGA	5	5	5	5	5	5	MUY ALTO
	[S3]	Servidor principal de base de datos SISRENTAS, ASTM Y SRTM	5	5	5	5	5	5	MUY ALTO
	[S4]	Correo electrónico institucional	4	5	5	5	5	5	MUY ALTO
DATOS / INFORMACIÓN	[D1]	Base de datos	5	5	5	5	5	5	MUY ALTO
	[D2]	Backups de base de datos	5	5	5	5	5	5	MUY ALTO
	[D3]	Credenciales (usuario y contraseña)	5	5	5	5	5	5	MUY ALTO
HARDWARE - EQUIPAMIENTO INFORMATICO	[HW1]	Equipos de cómputo y portátiles	5	5	5	5	5	5	MUY ALTO
	[HW2]	Fotocopiadora / Impresora	-	-	4	2	-	3	MEDIO
	[HW3]	Router	4	-	5	4	4	4	ALTO
	[HW4]	Switch	4	-	5	4	4	4	ALTO
SOTWARE - APLICACIONES INFORMÁTICAS	[SW1]	Software ofimático	5	5	5	5	5	5	MUY ALTO
	[SW2]	Sistema operativo	5	5	5	5	5	5	MUY ALTO
	[SW3]	Antivirus	5	5	5	5	5	5	MUY ALTO
	[SW4]	INFO	5	5	5	5	5	5	MUY ALTO
	[SW5]	SIAF	5	5	5	5	5	5	MUY ALTO
	[SW6]	SIGA	5	5	5	5	5	5	MUY ALTO
	[SW7]	RUB PVL	5	5	5	5	5	5	MUY ALTO
	[SW8]	SISMUN (SISTEMA MUNICIPAL)	5	5	5	5	5	5	MUY ALTO
	[SW9]	ASTM (APLICATIVOS DE SISTEMAS DE RECAUDACION TRIBUTARIA MUNICIPAL)	5	5	5	5	5	5	MUY ALTO
	[SW10]	SRTM (SISTEMA DE RECAUDACION TRIBUTARIA MUNICIPAL)	5	5	5	5	5	5	MUY ALTO

	[SW11]	SISRENTAS	5	5	5	5	5	**5**	**MUY ALTO**
REDES DE COMUNICACIÓN	[COM1]	Red Wifi	3	4	3	4	5	**4**	**ALTO**
	[COM2]	Red LAN	5	5	5	5	5	**5**	**MUY ALTO**
	[COM3]	Internet	4	5	5	4	4	**4**	**ALTO**
	[COM4]	Telefonía	3	4	4	3	3	**3**	**MEDIO**
EQUIPAMIENTO AUXILIAR	[AUX1]	Cableado	5	5	5	5	5	**5**	**MUY ALTO**
	[AUX2]	UPS	5	5	5	5	5	**5**	**MUY ALTO**
	[AUX3]	Estabilizador	-	5	5	-	-	**5**	**MUY ALTO**
	[AUX4]	Mobiliario	-	-	4	-	3	**4**	**ALTO**
SOPORTE DE INFORMACION	[MEDIA1]	Disco Duro Externo	5	5	5	-	5	**5**	**MUY ALTO**
	[MEDIA2]	Usb's	5	5	5	-	5	**5**	**MUY ALTO**
INSTALACIONES	[L1]	Infraestructura	-	5	5	-	5	**5**	**MUY ALTO**
	[L2]	Oficinas	-	5	5	-	5	**5**	**MUY ALTO**
PERSONAL	[P1]	Titular de la entidad	5	1	5	-	5	**4**	**ALTO**
	[P2]	Responsables de las áreas	5	1	5	-	5	**4**	**ALTO**
	[P3]	Encargado de informática	5	1	5	-	5	**4**	**ALTO**
	[P4]	Usuarios	5	1	5	-	5	**4**	**ALTO**

4.2.3. Identificación de las amenazas por activo de TI

Se busca identificar y analizar las posibles amenazas o riesgos que pueden afectar a los activos de una organización

En esta actividad se busca identificar y analizar potenciales amenazas que pueden afectar parcial o totalmente los activos de TI. Es decir, se identifica y relaciona las amenazas con cada activo de TI evaluado.

Tomando como referencia el catálogo propuesto por la metodología Magerit v.3 (ver Anexo 08). Se obtuvo los siguientes resultados.

Tabla 12: Listado de amenazas tipo por Activo de TI

LISTADO DE AMENAZAS POR ACTIVO DE TI				
TIPO DE ACTIVO	**CODIGO**	**ACTIVO**	**AMENAZA**	**DESCRIPCION**
ACTIVOS ESENCIALES	**[AE1]**	Datos de Gestión interna	[AN.*] Desastres naturales	Perdida de información sensible de la MDA debido a accesos inadecuados a la dicha información de datos y por falta de protección en los archivos.
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	
	[AE2]	Órdenes de Compra y de Servicio	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	
	[AE3]	Documentos digitales	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	
	[AE4]	Documentos físicos	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	
	[AE5]	Información pública	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	
SERVICIOS	**[S1]**	Servidor principal de dominio	[AN.*] Desastres naturales	Paralización de procesos y actividades de los softwares que almacena el servidor, no se accede a los servicios de red, pérdida de recursos.
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	
			[AE.1]Errores de los usuarios	
			[AE.2] Errores del administrador	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.19] Revelación de información	

			[AA.22] Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	
			[AA.24] Denegación de servicio	
	[S2]	Servidor principal de base de datos INFO, SIAF Y SIGA	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	
			[AE.1]Errores de los usuarios	
			[AE.2] Errores del administrador	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.19] Revelación de información	
			[AA.22] Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	
			[AA.24] Denegación de servicio	
	[S3]	Servidor principal de base de datos SISRENTAS, ASTM Y SRTM	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	
			[AE.1]Errores de los usuarios	
			[AE.2] Errores del administrador	
			[AE.9] Errores de [re-]encaminamiento	

			[AE.15] Alteración accidental de la información	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.19] Revelación de información	
			[AA.22] Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	
			[AA.24] Denegación de servicio	
	[S4]	Correo electrónico institucional	[AE.9] Errores de [re-]encaminamiento	
			[AE.18] Destrucción de información	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.18] Destrucción de información	
DATOS / INFORMACIÓN	[D1]	Base de datos	[AE.1] Errores de los usuarios	Perdida de información sensible de la MDA debido a accesos inadecuados a las bases de datos y por por falta de protección en los dispositivos de almacenamiento.
			[AE.2] Errores del administrador	
			[AE.15] Alteración accidental de la información	
			[AE.18] Destrucción de información	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.19] Revelación de información	
	[D2]	Backups de base de datos	[AE.1] Errores de los usuarios	
			[AE.2] Errores del administrador	
			[AE.15] Alteración accidental de la información	
			[AE.18] Destrucción de información	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	

			[AA.19] Revelación de información	
	[D3]	Credenciales (usuario y contraseña)	[AE.1] Errores de los usuarios	
			[AE.2] Errores del administrador	
			[AE.15] Alteración accidental de la información	
			[AE.18] Destrucción de información	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.19] Revelación de información	
HARDWARE - EQUIPAMIENTO INFORMATICO	**[HW1]**	Equipos de cómputo y portátiles	[AN.*] Desastres naturales	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones de la MDA.
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	
			[AE.2] Errores del administrador	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
			[AA.11] Acceso no autorizado	
			[AA.26] Ataque destructivo	
	[HW2]	Fotocopiadora / Impresora	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
			[AA.26] Ataque destructivo	
	[HW3]	Router	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	

			[AI.6] Corte del suministro eléctrico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
			[AA.26] Ataque destructivo	
	[HW4]	Switch	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
			[AA.26] Ataque destructivo	
SOTWARE - APLICACIONES INFORMÁTICAS	**[SW1]**	Software ofimático	[AI.5] Avería de origen físico o lógico	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente pérdida de recursos debido a Infección de Virus Informáticos, por el mantenimiento deficiente de cada software, perdida y divulgación de la información sensible que almacena cada una de ellas.
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.8] Difusión de software dañino	
	[SW2]	Sistema operativo	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.8] Difusión de software dañino	
	[SW3]	Antivirus	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.8] Difusión de software dañino	
	[SW4]	INFO	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	

			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
	[SW5]	SIAF	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	

			[AA.22] Manipulación de programas	
	[SW6]	SIGA	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
	[SW7]	RUB PVL	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	

			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
	[SW8]	SISMUN (SISTEMA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
	[SW9]	ASTM (APLICATIVOS DE SISTEMAS DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	

			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
	[SW10]	SRTM (SISTEMA DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	
			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
	[SW11]	SISRENTAS	[AI.5] Avería de origen físico o lógico	
			[AE.2] Errores del administrador	
			[AE.8] Difusión de software dañino	
			[AE.9] Errores de [re-]encaminamiento	

			[AE.15] Alteración accidental de la información	
			[AE.18]Destrucción de información	
			[AE.20] Vulnerabilidades de los programas (software)	
			[AE.21] Errores de mantenimiento / actualización de programas (software)	
			[AA.5] Suplantación de la identidad del usuario	
			[AA.6] Abuso de privilegios de acceso	
			[AA.8] Difusión de software dañino	
			[AA.11] Acceso no autorizado	
			[AA.15] Modificación deliberada de la información	
			[AA.18] Destrucción de información	
			[AA.19] Revelación de información	
			[AA.22] Manipulación de programas	
REDES DE COMUNICACIÓN	**[COM1]**	Red Wifi	[AI.8] Fallo de servicios de comunicaciones	Paralización de servicios de comunicación
			[AE.2] Errores del administrador	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.12] Análisis de tráfico	
			[AA.24] Denegación de servicio	
	[COM2]	Red LAN	[AI.8] Fallo de servicios de comunicaciones	
			[AE.2] Errores del administrador	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.12] Análisis de tráfico	
			[AA.24] Denegación de servicio	
	[COM3]	Internet	[AI.8] Fallo de servicios de comunicaciones	
			[AE.2] Errores del administrador	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.12] Análisis de tráfico	
			[AA.24] Denegación de servicio	
	[COM4]	Telefonía	[AI.8] Fallo de servicios de comunicaciones	
			[AE.2] Errores del administrador	
			[AE.24] Caída del sistema por agotamiento de recursos	
			[AA.12] Análisis de tráfico	

			[AA.14] Interceptación de información (escucha)	
			[AA.24] Denegación de servicio	
EQUIPAMIENTO AUXILIAR	**[AUX1]**	Cableado	[AN.*] Desastres naturales	Pérdida de información sensible debido a fallas de los equipos auxiliares que soportan las operaciones de la entidad.
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Avería de origen físico o lógico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
	[AUX2]	UPS	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Avería de origen físico o lógico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
	[AUX3]	Estabilizador	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	
			[AI.4] Avería de origen físico o lógico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	
	[AUX4]	Mobiliario	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
SOPORTE DE INFORMACION	**[MEDIA1]**	Disco Duro Externo	[AN.*] Desastres naturales	Perdida de información sensible de la MDA debido a desastres naturales o industriales, por accesos no autorizados.
			[AI.*] Desastres industriales	
			[AI.10] Degradación de los soportes de almacenamiento de la información	
			[AE.18] Destrucción de información	
			[AE.25] Pérdida de equipos	
			[AA.18] Destrucción de información	
			[AA.25] Robo	
	[MEDIA2]	Usb's	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AI.10] Degradación de los soportes de almacenamiento de la información	
			[AE.18] Destrucción de información	
			[AE.25] Pérdida de equipos	

			[AA.18] Destrucción de información	
			[AA.25] Robo	
INSTALACIONES	**[L1]**	Infraestructura	[AN.*] Desastres naturales	Sabotaje a las instalaciones
			[AI.*] Desastres industriales	
			[AA.11] Acceso no autorizado	
			[AA.26] Ataque destructivo	
	[L2]	Oficinas	[AN.*] Desastres naturales	
			[AI.*] Desastres industriales	
			[AA.11] Acceso no autorizado	
			[AA.26] Ataque destructivo	
PERSONAL	**[P1]**	Titular de la entidad	[AE.7] Deficiencias en la organización	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos, modificación, divulgación y destrucción de la información
			[AE.28] Indisponibilidad del personal	
			[AA.28] Indisponibilidad del personal	
			[AA.29] Extorsión	
			[AA.30]Ingeniería social	
	[P2]	Responsables de las áreas	[AE.7] Deficiencias en la organización	
			[AE.28] Indisponibilidad del personal	
			[AA.28] Indisponibilidad del personal	
			[AA.29] Extorsión	
			[AA.30]Ingeniería social	
	[P3]	Encargado de informática	[AE.7] Deficiencias en la organización	
			[AE.28] Indisponibilidad del personal	
			[AA.28] Indisponibilidad del personal	
			[AA.29] Extorsión	
			[AA.30]Ingeniería social	
	[P4]	Usuarios	[AE.7] Deficiencias en la organización	
			[AE.28] Indisponibilidad del personal	
			[AA.28] Indisponibilidad del personal	
			[AA.29] Extorsión	
			[AA.30]Ingeniería social	

4.2.4. Identificación de vulnerabilidades de cada activo de TI.

En esta actividad se efectúa un análisis de las insuficiencias, falencias y carencias que presenta la Municipalidad Distrital de Amarilis en sus diversos procesos de Tecnologías de la Información relacionados con la salvaguarda de los recursos informáticos. El producto de este análisis permite

identificar cuáles son las debilidades internas que podrían ser aprovechadas por amenazas para concretar ataques o fallos en los activos informáticos.

Tabla 13: Listado de vulnerabilidades tipo por Activo de TI – Amenaza

TIPO DE ACTIVO	CODIGO	ACTIVO	AMENAZA	VULNERABILIDAD
ACTIVOS ESENCIALES	[AE1]	Datos de Gestión interna	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
	[AE2]	Órdenes de Compra y de Servicio	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
	[AE3]	Documentos digitales	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
	[AE4]	Documentos físicos	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
	[AE5]	Información pública	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
SERVICIOS	[S1]	Servidor principal de dominio	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor

			[AE.2] Errores del administrador	
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
	[S2]	Servidor principal de base de datos INFO, SIAF Y SIGA	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor
			[AE.2] Errores del administrador	
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada

			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
	[S3]	Servidor principal de base de datos SISRENTAS, ASTM Y SRTM	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor
			[AE.2] Errores del administrador	
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor
				Falta de Gestión de contraseñas (demasiado predecible)

			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
	[S4]	Correo electrónico institucional	[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
DATOS / INFORMACIÓN	**[D1]**	Base de datos	[AE.1] Errores de los usuarios	Fallas en la manipulación o uso de la base de datos
			[AE.2] Errores del administrador	
			[AE.15] Alteración accidental de la información	
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario

			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[D2]	Backups de base de datos	[AE.1] Errores de los usuarios	Fallas en la manipulación de las Backups de base de datos
			[AE.2] Errores del administrador	
			[AE.15] Alteración accidental de la información	
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[D3]	Credenciales (usuario y contraseña)	[AE.1] Errores de los usuarios	Fallas en la manipulación o asignación de credenciales
			[AE.2] Errores del administrador	
			[AE.15] Alteración accidental de la información	
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de control de personas no autorizadas

			[AA.5] Suplantación de la identidad del usuario	Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
HARDWARE - EQUIPAMIENTO INFORMATICO	**[HW1]**	Equipos de cómputo y portátiles	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica
			[AE.2] Errores del administrador	Fallas en la manipulación de hardware
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
				Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas
	[HW2]	Fotocopiadora / Impresora	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware
			[AI.4] Contaminación electromagnética	

			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas
	[HW3]	Router	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas
	[HW4]	Switch	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware
			[AI.4] Contaminación electromagnética	
			[AI.4] Avería de origen físico o lógico	
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas
SOTWARE - APLICACIONES INFORMÁTICAS	**[SW1]**	Software ofimático	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software

			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
	[SW2]	Sistema operativo	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
	[SW3]	Antivirus	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
	[SW4]	INFO	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software

			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia en antivirus)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas

				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[SW5]	SIAF	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad

			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[SW6]	SIGA	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
				Falta de control de personas no autorizadas

			[AA.5] Suplantación de la identidad del usuario	Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[SW7]	RUB PVL	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas

				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[SW8]	SISMUN (SISTEMA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad

				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas

				Falta de Gestión de contraseñas (demasiado predecible)
	[SW9]	ASTM (APLICATIVOS DE SISTEMAS DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)

			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[SW10]	SRTM (SISTEMA DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario

			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
	[SW11]	SISRENTAS	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software

			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad
				Falta de licencia de antivirus (pirateado)
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.19] Revelación de información	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas
				Falta de Gestión de contraseñas (demasiado predecible)
REDES DE COMUNICACIÓN	**[COM1]**	Red Wifi	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad

			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
	[COM2]	Red LAN	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
	[COM3]	Internet	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
	[COM4]	Telefonía	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad
			[AA.14] Interceptación de información (escucha)	Falta de un plan de ciberseguridad

			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad
EQUIPAMIENTO AUXILIAR	[AUX1]	Cableado	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares
			[AI.4] Avería de origen físico o lógico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
	[AUX2]	UPS	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares
			[AI.4] Avería de origen físico o lógico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
	[AUX3]	Estabilizador	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares
			[AI.4] Avería de origen físico o lógico	
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware
	[AUX4]	Mobiliario	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
SOPORTE DE INFORMACION	[MEDIA1]	Disco Duro Externo	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.10] Degradación de los soportes de almacenamiento de la información	Falta de un plan de mantenimiento preventivo y correctivo de los soportes de información

			[AE.18] Destrucción de información	Falta de control de personas no autorizadas
			[AE.25] Pérdida de equipos	Falta de control de personas no autorizadas
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
			[AA.25] Robo	Falta de control de personas no autorizadas
	[MEDIA2]	Usb's	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AI.10] Degradación de los soportes de almacenamiento de la información	Falta de un plan de mantenimiento preventivo y correctivo de los soportes de información
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas
			[AE.25] Pérdida de equipos	Falta de control de personas no autorizadas
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas
			[AA.25] Robo	Falta de control de personas no autorizadas
INSTALACIONES	**[L1]**	Infraestructura	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AA.11] Acceso no autorizado	Falta de control de personas no autorizadas
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas
	[L2]	Oficinas	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones
			[AI.*] Desastres industriales	
			[AA.11] Acceso no autorizado	Falta de control de personas no autorizadas
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas
PERSONAL	**[P1]**	Titular de la entidad	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing

			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing
	[P2]	Responsables de las áreas	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing
	[P3]	Encargado de informática	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing
	[P4]	Usuarios	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing

4.3 Fase de Valoración de los Escenarios de Riesgos de TI

El propósito de esta etapa es evaluar los niveles de exposición a los diversos escenarios de riesgo (Activo-Amenaza-Vulnerabilidad) previamente identificados, a través de la evaluación del impacto y las probabilidades de que ocurran.

se emplearon como guía escalas de niveles destinadas a evaluar los posibles impactos y la probabilidad de ocurrencia, respectivamente. Estas escalas fueron desarrolladas siguiendo los criterios establecidos en la norma ISO/IEC 27005 y la metodología Magerit. Además, se establecieron escalas de referencia para categorizar los niveles de exposición al riesgo, así como para determinar la disposición y la tolerancia al riesgo, utilizando como base la propuesta de la metodología Magerit.

4.3.1. Estimación del Impacto de los Escenarios de Riesgo

Esta tarea posibilitó evaluar el impacto que tendría cada posible situación de riesgo en la Municipalidad Distrital de Amarilis, focalizándose especialmente en el resguardo de la información.

La evaluación de dichas consecuencias se llevó a cabo mediante el empleo de una escala conformada por cinco (05) niveles, la cual se presenta a continuación:

Tabla 14: Escala de niveles para la estimación del impacto de los escenarios de riesgo

NIVEL	IMPACTO	DESCRIPCION
1	INSIGNIFICANTE	Tiene un efecto nulo o muy pequeño en las operaciones, procesos y actividades de la institución.
2	MENOR	Afecta parcialmente las operaciones, procesos y actividades de la institución.
3	MODERADO	Operativamente es sostenible, pero dificulta o retrasa las operaciones, procesos y actividades de la institución.
4	MAYOR	Interrumpe significativamente las operaciones, procesos y actividades de la institución.
5	CATASTRÓFICO	Paraliza por completo todas las operaciones, procesos y actividades de la institución

4.3.2. Estimación de la Probabilidad de Ocurrencia de los Escenarios de Riesgo

Esta tarea posibilitó calcular la probabilidad de que se den cada uno de los escenarios de riesgo reconocidos, tomando como referencia el registro de sucesos previos en la Municipalidad Distrital de Amarilis.

La evaluación de las probabilidades se llevó a cabo empleando una escala compuesta por cinco (05) niveles, la cual se presenta a continuación:

Tabla 15: Estimación de la probabilidad de ocurrencia de los escenarios de riesgo

NIVEL	PROBABILIDAD	DESCRIPCION
1	RARO	No se registra en los últimos 5 años
2	IMPROBABLE	Se podría presentar una vez cada 5 años
3	POSIBLE	Se podría presentar una vez al año
4	PROBABLE	Se podría presentar una vez cada mes
5	CASI SEGURO	Se podría presentar varias veces en el mes

4.3.3. Cálculo de los Niveles de Exposición a los Riesgos

Se llevó a cabo la evaluación de los niveles de exposición a los posibles riesgos de cada escenario de riesgo asociado a cada activo de Tecnologías de la Información mediante la siguiente fórmula:

$$\boldsymbol{Nivel\ de\ Riesgo = Impacto\ x\ Probabilidad\ de\ Ocurrencia}$$

El resultado de este producto se ubicará en el siguiente mapa de calor.

Tabla 16: Mapa de calor para el cálculo de los niveles de exposición a los riesgos

NIVELES DE EXPOSICIÓN A LOS RIESGOS		PROBABILIDAD DE OCURRENCIA				
IMPACTO DE LOS PROCESOS		RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI SEGURO
		1	2	3	4	5
CATASTRÓFICO	5	BAJO	MEDIO	ALTO	MUY ALTO	MUY ALTO
MAYOR	4	BAJO	BAJO	MEDIO	ALTO	MUY ALTO
MODERADO	3	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
MÍNIMO	2	MUY BAJO	BAJO	BAJO	BAJO	MEDIO
INSIGNIFICANTE	1	MUY BAJO	MUY BAJO	MUY BAJO	BAJO	BAJO

Tabla 17: Mapa de calor para el cálculo de los niveles de exposición a los riesgos (Cuantificado)

NIVELES DE EXPOSICIÓN A LOS RIESGOS		PROBABILIDAD DE OCURRENCIA				
IMPACTO DE LOS PROCESOS		RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI SEGURO
		1	2	3	4	5
CATASTRÓFICO	5	5	10	15	20	25
MAYOR	4	4	8	12	16	20
MODERADO	3	3	6	9	12	15
MÍNIMO	2	2	4	6	8	10
INSIGNIFICANTE	1	1	2	3	4	5

Conforme se visualiza en el análisis de riesgo mediante el mapa de calor, se propusieron cinco (05) niveles de exposición, los cuales se detallan a continuación:

Nivel Muy Bajo: Asignado cuando las deficiencias en el control actual no generan una degradación significativa en los sistemas, pérdidas económicas o comerciales relevantes, ni obstaculizan el logro de los objetivos de seguridad.

Nivel Bajo: Designado para deficiencias en el control actual que causan daños menores a la Entidad Financiera, es decir, pérdidas, pero no de magnitud significativa.

Nivel Medio: Asignado a deficiencias en el control actual que podrían resultar en pérdidas significativas, aunque aún dentro de límites aceptables para la entidad.

Nivel Alto: Designado cuando las deficiencias en el control actual podrían conllevar pérdidas importantes de índole económica, operativa y de seguridad.

Nivel Muy Alto: Asignado cuando las deficiencias en el control actual exponen a la entidad a pérdidas materiales y/o económicas, o a sanciones legales inaceptables.

A continuación, se presentan los resultados del cálculo de los niveles de exposición a los riesgos:

Tabla 18: Estimación de los impactos y probabilidades de ocurrencia de las amenazas y cálculo de los niveles de exposición a los riesgos (NR)

ESTIMACIÓN DE LOS IMPACTOS Y PROBABILIDADES DE OCURRENCIA DE LAS AMENAZAS Y CÁLCULO DE LOS NIVELES DE EXPOSICIÓN A LOS RIESGOS (NR)											
VALORACIÓN DEL NIVEL DE CRITICIDAD DE LOS ACTIVOS					IMPACTO ESTIMADO EN LOS PROCESOS		PROBABILIDAD DE QUE LA AMENAZA EXPLOTE EN LA VULNERABILIDAD		NIVEL DE EXPOSICION AL RIESGO		
TIPO DE ACTIVO	CODIGO	ACTIVO	AMENAZA	VULNERABILIDAD	NIVEL	CATEGORIA	NIVEL	CATEGORIA	ID RIESGO	NIVEL	CATEGORIA
ACTIVOS ESENCIALES	[AE1]	Datos de Gestión interna	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	4	MAYOR	3	POSIBLE	R1	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R2	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R3	16	ALTO
	[AE2]	Órdenes de Compra y de Servicio	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	4	MAYOR	3	POSIBLE	R4	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R5	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R6	16	ALTO
	[AE3]	Documentos digitales	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	4	MAYOR	3	POSIBLE	R7	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R8	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R9	16	ALTO
	[AE4]	Documentos físicos	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por	4	MAYOR	3	POSIBLE	R10	12	MEDIO

			[AI.*] Desastres industriales	factores de desastres naturales e industriales	4	MAYOR	3	POSIBLE	R11	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R12	16	ALTO
	[AE5]	Información pública	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	4	MAYOR	3	POSIBLE	R13	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R14	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R15	16	ALTO
SERVICIOS	[S1]	Servidor principal de dominio	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales	5	CATASTROFICO	3	POSIBLE	R16	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R17	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores	5	CATASTROFICO	4	PROBABLE	R18	20	MUY ALTO
			[AI.4] Contaminación electromagnética		5	CATASTROFICO	4	PROBABLE	R19	20	MUY ALTO
			[AI.4] Avería de origen físico o lógico		5	CATASTROFICO	4	PROBABLE	R20	20	MUY ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	5	CATASTROFICO	5	CASI SEGURO	R21	25	MUY ALTO
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor	5	CATASTROFICO	5	CASI SEGURO	R22	25	MUY ALTO
			[AE.2] Errores del administrador		5	CATASTROFICO	5	CASI SEGURO	R23	25	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R24	16	ALTO

			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor	5	CATASTROFICO	5	CASI SEGURO	R25	25	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R26	16	ALTO
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	5	CATASTROFICO	5	CASI SEGURO	R27	25	MUY ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	5	CASI SEGURO	R28	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R29	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	5	CASI SEGURO	R30	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	5	CASI SEGURO	R31	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R32	16	ALTO
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas	5	CATASTROFICO	5	CASI SEGURO	R33	25	MUY ALTO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R34	20	MUY ALTO
	[S2]	Servidor principal de base de datos INFO, SIAF Y SIGA	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales	5	CATASTROFICO	3	POSIBLE	R35	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R36	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores	5	CATASTROFICO	4	PROBABLE	R37	20	MUY ALTO
			[AI.4] Contaminación electromagnética		5	CATASTROFICO	5	CASI SEGURO	R38	25	MUY ALTO

			[AI.4] Avería de origen físico o lógico		5	CATASTROFICO	5	CASI SEGURO	R39	25	MUY ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	5	CATASTROFICO	5	CASI SEGURO	R40	25	MUY ALTO
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor	5	CATASTROFICO	5	CASI SEGURO	R41	25	MUY ALTO
			[AE.2] Errores del administrador		5	CATASTROFICO	5	CASI SEGURO	R42	25	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R43	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor	5	CATASTROFICO	5	CASI SEGURO	R44	25	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R45	16	ALTO
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	5	CATASTROFICO	5	CASI SEGURO	R46	25	MUY ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	5	CASI SEGURO	R47	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R48	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	5	CASI SEGURO	R49	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	5	CASI SEGURO	R50	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R51	16	ALTO

			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas	5	CATASTROFICO	5	CASI SEGURO	R52	25	MUY ALTO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R53	20	MUY ALTO
	[S3]	Servidor principal de base de datos SISRENTAS, ASTM Y SRTM	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales	5	CATASTROFICO	3	POSIBLE	R54	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R55	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores	5	CATASTROFICO	4	PROBABLE	R56	20	MUY ALTO
			[AI.4] Contaminación electromagnética		5	CATASTROFICO	4	PROBABLE	R57	20	MUY ALTO
			[AI.4] Avería de origen físico o lógico		5	CATASTROFICO	4	PROBABLE	R58	20	MUY ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	5	CATASTROFICO	5	CASI SEGURO	R59	25	MUY ALTO
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor	5	CATASTROFICO	5	CASI SEGURO	R60	25	MUY ALTO
			[AE.2] Errores del administrador		5	CATASTROFICO	5	CASI SEGURO	R61	25	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R62	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor	5	CATASTROFICO	5	CASI SEGURO	R63	25	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R64	16	ALTO

			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	5	CATASTROFICO	5	CASI SEGURO	R65	25	MUY ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	5	CASI SEGURO	R66	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R67	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	5	CASI SEGURO	R68	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	5	CASI SEGURO	R69	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R70	16	ALTO
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas	5	CATASTROFICO	5	CASI SEGURO	R71	25	MUY ALTO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R72	20	MUY ALTO
	[S4]	Correo electrónico institucional	[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	3	POSIBLE	R73	12	MEDIO
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	5	CASI SEGURO	R74	25	MUY ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R75	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R76	16	ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R77	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R78	20	MUY ALTO

DATOS / INFORMACIÓN	[D1]	Base de datos	[AE.1] Errores de los usuarios	Fallas en la manipulación o uso de la base de datos	5	CATASTROFICO	4	PROBABLE	R79	20	MUY ALTO
			[AE.2] Errores del administrador		5	CATASTROFICO	4	PROBABLE	R80	20	MUY ALTO
			[AE.15] Alteración accidental de la información		5	CATASTROFICO	4	PROBABLE	R81	20	MUY ALTO
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R82	20	MUY ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R83	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R84	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R85	16	ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R86	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R87	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R88	16	ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R89	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R90	16	ALTO
	[D2]	Backups de base de datos	[AE.1] Errores de los usuarios	Fallas en la manipulación de las Backups de base de datos	5	CATASTROFICO	4	PROBABLE	R91	20	MUY ALTO
			[AE.2] Errores del administrador		5	CATASTROFICO	4	PROBABLE	R92	20	MUY ALTO

			[AE.15] Alteración accidental de la información		5	CATASTROFICO	4	PROBABLE	R93	20	MUY ALTO
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R94	20	MUY ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R95	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R96	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R97	16	ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R98	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R99	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R100	16	ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R101	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R102	16	ALTO
	[D3]	Credenciales (usuario y contraseña)	[AE.1] Errores de los usuarios	Fallas en la manipulación o asignación de credenciales	5	CATASTROFICO	4	PROBABLE	R103	20	MUY ALTO
			[AE.2] Errores del administrador		5	CATASTROFICO	4	PROBABLE	R104	20	MUY ALTO
			[AE.15] Alteración accidental de la información		5	CATASTROFICO	4	PROBABLE	R105	20	MUY ALTO
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R106	20	MUY ALTO

			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R107	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R108	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R109	16	ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R110	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R111	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R112	16	ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R113	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R114	16	ALTO
HARDWARE - EQUIPAMIENTO INFORMATICO	**[HW1]**	Equipos de cómputo y portátiles	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R115	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R116	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	5	CATASTROFICO	4	PROBABLE	R117	20	MUY ALTO
			[AI.4] Contaminación electromagnética		5	CATASTROFICO	4	PROBABLE	R118	20	MUY ALTO
			[AI.4] Avería de origen físico o lógico		5	CATASTROFICO	4	PROBABLE	R119	20	MUY ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	5	CATASTROFICO	5	CASI SEGURO	R120	25	MUY ALTO
			[AE.2] Errores del administrador	Fallas en la manipulación de hardware	4	MAYOR	4	PROBABLE	R121	16	ALTO

			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R122	16	ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	4	MAYOR	3	POSIBLE	R123	12	MEDIO
				Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R124	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R125	16	ALTO
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R126	16	ALTO
	[HW2]	Fotocopiadora / Impresora	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	4	MAYOR	3	POSIBLE	R127	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R128	12	MEDIO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	4	MAYOR	4	PROBABLE	R129	16	ALTO
			[AI.4] Contaminación electromagnética		4	MAYOR	4	PROBABLE	R130	16	ALTO
			[AI.4] Avería de origen físico o lógico		4	MAYOR	4	PROBABLE	R131	16	ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	4	MAYOR	5	CASI SEGURO	R132	20	MUY ALTO
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R133	16	ALTO
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R134	16	ALTO

	[HW3]	Router	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R135	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R136	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	5	CATASTROFICO	4	PROBABLE	R137	20	MUY ALTO
			[AI.4] Contaminación electromagnética		5	CATASTROFICO	4	PROBABLE	R138	20	MUY ALTO
			[AI.4] Avería de origen físico o lógico		5	CATASTROFICO	4	PROBABLE	R139	20	MUY ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	5	CATASTROFICO	5	CASI SEGURO	R140	25	MUY ALTO
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R141	16	ALTO
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R142	16	ALTO
	[HW4]	Switch	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R143	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R144	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	5	CATASTROFICO	4	PROBABLE	R145	20	MUY ALTO
			[AI.4] Contaminación electromagnética		5	CATASTROFICO	4	PROBABLE	R146	20	MUY ALTO
			[AI.4] Avería de origen físico o lógico		5	CATASTROFICO	4	PROBABLE	R147	20	MUY ALTO
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	4	MAYOR	5	CASI SEGURO	R148	20	MUY ALTO

			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R149	16	ALTO
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R150	16	ALTO
SOTWARE - APLICACIONES INFORMÁTICAS	[SW1]	Software ofimático	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	5	CASI SEGURO	R151	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	4	MAYOR	4	PROBABLE	R152	16	ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	4	MAYOR	3	POSIBLE	R153	12	MEDIO
				Falta de licencia de antivirus (pirateado)	4	MAYOR	3	POSIBLE	R154	12	MEDIO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R155	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	4	MAYOR	3	POSIBLE	R156	12	MEDIO
				Falta de licencia de antivirus (pirateado)	4	MAYOR	3	POSIBLE	R157	12	MEDIO
	[SW2]	Sistema operativo	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	5	CASI SEGURO	R158	25	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	4	MAYOR	4	PROBABLE	R159	16	ALTO

			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R160	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	3	POSIBLE	R161	15	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R162	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	4	MAYOR	3	POSIBLE	R163	12	MEDIO
				Falta de licencia de antivirus (pirateado)	4	MAYOR	3	POSIBLE	R164	12	MEDIO
	[SW3]	Antivirus	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	5	CASI SEGURO	R165	25	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R166	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R167	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	3	POSIBLE	R168	15	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	5	CATASTROFICO	4	PROBABLE	R169	20	MUY ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R170	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	3	POSIBLE	R171	15	ALTO

	[SW4]	INFO	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R172	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R173	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R174	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R175	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R176	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R177	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R178	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R179	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R180	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R181	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia en antivirus)	4	MAYOR	4	PROBABLE	R182	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R183	16	ALTO

				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R184	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R185	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R186	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R187	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R188	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R189	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R190	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R191	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R192	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R193	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R194	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R195	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R196	16	ALTO
	[SW5]	SIAF	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R197	20	MUY ALTO

			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R198	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R199	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R200	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R201	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R202	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R203	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R204	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R205	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R206	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R207	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R208	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R209	16	ALTO

			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R210	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R211	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R212	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R213	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R214	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R215	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R216	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R217	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R218	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R219	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R220	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R221	16	ALTO
	[SW6]	SIGA	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R222	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R223	20	MUY ALTO

			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R224	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R225	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R226	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R227	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R228	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R229	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R230	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R231	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R232	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R233	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R234	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R235	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R236	15	ALTO

				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R237	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R238	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R239	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R240	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R241	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R242	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R243	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R244	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R245	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R246	16	ALTO
	[SW7]	RUB PVL	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R247	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R248	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R249	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R250	20	MUY ALTO

			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R251	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R252	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R253	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R254	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R255	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R256	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R257	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R258	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R259	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R260	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R261	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R262	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R263	20	MUY ALTO

			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R264	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R265	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R266	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R267	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R268	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R269	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R270	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R271	16	ALTO
	[SW8]	SISMUN (SISTEMA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R272	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R273	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R274	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R275	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R276	16	ALTO

			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R277	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R278	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R279	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R280	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R281	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R282	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R283	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R284	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R285	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R286	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R287	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R288	20	MUY ALTO
				Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R289	20	MUY ALTO

			[AA.15] Modificación deliberada de la información	Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R290	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R291	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R292	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R293	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R294	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R295	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R296	16	ALTO
	[SW9]	ASTM (APLICATIVOS DE SISTEMAS DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R297	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R298	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R299	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R300	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R301	16	ALTO
				Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R302	20	MUY ALTO

			[AE.15] Alteración accidental de la información	Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R303	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R304	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R305	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R306	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R307	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R308	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R309	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R310	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R311	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R312	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R313	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R314	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R315	20	MUY ALTO

			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R316	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R317	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R318	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R319	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R320	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R321	16	ALTO
	[SW10]	SRTM (SISTEMA DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R322	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R323	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R324	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R325	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R326	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R327	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R328	20	MUY ALTO

			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R329	15	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R330	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R331	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R332	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R333	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R334	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R335	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R336	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R337	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R338	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R339	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R340	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R341	20	MUY ALTO

				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R342	20	MUY ALTO
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R343	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R344	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R345	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R346	16	ALTO
	[SW11]	SISRENTAS	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	5	CATASTROFICO	4	PROBABLE	R347	20	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	5	CATASTROFICO	4	PROBABLE	R348	20	MUY ALTO
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R349	20	MUY ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R350	20	MUY ALTO
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	4	MAYOR	4	PROBABLE	R351	16	ALTO
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	5	CATASTROFICO	4	PROBABLE	R352	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R353	20	MUY ALTO
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	3	POSIBLE	R354	15	ALTO

				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	3	POSIBLE	R355	15	ALTO
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	4	MAYOR	4	PROBABLE	R356	16	ALTO
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	4	MAYOR	4	PROBABLE	R357	16	ALTO
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R358	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R359	16	ALTO
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	4	MAYOR	4	PROBABLE	R360	16	ALTO
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R361	15	ALTO
				Falta de licencia de antivirus (pirateado)	5	CATASTROFICO	4	PROBABLE	R362	20	MUY ALTO
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	5	CATASTROFICO	4	PROBABLE	R363	20	MUY ALTO
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R364	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R365	20	MUY ALTO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	5	CATASTROFICO	4	PROBABLE	R366	20	MUY ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	5	CATASTROFICO	4	PROBABLE	R367	20	MUY ALTO

			[AA.19] Revelación de información	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R368	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R369	16	ALTO
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	4	MAYOR	4	PROBABLE	R370	16	ALTO
				Falta de Gestión de contraseñas (demasiado predecible)	4	MAYOR	4	PROBABLE	R371	16	ALTO
REDES DE COMUNICACIÓN	[COM1]	Red Wifi	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	5	CATASTROFICO	5	CASI SEGURO	R372	25	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	4	MAYOR	4	PROBABLE	R373	16	ALTO
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	5	CATASTROFICO	5	CASI SEGURO	R374	25	MUY ALTO
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	4	MAYOR	3	POSIBLE	R375	12	MEDIO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R376	15	ALTO
	[COM2]	Red LAN	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	5	CATASTROFICO	5	CASI SEGURO	R377	25	MUY ALTO

			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	4	MAYOR	4	PROBABLE	R378	16	ALTO
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	5	CATASTROFICO	5	CASI SEGURO	R379	25	MUY ALTO
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	4	MAYOR	3	POSIBLE	R380	12	MEDIO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R381	15	ALTO
	[COM3]	Internet	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	5	CATASTROFICO	5	CASI SEGURO	R382	25	MUY ALTO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	4	MAYOR	4	PROBABLE	R383	16	ALTO
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	5	CATASTROFICO	5	CASI SEGURO	R384	25	MUY ALTO
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	4	MAYOR	3	POSIBLE	R385	12	MEDIO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	5	CATASTROFICO	3	POSIBLE	R386	15	ALTO

	[COM4]	Telefonia	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	3	MODERADO	3	POSIBLE	R387	9	MEDIO
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	3	MODERADO	3	POSIBLE	R388	9	MEDIO
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	3	MODERADO	3	POSIBLE	R389	9	MEDIO
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	3	MODERADO	3	POSIBLE	R390	9	MEDIO
			[AA.14] Interceptación de información (escucha)	Falta de un plan de ciberseguridad	4	MAYOR	3	POSIBLE	R391	12	MEDIO
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	3	MODERADO	3	POSIBLE	R392	9	MEDIO
EQUIPAMIENTO AUXILIAR	[AUX1]	Cableado	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R393	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R394	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares	4	MAYOR	4	PROBABLE	R395	16	ALTO
			[AI.4] Avería de origen físico o lógico		4	MAYOR	4	PROBABLE	R396	16	ALTO
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R397	16	ALTO

	[AUX2]	UPS	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R398	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R399	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares	4	MAYOR	4	PROBABLE	R400	16	ALTO
			[AI.4] Avería de origen físico o lógico		4	MAYOR	4	PROBABLE	R401	16	ALTO
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R402	16	ALTO
	[AUX3]	Estabilizador	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R403	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R404	15	ALTO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares	4	MAYOR	4	PROBABLE	R405	16	ALTO
			[AI.4] Avería de origen físico o lógico		4	MAYOR	4	PROBABLE	R406	16	ALTO
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	4	MAYOR	4	PROBABLE	R407	16	ALTO
	[AUX4]	Mobiliario	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	3	MODERADO	3	POSIBLE	R408	9	MEDIO
			[AI.*] Desastres industriales		3	MODERADO	3	POSIBLE	R409	9	MEDIO
SOPORTE DE INFORMACION	[MEDIA1]	Disco Duro Externo	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	4	MAYOR	3	POSIBLE	R410	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R411	12	MEDIO

			[AI.10] Degradación de los soportes de almacenamiento de la información	Falta de un plan de mantenimiento preventivo y correctivo de los soportes de información	4	MAYOR	4	PROBABLE	R412	16	ALTO
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R413	12	MEDIO
			[AE.25] Pérdida de equipos	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R414	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R415	12	MEDIO
			[AA.25] Robo	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R416	12	MEDIO
	[MEDIA2]	Usb's	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	4	MAYOR	3	POSIBLE	R417	12	MEDIO
			[AI.*] Desastres industriales		4	MAYOR	3	POSIBLE	R418	12	MEDIO
			[AI.10] Degradación de los soportes de almacenamiento de la información	Falta de un plan de mantenimiento preventivo y correctivo de los soportes de información	4	MAYOR	4	PROBABLE	R419	16	ALTO
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R420	12	MEDIO
			[AE.25] Pérdida de equipos	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R421	12	MEDIO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R422	12	MEDIO
			[AA.25] Robo	Falta de control de personas no autorizadas	4	MAYOR	3	POSIBLE	R423	12	MEDIO
INSTALACIONES	[L1]	Infraestructura	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R424	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R425	15	ALTO

			[AA.11] Acceso no autorizado	Falta de control de personas no autorizadas	3	MODERADO	4	PROBABLE	R426	12	MEDIO
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	3	MODERADO	4	PROBABLE	R427	12	MEDIO
	[L2]	Oficinas	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	5	CATASTROFICO	3	POSIBLE	R428	15	ALTO
			[AI.*] Desastres industriales		5	CATASTROFICO	3	POSIBLE	R429	15	ALTO
			[AA.11] Acceso no autorizado	Falta de control de personas no autorizadas	3	MODERADO	4	PROBABLE	R430	12	MEDIO
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	3	MODERADO	4	PROBABLE	R431	12	MEDIO
PERSONAL	[P1]	Titular de la entidad	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	4	MAYOR	3	POSIBLE	R432	12	MEDIO
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	2	IMPROBABLE	R433	10	MEDIO
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	2	IMPROBABLE	R434	10	MEDIO
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	5	CATASTROFICO	2	IMPROBABLE	R435	10	MEDIO
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	4	MAYOR	2	IMPROBABLE	R436	8	BAJO
	[P2]	Responsables de las áreas	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	4	MAYOR	4	PROBABLE	R437	16	ALTO
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	5	CASI SEGURO	R438	25	MUY ALTO
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	5	CASI SEGURO	R439	25	MUY ALTO

			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	5	CATASTROFICO	4	PROBABLE	R440	20	MUY ALTO
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	4	MAYOR	4	PROBABLE	R441	16	ALTO
	[P3]	Encargado de informática	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	4	MAYOR	4	PROBABLE	R442	16	ALTO
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	5	CASI SEGURO	R443	25	MUY ALTO
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	5	CASI SEGURO	R444	25	MUY ALTO
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	5	CATASTROFICO	4	PROBABLE	R445	20	MUY ALTO
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	4	MAYOR	4	PROBABLE	R446	16	ALTO
	[P4]	Usuarios	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	4	MAYOR	4	PROBABLE	R447	16	ALTO
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	5	CASI SEGURO	R448	25	MUY ALTO
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	5	CATASTROFICO	5	CASI SEGURO	R449	25	MUY ALTO
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	5	CATASTROFICO	4	PROBABLE	R450	20	MUY ALTO
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	4	MAYOR	4	PROBABLE	R451	16	ALTO

4.3.4. Determinación del apetito y tolerancia al riesgo

Para determinar qué niveles de exposición al riesgo son ACEPTABLES o NO ACEPTABLES para la Municipalidad Distrital de Amarilis, fue necesario establecer el apetito y la tolerancia al riesgo.

Los niveles de exposición al riesgo (NR) evaluados como Muy Alto o Alto son considerados por la Municipalidad Distrital de Amarilis como NO ACEPTABLES. Por lo tanto, requieren una atención inmediata mediante la implementación de controles y salvaguardas. El nivel de riesgo Medio se define como TOLERABLE y depende de la capacidad instalada de la Municipalidad Distrital de Amarilis, así como del costo de implementar los controles o salvaguardas necesarios para gestionar el riesgo. Los niveles de riesgo Bajo o Muy Bajo se consideran ACEPTABLES.

A continuación, se detallan los criterios de aceptación o no aceptación para cada uno de los niveles de riesgo intrínseco.

Tabla 19: Apetito al riesgo de TI según el nivel de exposición al riesgo

APETITO AL RIESGO DE TI SEGÚN EL NIVEL DE EXPOSICIÓN AL RIESGO	
NIVEL DE RIESGO	**APETITO AL RIESGO**
MUY ALTO	**RIESGO NO ACEPTABLE**
ALTO	**RIESGO NO ACEPTABLE**
MEDIO	**TOLERABLE**
BAJO	**RIESGO ACEPTABLE**
MUY BAJO	**RIESGO ACEPTABLE**

4.4 Fase de Tratamiento de Riesgo

El propósito de esta etapa consiste en elaborar un plan de manejo para los riesgos evaluados como No Aceptables y, en algunos casos, para aquellos riesgos que se consideren tolerables.

En situaciones donde los niveles de riesgo son Aceptables, la entidad se compromete a mantener las medidas de mitigación existentes y a aceptar el riesgo.

Durante esta fase, se determinarán e implementarán los controles o precauciones necesarios para abordar cada una de las amenazas que hayan sido evaluadas con niveles de riesgo considerados No Tolerables, es decir, clasificados como Alto o Muy Alto.

4.4.1. Identificación de los controles/salvaguardas de seguridad y Definición de la estrategia de implementación de controles/salvaguardas

Seleccionar los controles implica establecer la estrategia de aplicación correspondiente. Al adaptar las propuestas de implementación de controles según la norma ISO/IEC 27005, se proponen las siguientes estrategias:

Tabla 20: Estrategia de implementación de controles/salvaguardas

ESTRATEGIA DE IMPLEMENTACIÓN DE CONTROLES/SALVAGUARDAS	
ACEPTAR RIESGO	Cuando los niveles de riesgo se encuentran dentro de los límites considerados aceptables.
ELECCIÓN DE CONTROLES	Con el propósito de reducir los riesgos, se actúa cuando los niveles de exposición al riesgo se sitúan en los intervalos de tolerancia o No aceptabilidad, siempre y cuando existan los medios humanos, tecnológicos y económicos necesarios para llevar a cabo la implementación.
TRANSFERENCIA DE RIESGOS A TERCEROS	En situaciones donde los niveles de exposición al riesgo se sitúan en los márgenes de tolerancia o No aceptabilidad, y no se dispone de los recursos humanos y tecnológicos necesarios para la implementación, pero sí se cuenta con los recursos financieros suficientes, se considera la posibilidad de contratar a un tercero especializado.
EVITAR AUMENTO DEL RIESGO	En casos en los que los niveles de exposición al riesgo se encuentran dentro de los márgenes de tolerancia o No aceptabilidad, pero la implementación carece de los recursos humanos, tecnológicos y económicos necesarios.

A continuación, se muestran los resultados en la siguiente tabla:

Tabla 21:Implementación de controles según el nivel de exposición al riesgo

IMPLEMENTACIÓN DE CONTROLES SEGÚN EL NIVEL DE EXPOSICIÓN AL RIESGO											
VALORACIÓN DEL NIVEL DE CRITICIDAD DE LOS ACTIVOS					NIVEL DE EXPOSICION AL RIESGO (NR)			APETITO AL RIESGO	CONTROL		ESTRATEGIA DE IMPLEMENTACIÓN
TIPO DE ACTIVO	CODIGO	ACTIVO	AMENAZA	VULNERABILIDAD	ID RIESGO	NIVEL	CATEGORIA		ID CONTROL	DESCRIPCION	
ACTIVOS ESENCIALES	[AE1]	Datos de Gestión interna	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	R1	12	MEDIO	TOLERABLE	C1	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R2	12	MEDIO	TOLERABLE	C2	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R3	16	ALTO	RIESGO NO ACEPTABLE	C3	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[AE2]	Órdenes de Compra y de Servicio	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	R4	12	MEDIO	TOLERABLE	C4	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R5	12	MEDIO	TOLERABLE	C5	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R6	16	ALTO	RIESGO NO ACEPTABLE	C6	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[AE3]	Documentos digitales	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	R7	12	MEDIO	TOLERABLE	C7	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R8	12	MEDIO	TOLERABLE	C8	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R9	16	ALTO	RIESGO NO ACEPTABLE	C9	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[AE4]	Documentos físicos	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	R10	12	MEDIO	TOLERABLE	C10	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R11	12	MEDIO	TOLERABLE	C11	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO

			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R12	16	ALTO	RIESGO NO ACEPTABLE	C12	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[AE5]	Información pública	[AN.*] Desastres naturales	Falta de copias de seguridad digitales por factores de desastres naturales e industriales	R13	12	MEDIO	TOLERABLE	C13	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R14	12	MEDIO	TOLERABLE	C14	Implementar un plan de digitalización de documentos físicos	EVITAR AUMENTO DEL RIESGO
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R15	16	ALTO	RIESGO NO ACEPTABLE	C15	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
SERVICIOS	[S1]	Servidor principal de dominio	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales	R16	15	ALTO	RIESGO NO ACEPTABLE	C16	Implementar un servidor de salvaguarda	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R17	15	ALTO	RIESGO NO ACEPTABLE	C17	Implementar un servidor de salvaguarda	EVITAR AUMENTO DEL RIESGO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores	R18	20	MUY ALTO	RIESGO NO ACEPTABLE	C18	Implementar un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Contaminación electromagnética		R19	20	MUY ALTO	RIESGO NO ACEPTABLE	C19	Implementar un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R20	20	MUY ALTO	RIESGO NO ACEPTABLE	C20	Implementar un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	R21	25	MUY ALTO	RIESGO NO ACEPTABLE	C21	Acondicionar una sala para servidores con controles y requisitos minimos que requiera el servidor.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor	R22	25	MUY ALTO	RIESGO NO ACEPTABLE	C22	Capacitación a los usuarios de la manipulación y el uso de los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador		R23	25	MUY ALTO	RIESGO NO ACEPTABLE	C23	Capacitación al personal en administración de servidores	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R24	16	ALTO	RIESGO NO ACEPTABLE	C24	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor	R25	25	MUY ALTO	RIESGO NO ACEPTABLE	C25	Capacitación a los usuarios de la manipulación y el uso de los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R26	16	ALTO	RIESGO NO ACEPTABLE	C26	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	R27	25	MUY ALTO	RIESGO NO ACEPTABLE	C27	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R28	20	MUY ALTO	RIESGO NO ACEPTABLE	C28	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R29	16	ALTO	RIESGO NO ACEPTABLE	C29	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de un administración de privilegios de usuario	R30	20	MUY ALTO	RIESGO NO ACEPTABLE	C30	Implementar una administración de privilegios de usuario	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R31	20	MUY ALTO	RIESGO NO ACEPTABLE	C31	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R32	16	ALTO	RIESGO NO ACEPTABLE	C32	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas	R33	25	MUY ALTO	RIESGO NO ACEPTABLE	C33	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R34	20	MUY ALTO	RIESGO NO ACEPTABLE	C34	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS

	[S2]	Servidor principal de base de datos INFO, SIAF Y SIGA	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales	R35	15	ALTO	RIESGO NO ACEPTABLE	C35	Implementar un servidor de salvaguarda	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R36	15	ALTO	RIESGO NO ACEPTABLE	C36	Implementar un servidor de salvaguarda	EVITAR AUMENTO DEL RIESGO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores	R37	20	MUY ALTO	RIESGO NO ACEPTABLE	C37	No existe un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Contaminación electromagnética		R38	25	MUY ALTO	RIESGO NO ACEPTABLE	C38	No existe un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R39	25	MUY ALTO	RIESGO NO ACEPTABLE	C39	Implementar un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	R40	25	MUY ALTO	RIESGO NO ACEPTABLE	C40	Acondicionar una sala para servidores con controles y requisitos minimos que requiera el servidor.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor	R41	25	MUY ALTO	RIESGO NO ACEPTABLE	C41	Capacitación a los usuarios de la manipulación y el uso de los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador		R42	25	MUY ALTO	RIESGO NO ACEPTABLE	C42	Capacitación al personal en administración de servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R43	16	ALTO	RIESGO NO ACEPTABLE	C43	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor	R44	25	MUY ALTO	RIESGO NO ACEPTABLE	C44	Capacitación a los usuarios de la manipulación y el uso de los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R45	16	ALTO	RIESGO NO ACEPTABLE	C45	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES

			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	R46	25	MUY ALTO	RIESGO NO ACEPTABLE	C46	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R47	20	MUY ALTO	RIESGO NO ACEPTABLE	C47	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R48	16	ALTO	RIESGO NO ACEPTABLE	C48	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R49	20	MUY ALTO	RIESGO NO ACEPTABLE	C49	Implementar una administración de privilegios de usuario	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R50	20	MUY ALTO	RIESGO NO ACEPTABLE	C50	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R51	16	ALTO	RIESGO NO ACEPTABLE	C51	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas	R52	25	MUY ALTO	RIESGO NO ACEPTABLE	C52	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R53	20	MUY ALTO	RIESGO NO ACEPTABLE	C53	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
	[S3]	Servidor principal de base de datos SISRENTAS, ASTM Y SRTM	[AN.*] Desastres naturales	Falta de un servidor de salvaguarda por factores de desastres naturales e industriales	R54	15	ALTO	RIESGO NO ACEPTABLE	C54	Implementar un servidor de salvaguarda	EVITAR AUMENTO DEL RIESGO
			[AI.*] Desastres industriales		R55	15	ALTO	RIESGO NO ACEPTABLE	C55	Implementar un servidor de salvaguarda	EVITAR AUMENTO DEL RIESGO
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo a los servidores	R56	20	MUY ALTO	RIESGO NO ACEPTABLE	C56	No existe un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Contaminación electromagnética		R57	20	MUY ALTO	RIESGO NO ACEPTABLE	C57	No existe un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AI.4] Avería de origen físico o lógico		R58	20	MUY ALTO	RIESGO NO ACEPTABLE	C58	Implementar un plan de mantenimiento a los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	R59	25	MUY ALTO	RIESGO NO ACEPTABLE	C59	Acondicionar una sala para servidores con controles y requisitos minimos que requiera el servidor.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.1]Errores de los usuarios	Fallas en la manipulación o uso del servidor	R60	25	MUY ALTO	RIESGO NO ACEPTABLE	C60	Capacitación a los usuarios de la manipulación y el uso de los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador		R61	25	MUY ALTO	RIESGO NO ACEPTABLE	C61	Capacitación al personal en administración de servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R62	16	ALTO	RIESGO NO ACEPTABLE	C62	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del servidor	R63	25	MUY ALTO	RIESGO NO ACEPTABLE	C63	Capacitación a los usuarios de la manipulación y el uso de los servidores	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R64	16	ALTO	RIESGO NO ACEPTABLE	C64	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para los servidores	R65	25	MUY ALTO	RIESGO NO ACEPTABLE	C65	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R66	20	MUY ALTO	RIESGO NO ACEPTABLE	C66	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R67	16	ALTO	RIESGO NO ACEPTABLE	C67	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R68	20	MUY ALTO	RIESGO NO ACEPTABLE	C68	Implementar una administración de privilegios de usuario	ELECCIÓN DE CONTROLES

			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R69	20	MUY ALTO	RIESGO NO ACEPTABLE	C69	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R70	16	ALTO	RIESGO NO ACEPTABLE	C70	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de los equipos	Falta de control de personas no autorizadas	R71	25	MUY ALTO	RIESGO NO ACEPTABLE	C71	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R72	20	MUY ALTO	RIESGO NO ACEPTABLE	C72	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
	[S4]	Correo electrónico institucional	[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R73	12	MEDIO	TOLERABLE	C73	Implementar mecanismos para detectar y corregir errores en el proceso envío y recepción de paquetes de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	R74	25	MUY ALTO	RIESGO NO ACEPTABLE	C74	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R75	16	ALTO	RIESGO NO ACEPTABLE	C75	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R76	16	ALTO	RIESGO NO ACEPTABLE	C76	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R77	20	MUY ALTO	RIESGO NO ACEPTABLE	C77	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R78	20	MUY ALTO	RIESGO NO ACEPTABLE	C78	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
DATOS / INFORMACIÓN	**[D1]**	Base de datos	[AE.1] Errores de los usuarios	Fallas en la manipulación o uso de la base de datos	R79	20	MUY ALTO	RIESGO NO ACEPTABLE	C79	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador		R80	20	MUY ALTO	RIESGO NO ACEPTABLE	C80	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.15] Alteración accidental de la información		R81	20	MUY ALTO	RIESGO NO ACEPTABLE	C81	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	R82	20	MUY ALTO	RIESGO NO ACEPTABLE	C82	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R83	16	ALTO	RIESGO NO ACEPTABLE	C83	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R84	16	ALTO	RIESGO NO ACEPTABLE	C84	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R85	16	ALTO	RIESGO NO ACEPTABLE	C85	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R86	20	MUY ALTO	RIESGO NO ACEPTABLE	C86	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R87	16	ALTO	RIESGO NO ACEPTABLE	C87	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R88	16	ALTO	RIESGO NO ACEPTABLE	C88	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R89	16	ALTO	RIESGO NO ACEPTABLE	C89	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R90	16	ALTO	RIESGO NO ACEPTABLE	C90	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[D2]	Backups de base de datos	[AE.1] Errores de los usuarios	Fallas en la manipulación de las Backups de base de datos	R91	20	MUY ALTO	RIESGO NO ACEPTABLE	C91	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador		R92	20	MUY ALTO	RIESGO NO ACEPTABLE	C92	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.15] Alteración accidental de la información		R93	20	MUY ALTO	RIESGO NO ACEPTABLE	C93	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	R94	20	MUY ALTO	RIESGO NO ACEPTABLE	C94	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R95	16	ALTO	RIESGO NO ACEPTABLE	C95	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R96	16	ALTO	RIESGO NO ACEPTABLE	C96	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R97	16	ALTO	RIESGO NO ACEPTABLE	C97	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R98	20	MUY ALTO	RIESGO NO ACEPTABLE	C98	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R99	16	ALTO	RIESGO NO ACEPTABLE	C99	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R100	16	ALTO	RIESGO NO ACEPTABLE	C100	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R101	16	ALTO	RIESGO NO ACEPTABLE	C101	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R102	16	ALTO	RIESGO NO ACEPTABLE	C102	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[D3]	Credenciales (usuario y contraseña)	[AE.1] Errores de los usuarios	Fallas en la manipulación o asignación de credenciales	R103	20	MUY ALTO	RIESGO NO ACEPTABLE	C103	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador		R104	20	MUY ALTO	RIESGO NO ACEPTABLE	C104	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.15] Alteración accidental de la información		R105	20	MUY ALTO	RIESGO NO ACEPTABLE	C105	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de la base de datos	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	R106	20	MUY ALTO	RIESGO NO ACEPTABLE	C106	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R107	16	ALTO	RIESGO NO ACEPTABLE	C107	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R108	16	ALTO	RIESGO NO ACEPTABLE	C108	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R109	16	ALTO	RIESGO NO ACEPTABLE	C109	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R110	20	MUY ALTO	RIESGO NO ACEPTABLE	C110	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R111	16	ALTO	RIESGO NO ACEPTABLE	C111	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R112	16	ALTO	RIESGO NO ACEPTABLE	C112	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R113	16	ALTO	RIESGO NO ACEPTABLE	C113	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R114	16	ALTO	RIESGO NO ACEPTABLE	C114	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
HARDWARE - EQUIPAMIENTO INFORMATICO	**[HW1]**	Equipos de cómputo y portátiles	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R115	15	ALTO	RIESGO NO ACEPTABLE	C115	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R116	15	ALTO	RIESGO NO ACEPTABLE	C116	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y	R117	20	MUY ALTO	RIESGO NO ACEPTABLE	C117	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AI.4] Contaminación electromagnética	correctivo del hardware	R118	20	MUY ALTO	RIESGO NO ACEPTABLE	C118	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R119	20	MUY ALTO	RIESGO NO ACEPTABLE	C119	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	R120	25	MUY ALTO	RIESGO NO ACEPTABLE	C120	Realizar un diagnóstico de las instalaciones eléctricas para tomar decisiones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Fallas en la manipulación de hardware	R121	16	ALTO	RIESGO NO ACEPTABLE	C121	Capacitación a los usuarios para el uso de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R122	16	ALTO	RIESGO NO ACEPTABLE	C122	Contratar a personal especializado para el mantenimiento de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R123	12	MEDIO	TOLERABLE	C123	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de control de personas no autorizadas	R124	16	ALTO	RIESGO NO ACEPTABLE	C124	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R125	16	ALTO	RIESGO NO ACEPTABLE	C125	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	R126	16	ALTO	RIESGO NO ACEPTABLE	C126	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[HW2]	Fotocopiadora / Impresora	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R127	12	MEDIO	TOLERABLE	C127	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R128	12	MEDIO	TOLERABLE	C128	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	R129	16	ALTO	RIESGO NO ACEPTABLE	C129	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Contaminación electromagnética		R130	16	ALTO	RIESGO NO ACEPTABLE	C130	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AI.4] Avería de origen físico o lógico		R131	16	ALTO	RIESGO NO ACEPTABLE	C131	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	R132	20	MUY ALTO	RIESGO NO ACEPTABLE	C132	Realizar un diagnóstico de las instalaciones eléctricas para tomar decisiones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R133	16	ALTO	RIESGO NO ACEPTABLE	C133	Contratar a personal especializado para el mantenimiento de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	R134	16	ALTO	RIESGO NO ACEPTABLE	C134	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[HW3]	Router	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R135	15	ALTO	RIESGO NO ACEPTABLE	C135	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R136	15	ALTO	RIESGO NO ACEPTABLE	C136	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	R137	20	MUY ALTO	RIESGO NO ACEPTABLE	C137	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Contaminación electromagnética		R138	20	MUY ALTO	RIESGO NO ACEPTABLE	C138	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R139	20	MUY ALTO	RIESGO NO ACEPTABLE	C139	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	R140	25	MUY ALTO	RIESGO NO ACEPTABLE	C140	Realizar un diagnóstico de las instalaciones eléctricas para tomar decisiones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R141	16	ALTO	RIESGO NO ACEPTABLE	C141	Contratar a personal especializado para el mantenimiento de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	R142	16	ALTO	RIESGO NO ACEPTABLE	C142	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[HW4]	Switch	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y	R143	15	ALTO	RIESGO NO ACEPTABLE	C143	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AI.*] Desastres industriales	correctivo de las instalaciones	R144	15	ALTO	RIESGO NO ACEPTABLE	C144	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo del hardware	R145	20	MUY ALTO	RIESGO NO ACEPTABLE	C145	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Contaminación electromagnética		R146	20	MUY ALTO	RIESGO NO ACEPTABLE	C146	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R147	20	MUY ALTO	RIESGO NO ACEPTABLE	C147	Implementar un plan de mantenimiento preventivo y correctivo de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.6] Corte del suministro eléctrico	Falta de un respaldo de energía eléctrica	R148	20	MUY ALTO	RIESGO NO ACEPTABLE	C148	Realizar un diagnóstico de las instalaciones eléctricas para tomar decisiones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R149	16	ALTO	RIESGO NO ACEPTABLE	C149	Contratar a personal especializado para el mantenimiento de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	R150	16	ALTO	RIESGO NO ACEPTABLE	C150	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
SOTWARE - APLICACIONES INFORMÁTICAS	**[SW1]**	Software ofimático	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R151	20	MUY ALTO	RIESGO NO ACEPTABLE	C151	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R152	16	ALTO	RIESGO NO ACEPTABLE	C152	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R153	12	MEDIO	TOLERABLE	C153	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R154	12	MEDIO	TOLERABLE	C154	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R155	16	ALTO	RIESGO NO ACEPTABLE	C155	Adquirir licencias de software original	ELECCIÓN DE CONTROLES

			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R156	12	MEDIO	TOLERABLE	C156	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R157	12	MEDIO	TOLERABLE	C157	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
	[SW2]	Sistema operativo	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R158	25	MUY ALTO	RIESGO NO ACEPTABLE	C158	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R159	16	ALTO	RIESGO NO ACEPTABLE	C159	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R160	15	ALTO	RIESGO NO ACEPTABLE	C160	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R161	15	ALTO	RIESGO NO ACEPTABLE	C161	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R162	16	ALTO	RIESGO NO ACEPTABLE	C162	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R163	12	MEDIO	TOLERABLE	C163	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R164	12	MEDIO	TOLERABLE	C164	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
	[SW3]	Antivirus	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R165	25	MUY ALTO	RIESGO NO ACEPTABLE	C165	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R166	20	MUY ALTO	RIESGO NO ACEPTABLE	C166	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R167	15	ALTO	RIESGO NO ACEPTABLE	C167	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS

				Falta de licencia de antivirus (pirateado)	R168	15	ALTO	RIESGO NO ACEPTABLE	C168	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R169	20	MUY ALTO	RIESGO NO ACEPTABLE	C169	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R170	15	ALTO	RIESGO NO ACEPTABLE	C170	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R171	15	ALTO	RIESGO NO ACEPTABLE	C171	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
	[SW4]	INFO	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R172	20	MUY ALTO	RIESGO NO ACEPTABLE	C172	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R173	20	MUY ALTO	RIESGO NO ACEPTABLE	C173	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R174	20	MUY ALTO	RIESGO NO ACEPTABLE	C174	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R175	20	MUY ALTO	RIESGO NO ACEPTABLE	C175	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R176	16	ALTO	RIESGO NO ACEPTABLE	C176	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R177	20	MUY ALTO	RIESGO NO ACEPTABLE	C177	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R178	20	MUY ALTO	RIESGO NO ACEPTABLE	C178	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R179	15	ALTO	RIESGO NO ACEPTABLE	C179	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R180	15	ALTO	RIESGO NO ACEPTABLE	C180	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R181	16	ALTO	RIESGO NO ACEPTABLE	C181	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia en antivirus)	R182	16	ALTO	RIESGO NO ACEPTABLE	C182	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R183	16	ALTO	RIESGO NO ACEPTABLE	C183	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R184	16	ALTO	RIESGO NO ACEPTABLE	C184	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R185	16	ALTO	RIESGO NO ACEPTABLE	C185	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R186	15	ALTO	RIESGO NO ACEPTABLE	C186	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R187	20	MUY ALTO	RIESGO NO ACEPTABLE	C187	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R188	20	MUY ALTO	RIESGO NO ACEPTABLE	C188	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R189	20	MUY ALTO	RIESGO NO ACEPTABLE	C189	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R190	20	MUY ALTO	RIESGO NO ACEPTABLE	C190	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES

			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R191	20	MUY ALTO	RIESGO NO ACEPTABLE	C191	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R192	20	MUY ALTO	RIESGO NO ACEPTABLE	C192	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R193	16	ALTO	RIESGO NO ACEPTABLE	C193	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R194	16	ALTO	RIESGO NO ACEPTABLE	C194	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R195	16	ALTO	RIESGO NO ACEPTABLE	C195	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R196	16	ALTO	RIESGO NO ACEPTABLE	C196	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW5]	SIAF	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R197	20	MUY ALTO	RIESGO NO ACEPTABLE	C197	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R198	20	MUY ALTO	RIESGO NO ACEPTABLE	C198	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R199	20	MUY ALTO	RIESGO NO ACEPTABLE	C199	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R200	20	MUY ALTO	RIESGO NO ACEPTABLE	C200	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R201	16	ALTO	RIESGO NO ACEPTABLE	C201	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R202	20	MUY ALTO	RIESGO NO ACEPTABLE	C202	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R203	20	MUY ALTO	RIESGO NO ACEPTABLE	C203	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R204	15	ALTO	RIESGO NO ACEPTABLE	C204	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R205	15	ALTO	RIESGO NO ACEPTABLE	C205	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R206	16	ALTO	RIESGO NO ACEPTABLE	C206	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R207	16	ALTO	RIESGO NO ACEPTABLE	C207	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R208	16	ALTO	RIESGO NO ACEPTABLE	C208	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R209	16	ALTO	RIESGO NO ACEPTABLE	C209	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R210	16	ALTO	RIESGO NO ACEPTABLE	C210	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R211	15	ALTO	RIESGO NO ACEPTABLE	C211	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R212	20	MUY ALTO	RIESGO NO ACEPTABLE	C212	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R213	20	MUY ALTO	RIESGO NO ACEPTABLE	C213	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R214	20	MUY ALTO	RIESGO NO ACEPTABLE	C214	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R215	20	MUY ALTO	RIESGO NO ACEPTABLE	C215	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R216	20	MUY ALTO	RIESGO NO ACEPTABLE	C216	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R217	20	MUY ALTO	RIESGO NO ACEPTABLE	C217	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R218	16	ALTO	RIESGO NO ACEPTABLE	C218	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R219	16	ALTO	RIESGO NO ACEPTABLE	C219	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R220	16	ALTO	RIESGO NO ACEPTABLE	C220	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R221	16	ALTO	RIESGO NO ACEPTABLE	C221	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW6]	SIGA	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R222	20	MUY ALTO	RIESGO NO ACEPTABLE	C222	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R223	20	MUY ALTO	RIESGO NO ACEPTABLE	C223	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R224	20	MUY ALTO	RIESGO NO ACEPTABLE	C224	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R225	20	MUY ALTO	RIESGO NO ACEPTABLE	C225	Adquirir licencias de software original	ELECCIÓN DE CONTROLES

			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R226	16	ALTO	RIESGO NO ACEPTABLE	C226	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R227	20	MUY ALTO	RIESGO NO ACEPTABLE	C227	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R228	20	MUY ALTO	RIESGO NO ACEPTABLE	C228	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R229	15	ALTO	RIESGO NO ACEPTABLE	C229	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R230	15	ALTO	RIESGO NO ACEPTABLE	C230	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R231	16	ALTO	RIESGO NO ACEPTABLE	C231	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R232	16	ALTO	RIESGO NO ACEPTABLE	C232	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R233	16	ALTO	RIESGO NO ACEPTABLE	C233	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R234	16	ALTO	RIESGO NO ACEPTABLE	C234	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R235	16	ALTO	RIESGO NO ACEPTABLE	C235	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R236	15	ALTO	RIESGO NO ACEPTABLE	C236	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS

				Falta de licencia de antivirus (pirateado)	R237	20	MUY ALTO	RIESGO NO ACEPTABLE	C237	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R238	20	MUY ALTO	RIESGO NO ACEPTABLE	C238	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R239	20	MUY ALTO	RIESGO NO ACEPTABLE	C239	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R240	20	MUY ALTO	RIESGO NO ACEPTABLE	C240	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R241	20	MUY ALTO	RIESGO NO ACEPTABLE	C241	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R242	20	MUY ALTO	RIESGO NO ACEPTABLE	C242	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R243	16	ALTO	RIESGO NO ACEPTABLE	C243	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R244	16	ALTO	RIESGO NO ACEPTABLE	C244	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R245	16	ALTO	RIESGO NO ACEPTABLE	C245	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R246	16	ALTO	RIESGO NO ACEPTABLE	C246	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW7]	RUB PVL	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R247	20	MUY ALTO	RIESGO NO ACEPTABLE	C247	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R248	20	MUY ALTO	RIESGO NO ACEPTABLE	C248	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R249	20	MUY ALTO	RIESGO NO ACEPTABLE	C249	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R250	20	MUY ALTO	RIESGO NO ACEPTABLE	C250	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R251	16	ALTO	RIESGO NO ACEPTABLE	C251	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R252	20	MUY ALTO	RIESGO NO ACEPTABLE	C252	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R253	20	MUY ALTO	RIESGO NO ACEPTABLE	C253	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R254	15	ALTO	RIESGO NO ACEPTABLE	C254	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R255	15	ALTO	RIESGO NO ACEPTABLE	C255	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R256	16	ALTO	RIESGO NO ACEPTABLE	C256	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R257	16	ALTO	RIESGO NO ACEPTABLE	C257	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R258	16	ALTO	RIESGO NO ACEPTABLE	C258	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R259	16	ALTO	RIESGO NO ACEPTABLE	C259	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES

			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R260	16	ALTO	RIESGO NO ACEPTABLE	C260	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R261	15	ALTO	RIESGO NO ACEPTABLE	C261	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R262	20	MUY ALTO	RIESGO NO ACEPTABLE	C262	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R263	20	MUY ALTO	RIESGO NO ACEPTABLE	C263	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R264	20	MUY ALTO	RIESGO NO ACEPTABLE	C264	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R265	20	MUY ALTO	RIESGO NO ACEPTABLE	C265	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R266	20	MUY ALTO	RIESGO NO ACEPTABLE	C266	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R267	20	MUY ALTO	RIESGO NO ACEPTABLE	C267	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R268	16	ALTO	RIESGO NO ACEPTABLE	C268	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R269	16	ALTO	RIESGO NO ACEPTABLE	C269	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R270	16	ALTO	RIESGO NO ACEPTABLE	C270	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R271	16	ALTO	RIESGO NO ACEPTABLE	C271	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW8]	SISMUN (SISTEMA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y	R272	20	MUY ALTO	RIESGO NO ACEPTABLE	C272	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS

				correctivo del software							
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R273	20	MUY ALTO	RIESGO NO ACEPTABLE	C273	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R274	20	MUY ALTO	RIESGO NO ACEPTABLE	C274	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R275	20	MUY ALTO	RIESGO NO ACEPTABLE	C275	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R276	16	ALTO	RIESGO NO ACEPTABLE	C276	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R277	20	MUY ALTO	RIESGO NO ACEPTABLE	C277	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R278	20	MUY ALTO	RIESGO NO ACEPTABLE	C278	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R279	15	ALTO	RIESGO NO ACEPTABLE	C279	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R280	15	ALTO	RIESGO NO ACEPTABLE	C280	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R281	16	ALTO	RIESGO NO ACEPTABLE	C281	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R282	16	ALTO	RIESGO NO ACEPTABLE	C282	Adquirir licencias de software original	ELECCIÓN DE CONTROLES

			programas (software)							
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R283	16	ALTO	RIESGO NO ACEPTABLE	C283	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R284	16	ALTO	RIESGO NO ACEPTABLE	C284	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R285	16	ALTO	RIESGO NO ACEPTABLE	C285	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R286	15	ALTO	RIESGO NO ACEPTABLE	C286	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R287	20	MUY ALTO	RIESGO NO ACEPTABLE	C287	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R288	20	MUY ALTO	RIESGO NO ACEPTABLE	C288	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R289	20	MUY ALTO	RIESGO NO ACEPTABLE	C289	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R290	20	MUY ALTO	RIESGO NO ACEPTABLE	C290	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R291	20	MUY ALTO	RIESGO NO ACEPTABLE	C291	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R292	20	MUY ALTO	RIESGO NO ACEPTABLE	C292	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R293	16	ALTO	RIESGO NO ACEPTABLE	C293	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R294	16	ALTO	RIESGO NO ACEPTABLE	C294	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES

			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R295	16	ALTO	RIESGO NO ACEPTABLE	C295	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R296	16	ALTO	RIESGO NO ACEPTABLE	C296	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW9]	ASTM (APLICATIVOS DE SISTEMAS DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R297	20	MUY ALTO	RIESGO NO ACEPTABLE	C297	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R298	20	MUY ALTO	RIESGO NO ACEPTABLE	C298	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R299	20	MUY ALTO	RIESGO NO ACEPTABLE	C299	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R300	20	MUY ALTO	RIESGO NO ACEPTABLE	C300	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R301	16	ALTO	RIESGO NO ACEPTABLE	C301	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R302	20	MUY ALTO	RIESGO NO ACEPTABLE	C302	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R303	20	MUY ALTO	RIESGO NO ACEPTABLE	C303	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R304	15	ALTO	RIESGO NO ACEPTABLE	C304	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas	R305	15	ALTO	RIESGO NO ACEPTABLE	C305	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES

				(demasiado predecible)							
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R306	16	ALTO	RIESGO NO ACEPTABLE	C306	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R307	16	ALTO	RIESGO NO ACEPTABLE	C307	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R308	16	ALTO	RIESGO NO ACEPTABLE	C308	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R309	16	ALTO	RIESGO NO ACEPTABLE	C309	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R310	16	ALTO	RIESGO NO ACEPTABLE	C310	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R311	15	ALTO	RIESGO NO ACEPTABLE	C311	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R312	20	MUY ALTO	RIESGO NO ACEPTABLE	C312	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R313	20	MUY ALTO	RIESGO NO ACEPTABLE	C313	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R314	20	MUY ALTO	RIESGO NO ACEPTABLE	C314	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R315	20	MUY ALTO	RIESGO NO ACEPTABLE	C315	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R316	20	MUY ALTO	RIESGO NO ACEPTABLE	C316	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES

				Falta de Gestión de contraseñas (demasiado predecible)	R317	20	MUY ALTO	RIESGO NO ACEPTABLE	C317	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R318	16	ALTO	RIESGO NO ACEPTABLE	C318	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R319	16	ALTO	RIESGO NO ACEPTABLE	C319	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R320	16	ALTO	RIESGO NO ACEPTABLE	C320	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R321	16	ALTO	RIESGO NO ACEPTABLE	C321	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW10]	SRTM (SISTEMA DE RECAUDACION TRIBUTARIA MUNICIPAL)	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R322	20	MUY ALTO	RIESGO NO ACEPTABLE	C322	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R323	20	MUY ALTO	RIESGO NO ACEPTABLE	C323	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R324	20	MUY ALTO	RIESGO NO ACEPTABLE	C324	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R325	20	MUY ALTO	RIESGO NO ACEPTABLE	C325	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R326	16	ALTO	RIESGO NO ACEPTABLE	C326	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R327	20	MUY ALTO	RIESGO NO ACEPTABLE	C327	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS

				Falta de Gestión de contraseñas (demasiado predecible)	R328	20	MUY ALTO	RIESGO NO ACEPTABLE	C328	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R329	15	ALTO	RIESGO NO ACEPTABLE	C329	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R330	15	ALTO	RIESGO NO ACEPTABLE	C330	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R331	16	ALTO	RIESGO NO ACEPTABLE	C331	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R332	16	ALTO	RIESGO NO ACEPTABLE	C332	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R333	16	ALTO	RIESGO NO ACEPTABLE	C333	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R334	16	ALTO	RIESGO NO ACEPTABLE	C334	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R335	16	ALTO	RIESGO NO ACEPTABLE	C335	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R336	15	ALTO	RIESGO NO ACEPTABLE	C336	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R337	20	MUY ALTO	RIESGO NO ACEPTABLE	C337	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R338	20	MUY ALTO	RIESGO NO ACEPTABLE	C338	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R339	20	MUY ALTO	RIESGO NO ACEPTABLE	C339	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES

				Falta de Gestión de contraseñas (demasiado predecible)	R340	20	MUY ALTO	RIESGO NO ACEPTABLE	C340	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R341	20	MUY ALTO	RIESGO NO ACEPTABLE	C341	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R342	20	MUY ALTO	RIESGO NO ACEPTABLE	C342	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R343	16	ALTO	RIESGO NO ACEPTABLE	C343	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R344	16	ALTO	RIESGO NO ACEPTABLE	C344	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R345	16	ALTO	RIESGO NO ACEPTABLE	C345	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R346	16	ALTO	RIESGO NO ACEPTABLE	C346	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
	[SW11]	SISRENTAS	[AI.5] Avería de origen físico o lógico	Falta de un plan de mantenimiento preventivo y correctivo del software	R347	20	MUY ALTO	RIESGO NO ACEPTABLE	C347	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso Incorrecto del software	R348	20	MUY ALTO	RIESGO NO ACEPTABLE	C348	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R349	20	MUY ALTO	RIESGO NO ACEPTABLE	C349	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de licencia de antivirus (pirateado)	R350	20	MUY ALTO	RIESGO NO ACEPTABLE	C350	Adquirir licencias de software original	ELECCIÓN DE CONTROLES

			[AE.9] Errores de [re-]encaminamiento	Falta de una administración de redes y configuración predeterminada	R351	16	ALTO	RIESGO NO ACEPTABLE	C351	Implementación de políticas y procedimientos claros, la capacitación del personal y la utilización de herramientas de monitoreo y gestión de redes.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.15] Alteración accidental de la información	Fallas en la manipulación o uso del software	R352	20	MUY ALTO	RIESGO NO ACEPTABLE	C352	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto del software	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R353	20	MUY ALTO	RIESGO NO ACEPTABLE	C353	Implementar una gestión de contraseñas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18]Destrucción de información	Falta de control de personas no autorizadas	R354	15	ALTO	RIESGO NO ACEPTABLE	C354	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R355	15	ALTO	RIESGO NO ACEPTABLE	C355	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AE.20] Vulnerabilidades de los programas (software)	Falta de un plan de mantenimiento preventivo y correctivo del software	R356	16	ALTO	RIESGO NO ACEPTABLE	C356	Implementar un plan de mantenimiento preventivo y correctivo de software	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.21] Errores de mantenimiento / actualización de programas (software)	Fallas en el software, falta de actualización de parches (Falta de Licencia)	R357	16	ALTO	RIESGO NO ACEPTABLE	C357	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.5] Suplantación de la identidad del usuario	Falta de control de personas no autorizadas	R358	16	ALTO	RIESGO NO ACEPTABLE	C358	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	TRANSFERENCIA DE RIESGOS A TERCEROS
				Falta de Gestión de contraseñas (demasiado predecible)	R359	16	ALTO	RIESGO NO ACEPTABLE	C359	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.6] Abuso de privilegios de acceso	Falta de una administración de privilegios de usuario	R360	16	ALTO	RIESGO NO ACEPTABLE	C360	Implementar controles de acceso basado en roles	ELECCIÓN DE CONTROLES
			[AA.8] Difusión de software dañino	Falta de políticas de ciberseguridad	R361	15	ALTO	RIESGO NO ACEPTABLE	C361	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS

				Falta de licencia de antivirus (pirateado)	R362	20	MUY ALTO	RIESGO NO ACEPTABLE	C362	Adquirir licencias de software original	ELECCIÓN DE CONTROLES
			[AA.11] Acceso no autorizado	Falta de políticas de ciberseguridad	R363	20	MUY ALTO	RIESGO NO ACEPTABLE	C363	Implementar políticas de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.15] Modificación deliberada de la información	Falta de control de personas no autorizadas	R364	20	MUY ALTO	RIESGO NO ACEPTABLE	C364	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R365	20	MUY ALTO	RIESGO NO ACEPTABLE	C365	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R366	20	MUY ALTO	RIESGO NO ACEPTABLE	C366	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R367	20	MUY ALTO	RIESGO NO ACEPTABLE	C367	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.19] Revelación de información	Falta de control de personas no autorizadas	R368	16	ALTO	RIESGO NO ACEPTABLE	C368	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R369	16	ALTO	RIESGO NO ACEPTABLE	C369	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
			[AA.22] Manipulación de programas	Falta de control de personas no autorizadas	R370	16	ALTO	RIESGO NO ACEPTABLE	C370	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
				Falta de Gestión de contraseñas (demasiado predecible)	R371	16	ALTO	RIESGO NO ACEPTABLE	C371	Implementar una gestión de contraseñas	ELECCIÓN DE CONTROLES
REDES DE COMUNICACIÓN	**[COM1]**	Red Wifi	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	R372	25	MUY ALTO	RIESGO NO ACEPTABLE	C372	Implementar mecanismos que se utiliza para detectar y corregir fallas en los servicios de comunicaciones antes de que afecten a los usuarios finales.	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	R373	16	ALTO	RIESGO NO ACEPTABLE	C373	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de las redes de comunicaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	R374	25	MUY ALTO	RIESGO NO ACEPTABLE	C374	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	R375	12	MEDIO	TOLERABLE	C375	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R376	15	ALTO	RIESGO NO ACEPTABLE	C376	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
	[COM2]	Red LAN	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	R377	25	MUY ALTO	RIESGO NO ACEPTABLE	C377	Implementar mecanismos que se utiliza para detectar y corregir fallas en los servicios de comunicaciones antes de que afecten a los usuarios finales.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	R378	16	ALTO	RIESGO NO ACEPTABLE	C378	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de las redes de comunicaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	R379	25	MUY ALTO	RIESGO NO ACEPTABLE	C379	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	R380	12	MEDIO	TOLERABLE	C380	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R381	15	ALTO	RIESGO NO ACEPTABLE	C381	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS

	[COM3]	Internet	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	R382	25	MUY ALTO	RIESGO NO ACEPTABLE	C382	Implementar mecanismos que se utiliza para detectar y corregir fallas en los servicios de comunicaciones antes de que afecten a los usuarios finales.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	R383	16	ALTO	RIESGO NO ACEPTABLE	C383	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de las redes de comunicaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	R384	25	MUY ALTO	RIESGO NO ACEPTABLE	C384	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES
			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	R385	12	MEDIO	TOLERABLE	C385	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R386	15	ALTO	RIESGO NO ACEPTABLE	C386	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
	[COM4]	Telefonía	[AI.8] Fallo de servicios de comunicaciones	Falta de un plan de mantenimiento preventivo y correctivo de los equipos de redes de comunicación	R387	9	MEDIO	TOLERABLE	C387	Implementar mecanismos que se utiliza para detectar y corregir fallas en los servicios de comunicaciones antes de que afecten a los usuarios finales.	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.2] Errores del administrador	Mala administración, manipulación y Uso de los equipos de redes y comunicación	R388	9	MEDIO	TOLERABLE	C388	Capacitación al administrador y a los usuarios de la manipulación y el uso correcto de las redes de comunicaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.24] Caída del sistema por agotamiento de recursos	Falta de un estudio previo para las condiciones mínimas y necesarias para las redes de comunicación	R389	9	MEDIO	TOLERABLE	C389	Monitoreo constante de los recursos del sistema para detectar cualquier sobrecarga o agotamiento de recursos antes de que cause la caída del sistema	ELECCIÓN DE CONTROLES

			[AA.12] Análisis de tráfico	Falta de un plan de ciberseguridad	R390	9	MEDIO	TOLERABLE	C390	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.14] Interceptación de información (escucha)	Falta de un plan de ciberseguridad	R391	12	MEDIO	TOLERABLE	C391	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.24] Denegación de servicio	Falta de un plan de ciberseguridad	R392	9	MEDIO	TOLERABLE	C392	Implementar un plan de ciberseguridad	TRANSFERENCIA DE RIESGOS A TERCEROS
EQUIPAMIENTO AUXILIAR	**[AUX1]**	Cableado	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R393	15	ALTO	RIESGO NO ACEPTABLE	C393	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R394	15	ALTO	RIESGO NO ACEPTABLE	C394	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares	R395	16	ALTO	RIESGO NO ACEPTABLE	C395	Implementar un plan de mantenimiento preventivo y correctivo del equipamiento auxiliar	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R396	16	ALTO	RIESGO NO ACEPTABLE	C396	Implementar un plan de mantenimiento preventivo y correctivo del equipamiento auxiliar	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R397	16	ALTO	RIESGO NO ACEPTABLE	C397	Contratar personal especializado para los mantenimientos de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
	[AUX2]	UPS	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R398	15	ALTO	RIESGO NO ACEPTABLE	C398	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R399	15	ALTO	RIESGO NO ACEPTABLE	C399	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los	R400	16	ALTO	RIESGO NO ACEPTABLE	C400	Implementar un plan de mantenimiento preventivo y correctivo del equipamiento auxiliar	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AI.4] Avería de origen físico o lógico	equipamientos auxiliares	R401	16	ALTO	RIESGO NO ACEPTABLE	C401	Implementar un plan de mantenimiento preventivo y correctivo del equipamiento auxiliar	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R402	16	ALTO	RIESGO NO ACEPTABLE	C402	Contratar personal especializado para los mantenimientos de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
	[AUX3]	Estabilizador	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R403	15	ALTO	RIESGO NO ACEPTABLE	C403	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R404	15	ALTO	RIESGO NO ACEPTABLE	C404	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.3] Contaminación mecánica	Falta de un plan de mantenimiento preventivo y correctivo de los equipamientos auxiliares	R405	16	ALTO	RIESGO NO ACEPTABLE	C405	Implementar un plan de mantenimiento preventivo y correctivo del equipamiento auxiliar	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.4] Avería de origen físico o lógico		R406	16	ALTO	RIESGO NO ACEPTABLE	C406	Implementar un plan de mantenimiento preventivo y correctivo del equipamiento auxiliar	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de personal especializado para los mantenimientos de hardware	R407	16	ALTO	RIESGO NO ACEPTABLE	C407	Contratar personal especializado para los mantenimientos de hardware	TRANSFERENCIA DE RIESGOS A TERCEROS
	[AUX4]	Mobiliario	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R408	9	MEDIO	TOLERABLE	C408	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R409	9	MEDIO	TOLERABLE	C409	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
SOPORTE DE INFORMACION	[MEDIA1]	Disco Duro Externo	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R410	12	MEDIO	TOLERABLE	C410	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R411	12	MEDIO	TOLERABLE	C411	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.10] Degradación de los soportes de almacenamiento de la información	Falta de un plan de mantenimiento preventivo y correctivo de los	R412	16	ALTO	RIESGO NO ACEPTABLE	C412	Implementar plan de mantenimiento preventivo y correctivo de los soportes de información	TRANSFERENCIA DE RIESGOS A TERCEROS

				soportes de información							
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	R413	12	MEDIO	TOLERABLE	C413	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AE.25] Pérdida de equipos	Falta de control de personas no autorizadas	R414	12	MEDIO	TOLERABLE	C414	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R415	12	MEDIO	TOLERABLE	C415	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.25] Robo	Falta de control de personas no autorizadas	R416	12	MEDIO	TOLERABLE	C416	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[MEDIA2]	Usb's	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R417	12	MEDIO	TOLERABLE	C417	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R418	12	MEDIO	TOLERABLE	C418	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.10] Degradación de los soportes de almacenamiento de la información	Falta de un plan de mantenimiento preventivo y correctivo de los soportes de información	R419	16	ALTO	RIESGO NO ACEPTABLE	C419	Implementar plan de mantenimiento preventivo y correctivo de los soportes de información	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.18] Destrucción de información	Falta de control de personas no autorizadas	R420	12	MEDIO	TOLERABLE	C420	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AE.25] Pérdida de equipos	Falta de control de personas no autorizadas	R421	12	MEDIO	TOLERABLE	C421	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.18] Destrucción de información	Falta de control de personas no autorizadas	R422	12	MEDIO	TOLERABLE	C422	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.25] Robo	Falta de control de personas no autorizadas	R423	12	MEDIO	TOLERABLE	C423	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
INSTALACIONES	**[L1]**	Infraestructura	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y	R424	15	ALTO	RIESGO NO ACEPTABLE	C424	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AI.*] Desastres industriales	correctivo de las instalaciones	R425	15	ALTO	RIESGO NO ACEPTABLE	C425	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.11] Acceso no autorizado	Falta de control de personas no autorizadas	R426	12	MEDIO	TOLERABLE	C426	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	R427	12	MEDIO	TOLERABLE	C427	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
	[L2]	Oficinas	[AN.*] Desastres naturales	Falta de un plan de mantenimiento preventivo y correctivo de las instalaciones	R428	15	ALTO	RIESGO NO ACEPTABLE	C428	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AI.*] Desastres industriales		R429	15	ALTO	RIESGO NO ACEPTABLE	C429	Implementar un plan de mantenimiento preventivo y correctivo de las instalaciones	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.11] Acceso no autorizado	Falta de control de personas no autorizadas	R430	12	MEDIO	TOLERABLE	C430	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
			[AA.26] Ataque destructivo	Falta de control de personas no autorizadas	R431	12	MEDIO	TOLERABLE	C431	Adquirir e instalar cámaras de seguridad para realizar el control de accesos	ELECCIÓN DE CONTROLES
PERSONAL	**[P1]**	Titular de la entidad	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	R432	12	MEDIO	TOLERABLE	C432	Capacitación y reforzamiento sobre las habilidades blandas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	R433	10	MEDIO	TOLERABLE	C433	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	R434	10	MEDIO	TOLERABLE	C434	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R435	10	MEDIO	TOLERABLE	C435	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R436	8	BAJO	RIESGO ACEPTABLE	C436	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS
	[P2]	Responsables de las áreas	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	R437	16	ALTO	RIESGO NO ACEPTABLE	C437	Capacitación y reforzamiento sobre las habilidades blandas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	R438	25	MUY ALTO	RIESGO NO ACEPTABLE	C438	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	R439	25	MUY ALTO	RIESGO NO ACEPTABLE	C439	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R440	20	MUY ALTO	RIESGO NO ACEPTABLE	C440	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R441	16	ALTO	RIESGO NO ACEPTABLE	C441	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS
	[P3]	Encargado de informática	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	R442	16	ALTO	RIESGO NO ACEPTABLE	C442	Capacitación y reforzamiento sobre las habilidades blandas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	R443	25	MUY ALTO	RIESGO NO ACEPTABLE	C443	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	R444	25	MUY ALTO	RIESGO NO ACEPTABLE	C444	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS

			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R445	20	MUY ALTO	RIESGO NO ACEPTABLE	C445	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R446	16	ALTO	RIESGO NO ACEPTABLE	C446	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS
	[P4]	Usuarios	[AE.7] Deficiencias en la organización	Ausencia de buen clima laboral	R447	16	ALTO	RIESGO NO ACEPTABLE	C447	Capacitación y reforzamiento sobre las habilidades blandas	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AE.28] Indisponibilidad del personal	Falta de personal capacitado	R448	25	MUY ALTO	RIESGO NO ACEPTABLE	C448	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.28] Indisponibilidad del personal	Falta de personal capacitado	R449	25	MUY ALTO	RIESGO NO ACEPTABLE	C449	Capacitar al personal	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.29] Extorsión	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R450	20	MUY ALTO	RIESGO NO ACEPTABLE	C450	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS
			[AA.30]Ingeniería social	Falta del Cumplimiento de las obligaciones y deberes del outsourcing	R451	16	ALTO	RIESGO NO ACEPTABLE	C451	Analizar, actualizar y basarse en el RASA (Reglamento de Aplicación de Sanciones Administrativas) Y TISA (Tabla de infracciones y Sanciones Administrativas)	TRANSFERENCIA DE RIESGOS A TERCEROS

4.5 Fase de Auditoría de los procesos

Se desarrollará mediante la metodología COBIT 4.1, para esto se sigue estas actividades:

4.5.1. Determinar los procesos a auditar

De acuerdo a la *Ilustración 1*: Objetivos de COBIT 4.1.

(COBIT 4.1., 2007), los procesos se clasifican en 04 dominios (Planear y Organizar, Adquirir e implementar, Entregar y dar soporte; y Monitorear y Evaluar), los procesos que se auditarán en la Municipalidad Distrital de Amarilis serán los siguientes:

Tabla 22: Dominios y sus respectivos Procesos de la metodología COBIT 4.1

Dominio	Procesos	
Planear y Organizar	PO1	Definir un plan estrategia de TI
	PO2	Definir la arquitectura de la información
	PO3	Definir la dirección tecnológica
	PO4	Definir los procesos, organización y relaciones de TI
	PO5	Administrar la Inversión en TI
	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia
	PO7	Administrar Recursos Humanos de TI
	PO8	Administrar la Calidad
	PO9	Evaluar y administrar los riesgos TI
	P10	Administrar Proyectos
Adquirir e Implementar	AI1	Identificar las soluciones automatizadas
	AI2	Adquirir y mantener software aplicativo
	AI3	Adquirir y mantener la infraestructura tecnológica
	AI4	Facilitar la operación y el uso
	AI5	Adquirir recursos de TI
	AI6	Administrar cambios
	AI7	Instalar y acreditar soluciones y cambios
Entregar y Dar Soporte	DS1	Definir y administra los niveles de servicio
	DS2	Administrar los Servicios de Terceros
	DS3	Administrar el desempeño capacidad
	DS4	Asegurar el servicio continuo
	DS5	Garantizar la seguridad de los sistemas
	DS6	Identificar y asignar costos
	DS7	Educar y entrenar a los usuarios
	DS8	Administrar la mesa de servicio y los incidentes
	DS9	Administrar la configuración
	DS10	Administrar los problemas
	DS11	Administrar los datos
	DS12	Administrar el ambiente físico
	DS13	Administrar las operaciones
Monitorear y Evaluar	ME1	Monitoreo y evaluar el desempeño de TI
	ME2	Monitorear y evaluar el control interno
	ME3	Garantizar el cumplimiento regulatorio
	ME4	Proporcionar gobierno de TI

4.5.2. Determinar los niveles de Madurez de los procesos

Se presentarán fichas individuales de acuerdo al Anexo 09 para cada objetivo, realizando un examen de los niveles de madurez de COBIT 4.1. El propósito es identificar el nivel mínimo no alcanzado por la Organización y, al mismo tiempo, evaluar el grado correspondiente en dicho objetivo.

4.5.3. Reporte General de Grados de Madurez

De acuerdo a las fichas individuales de acuerdo al Anexo 09 se tienen los siguientes resultados.

Tabla 23:Reporte General de Grados de Madurez

DOMINIO	PROCESO		NIVEL DE MADUREZ
PLANEAR Y ORGANIZAR	PO1	Definir un plan estrategia de TI	0
	PO2	Definir la arquitectura de la información	1
	PO3	Definir la dirección tecnológica	1
	PO4	Definir los procesos, organización y relaciones de TI	2
	PO5	Administrar la Inversión en TI	1
	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia	0
	PO7	Administrar Recursos Humanos de TI	1
	PO8	Administrar la Calidad	0
	PO9	Evaluar y administrar los riesgos TI	1
	P10	Administrar Proyectos	0
ADQUIRIR E IMPLEMENTAR	AI1	Identificar las soluciones automatizadas	2
	AI2	Adquirir y mantener software aplicativo	1
	AI3	Adquirir y mantener la infraestructura tecnológica	1
	AI4	Facilitar la operación y el uso	0
	AI5	Adquirir recursos de TI	4
	AI6	Administrar cambios	1
	AI7	Instalar y acreditar soluciones y cambios	0
ENTREGAR Y DAR SOPORTE	DS1	Definir y administra los niveles de servicio	0
	DS2	Administrar los Servicios de Terceros	2
	DS3	Administrar el desempeño capacidad	1
	DS4	Asegurar el servicio continuo	0
	DS5	Garantizar la seguridad de los sistemas	0
	DS6	Identificar y asignar costos	0
	DS7	Educar y entrenar a los usuarios	0
	DS8	Administrar la mesa de servicio y los incidentes	0
	DS9	Administrar la configuración	1
	DS10	Administrar los problemas	2
	DS11	Administrar los datos	1
	DS12	Administrar el ambiente físico	1
	DS13	Administrar las operaciones	1

MONITOREAR Y EVALUAR	ME1	Monitoreo y evaluar el desempeño de TI	0
	ME2	Monitorear y evaluar el control interno	0
	ME3	Garantizar el cumplimiento regulatorio	1
	ME4	Proporcionar gobierno de TI	2

4.5.4. Resumen de Análisis por dominio

4.5.4.1. Dominio: Planear y Organizar (PO)

Las estrategias de tecnología de la información y las del negocio no están alineadas de manera efectiva en la Municipalidad Distrital de Amarilis. La utilización óptima de los recursos no se logra, ya que no se aprovechan al máximo, y además, la entidad carece de los recursos necesarios para llevar a cabo ciertas tareas. Existe una falta de comprensión por parte del personal de la Municipalidad Distrital de Amarilis sobre los objetivos de TI; son pocos los usuarios que reconocen la importancia de estos para alcanzar las metas de la entidad.

4.5.4.2. Dominio: Adquirir e Implementar (AI)

Con el fin de llevar a cabo la estrategia de Tecnologías de la Información (TI), es necesario reconocer, elaborar o adquirir las soluciones tecnológicas correspondientes, además de llevar a cabo su implementación e integración en los procesos.

4.5.4.3. Dominio: Entrega y Dar Soporte (DS)

Los servicios de tecnología de la información se entregan de manera parcial, siguiendo las prioridades del negocio. Los costos de TI no están completamente optimizados. La ausencia de un plan de continuidad impide la implementación total de la disponibilidad de los sistemas de TI, y la integridad y confidencialidad no se encuentran optimizadas.

4.5.4.4. Dominio: Monitorear y Evaluar (ME)

En La Municipalidad Distrital de Amarilis, la dirección no supervisa ni evalúa adecuadamente el sistema de control interno. Se observa una falta de conexión en el rendimiento de la tecnología de la información con los objetivos comerciales. La medición de riesgos, así como la presentación de informes sobre estos, el cumplimiento, el rendimiento y el control no se llevan a cabo de manera óptima

4.5.5. Resumen de Procesos y criterios de información por impacto

A través de la sugerencia presentada por COSO, es posible asignar un valor promedio al impacto de los criterios de información. Luego de calcular los promedios, procedemos a la asignación, como se detalla en la tabla siguiente.

Tabla 24: Valores de acuerdo al grado de impacto

GRADO DE IMPACTO	VALOR
PRIMARIO (P)	0.86
SECUNDARIO (S)	0.63

A continuación, se muestra la tabla con todos los valores de grado de impacto.

Tabla 25: Resumen de Procesos y Criterios de Información por Impacto

OBJETIVOS DE CONTROL COBIT		NIVEL DE MADUREZ	CRITERIO DE INFORMACION DE COBIT							RECURSOS DE TI COBIT			
			EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	PERSONAS	INFORMACION	APLICACIÓN	INFRAESTRUCTURA
PLANEAR Y ORGANIZAR													
PO1	**Definir un plan estrategia de TI**		0.86	0.63	-	-	-	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**0**	0.00	0.00	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	-	-	-	-				
PO2	**Definir la arquitectura de la información**		0.63	0.86	0.63	0.86	-	-	-		X	X	
	Total Real (Impacto * Nivel Real)	**1**	0.63	0.86	0.63	0.86	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	3.15	4.30	3.15	4.30	-	-	-				
PO3	**Definir la dirección tecnológica**		0.86	0.86	-	-	-	-	-			X	X
	Total Real (Impacto * Nivel Real)	**1**	0.86	0.86	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
PO4	**Definir los procesos, organización y relaciones de TI**		0.86	0.86	-	-	-	-	-	X			
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
PO5	**Administrar la Inversión en TI**		0.86	0.86	-	-	-	-	0.63	X		X	X
	Total Real (Impacto * Nivel Real)	**1**	0.86	0.86	-	-	-	-	0.63				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	3.15				
PO6	**Comunicar las Aspiraciones y la Dirección de la Gerencia**		0.86	-	-	-	-	0.63	-		X		X
	Total Real (Impacto * Nivel Real)	**0**	0.00	-	-	-	-	0.00	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	-	-	-	-	3.15	-				
PO7	**Administrar Recursos Humanos de TI**		0.86	0.86	-	-	-	-	-				X
	Total Real (Impacto * Nivel Real)	**1**	0.86	0.86	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
PO8	**Administrar la Calidad**		0.86	0.86	-	0.63	-	-	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**0**	0.00	0.00	-	0.00	-	-	0.00				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	3.15	-	-	3.15				
PO9	**Evaluar y administrar los riesgos TI**		0.63	0.63	0.86	0.86	0.86	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**1**	0.63	0.63	0.86	0.86	0.86	0.63	0.63				
	Total Ideal (Impacto * Nivel Ideal)	**5**	3.15	3.15	4.30	4.30	4.30	3.15	3.15				
PO10	**Administrar Proyectos**		0.86	0.86	-	-	-	-	-	X		X	X
	Total Real (Impacto * Nivel Real)	**0**	0.00	0.00	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
ADQUIRIR E IMPLEMENTAR													
AI1	**Identificar las soluciones automatizadas**		0.86	0.63	-	-	-	-	-			X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.26	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	-	-	-	-				
AI2	**Adquirir y mantener software aplicativo**		0.86	0.86	-	-	0.63	-	0.63			X	
	Total Real (Impacto * Nivel Real)	**1**	0.86	0.86	-	-	0.63	-	0.63				

	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	-	-	3.15	-	3.15				
AI3	**Adquirir y mantener la infraestructura tecnológica**		0.63	0.86	-	0.63	0.63	-	-				X
	Total Real (Impacto * Nivel Real)	1	0.63	0.86	-	0.63	0.63	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	3.15	4.30	-	3.15	3.15	-	-				
AI4	**Facilitar la operación y el uso**		0.86	0.86	-	0.63	0.63	0.63	0.63	X		X	X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	-	0.00	0.00	0.00	0.00				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	-	3.15	3.15	3.15	3.15				
AI5	**Adquirir recursos de TI**		0.63	0.86	-	-	-	0.63	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	4	2.52	3.44	-	-	-	2.52	-				
	Total Ideal (Impacto * Nivel Ideal)	5	3.15	4.30	-	-	-	3.15	-				
AI6	**Administrar cambios**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	1	0.86	0.86	0.63	0.63	0.63	0.63	0.63				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
AI7	**Instalar y acreditar soluciones y cambios**		0.86	0.63	-	0.63	0.63	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	-	0.00	0.00	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	3.15	-	3.15	3.15	-	-				
ENTREGAR Y DAR SOPORTE													
DS1	**Definir y administra los niveles de servicio**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
DS2	**Administrar los Servicios de Terceros**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	2	1.72	1.72	1.26	1.26	1.26	1.26	1.26				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
DS3	**Administrar el desempeño capacidad**		0.86	0.86	-	-	0.63	-	-			X	X
	Total Real (Impacto * Nivel Real)	1	0.86	0.86	-	-	0.63	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	-	-	3.15	-	-				
DS4	**Asegurar el servicio continuo**		0.86	0.63	-	-	0.86	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	-	-	0.00	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	3.15	-	-	4.30	-	-				
DS5	**Garantizar la seguridad de los sistemas**		-	-	0.86	0.86	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	-	-	0.00	0.00	0.00	0.00	0.00				
	Total Ideal (Impacto * Nivel Ideal)	5	-	-	4.30	4.30	3.15	3.15	3.15				
DS6	**Identificar y asignar costos**		-	0.86	-	-	-	-	0.86	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	-	0.00	-	-	-	-	0.00				
	Total Ideal (Impacto * Nivel Ideal)	5	-	4.30	-	-	-	-	4.30				
DS7	**Educar y entrenar a los usuarios**		0.86	0.63	-	-	-	-	-	X			
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	3.15	-	-	-	-	-				
DS8	**Administrar la mesa de servicio y los incidentes**		0.86	0.86	-	-	-	-	-	X			X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	-	-	-	-	-				
DS9	**Administrar la configuración**		0.86	0.63	-	-	0.63	-	0.63		X	X	X
	Total Real (Impacto * Nivel Real)	1	0.86	0.63	-	-	0.63	-	0.63				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	3.15	-	-	3.15	-	3.15				
DS10	**Administrar los problemas**		0.86	0.86	-	-	0.63	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	2	1.72	1.72	-	-	1.26	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	-	-	3.15	-	-				
DS11	**Administrar los datos**		-	-	-	0.86	-	-	0.86		X		
	Total Real (Impacto * Nivel Real)	1	-	-	-	0.86	-	-	0.86				

	Total Ideal (Impacto * Nivel Ideal)	5	-	-	-	4.30	-	-	4.30				
DS12	Administrar el ambiente físico		-	-	-	0.86	0.86	-	-			X	
	Total Real (Impacto * Nivel Real)	1	-	-	-	0.86	0.86	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	-	-	-	4.30	4.30	-	-				
DS13	Administrar las operaciones		0.86	0.86	-	0.63	0.63	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	1	0.86	0.86	-	0.63	0.63	-	-				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	-	3.15	3.15	-	-				
MONITOREAR Y EVALUAR													
ME1	Monitoreo y evaluar el desempeño de TI		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
ME2	Monitorear y evaluar el control interno		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
ME3	Garantizar el cumplimiento regulatorio		-	-	-	-	-	0.86	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	1	-	-	-	-	-	0.86	0.63				
	Total Ideal (Impacto * Nivel Ideal)	5	-	-	-	-	-	4.30	3.15				
ME4	Proporcionar gobierno de TI		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	2	1.72	1.72	1.26	1.26	1.26	1.26	1.26				
	Total Ideal (Impacto * Nivel Ideal)	5	4.30	4.30	3.15	3.15	3.15	3.15	3.15				

4.5.6. Resultados finales del impacto sobre los criterios de información

A continuación, se muestra los resultados finales del impacto sobre los criterios de información y el porcentaje promedio obtenido de los criterios de información de información es de **15.82%,** de acuerdo a la Tabla 5: Calificación COSO, este resultado obtenido se encuentra en el nivel **BAJO,** significa que los criterios de la información COBIT que son la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad corren un mayor riesgo de sufrir una violación de datos, lo que puede tener un impacto significativo en su reputación, sus finanzas y sus operaciones.

Se detalla los resultados en la siguiente tabla.

Tabla 26: Resultados Finales del Impacto sobre los Criterios de Información

	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	
Total Real (Impacto * Nivel Real)	19.89	20.58	4.64	7.85	9.28	7.16	7.16	
Total Ideal (Impacto * Nivel Ideal)	120.10	113.50	30.65	56.15	60.15	38.95	52.70	
Porcentaje Alcanzado	16.56%	18.13%	15.14%	13.98%	15.43%	18.38%	13.59%	**15.82%**

4.5.6.1 Resultados finales del impacto sobre los criterios de información

El objetivo de esto es alcanzar el 100% en cada criterio de información para poder decir con certeza que la información sea efectiva, eficiente, confidencial, integra, disponible, cumplimiento y confiable.

Los criterios de información se encuentran en el siguiente porcentaje todos sobre el 100%.

El criterio de información “EFECTIVIDAD” consiste en que la información relevante sea entregada de forma consistente, utilizable, oportuna y correcta este criterio obtuvo un promedio del 16.56%, en este criterio no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

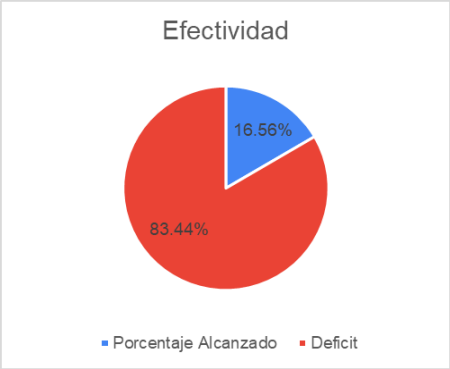


Ilustración 5: Resultado final del impacto sobre el criterio de información EFECTIVIDAD

El criterio de información “EFICIENCIA” consiste en que la información debe ser generada optimizando los recursos, este criterio obtuvo un promedio del 18.13%, en este criterio no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

Ilustración 6: Resultado final del impacto sobre el criterio de información EFICIENCIA

El criterio de información “CONFIDENCIALIDAD” consiste en que la información vital de la entidad sea protegida contra la revelación no autorizada, este criterio obtuvo un promedio del 15.14%, en este criterio no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

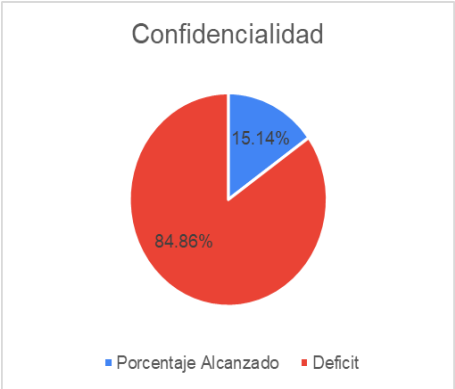


Ilustración 7: Resultado final del impacto sobre el criterio de información CONFIDENCIALIDAD

El criterio de información “INTEGRIDAD” consiste en que la información tiene que ser precisa, completa y valida, este criterio obtuvo un promedio del 13.98%, en este criterio no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

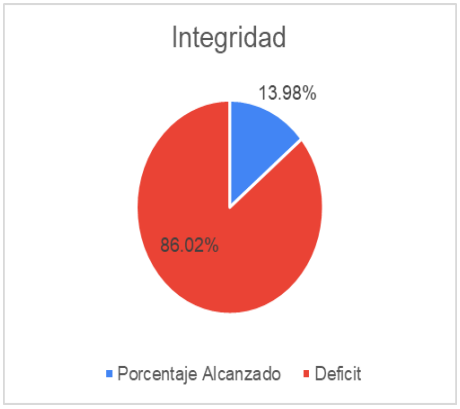


Ilustración 8: Resultado final del impacto sobre el criterio de información INTEGRIDAD

El criterio de información “DISPONIBILIDAD” consiste en que la información esté disponible cuando esta sea necesaria y requerida por parte de las áreas de la entidad en cualquier momento, este criterio obtuvo un promedio del 15.43%, en este criterio no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

Ilustración 9: Resultado final del impacto sobre el criterio de información DISPONIBILIDAD

El criterio de información “CUMPLIMIENTO” consiste en que se debe respetar la normatividad, leyes, reglamentos y acuerdos contractuales a los que está sujeta el proceso del negocio, como políticas internas, este criterio obtuvo un promedio del 18.38%, no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

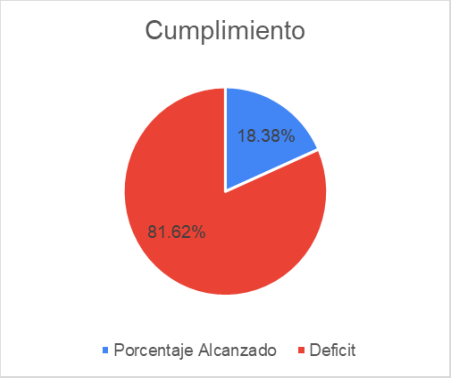


Ilustración 10: Resultado final del impacto sobre el criterio de información CUMPLIMIENTO

El criterio de información “CONFIABILIDAD” consiste en que se debe respetar y proporcionar la información correcta y apropiada, con el fin de que la Gerencia Municipal administre la entidad, este criterio obtuvo un promedio del 13.59%, en este criterio no cumple con los objetivos establecidos como se aprecia en la siguiente ilustración.

Ilustración 11: Resultado final del impacto sobre el criterio de información CONFIABILIDAD

4.6 Fase de Diseño de las Políticas de Seguridad

Tras realizar un exhaustivo análisis en este estudio, llegamos a la conclusión de proponer políticas de seguridad que se ajusten mejor a las necesidades de la Municipalidad Distrital de Amarilis. Estas políticas se han obtenido del conjunto de políticas de seguridad de información de la metodología COBIT con la finalidad de proporcionar un conjunto de directrices y normas que establecen cómo se deben manejar y proteger los activos de información para el resguardo de la información dentro de la Municipalidad Distrital de Amarilis. A continuación, presentamos las políticas propuestas según la metodología COBIT 4.1.

- **PSIMDA – D01** POLÍTICA DE SEGURIDAD

  Es una declaración de alto nivel y debe describir claramente los enlaces a otras políticas específicas, esto incluye:

  - Una definición de seguridad de la información para la empresa
  - Las responsabilidades asociadas con la seguridad de la información
  - La visión relativa a la seguridad de la información, acompañada de las metas y métricas apropiadas y una explicación de cómo dicha visión es apoyada por la cultura y la concienciación sobre seguridad de la información
  - Explicación de cómo la política de seguridad de la información se alinea con otras políticas de alto nivel
  - Elaboración de aspectos específicos de seguridad de información, tales como la gestión de datos, la evaluación de riesgos de la información y el cumplimiento de las obligaciones legales, reglamentarias y contractuales
  - Potencialmente, la gestión del presupuesto y coste del ciclo de vida de la seguridad de información. Pueden añadirse, también, los planes estratégicos de seguridad de la información y la gestión de la cartera asociada a los mismos.

- **PSIMDA – D02** ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

  Esta política específica aborda la forma en que la organización estructura sus procesos y prácticas para asegurar la confidencialidad, integridad y disponibilidad de la información. En los objetivos incluye lo siguiente.

  - Establecer un Marco Normativo Integral
  - Definir Roles y Responsabilidades Claras
  - Implementar Controles de Acceso Avanzados
  - Desarrollar y Mantener un Plan de Continuidad del Negocio Integral
  - Gestionar y Proteger Claves de Forma Rigurosa
  - Conducir Evaluaciones Periódicas de Riesgos y Vulnerabilidades
  - Asegurar la Conformidad con Normativas y Requisitos Específicos
  - Promover la Conciencia y Cultura de Seguridad
  - Desarrollar e Implementar un Equipo de Respuesta a Incidentes Ágil
  - Mejora Continua y Adaptación a Cambios Tecnológicos
  - Auditorías Internas y Externas Regulares
  - Establecer un Marco para la Gestión de Identidades y Accesos

- **PSIMDA – D03** SEGURIDAD DE LOS RECURSOS HUMANOS

  Esta política de seguridad permite gestionar la seguridad de la información en relación con el factor humano. Esta política se centra en aspectos específicos relacionados con el personal de la organización para garantizar que las personas que tienen acceso a los sistemas, datos y otros recursos de información cumplan con las prácticas de seguridad establecidas. Los objetivos que incluyen son los siguientes.

  - Procedimientos de Incorporación
  - Formación en Seguridad
  - Gestión de Accesos
  - Responsabilidades y Obligaciones del Personal

- Gestión de Cambios de Personal
- Uso Apropiado de los Recursos de Información
- Confidencialidad de la Información
- Conformidad con Normativas y Políticas Internas
- Cultura de Seguridad

- **PSIMDA – D04** GESTIÓN DE LOS ACTIVOS

  Los objetivos de esta política incluyen:

  - Categorización y propiedad de los sistemas
  - Uso y priorización de recursos
  - Administración del ciclo de vida de activos
  - Implementación de medidas de protección para los activos

- **PSIMDA – D05** CONTROL DE ACCESOS

  La política de gestión de acceso busca proporcionar un acceso apropiado a las partes interesadas, tanto internas como externas, para lograr los objetivos del negocio. La evaluación de este cumplimiento puede llevarse a cabo mediante indicadores de rendimiento como:

  - El número de violaciones de acceso que exceden los límites establecidos.
  - La cantidad de interrupciones laborales causadas por insuficiencia de derechos de acceso.
  - El número de incidentes o descubrimientos de auditoría relacionados con la segregación de funciones.

  Además, la política de gestión de acceso se esfuerza por garantizar que el acceso de emergencia se otorgue y revoque de manera oportuna, y esto puede ser evaluado mediante métricas tales como:

  - El número de solicitudes de acceso de emergencia.

- El número de cuentas de emergencia activas que superan los límites de tiempo aprobados.

En términos generales, la política de gestión de acceso aborda diversas áreas, incluyendo:

- El ciclo de vida del suministro de acceso físico y lógico.
- La implementación del principio de privilegio mínimo o necesidad de conocer.
- La segregación de funciones.
- Procedimientos de acceso en situaciones de emergencia.

Este enfoque integral garantiza que el acceso a los recursos sea eficiente y cumpla con los estándares establecidos, facilitando la evaluación continua y la mejora de las prácticas de seguridad.

- **PSIMDA – D06** CRIPTOGRAFÍA

  El propósito de esta política de seguridad es resguardar la disponibilidad, integridad y confiabilidad de la información. Para cumplir con este propósito, se requiere la implementación de controles criptográficos, como se especifica en la política sobre el uso de dichos controles y la gestión de claves.

- **PSIMDA – D07** SEGURIDAD FÍSICA Y AMBIENTAL

  El objetivo de esta política es brindar orientación en relación con:

  - Salvaguardar ubicaciones físicas.
  - Implementar controles ambientales que respalden las operaciones de soporte.

  La eficacia en la protección de la ubicación física puede evaluarse mediante la identificación de vulnerabilidades explotables y la incidencia de incidentes vinculados a amenazas asociadas con la ubicación física, tales como actos delictivos, riesgos industriales o de transporte, y amenazas naturales. En cuanto a los controles ambientales, su validez puede ser comprobada a través de la identificación de

vulnerabilidades explotables y la ocurrencia de incidentes atribuidos a sistemas de control ambiental.

Esta política, de manera indirecta, contribuye a la optimización de los costos de seguros. Una métrica pertinente podría ser la tendencia en los costos de seguros asociados con pérdidas debidas a amenazas físicas, delictivas y ambientales.

El ámbito de aplicación de la política abarca:

- Selección de instalaciones, que incluye criterios y atributos de construcción.
    - Normativas de control ambiental.
    - Normativas de control de acceso físico para empleados, proveedores y visitantes.
- Supervisión de seguridad de la información y detección de intrusiones físicas.

Esta política se dirige a los empleados, a todas las unidades de negocio, a los proveedores que transporten activos/equipos de la organización y a todos los visitantes. Las actualizaciones y revalidaciones deben contar con la participación de las áreas de instalaciones, asesoría jurídica, seguridad de la información y los responsables de datos y sistemas. Cualquier nueva política o actualización deberá distribuirse a empleados, contratistas y proveedores según lo establecido en los contratos, así como a empleados temporales.

- **PSIMDA – D08** SEGURIDAD DE OPERACIONES

  Los objetivos de esta política incluyen:

  - El establecimiento de estructuras y aplicaciones en el ámbito de la seguridad de la información de Tecnologías de la Información, abordando aspectos como el Comité Directivo, normativas y pautas.
  - La atención a las Operaciones internas y externas mediante el enfoque en Arquitecturas y Normativas de Seguridad de la Información.

- La formulación de Procedimientos Operativos relacionados con la Seguridad de la Información de Tecnologías de la Información.

- **PSIMDA – D09** SEGURIDAD DE LAS COMUNICACIONES

  Los objetivos de esta política abarcan:

  - El desarrollo de arquitecturas y aplicaciones relacionadas con la seguridad de la información en Tecnologías de la Información, con enfoque en el Comité Directivo, estándares y pautas.
  - La consideración de Normativas de Seguridad de la Información (ANS) en operaciones tanto internas como externas.
  - La formulación de Procedimientos Operativos para la Seguridad de la Información en el ámbito de las Tecnologías de la Información.

- **PSIMDA – D10** ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

  Los propósitos de esta política incluyen:

  - Garantizar la seguridad de la información a lo largo del ciclo de vida del proceso.
  - Asegurar la seguridad de la información en el desarrollo de los requisitos.
  - Salvaguardar la seguridad de la información en los procedimientos de compra/adquisición.
  - Implementar prácticas seguras de programación.
  - Integrar la seguridad de la información con la gestión de cambios y configuraciones.

- **PSIMDA – D11** RELACIONES CON PROVEEDORES

  Esta política de seguridad permite gestionar la seguridad de la información en el contexto de sus interacciones y relaciones con proveedores externos. Esta política tiene como objetivo garantizar que los proveedores cumplan con los estándares de seguridad

de la información establecidos por la organización, minimizando los riesgos asociados con la tercerización de servicios o el intercambio de información con terceros.

- Evaluación de Proveedores
- Requisitos de Seguridad
- Contratos de Seguridad
- Gestión de Accesos y Permisos
- Gestión de Riesgos
- Auditorías y Revisiones.
- Gestión de Documentación como establecer prácticas para la gestión segura de la documentación compartida con proveedores, incluyendo la protección de la propiedad intelectual y la información confidencial.

- **PSIMDA – D12** GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

El ámbito de aplicación de esta política aborda la necesidad de responder de manera pronta a los incidentes con el propósito de restablecer las operaciones comerciales. La política debe abarcar:

- Una definición de incidente de seguridad de información.
- Un enunciado sobre la gestión prevista de los incidentes.
- Requisitos para la formación del equipo de respuesta a incidentes, detallando roles y responsabilidades.
- Requisitos para la elaboración de un plan de respuesta a incidentes probado, que contenga procedimientos y pautas documentados en relación con:
    - La gravedad de los incidentes.
    - Procesos de comunicación (notificación) y escalado.
- Recuperación, que incluye:
    - Objetivos de Tiempo de Recuperación (RTOs) para restablecer la confianza.

        - Investigación y preservación del proceso.
    - Pruebas y capacitación.
    - Reuniones posteriores a los incidentes para documentar el análisis de las causas fundamentales, así como las mejoras en las prácticas de seguridad de la información para prevenir eventos similares en el futuro.
    - Documentación de los incidentes y su cierre.
    - Esta política está dirigida a las unidades de negocio correspondientes y a los empleados clave. Las actualizaciones y revalidaciones deben incluir la participación de la función de seguridad de la información. Cualquier política nueva o actualizada debe ser distribuida a los empleados clave.

- **PSIMDA – D13** ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

  Los objetivos de esta política abarcan:

    - Realizar un Análisis de Impacto en el Negocio (BIA).
    - Desarrollar planes de contingencia empresarial con pruebas de recuperación contrastadas.
    - Establecer requisitos de recuperación para los sistemas críticos.
    - Definir umbrales y desencadenantes para contingencias y la escalada de incidentes.
    - Crear un Plan de Recuperación de Desastres (DRP).
    - Implementar actividades de formación y pruebas.

- **PSIMDA – D14** CUMPLIMIENTO

  Los objetivos de esta política incluyen:

    - La evaluación del cumplimiento de la seguridad de la información en Tecnologías de la Información a través de procesos que aborden aspectos regulatorios, contractuales y corporativos.

- El establecimiento de métricas de desarrollo.
- La creación de repositorios de evaluación que consideren la audiencia, el contenido, la estructura y el seguimiento.

4.6.1 Políticas de seguridad y su respectivo manual

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D01**	
DOMINIO	**POLÍTICA DE SEGURIDAD**		
OBJETIVO	Proporcionar una directriz, reglas y procedimientos que permita solventar los problemas de seguridad de la información en la Municipalidad Distrital de Amarilis de acuerdo con las leyes y regulaciones vigentes en la que se encuentra la seguridad de la información.		
Objetivo de Control: Política de Seguridad de la Información			
Documento de Políticas de Seguridad de la Información			
	El responsable de la oficina de informática de la Municipalidad Distrital de Amarilis dispondrá de este documento de políticas de seguridad de la información que deberá ser aprobado por el área responsable para luego ser publicado y comunicado a los empleados y partes externas relacionadas con las áreas involucradas.		
Revisión de la Política de Seguridad de la Información			
	Cada una de las políticas se deberá revisar de forma semestral o por su defecto anualmente y de manera obligatoria cuando se realicen cambios significativos en la Municipalidad Distrital de Amarilis a nivel tecnológico, administrativo, operativo, presupuestal, entre otros para garantizar la vigencia y lo más actualizado las políticas de seguridad de la información. Algunos cambios que se pueden considerar significativos en la Municipalidad Distrital de Amarilis son como; cambios en la estructura organizacional, cambios tecnológicos, innovación en el software, innovación y automatización en los procesos, actualizaciones de la normativa vigente entre otros.		

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D02**	

DOMINIO	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
OBJETIVO	Establecer una estructura organizacional solida que dirija la implementación y la gestión de la seguridad de la información dentro del entorno de la Municipalidad Distrital de Amarilis.

Objetivo de Control: Organización Interna	
Compromiso de las autoridades de la MDA con la seguridad de la información.	
	a) Realizar una verificación y supervisión de la implementación de las directrices descritas en este manual.
	b) Fomentar la difusión de este documento a través de la implementación de programas de formación, capacitación, concientización del equipo y su divulgación.
	c) Crear un **Comité de Seguridad de la Información** en la MDA (CSI) y nombrar a los encargados correspondientes. Este comité deberá realizar reuniones de manera regular o cuando sea necesario. Es fundamental llevar un registro de cada una de las reuniones realizadas junto con su respectiva acta.
Coordinación de la Seguridad de la información	
	La coordinación está a cargo del Comité de Gestión de Seguridad de la Información con las siguientes responsabilidades:
	a) Seguir las directrices y regulaciones de la Municipalidad Distrital de Amarilis en lo que respecta a la seguridad de la información.
	b) Supervisar que la alta dirección de la Municipalidad Distrital de Amarilis apruebe y ejecute el manual de políticas de seguridad de la información.
	c) Fomentar la divulgación de conocimientos relacionados con la seguridad de la información dentro de la Municipalidad Distrital de Amarilis.
	d) Nombrar personas encargadas de la gestión de información en cada unidad orgánica, lo cual se debe registrar en un documento, ya sea en formato físico o electrónico.
	e) Supervisar la gestión de la continuidad de los servicios en caso de incidentes de seguridad.
	f) Supervisar las acciones emprendidas por los empleados de la Municipalidad Distrital de Amarilis con el fin de mejorar la protección de la información.
	g) Administrar los recursos financieros, tecnológicos y humanos para supervisar la seguridad de la información.
	h) Implementar la serie de estándares técnicos del Instituto Nacional de Calidad (INACAL) ISO/IEC 27000 en la Municipalidad Distrital de Amarilis, adaptándolos según la disposición de cada normativa, conforme sea requerido.

	i) Nombrar de manera oficial a una persona como el Oficial de Seguridad de la Información, que actuará como el líder del equipo de Seguridad de la Información. Esta persona no debe ser parte del área de Tecnología de la Información y será responsable de informar directamente a la Gerencia General de la Municipalidad Distrital de Amarilis.
	j) Nombrar de manera oficial al encargado de la seguridad en el área de Tecnología de la Información en conjunto con el encargado del departamento de Tecnología de la Información de la Municipalidad Distrital de Amarilis.
	k) Examinar de forma regular, cada año, las políticas en relación a las leyes y regulaciones actuales.
	l) Dar el visto bueno y aprobar los reportes relativos a la seguridad de la información de la Municipalidad Distrital de Amarilis.
Asignación de responsabilidades para la seguridad de la información	
	El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:
	a) Elaborar métodos para administrar incidentes de seguridad y garantizar la protección de la Municipalidad Distrital de Amarilis tanto frente a amenazas internas como externas.
	b) Identificar y evaluar las herramientas y servicios apropiados para incorporar en la Municipalidad Distrital de Amarilis con el fin de identificar posibles amenazas.
	c) Elaborar un programa de formación con el objetivo de sensibilizar a todos los trabajadores en temas relacionados con la seguridad, el acceso a la información, los dispositivos de almacenamiento y fomentar una cultura de seguridad.
	d) Supervisar los riesgos con el fin de tomar medidas preventivas en la toma de decisiones.
	e) Supervisar la difusión y distribución de la información dentro de la compañía y fuera de la compañía.
	f) Informar a todo el personal acerca de las tácticas empleadas por los delincuentes cibernéticos para obtener información de forma ilegal y cómo sus acciones pueden resultar en la vulneración de datos.
	g) Elaborar y crear la documentación necesaria que describa las estrategias para evitar que personas no autorizadas accedan a los recursos, sistemas de información y áreas de trabajo.
	h) Realizar un monitore constante de las normas, procedimientos y controles de seguridad establecidos en la Municipalidad Distrital de Amarilis.
	i) Realizar juntas regulares con el Comité de Seguridad de la Información o en casos apropiados, también es esencial mantener un registro de dichas reuniones.
	j) Definir la clasificación de la información.
	El responsable de Seguridad del Área de Tecnología de la Información tendrá las siguientes responsabilidades:
	a) Asegurarse de que toda la documentación, ya sea en forma física o digital, esté al día, incluyendo procedimientos, diagramas, procesos y operaciones, entre otros.
	b) Regirse los protocolos establecidos al abordar los eventos relacionados con la seguridad.

	c) Supervisar la aptitud de los sistemas de operación para enfrentar posibles amenazas en el futuro.
	d) Supervisar el proceso de obtener copias de seguridad de los datos.
	e) Elaborar métodos para notificar errores en el manejo de datos o en sistemas de transmisión de información.
	f) Aplicar medidas de seguridad siguiendo las pautas, regulaciones y estándares internacionales recomendados.
	g) Establecer y aplicar protocolos para gestionar dispositivos de almacenamiento informático, como discos duros y memorias flash, junto con documentos impresos, y asegurarse de eliminarlos adecuadamente al finalizar su vida útil.
	h) Gestionar los eventos de seguridad cibernética siguiendo los protocolos predefinidos.
Proceso de autorización para nuevos servicios de procesamiento de la información.	
	a) Establecer a una persona encargada de los nuevos servicios a implementar, la cual se encargará de supervisar el acceso de los usuarios de acuerdo a su función en el sistema.
	b) Se pedirá permiso al Oficial de Seguridad de la Información con el fin de garantizar el seguimiento de las políticas establecidas en este documento.
	c) Comprobar tanto el hardware como el software de la empresa para garantizar su compatibilidad y asegurarse de que satisfacen los requisitos esenciales para funcionar con los elementos del sistema.
	d) Para prevenir la introducción de nuevas vulnerabilidades en la Municipalidad Distrital de Amarilis, es esencial reconocer y aplicar los controles requeridos al gestionar servicios de procesamiento de datos personales, privados o de terceros.
Contacto con grupos de intereses especiales	
	a) Adquirir sabiduría acerca de las prácticas óptimas y estar al tanto de datos pertinentes
	b) Asegurar que la comprensión de la seguridad de la información sea exhaustiva y esté actualizada con información actualizada.
	c) Obtener datos actualizados sobre los incidentes y debilidades más comunes en las empresas a nivel local, regional, nacional e internacional.
	d) Consultar con expertos en seguridad de la información para obtener asesoramiento especializado.
	e) Facilitar la comunicación y el intercambio de datos entre los diferentes componentes de la Municipalidad Distrital de Amarilis acerca de las últimas tecnologías, productos, riesgos o debilidades.
	f) Suministrar conexiones apropiadas en situaciones relacionadas con eventos de seguridad de la información.
Seguridad de la información en la gestión de proyectos	
	a) Es necesario incorporar los objetivos de seguridad de la información dentro de los objetivos del proyecto.

	b) Llevar a cabo una evaluación de riesgos de seguridad de la información al inicio del proyecto con el fin de reconocer los controles requeridos.
	c) Detectar posibles peligros relacionados con la seguridad de los datos en todas las etapas del enfoque de la gestión y administración de proyectos.
Objetivo de control: Dispositivos móviles y trabajo remoto	
Política de dispositivo móvil	
	a) Evitar el uso de teléfonos móviles en espacios públicos, salas de juntas y otros lugares desprotegidos con el propósito de prevenir accesos no autorizados o la divulgación de información confidencial.
	b) Es necesario proteger físicamente los dispositivos móviles contra el robo y permitir la capacidad de eliminar toda la información del dispositivo.
	c) Para proteger los datos, es necesario asegurarse de que los dispositivos móviles proporcionados por la Municipalidad Distrital de Amarilis o personales estén bloqueados físicamente a través de un código de acceso o un patrón de seguridad.
	Cuando se manejan dispositivos móviles como activo de la Municipalidad Distrital de Amarilis se debe considerar:
	a) La división entre el uso personal y laboral en el dispositivo, incluyendo el software diseñado para facilitar esta separación y garantizar la seguridad de los datos.
	b) Dar acceso a los datos de la entidad únicamente después de que el usuario haya aceptado un acuerdo de usuario final, en el cual reconozca sus responsabilidades.
	c) Reemplazo del dispositivo por parte de la Municipalidad Distrital de Amarilis en situaciones de robo, extravío o cuando ya no cuenta con la autorización para ser empleado.
Trabajo remoto	
	a) Solo el Gerente Municipal de la Municipalidad Distrital de Amarilis podrá autorizar la modalidad de trabajo remoto.
	Cuando se realice la modalidad de trabajo remoto se debe:
	- Considerar la integridad física del entorno en el que se llevará a cabo la labor.
	- Garantizar la seguridad de las comunicaciones esencial al acceder de forma remota a los sistemas internos de la Municipalidad Distrital de Amarilis
	- Evitar conectarse a redes inalámbricas que no garanticen la seguridad de acceso.
	- Establecer las especificaciones del firewall y las medidas de seguridad contra malware
	- Considerar la privacidad del entorno y evitar revelar información confidencial sobre otras personas que estén en el lugar.
	b) Para habilitar el trabajo a distancia en situaciones en las que sea necesario ofrecer servicios de implementación o asistencia a los usuarios, se requiere que el usuario presente una solicitud y que el líder del proyecto, además del Gerente Municipal de la Municipalidad Distrital de Amarilis, otorguen su autorización previa.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D03**	

DOMINIO	**SEGURIDAD DE LOS RECURSOS HUMANOS**
OBJETIVO	Proteger la información y los activos de la Municipalidad Distrital de Amarilis al enfocarse en el comportamiento y las acciones del personal, asegurando que conozcan sus responsabilidades y que estén alineados con las mejores prácticas de seguridad.
Objetivo de Control: Antes de la contratación	
Investigación de antecedentes	
	i) Examinar su CV (Curriculum Vitae) del solicitante, lo cual implica confirmar su identidad (mediante el DNI o pasaporte en el caso que sea extranjero), validar sus logros académicos y profesionales, revisar su historial legal y evaluar las referencias laborales.
	ii) La Municipalidad Distrital de Amarilis debe garantizar que el recurso contratado para desempeñar el rol de seguridad de la información posea los conocimientos requeridos para cumplir con dicha responsabilidad.
	iii) Es necesario proporcionar previamente información al equipo acerca del proceso de selección del próximo candidato.
Términos y condiciones de contratación	
	i) Previo a proporcionar acceso a los datos confidenciales de la Municipalidad Distrital de Amarilis, es necesario formalizar convenios y cláusulas de confidencialidad o pactos de no divulgación con la persona que solicite dicho acceso.
	ii) La Municipalidad Distrital de Amarilis debe garantizar que el concursante al puesto esté en conformidad con los términos y condiciones que la entidad ha establecido para cumplir con las normativas de seguridad de la información.
	iii) Brindar información acerca de las obligaciones legales que corresponden al trabajador o colaborador en cuanto a la salvaguardia de la información, el correcto empleo de los recursos de la Municipalidad Distrital de Amarilis, las instalaciones, dejando constancia de todas las acciones mediante documentos, reportes o registros escritos.
	iv) Establecer cláusulas y pactos de confidencialidad con los proveedores
Objetivo de control: Durante la contratación	
Responsabilidades de gestión	
	i) Aceptar y comprometerse con las funciones y deberes relacionados con la protección de datos antes de obtener autorización para acceder a los sistemas o información confidencial proporcionada por la Municipalidad Distrital de Amarilis.
	ii) Alcanzar un grado de conciencia centrado en la protección de la información, a fin de desempeñar sus tareas y obligaciones de manera exitosa en la Municipalidad Distrital de Amarilis**.**
	iii) Revisar y seguir las directrices de seguridad de datos de la Municipalidad Distrital de Amarilis y adherirse a los procedimientos operativos establecidos

Concienciación, formación y capacitación en seguridad de la información		
	i) Es necesario que todos los empleados de la Municipalidad Distrital de Amarilis participen en entrenamientos específicos sobre seguridad de datos, con el propósito de que comprendan sus obligaciones en cuanto a la protección de la información.	
	ii) Llevar a cabo campañas internas de concienciación que involucren a los empleados de la Municipalidad Distrital de Amarilis, brindándoles la oportunidad de adquirir un mayor conocimiento sobre la protección de la información a través de la utilización de carteles, comunicados, spots informativos, y otras iniciativas.	
		- Los procesos de concienciación deben establecerse de forma continua, dado que la Municipalidad Distrital de Amarilis está constantemente incorporando a nuevos miembros a su equipo.
		- La elaboración de campañas de concienciación debe ser cuidadosamente diseñada considerando todas las responsabilidades y roles de los trabajadores en la Municipalidad Distrital de Amarilis.
		- Es fundamental mantener la actualización constante de los programas de concientización, de modo que estén alineados en todo momento con las políticas y procedimientos establecidos por la Municipalidad Distrital de Amarilis
		- Es esencial que los programas de concienciación garanticen la comprensión de los contenidos por parte de los participantes.
	iii) Instruir a los empleados acerca de una cultura de seguridad puede llevarse a cabo mediante conversaciones, educación a distancia o recursos en línea, con el fin de adaptarse al ritmo laboral de los colaboradores.	
	La instrucción y capacitación en seguridad también deben abordar aspectos adicionales tales como:	
	i) Manifestar el respaldo a la protección de datos en la Municipalidad Distrital de Amarilis	
	ii) La obligación de familiarizarse y acatar las pautas de seguridad según se establecen en las políticas, normativas legales, reglamentos, contratos y convenios.	
	iii) La obligación individual de salvaguardar y resguardar la información confidencial de la Municipalidad Distrital de Amarilis y de las entidades externas colaboradoras, asegurando la integridad de dichos datos.	
	iv) Establecer conexiones internas en la Municipalidad Distrital de Amarilis para obtener datos adicionales y consultas sobre temas relacionados con la seguridad de la información, lo cual involucra recursos educativos disponibles.	
Proceso disciplinario		
	i) El procedimiento de disciplina debe garantizar un trato adecuado y equitativo al colaborador que ha incurrido en faltas relacionadas con la seguridad de los datos. Antes de iniciar cualquier indagación, es esencial verificar si ha ocurrido una vulneración de la seguridad en la Municipalidad Distrital de Amarilis.	
	ii) La evaluación del procedimiento disciplinario debe tener en cuenta elementos como la índole y seriedad de la falta cometida y cómo afecta a la Municipalidad Distrital de Amarilis, si se trata de la primera vez que el empleado comete la infracción o si ha ocurrido antes, y si recibió formación previa o no.	

	iii) El procedimiento disciplinario se emplea con el propósito de prevenir que los empleados transgredan las políticas y procedimientos de seguridad de la información de la Municipalidad Distrital de Amarilis, así como cualquier otra violación o infracción que demande medidas inmediatas, funcionando como un medio de disuasión
Objetivo de Control: Cierre o cambio de puesto de trabajo	
Cese o cambio de puesto de trabajo	
	i) La gestión de cambios en la responsabilidad o cargo implica tratarlo como la finalización de la posición actual junto con el comienzo de la nueva responsabilidad o puesto.
	ii) Cuando llegue el momento de concluir el contrato de trabajo o de efectuar un cambio de posición, es esencial llevar a cabo la transmisión de los documentos y datos de los cuales uno fue responsable durante su período laboral al recién designado, o en caso de que no se haya asignado a alguien nuevo, estos deberán ser entregados al Oficial de Seguridad de la Información.

<table>
<tr><td>  </td><td>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS</td><td>PSIMDA – D04</td><td>Digital ecológico y emprendedor.</td></tr>
<tr><td colspan="2">DOMINIO</td><td colspan="2">GESTIÓN DE LOS ACTIVOS</td></tr>
<tr><td colspan="2">OBJETIVO</td><td colspan="2">Identificar los recursos (Activos de información) en posesión de la Municipalidad Distrital de Amarilis y determinar quiénes son los encargados de asegurar su adecuada salvaguarda</td></tr>
<tr><td colspan="4">Objetivo de Control: Responsabilidad sobre los activos</td></tr>
<tr><td colspan="4">Inventario de Activos</td></tr>
<tr><td rowspan="8"></td><td colspan="3">i) El área de innovación tecnológica y TIC's de la Municipalidad Distrital de Amarilis tiene la responsabilidad de identificar los activos significativos en el proceso de la información a lo largo de su existencia y registrar su relevancia. Este ciclo abarca la creación, el manejo, el resguardo, la transferencia, la eliminación y la eliminación definitiva.</td></tr>
<tr><td colspan="3">ii) La precisión, actualización, coherencia y concordancia con otros registros son esenciales en el manejo de los activos. Se requiere la inclusión de los siguientes para el proceso de inventario de activo. Se deben inventariar los siguientes activos:</td></tr>
<tr><td rowspan="5"></td><td colspan="2">- Activos principales en formatos físicos o digitales.</td></tr>
<tr><td colspan="2">- Activos relacionados con el soporte de hardware.</td></tr>
<tr><td colspan="2">- Activos vinculados al soporte de software.</td></tr>
<tr><td colspan="2">- Activos que respaldan las redes.</td></tr>
<tr><td colspan="2">- Activos relativos a la estructura organizativa física.</td></tr>
<tr><td colspan="3">iii) Tomar en cuenta la normativa ISO/IEC 27005 ofrece una manera de categorizar los recursos que podrían incluirse en el registro del inventariado de la Municipalidad Distrital de Amarilis.</td></tr>
<tr><td colspan="3">iv) Es necesario renovar los datos del registro de inventario de existencias en un período de tiempo que no exceda medio año.</td></tr>
<tr><td colspan="4">Propiedad de los Activos</td></tr>
<tr><td rowspan="5"></td><td colspan="3">i) Asignar una persona encargada de supervisar los activos o grupos de activos no implica que dicha persona adquiera derechos de propiedad sobre los activos, como, por ejemplo, discos duros, servidores, monitores o routers. El personal responsable del activo deberá desempeñar las siguientes responsabilidades:</td></tr>
<tr><td rowspan="3"></td><td colspan="2">- Realizar un inventario de los activos asignados y mantenerlo actualizado según sea necesario.</td></tr>
<tr><td colspan="2">- Desarrollar normas de uso adecuado para dichos activos y ponerlas en práctica previa autorización de Gerencia Municipal.</td></tr>
<tr><td colspan="2">- Seleccionar, documentar y mantener actualizada la información relevante, así como definir los permisos de acceso correspondientes.</td></tr>
<tr><td colspan="3">- Garantizar que se lleve a cabo un inventario correcto de los bienes (activos de información).</td></tr>
<tr><td colspan="3">- Garantizar que los bienes (activos de información) estén correctamente categorizados y resguardados.</td></tr>
</table>

	- Examinar de manera regular las limitaciones y categorizaciones que regulan la entrada a recursos de importancia, considerando las directrices (políticas) sobre la gestión de acceso correspondientes.	
	- Asegurar una gestión adecuada al momento de la eliminación o destrucción del activo.	
Uso aceptable de los activos		
	i) Los requisitos de seguridad de la información deben tenerlo en consideración el personal interno y los usuarios externos que emplean o cuentan con acceso a los activos de la información de la Municipalidad Distrital de Amarilis	
	ii) La responsabilidad del uso de cualquier recurso o activo de procesamiento de información recae en el personal interno y en los usuarios externos.	
	iii) La Municipalidad Distrital de Amarilis posee todos los derechos sobre la información y documentos generados y transmitidos, utilizando cualquier medio o dispositivo electrónico.	
Devolución de los activos		
	i) Como parte de la finalización de su vínculo laboral, se requiere que tanto los empleados como los usuarios externos de La Municipalidad Distrital de Amarilis S.A. atraviesen un procedimiento de devolución de activos	
	ii) Cuando un trabajador o un usuario externo resulta crucial para el funcionamiento continuo, es necesario registrar y traspasar dicha información a La Municipalidad Distrital de Amarilis S.A.	
	iii) En el lapso de notificación de finalización, es responsabilidad de la entidad supervisar la reproducción y copia no autorizada de datos significativos realizada por ex empleados y proveedores que han concluido su vínculo con la Municipalidad Distrital de Amarilis	
Objetivo de Control: Clasificación de la información		
Directrices de clasificación		
	i) Es necesario categorizar la información en dos grupos: una que esté disponible al público y otra que se mantenga en confidencial/privado.	
	ii) Considerar la importancia legal, el grado de confidencialidad y el significado de los datos para la Municipalidad Distrital de Amarilis.	
		- Examinar la salvaguardia de los datos a través de los 3 pilares de la información que son la confidencialidad, la integridad y la disponibilidad.
	iii) La evaluación de los datos/información se llevará a cabo de forma periódica, ya sea de manera anual o con una frecuencia de tres años.	
Etiquetado y manipulación de la información		
	i) Los métodos utilizados para el etiquetado correcto, la información debe abarcar tanto la información en sí como sus recursos (activos) relacionados en formatos físicos y electrónicos.	
	ii) Las etiquetas deben ser de fácil identificación.	
	iii) Los empleados deben estar informados acerca de los procedimientos de marcado/etiquetado.	
	iv) Los sistemas que contienen información considerada confidencial o crítica deben llevar una etiqueta de clasificación adecuada durante su producción.	

	v) Los responsables de los recursos deben supervisar la marcación de dichos recursos.	
	vi) En el caso de etiquetas físicas, los responsables de los recursos (activos) deben verificar que las etiquetas estén debidamente rotuladas y legibles.	
	vii) Cuando se da de baja un recurso (activo), es necesario mantenerlo registrado en el inventario correspondiente y especificar su estado actual.	
	viii) El almacenamiento de los recursos de tecnología de la información debe realizarse conforme a las indicaciones del fabricante.	
	ix) La protección de las copias de seguridad temporales o permanentes en otro lugar debe ser garantizada.	
Objetivo de Control: Manejo de los soportes de almacenamiento		
Gestión de activos extraíbles		
	i) Es necesario que todos los activos se almacenen en un ambiente seguro y protegido, de acuerdo con las indicaciones proporcionadas por los fabricantes.	
	ii) En caso de que se considere vital la confidencialidad o la integridad de la información, se recomienda emplear técnicas criptográficas para salvaguardar los datos almacenados en dispositivos removibles.	
	iii) La duplicación de datos de valor en distintos soportes es una práctica que ayuda a minimizar el riesgo de pérdida o daño accidental.	
	iv) Llevar un registro de los dispositivos removibles contribuye a reducir las posibles pérdidas de datos.	
	v) La habilitación de unidades de almacenamiento removibles solo debe realizarse cuando exista una justificación válida.	
	vi) Cuando sea necesario transferir información a estos medios removibles, se aconseja mantener un monitoreo constante de la operación.	
Eliminación de activos		
	i) Los recursos (activos) que alberguen información confidencial de la Municipalidad Distrital de Amarilis deben ser descartados de manera segura que asegure el borrado completo de datos.	
	ii) Establecer pautas o métodos para la identificación de los objetos que puedan necesitar una eliminación segura.	
		- Recopilar todos los objetos y llevar a cabo su eliminación de manera segura, en lugar de hacerlo de forma individual
	iv) En caso de contar con servicios de recolección, es importante seleccionar un proveedor externo apropiado para llevar a cabo la eliminación de los objetos.	
	v) En cuanto a la eliminación de elementos sensibles, se debe documentar adecuadamente para mantener un control efectivo.	

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D05**	

DOMINIO	**CONTROL DE ACCESOS**
OBJETIVO	Proteger los activos de información de la Municipalidad Distrital de Amarilis al garantizar que el acceso a ellos se conceda de manera adecuada y controlada, minimizando así los riesgos de seguridad.
Objetivo de Control: Requisitos de negocio para el control de accesos.	
Política de control de accesos	
	i) Administrar la autorización de los usuarios considerando su función, actividades, tareas y deberes, aspectos que determinarán los derechos de acceso a la información que les corresponda.
	ii) Los derechos de acceso a la información se concederán según un modelo de conocimiento de información mínimo, es decir, proporcionar acceso a la información indispensable para cumplir con sus responsabilidades. Esto se basa en la necesidad de tener y la necesidad de conocer.
	iii) La coordinación y aprobación de los accesos a la información deben ser gestionadas en cada función de la Municipalidad Distrital de Amarilis, responsabilidad que recae en los encargados o jefes de cada función y los propietarios de los activos.
	iv) Los derechos de acceso a la información deben cumplir con las reglas de protección de la información crítica para salvaguardar su integridad y confidencialidad.
	v) Con el propósito de asegurar una continuidad aceptable, todas las funciones relacionadas con la gestión de información crítica deben contar con un responsable principal y un sustituto.
	vi) Cualquier acceso a la información debe quedar registrado de forma que sea posible identificar al usuario y la razón de uso de la información en cuestión.
	vii) Implementar un procedimiento que registre los cambios en los privilegios de acceso a la información y que indique cuándo debe llevarse a cabo dicho cambio.
Control de acceso a las redes y servicios asociados	
	i) Establecer protocolos de autorización para determinar quiénes tienen permiso de acceso a redes y servicios correspondientes.
	ii) Los miembros del equipo solo pueden ingresar a la red y utilizar servicios que han sido previamente aprobados para su utilización.
	iii) Implementar una infraestructura de red dedicada a invitados.
	- Garantizar que cualquier visitante acceda exclusivamente a esta infraestructura.
	- Mantener la red de invitados completamente separada de las demás redes locales.
	- La contraseña de acceso a esta red debe modificarse cada dos meses.
	iv) El área de innovación tecnológica y TIC's de la Municipalidad Distrital de Amarilis debe implementar medidas de control en los servicios y redes con el fin de proteger su acceso.

	v) Es imperativo mantener un registro (log) de todos los intentos de acceso a los servicios y redes de la Municipalidad Distrital de Amarilis.	
	vi) Se requiere la solicitud de requisitos de autenticación de usuario para acceder a distintos servicios de red.	
	vii) Llevar a cabo una supervisión constante del uso de los servicios de red.	
Objetivo de Control: Gestión de acceso de usuario		
Registro de usuario y cancelación de registro		
	i) Instaurar un procedimiento formal de registro y expurgo de usuarios, el cual deberá ser minuciosamente documentado y difundido, reflejando en su estructura los pasos a seguir y los individuos responsables para llevar a cabo las siguientes acciones:	
		- Nombrar un administrador de accesos encargado de supervisar los perfiles y roles de los usuarios.
		- Crear un registro que consigne el ingreso de usuarios tanto internos como externos, incluyendo detalles como el nombre del solicitante, el entorno al que busca acceder, la base de datos que pretende utilizar, la fecha de caducidad, la estimación del tiempo de utilización y la justificación correspondiente.
		- Asignar y habilitar los accesos de los usuarios.
		- Modificar los accesos de los usuarios según sea necesario.
		- Desactivar o eliminar el acceso de aquellos usuarios que se retiren de la empresa.
		- Identificar y eliminar de manera periódica los accesos duplicados de los usuarios.
		- Asegurarse de que los accesos duplicados no sean transferidos a otros usuarios.
		- Suspender el acceso de los empleados que soliciten licencias o permisos temporales.
		- Asignar accesos temporales a terceros en función de su período de permanencia en la Municipalidad Distrital de Amarilis.
Gestión de derechos de acceso privilegiado		
	i) El control de la concesión de privilegios de acceso requiere la implementación de un proceso formal de autorización.	
	ii) La asignación de privilegios de acceso a los usuarios debe basarse en la justificación y necesidad correspondiente.	
	iii) Es esencial mantener un registro de los custodios de activos críticos y de los registros de acceso a su información asociada.	
	iv) Se debe designar un responsable suplente para administrar los activos críticos, con el objetivo de garantizar la continuidad operativa de la Municipalidad Distrital de Amarilis a un nivel aceptable.	
	v) En situaciones donde personal no responsable de un activo necesite acceder a información para realizar modificaciones, se requerirá una solicitud formal.	
	vi) La solicitud de acceso debe ser entregada tanto al responsable del activo crítico como a un depósito de registros, con el propósito de mantener un historial completo de solicitudes.	

	vii) La aprobación o rechazo de la solicitud solamente puede ser decidida por el responsable del activo crítico
	viii) Es imprescindible mantener un registro de las solicitudes de acceso a sistemas, bases de datos y aplicaciones que almacenen información crítica o confidencial.
	ix) En situaciones de emergencia o circunstancias excepcionales, la Gerencia puede solicitar por escrito la autorización para que un recurso acceda a activos críticos o información confidencial.
	x) Todo acceso otorgado mediante una solicitud formal debe ser supervisado por el responsable del activo crítico para supervisar las actividades y asegurar la integridad de la información.
	xi) Debe mantenerse una documentación actualizada del proceso de autorización de acceso y un registro completo de todos los privilegios asignados a los recursos de la Municipalidad Distrital de Amarilis.
	xii) Se deben establecer criterios para la expiración de los privilegios de acceso.
	xiii) Es necesario llevar a cabo revisiones periódicas de los privilegios de acceso otorgados a los usuarios para garantizar que estén alineados con sus responsabilidades dentro de la Municipalidad Distrital de Amarilis.
	xiv) Establecer métodos para prevenir la utilización indebida de permisos de acceso privilegiado.
Revisión de los derechos de acceso de los usuarios	
	i) La persona encargada de la gestión de activos debe llevar a cabo una evaluación periódica de los permisos de acceso de los usuarios, con un intervalo máximo de 1 mes (30 días).
	ii) La revisión y reasignación de los derechos de acceso de los usuarios debe ser realizada al cambiar de rol dentro de la misma organización.
	iii) Las autorizaciones para los privilegios de acceso deben someterse a revisiones frecuentes.
	iv) La asignación de privilegios debe ser objeto de verificaciones regulares para asegurar que no se haya producido la divulgación de privilegios no autorizados.
	v) Cualquier modificación realizada en las cuentas con privilegios debe ser debidamente registrada, incluyendo la fecha y el motivo, para facilitar su revisión periódica.
Eliminación o ajuste de los derechos de acceso	
	i) En el lapso de conclusión de los vínculos laborales de los trabajadores, contratistas y terceras partes con la Municipalidad Distrital de Amarilis, es imperativo considerar la revocación de los privilegios de autorización correspondientes.
Objetivo de Control: Responsabilidades del usuario	
Uso de información confidencial para la autenticación	
	i) Los empleados deben estar obligados a adherirse a las políticas establecidas por La Municipalidad Distrital de Amarilis S.A. en lo que respecta a la utilización de la información de autenticación confidencial.
	ii) Es imperativo mantener la confidencialidad de la información de autenticación secreta y garantizar que no se comparta con distintos departamentos, incluyendo personas en posiciones de autoridad.

	iii) Se debe evitar la retención de un registro (ya sea en forma física, en software o en dispositivos móviles) de la información de autenticación secreta, a menos que se pueda asegurar un método de almacenamiento seguro, previamente aprobado, como una bóveda de contraseñas.	
	iv) En el caso de que las contraseñas sean utilizadas como información de autenticación secreta, se deben establecer contraseñas que cumplan con los siguientes criterios:	
		- Deben tener una longitud mínima de caracteres.
		- Deben incluir caracteres especiales.
		- No pueden contener nombres, números de teléfono ni fechas de nacimiento.
		- No deben contener palabras que figuren en el diccionario.
		- Deben ser exentas de caracteres consecutivos idénticos, completamente numéricas o totalmente alfabéticas.
		- Si la contraseña es temporal, se debe requerir su cambio en el primer inicio de sesión.
	v) Queda prohibido compartir información de autenticación secreta con otros usuarios en ningún caso.	
	vi) Es crucial asegurar la protección adecuada de las contraseñas cuando se utilizan como información de autenticación secreta en procedimientos automatizados durante el proceso de inicio de sesión y en el almacenamiento automático.	
	vii) No se debe emplear la información de autenticación con fines comerciales o no comerciales en ningún contexto.	
Objetivo de Control: Control de acceso a sistemas y aplicaciones		
Restricción del acceso a la información		
	i) Es esencial implementar interfaces de usuario que permitan gestionar las autorizaciones relacionadas con las funcionalidades de las aplicaciones o entornos.	
	ii) Supervisar con precisión a qué datos puede acceder un usuario específico.	
	iii) Administrar las facultades de acceso de los usuarios, incluyendo, entre otras, las acciones de lectura, escritura, eliminación y ejecución.	
	iv) Regular los permisos de acceso otorgados a otras aplicaciones.	
	v) Restringir la información contenida en los contextos de aplicaciones o ambientes, garantizando una gestión adecuada de la confidencialidad y la integridad de los datos.	
Procedimientos de inicio de sesión seguros		
	i) El proceso de autenticación no deberá revelar datos relativos al sistema o aplicación, con el propósito de eludir la presentación a un usuario no autorizado de cualquier información que pudiera comprometer la integridad de la Municipalidad Distrital de Amarilis.	
	ii) El procedimiento de inicio de sesión deberá emitir un mensaje de advertencia indicando que únicamente usuarios autorizados tienen permiso para acceder al entorno o sistema.	
	iii) En el transcurso del proceso de inicio de sesión, no se deberán proporcionar indicaciones o asistencias a un usuario no autorizado.	

	iv) Verificar la información de inicio de sesión una vez el usuario haya completado todos los campos de entrada sugeridos. En caso de un fallo en la autenticación, el sistema no deberá señalar cuáles datos son correctos o incorrectos.	
	v) Mantener un registro de los intentos de inicio de sesión, tanto los fallidos como los exitosos.	
		- Registrar la fecha y hora del inicio de sesión exitoso.
		- Registrar los detalles del intento fallido de inicio de sesión desde el último acceso exitoso.
	vi) Durante el proceso de inicio de sesión, evitar mostrar la clave ingresada.	
	vii) Cerrar las sesiones inactivas después de un período de inactividad predefinido, especialmente en lugares de alto riesgo como áreas públicas o entornos externos fuera del alcance de la seguridad de la Municipalidad Distrital de Amarilis o en dispositivos móviles.	
	viii) Establecer un tiempo de conexión definido para reforzar la seguridad en aplicaciones o entornos de alto riesgo y reducir la probabilidad de acceso no autorizado.	
Sistema de gestión de contraseñas		
	i) El sistema de administración de contraseñas debe ser interactivo, de fácil usabilidad, y debe asegurar la eficacia en la generación de contraseñas.	
	ii) El sistema de administración de contraseñas debe estar bajo la supervisión de un administrador y dos usuarios alternativos.	
		- El administrador debe llevar a cabo respaldos diarios de los datos almacenados en el sistema, especialmente las cuentas.
	iii) El sistema de administración de contraseñas seleccionado debe ser multiusuario y contar con una capacidad de gestión de usuarios, grupos y perfiles.	
	iv) El sistema de administración de contraseñas debe cumplir con las siguientes características:	
		- Imponer la obligación de que los usuarios cambien su contraseña en su primer inicio de sesión.
		- Mantener un historial de contraseñas previamente utilizadas y prevenir su reutilización.
		- Garantizar que las contraseñas no sean visibles en pantalla durante el proceso de inicio de sesión.
		- Almacenar las contraseñas de manera cifrada y protegida.
		- Utilizar un protocolo web seguro como certificado SSL (Secure Sockets Layer), es decir, HTTPS.
		- Facilitar la compartición segura de contraseñas.
		- Permitir que, en situaciones de emergencia, el administrador pueda otorgar permisos excepcionales para acceder a contraseñas almacenadas en el sistema, con el objetivo de mantener la continuidad de negocio. Esto, por supuesto, debe hacerse con la autorización de la dirección.
		- Habilitar la realización de copias de seguridad de las cuentas almacenadas.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D06**	

DOMINIO	**CRIPTOGRAFÍA**
OBJETIVO	Proteger la información sensible de la Municipalidad Distrital de Amarilis mediante el uso de técnicas criptográficas, garantizando su confidencialidad, integridad y disponibilidad.
Objetivo de Control: Controles Criptográficos	
Política sobre el uso de controles criptográficos	
	i) Establecer el grado de salvaguardia necesario para los datos que se pretenden resguardar en el sistema, tomando en consideración aspectos tales como el tipo, robustez y la calidad del algoritmo de cifrado empleado.
	ii) Implementar salvaguardias criptográficas para asegurar la protección de las claves de acceso a los entornos, servidores, información y servicios.
	- Es esencial que dichas claves sean resguardadas mediante la técnica de cifrado cuando son almacenadas en la base de datos.
	iii) Establecer protocolos de gestión de claves en situaciones de extravío, reemplazo o deterioro de una clave.
	iv) Determinar los algoritmos de codificación que serán empleados en la Municipalidad Distrital de Amarilis, de acuerdo a los controles que se pretenden implementar.
	v) Implementar salvaguardias criptográficas al transmitir información confidencial fuera de los confines de la Municipalidad Distrital de Amarilis.
	vi) Emplear certificados electrónicos oficialmente reconocidos por el Estado para autenticar cualquier documento, transacción o interacción con el sistema, así como para las aplicaciones y otros procesos similares.
	- Estos certificados deben ser expedidos por organizaciones de renombre, que cumplan con estándares rigurosos y procedimientos adecuados.
Gestión de claves	
	i) Salvaguardar la integridad de todas las contraseñas, sin excepción, contra su alteración, aniquilación, duplicación o divulgación no autorizada.
	ii) Garantizar la idoneidad en la protección de contraseñas mediante aplicaciones que generen, almacenen y archiven claves de forma segura.
	iii) Realizar cambios periódicos o actualizaciones de las contraseñas.
	iv) Emitir y adquirir certificados de clave pública.
	v) Facilitar a los usuarios la clave y las instrucciones para activarla y confirmar su recepción. A través del correo electrónico se verificará la entrega de la clave. Se hace imperativo modificar la clave por defecto.
	vi) Establecer protocolos para la modificación o actualización de las contraseñas, así como las pautas para determinar cuándo y cómo llevar a cabo dichos cambios.
	vii) Mantener un registro siempre actualizado para la gestión de las claves.
	viii) Eliminar las claves que ya no se empleen.
	ix) Recuperar las claves extraviadas o dañadas.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D07**	

DOMINIO	**SEGURIDAD FÍSICA Y AMBIENTAL**
OBJETIVO	Salvaguardar la información de la Municipalidad Distrital de Amarilis frente a posibles amenazas y riesgos relacionados con el entorno físico y ambiental en el que se encuentra y evitar el acceso físico no autorizado.
Objetivo de Control: Áreas Seguras	
Perímetro de seguridad física	
	Las siguientes directrices deben ser tenidas en cuenta en relación a los perímetros de seguridad:
	i) Se requiere la delimitación de zonas de seguridad en la Municipalidad Distrital de Amarilis, en función de los requisitos de protección de los activos.
	ii) Las estructuras deben mantener su integridad física, sin presentar aberturas ni defectos, y deben contar con salvaguardias físicas para prevenir el acceso no autorizado.
	- Estas salvaguardias pueden comprender barreras, sistemas de alarma y dispositivos de cierre.
	iii) Es imprescindible contar con una zona de recepción para supervisar el acceso físico al edificio. Cabe enfatizar que dicho acceso debe ser restringido a personal debidamente autorizado.
	iv) Es necesario instalar sistemas de detección de incendios y puertas de evacuación, en cumplimiento de las normativas nacionales e internacionales aplicables.
	v) Se recomienda implementar un sistema de vigilancia que abarque las entradas exteriores y las ventanas accesibles, extendiendo su cobertura a áreas como la sala de reuniones y los pasillos.
	vi) Las instalaciones destinadas al procesamiento de información bajo la administración de la Municipalidad Distrital de Amarilis deben mantenerse físicamente separadas de aquellas administradas por terceros externos.
Controles físicos de entrada	
	i) Mantener un registro que incluya el registro de la fecha de ingreso, hora de llegada y hora de salida de individuos ajenos a la Municipalidad Distrital de Amarilis, como visitantes, clientes o proveedores.
	- Debe llevarse a cabo mediante un libro de registro físico o una plantilla electrónica. Es imperativo garantizar que todas las admisiones sean monitorizadas de manera segura.
	ii) La autenticación de la identidad de los visitantes o clientes se debe llevar a cabo mediante la presentación de documentos de identificación adecuados, como la cédula de identidad.
	iii) La supervisión de la entrada de visitantes o clientes es obligatoria, a menos que su ingreso haya sido previamente autorizado.

	iv) Es fundamental asegurarse de que todos los miembros del personal, visitantes, clientes y otras partes externas porten algún tipo de identificación o insignia de identificación visible.
	v) Los privilegios de acceso a zonas seguras deben ser revisados y actualizados en intervalos regulares, y estos cambios deben ser debidamente registrados y validados por la persona responsable.
Asegurar oficinas, habitaciones e instalaciones	
	i) Garantizar el cierre adecuado de las entradas y aberturas en ausencia de personal en el entorno de la oficina o en momentos en que la supervisión no esté presente.
	ii) Colocar los dispositivos de impresión, fotocopiado y escaneo en un enclave seguro.
	iii) Supervisar las infraestructuras críticas con el propósito de prevenir el acceso de individuos no autorizados.
	iv) Implementar cerraduras de alta seguridad en las puertas de acceso a la oficina.
Protección contra amenazas externas y ambientales	
	i) Es esencial buscar orientación especializada para el personal de respuesta ante emergencias, que incluye a bomberos, agentes de policía y personal militar, en cuanto a los protocolos a seguir en situaciones de sismos, inundaciones, incendios, movimientos telúricos o eventos catastróficos de origen humano.
	ii) Llevar a cabo una evaluación de las instalaciones eléctricas y ejecutar las labores de mantenimiento pertinentes, si fueran necesarias.
	iii) Realizar una inspección de los conductos de ventilación presentes en cada espacio de oficina y llevar a cabo las tareas de mantenimiento adecuadas en caso de requerirlas.
	iv) Ejecutar labores de mantenimiento en los sistemas de calefacción eléctrica ubicados en el interior de las oficinas.
El trabajo en áreas seguras	
	i) El personal debe tener conocimiento acerca de la existencia de zonas de seguridad.
	ii) Es imperativo ejercer control riguroso sobre las labores no supervisadas en las áreas seguras, tanto desde una perspectiva de seguridad integral como para prevenir actividades maliciosas que puedan comprometer la integridad de la Municipalidad Distrital de Amarilis.
	iii) Las áreas seguras desocupadas deben permanecer bajo llave y ser sometidas a inspecciones de manera regular.
	iv) La utilización de dispositivos como cámaras de vídeo, micrófonos y grabadoras, así como la activación de cámaras en dispositivos móviles, solo será autorizada previa autorización expresa.
Objetivo de Control: Seguridad de los equipos	
Ubicación y protección de equipos	
	i) Colocar los servidores en una zona restringida con el fin de reducir el acceso no autorizado.
	ii) Posicionar las instalaciones que manipulen datos confidenciales fuera del alcance de individuos no autorizados para prevenir la visualización de información durante su utilización.

	iii) Proteger los elementos que requieran una salvaguardia especial.
	iv) Asegurar las instalaciones de almacenamiento para evitar la entrada no autorizada.
	v) Implementar controles para mitigar el riesgo de posibles amenazas físicas o medioambientales, tales como explosiones, incendios, emisiones de humo, partículas de polvo, interferencias en las comunicaciones o radiación.
	vi) Establecer directrices que prohíban el consumo de alimentos, bebidas o tabaco en las áreas de procesamiento de información.
	vii) Identificar condiciones que puedan afectar el funcionamiento de las instalaciones de procesamiento de información, como la humedad y la temperatura.
Servicios de suministro	
	i) Registrar y consignar la inventariación de los recursos corporativos, tales como el abastecimiento hídrico, el sistema de calefacción, el control de la climatización, la ventilación y los servicios de alimentación eléctrica.
	ii) Mantener disponibles fuentes de energía interrumpible mediante Uninterruptible Power Supply, sistemas de alimentación ininterrumpida (UPS).
	iii) Supervisar de manera constante los sistemas de aprovisionamiento energético.
Seguridad del cableado	
	i) Salvaguardar la integridad del tendido de conductores mediante la implementación de un sistema de soporte, como un canalizador para cables u otro mecanismo apropiado, con el propósito de prevenir posibles perjuicios y desgaste.
	ii) Se aconseja la implementación de infraestructuras subterráneas para la transmisión de energía y datos en el ámbito de las telecomunicaciones y la energía eléctrica.
	iii) Etiquetar los conductores siguiendo las directrices establecidas por las normativas tanto nacionales como internacionales, con el objetivo de minimizar los errores asociados a su manipulación.
	iv) Es imperativo mantener una separación adecuada entre los cables destinados a la transmisión de energía y aquellos utilizados para las comunicaciones, con el fin de evitar cualquier interferencia indeseada.
	v) Registrar detalladamente la disposición del tendido de cables y las conexiones tanto alámbricas como inalámbricas de la Municipalidad Distrital de Amarilis en documentación oficial.
Mantenimiento de los equipos	
	i) Únicamente el personal especializado en labores de mantenimiento tiene la capacidad para llevar a cabo la reparación de los dispositivos en estado de deterioro.
	ii) Es esencial mantener un registro detallado de las incidencias y de todas las acciones emprendidas tanto en el mantenimiento preventivo como en el correctivo.
	iii) Previo a la puesta en marcha del equipo, es imprescindible asegurarse de que no ha sido objeto de manipulación, alteración o presenta un funcionamiento inadecuado.

	iv) Es fundamental adherirse a las pautas de mantenimiento propuestas por el fabricante del equipo.	
	v) En caso de requerirse, la información debe ser eliminada de la unidad, generando una copia de respaldo de la misma.	
Eliminación de activos		
	i) Es imperativo definir un plazo temporal concreto con el propósito de proceder con la liquidación de los recursos patrimoniales.	
	ii) Los recursos patrimoniales han de ser consignados como desvinculados de la Municipalidad Distrital de Amarilis cuando se torne pertinente y ajustado.	
	iii) Es esencial dejar constancia de la identificación, función y vinculación de la persona encargada de la administración o utilización de los recursos patrimoniales que serán objeto de eliminación.	
Seguridad de los equipos y activos fuera de las instalaciones		
	i) Vigilar los dispositivos y recursos que salgan de la Municipalidad Distrital de Amarilis en entornos de acceso público.	
	ii) Examinar las directrices proporcionadas por los fabricantes con el fin de garantizar la seguridad de los dispositivos en cualquier entorno.	
	iii) Fiscalizar las labores ejecutadas en dispositivos o medios fuera del entorno de la Municipalidad Distrital de Amarilis mediante una evaluación de riesgos, implementando las medidas de control apropiadas según lo requerido.	
	iv) Debe conservarse un registro de la cadena de custodia de los dispositivos en caso de transferencia entre múltiples individuos o entidades externas, debiendo incluir los nombres de las personas y la afiliación organizativa de los responsables del equipo.	
Eliminación segura o reutilización de equipo		
	i) Los dispositivos dañados en la Municipalidad Distrital de Amarilis deben someterse a una evaluación con el propósito de determinar si se requiere su destrucción física en lugar de su reparación o su descarte. Es importante señalar que la negligente eliminación puede poner en riesgo la seguridad de la información.	
	ii) Se hace imprescindible llevar a cabo el proceso de cifrado del disco, ya que esto disminuye de manera significativa la exposición de información confidencial.	
	iii) Únicamente es viable desechar un dispositivo cuando se cumplen las siguientes condiciones:	
		- El nivel de fortaleza del proceso de encriptación es suficiente y cubre la totalidad del disco, incluyendo el espacio libre.
		- Las claves de cifrado son de considerable longitud.
		- Las claves de cifrado se mantienen bajo estricta confidencialidad.
Equipo informático de usuario desatendido		
	i) Es imperativo desconectar el equipo no supervisado de las aplicaciones, entornos o servicios de red tan pronto como su utilidad haya concluido.	
	ii) Las sesiones activas en el equipo no supervisado deben ser finalizadas mediante un mecanismo de bloqueo, como la activación de un protector de pantalla protegido por una contraseña.	

	iii) La salvaguarda de las computadoras o dispositivos móviles contra el acceso no autorizado se logra mediante la implementación de un control basado en credenciales, ya sea mediante contraseñas o tokens.
Política de escritorio y pantalla clara	
	i) La salvaguardia de la información comercial sensible o crítica de la Municipalidad Distrital de Amarilis, tanto en formato físico como electrónico, requiere la implementación de medidas de seguridad apropiadas, como el resguardo en una instalación segura, como una caja de seguridad o armario, y su recuperación cuando sea necesario.
	ii) Durante los períodos en los que la computadora no se encuentre en uso, es esencial desconectarla o aplicar medidas de protección, como el bloqueo de la pantalla y el teclado mediante una contraseña o un mecanismo de autenticación.
	iii) Para mitigar los riesgos de acceso no autorizado y la posible exposición de la información, se recomienda mantener la pantalla del escritorio libre de información confidencial durante y después de las horas laborables en la Municipalidad Distrital de Amarilis.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D08**	

DOMINIO	**SEGURIDAD DE OPERACIONES**
OBJETIVO	Garantizar que las operaciones de la Municipalidad Distrital de Amarilis se realicen de manera segura y sin interrupciones debido a amenazas de seguridad, lo que contribuye a proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos.
Objetivo de Control: Responsabilidades y procedimientos de operación	
Documentación de procedimientos de operación	
	i) Registrar documentariamente el proceso y gestión de información, tanto de manera automatizada como manual.
	ii) Registrar documentariamente la configuración de los sistemas informáticos.
	iii) Registrar documentariamente los requisitos de programación, incluyendo las interdependencias con otros sistemas.
	iv) Registrar documentariamente el procedimiento para gestionar errores, limitaciones y excepciones que puedan surgir durante la ejecución.
	v) Registrar documentariamente el procedimiento de reinicio en caso de fallo del sistema.
	vi) Registrar documentariamente los contactos de los diversos clientes en caso de sucesos inusuales.
	vii) Registrar documentariamente el procedimiento de reproducción de páginas de prueba.
	vii) Registrar documentariamente la configuración del navegador para la utilización del sistema por parte del cliente.
Gestión del cambio	
	i) Detección y registro de modificaciones sustanciales.
	ii) Elaboración y ejecución de pruebas para las modificaciones.
	iii) Análisis de los potenciales efectos, incluyendo aquellos relacionados con la seguridad de la información.
	iv) Es necesario establecer un procedimiento formal de autorización para implementar las modificaciones deseadas.
	v) Transmitir los detalles de la modificación al personal pertinente.
	vi) Comprobación de la conformidad con los requisitos de seguridad de la información.
	vii) Asignar responsables de la gestión de cambios en los equipos y software.
Gestión de capacidades	
	i) Llevar a cabo la supresión de información redundante con el propósito de liberar capacidad de almacenamiento en el disco.
	ii) Mejorar la eficiencia de los procedimientos y aplicaciones mediante la ejecución en lotes.
	iii) Optimizar la estructura lógica de la aplicación y automatizar las solicitudes hacia la base de datos.

	iv) Limitar la capacidad de transferencia de datos, especialmente en relación a los servicios que demandan significativos recursos si no son esenciales ni vitales para las operaciones empresariales.
Separación de entornos de desarrollo, pruebas, producción y capacitación	
	i) Es esencial elaborar la documentación relativa a las normativas concernientes a la migración de software desde el entorno de desarrollo hacia el entorno de producción.
	ii) Se recomienda segregar los entornos de desarrollo, pruebas, producción y capacitación, garantizando su aislamiento.
	iii) Previo a cualquier modificación en los sistemas de producción, es imperativo llevar a cabo pruebas exhaustivas en un entorno de preproducción, antes de aplicar dichos cambios en el ambiente de producción.
	iv) Es fundamental crear un entorno de pruebas que sea lo más similar posible al entorno de producción.
	v) Los entornos de desarrollo y producción deben operar en sistemas, dominios o directorios separados.
	vi) Es necesario establecer distintos perfiles de usuarios para los entornos de desarrollo, pruebas y producción.
	vii) En los entornos de pruebas, se debe evitar la replicación de información confidencial.
	viii) En situaciones de extrema necesidad, se deberá solicitar una autorización previa cuando el personal de desarrollo requiera acceso al entorno de producción.
Objetivo de control: Protección contra código malicioso	
Protección contra el código malicioso	
	i) Garantizar que únicamente se utilice software debidamente autorizado en la Municipalidad Distrital de Amarilis.
	ii) Garantizar que los sistemas operativos y sistemas de procesamiento de datos estén siempre al día mediante la instalación de las últimas versiones disponibles.
	iii) Garantizar que todos los ordenadores sin software antivirus y contra código malicioso sean equipados con estas soluciones de seguridad.
	iv) Planificar acciones específicas para restablecer la operatividad de sistemas y aplicaciones tras incidentes de malware, incorporando medidas de respaldo y recuperación.
	v) Establecer procesos para la recopilación constante de datos provenientes de sitios web que difunden información sobre malware emergente.
	vi) Generar contenido educativo relacionado con amenazas de seguridad informática, como virus y código malicioso.
	vii) Sensibilizar al equipo de trabajo sobre el impacto de los virus y la forma de reaccionar ante esta peligrosa amenaza.
Objetivo de control: Copia de Seguridad	
Copia de seguridad de la información	
	i) Establecer directrices de etiquetado para las copias de seguridad que incluyan la marcación de su contenido, fecha y política de retención.
	ii) Conforme a los requisitos establecidos por la Municipalidad Distrital de Amarilis, es imperativo definir la naturaleza y la frecuencia de los respaldos,

	considerando la opción entre respaldos completos y diferenciales, así como la cadencia en días, meses o años.
	iii) Es esencial garantizar que las copias de seguridad cuenten con registros exhaustivos y procedimientos de restauración debidamente documentados.
	iv) Las copias de seguridad deben ser almacenadas en una ubicación remota para resguardar su integridad.
	v) La seguridad de las copias de seguridad se debe reforzar mediante el uso de técnicas de cifrado.
	vi) Se requiere establecer protocolos para el retiro y archivo de las copias de seguridad al alcanzar el fin de su ciclo de vida.
	vii) La capacidad de recuperación de datos respaldados debe ser sometida a pruebas rigurosas en entornos de prueba y no debe realizarse la sobreescritura en el entorno de producción.
	viii) Los medios de respaldo deben ser evaluados periódicamente para asegurar su idoneidad en situaciones de emergencia o cuando su uso sea necesario.
Objetivo de control: Registro y monitoreo	
Registro de eventos	
	i) Efectuar el registro de identificaciones de usuarios.
	ii) Efectuar el registro de identificaciones de usuarios.
	iii) Registrar información sobre fechas, horarios y detalles de eventos críticos, como el inicio de sesión y el cierre de sesión.
	iv) Documentar los intentos de acceso exitosos y los rechazos del sistema.
	v) Documentar los cambios efectuados en la configuración del sistema.
	vi) Registrar el uso de utilidades y aplicaciones del sistema.
	vii) Realizar el seguimiento y registro de las direcciones de red y los protocolos utilizados.
	viii) Capturar las alarmas planificadas por el sistema de control de acceso.
	ix) Registrar las transacciones llevadas a cabo por los usuarios en diversos entornos.
Protección del registro de la información	
	i) Salvaguardar las modificaciones en las categorías de mensajes bajo registro.
	ii) Resguardar los ficheros de registro que están siendo objeto de edición o supresión.
	iii) Comprobar la capacidad de retención de los medios empleados en el registro.
Registro de actividad del administrador y operador del sistema	
	i) Conservar el archivo con los siguientes datos como; El instante en que se produjo el suceso, Datos minuciosos acerca del incidente, La identificación del administrador y del usuario encargado; y Procedimientos vinculados.
Sincronización del reloj	
	i) Coordinar la temporización de los sistemas de procesamiento de información según un protocolo o servicio de tiempo en red con el fin de conservar su sincronización en una marca temporal precisa.
	ii) Supervisar la configuración de los relojes para optimizar la precisión de los registros de auditoría.

	iii) Tomar en cuenta las especificaciones locales para ajustar la fecha y hora, por ejemplo, en función de la ubicación geográfica, en el caso de brindar asistencia a clientes internacionales.	
	iv) Garantizar una configuración adecuada de los relojes con el propósito de obtener registros de alta precisión.	
Objetivo de Control: Control del software de explotación		
Instalación de software en sistemas de producción		
	i) La etapa de despliegue en el entorno productivo solo debe ejecutarse después de haber realizado pruebas exhaustivas con resultados satisfactorios. Es necesario llevar a cabo pruebas que abarquen aspectos como la usabilidad, la seguridad, el impacto en otros sistemas y la fiabilidad.	
	ii) Los entornos de producción deben contener exclusivamente el código ejecutable que ha sido previamente autorizado, excluyendo así cualquier código de desarrollo.	
	iii) Se requiere establecer una estrategia de revisión antes de llevar a cabo la implementación de cambios.	
	iv) Es imperativo mantener un registro de auditoría que documente todas las actualizaciones realizadas en el entorno de producción.	
	v) Se debe conservar versiones previas de los entornos de producción como una medida de contingencia.	
	vi) Las versiones anteriores de los entornos de producción deben ser archivadas junto con toda la información relevante, parámetros necesarios, procedimientos y detalles de configuración.	
Objetivo de Control: Gestión de la vulnerabilidad técnica		
Gestión de las vulnerabilidades técnicas		
	i) Cuando se detecta una deficiencia técnica, La Municipalidad Distrital de Amarilis se ve en la necesidad de reconocer los peligros vinculados y las medidas que deben ser adoptadas.	
		- Las medidas a implementar han de llevarse a cabo en concordancia con las regulaciones asociadas a la gestión de modificaciones o siguiendo los protocolos para hacer frente a incidencias de seguridad de la información.
		- La supervisión y evaluación periódica de la gestión de deficiencias es esencial.
	ii) Es imperativo que los ajustes sean sujetos a una aprobación y revisión rigurosa antes de su implementación, con el fin de asegurar su eficacia y eficacia.	
Restricciones en la instalación de software		
	i) Reconocer cuáles categorías de implementaciones de software son admisibles, tales como las relacionadas con mejoras en la seguridad y correcciones de vulnerabilidades.	
	ii) Determinar cuáles clases de implementaciones están vedadas, como aquellas dedicadas exclusivamente al uso personal de software.	
	iii) Es imperativo otorgar los permisos de implementación de manera ponderada, considerando cuidadosamente la función que desempeña el usuario en cuestión.	

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	PSIMDA – D09	

DOMINIO	SEGURIDAD DE LAS COMUNICACIONES
OBJETIVO	Proteger la confidencialidad, integridad y disponibilidad de la información que se transmite a través de diversas tecnologías de comunicación, como redes, correo electrónico y mensajería instantánea, entre otras.
Objetivo de Control: Gestión de seguridad en las redes.	
Control de red	
	i) Asignar encargados y elaborar protocolos que gestionen la administración de las infraestructuras de comunicación.
	ii) Es imperativo instaurar medidas de seguridad con el propósito de preservar la confidencialidad e integridad de los datos mediante la redirección de puertos y el acceso a través de una Red Privada Virtual VPNs.
	iii) Se requiere llevar a cabo procesos de autenticación en los sistemas de comunicación en red.
	iv) Es fundamental imponer restricciones en la conectividad de los sistemas de comunicación en red.
	v) Realizar una supervisión adecuada para identificar acciones que puedan poner en riesgo la continuidad del sistema.
	vi) Contar con documentación que describa la estructura de las redes que abarcan las conexiones de datos, Internet y las redes locales de la Municipalidad Distrital de Amarilis.
	vii) Desarrollar mecanismos de control para garantizar la confidencialidad e integridad de los datos transmitidos a través de redes públicas o inalámbricas.
Mecanismos de seguridad asociados a servicios de red.	
	i) Integrar tecnologías destinadas a garantizar la seguridad de los servicios de red, tales como métodos de autenticación avanzados, protocolos de encriptación robustos y mecanismos de control de sesiones.
	ii) Desarrollar procedimientos que impongan restricciones al acceso a servicios o aplicaciones en la red en los casos en que resulte indispensable.
	iii) Establecer los parámetros técnicos requeridos para establecer conexiones seguras con los servidores de red, de conformidad con las normativas de seguridad y las políticas de interconexión de la infraestructura de red.
Segregación de redes	
	i) Fragmentar la infraestructura de red en múltiples dominios de red. Estos dominios pueden ser seleccionados en base a criterios de seguridad, como el nivel de confianza, por ejemplo (dominio de acceso público, acceso a servidores, acceso a entornos específicos).
	ii) La delimitación de cada entorno debe ser claramente establecida mediante dispositivos de conexión, como cortafuegos o enrutadores de filtrado, por ejemplo.

	iii) La gestión de redes inalámbricas requiere una atención particular debido a la definición de su perímetro de red.
Objetivo de Control: Intercambio de información con partes externas	
Políticas y procedimientos de intercambio de información	
	i) Elaborar protocolos concebidos con el propósito de salvaguardar la información intercambiada contra la replicación, alteración, desvío y aniquilamiento.
	ii) Formular procedimientos que posibiliten la identificación y salvaguarda contra el software malicioso.
	iii) Establecer pautas operativas para el resguardo de la información electrónica de naturaleza confidencial.
	iv) Aplicar estrategias criptográficas, como ejemplarmente la encriptación, con el fin de preservar la confidencialidad, integridad y autenticidad de la información.
	v) Sensibilizar al personal respecto a la importancia de adoptar precauciones adecuadas para evitar la divulgación de información de carácter confidencial.
	vi) Evitar depositar información sensible en dispositivos de copiado, impresión o superficies de trabajo.
	vii) Abstenerse de revelar datos confidenciales mientras se mantiene una comunicación telefónica activa.
	viii Abstenerse de dejar mensajes que incluyan información confidencial en sistemas de contestación automática, dado que podrían ser accesibles por individuos no autorizados.
Acuerdos de intercambio	
	i) Establecer directrices de gestión con el propósito de supervisar y comunicar la transferencia, el despacho y la recepción.
	ii) Formular protocolos para garantizar la trazabilidad y la autenticación.
	iii) Instaurar estándares técnicos mínimos para el envasado y la transmisión segura de datos.
	iv) Consensuar responsabilidades ante eventualidades en la seguridad de la información, como, por ejemplo, la pérdida de datos.
	v) Utilizar un sistema de etiquetado para información confidencial o crítica, asegurándose de que las etiquetas sean legibles.
	vi) Mantener una cadena de custodia para los datos en tránsito.
Mensajería instantánea	
	i) Garantizar la adecuada enrutación y la transmisión precisa del mensaje.
	ii) Sustentar la integridad y la continuidad operativa del servicio.
	iii) Implementar niveles robustos de autenticación que gestionen la entrada desde redes de acceso público.
Acuerdos de confidencialidad y secreto	
	i) Evaluar la estimación temporal de un convenio, incluso en situaciones en las cuales sea imperativo preservar la confidencialidad.
	ii) Prescribir las medidas requeridas al concluir un convenio.

	iii) Estipular los parámetros para la restitución o eliminación de información en el momento de la terminación contractual.
	iv) La rúbrica de acuerdos de confidencialidad se impone de manera universal a todos los empleados de La Municipalidad Distrital de Amarilis S.A., sin excepción alguna.
	v) Precisar la naturaleza de los datos a resguardar, como, por ejemplo, los datos considerados como confidenciales.
	vi) Exponer de manera pormenorizada las acciones a seguir en caso de que se incumpla con las disposiciones del convenio.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D10**	

DOMINIO	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**
OBJETIVO	Garantizar que la integridad de la información se convierta en un elemento fundamental en la arquitectura de los sistemas de información de la Municipalidad Distrital de Amarilis.

Objetivo de Control: Requisitos de seguridad de los sistemas de información.	
Análisis y especificación de los requisitos de seguridad de la información	
	i) Configurar los criterios de seguridad, tales como (Encriptación, Gestión de sesiones).
	ii) Notificar a los usuarios y operadores acerca de sus obligaciones y responsabilidades.
	iii) Establecer los requisitos de seguridad y los mecanismos necesarios, tomando en consideración el impacto económico y las posibles consecuencias de un fallo en la seguridad.
	iv) Evaluar las demandas de salvaguardia necesarias para los recursos implicados en cuanto a su disponibilidad, confidencialidad e integridad.
Protección de las transacciones por redes telemáticas	
	i) Contemplar la aplicación de rúbricas electrónicas por parte de todas las entidades participantes.
	ii) El canal de transmisión entre todas las partes interesadas se halla sometido a un proceso de cifrado.
	iii) Implementar salvaguardias para los protocolos empleados en las comunicaciones con las entidades involucradas.
Objetivo de Control: Seguridad en los procesos de desarrollo y soporte	
Política de desarrollo seguro de software	
	i) Tener en cuenta la implementación de entornos de desarrollo resistentes a amenazas.
	ii) Garantizar la integridad en todas las etapas del ciclo de vida del desarrollo de software, como; Garantizar la seguridad en la metodología de desarrollo de software y Establecer directrices de codificación segura específicas para cada lenguaje de programación empleado.
	iii) Especificar requisitos relacionados con la seguridad durante la fase de diseño.
	iv) Emplear repositorios de código seguros.
	v) Poner un fuerte énfasis en la seguridad en el proceso de control de versiones.
	vi) Concientizar al personal sobre las necesidades de seguridad en las aplicaciones.
	vii) Establecer puntos de control de seguridad en los hitos clave del proyecto.
	viii) Fomentar la capacidad de los desarrolladores para identificar y solucionar vulnerabilidades, así como para prevenirlas.

Procedimientos de control de cambio del sistema	
	i) Asegurar que las modificaciones sean emitidas por usuarios con la debida autorización.
	ii) Evaluar los mecanismos de control y los procedimientos de integridad con el fin de prevenir su compromiso debido a las alteraciones.
	iii) Identificar y autenticar el código crítico de seguridad para reducir la probabilidad de vulnerabilidades de seguridad ampliamente conocidas.
	iv) Verificar que los cambios sean aprobados por usuarios con autorización previa a su implementación.
	v) Mantener un sistema de versionamiento para registrar todas las actualizaciones del software.
	vi) Garantizar que la ejecución de las modificaciones ocurra en el momento apropiado sin ocasionar interrupciones en los procesos empresariales.
Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	
	i) Examinar los protocolos de supervisión de la aplicación con el fin de cerciorarse de que no se hayan visto comprometidos por las modificaciones en el entorno del sistema operativo.
	ii) Verificar que la notificación de las modificaciones en la infraestructura operativa sea entregada de manera oportuna para posibilitar pruebas y revisiones previas a la implementación.
	iii) Asegurarse de que se efectúen las adecuadas adaptaciones en los planes de continuidad empresarial.
Restricciones a los cambios en los paquetes de software	
	i) Interoperabilidad con otro software en funcionamiento.
	ii) Aprobación del proveedor del conjunto de software.
	iii) Posibilidad de que las modificaciones incorporadas enfrenten desafíos.
	iv) Ajustes necesarios por parte del proveedor, como mejoras normativas del programa.
Entorno de desarrollo seguro	
	i) Garantizar la procedencia de los datos del entorno de origen, asegurando la autenticidad de las fuentes y preservando su integridad a lo largo de todo el ciclo de vida dentro del sistema.
	ii) Cumplimiento de los requisitos tanto internos como externos, incluyendo normativas y políticas pertinentes.
	iii) Gestión de los mecanismos de acceso al ambiente de desarrollo.
	iv) Las copias de respaldo se resguardan en ubicaciones externas al sitio principal.
	v) Implementación de la segregación entre distintos entornos de desarrollo.
	vi) Supervisión constante de los cambios ocurridos en el entorno y en el código alojado en el mismo.
	vii) Confianza en la idoneidad del personal que labora en el entorno.
	viii) Ejercicio de un control riguroso sobre el flujo de datos hacia y desde el entorno.
Pruebas de aceptación	

	i) Emplear soluciones automatizadas destinadas a la evaluación del código o a sistemas de detección de debilidades con el propósito de analizar las imperfecciones.
	ii) Es esencial llevar a cabo las evaluaciones en un ambiente de pruebas realista con el fin de asegurar que no se incorporen vulnerabilidades al entorno de la Municipalidad Distrital de Amarilis y que las pruebas sean de confianza.
Pruebas de funcionalidad durante el desarrollo de los sistemas	
	i) Los sistemas recién desarrollados y las versiones actualizadas necesitan someterse a pruebas minuciosas y verificaciones rigurosas durante las fases de desarrollo.
	ii) La responsabilidad de llevar a cabo las pruebas de funcionalidad recae en el equipo de desarrollo.
	iii) El alcance de las pruebas debe ser adecuado en relación con la relevancia y la naturaleza del sistema en cuestión.
Objetivo de Control: Datos de prueba	
Protección de los datos usados en las pruebas	
	i) Solicitar una autorización de forma individual en cada ocasión en que se efectúe una duplicación de datos en un entorno de evaluación.
	ii) Conducir pruebas de los sistemas en el entorno de pruebas utilizando información obtenida del entorno de producción.
	iii) Realizar modificaciones en los datos dentro del ámbito de pruebas con el propósito de lograr resultados satisfactorios.
	iv) Borrar de inmediato, una vez culminadas las pruebas, la información proveniente del entorno de producción.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	PSIMDA – D11	

DOMINIO	RELACIONES CON PROVEEDORES
OBJETIVO	Proteger la información de la Municipalidad Distrital de Amarilis cuando se comparte o se trabaja con proveedores externos, garantizando que se mantenga la confidencialidad, integridad y disponibilidad de los datos críticos.

Objetivo de Control: Seguridad de la información en las relaciones con proveedores	
Política de seguridad de la información para proveedores	
	i) Identificar y registrar las categorías de proveedores, tales como servicios de tecnología de la información, soluciones logísticas, servicios financieros, y componentes de infraestructura de TI, a los cuales la empresa otorgará permisos para acceder a su base de datos.
	ii) Establecer un procedimiento concreto para administrar las relaciones con los proveedores.
	iii) Diseñar protocolos y métodos para supervisar el cumplimiento de los requisitos de seguridad de la información establecidos para cada categoría de proveedores y su nivel de acceso correspondiente.
	iv) Gestionar eventualidades e imprevistos vinculados al acceso otorgado a los proveedores, incluyendo las responsabilidades tanto de la empresa como de los proveedores.
	v) Impartir instrucción al personal de la Municipalidad Distrital de Amarilis que interacciona con los proveedores respecto a las normativas adecuadas de interacción y conducta basadas en la tipología de proveedor y en su nivel de acceso a los sistemas e información corporativa.
	vi) Definir acuerdos relativos a los niveles de servicio de asistencia y mantenimiento con los proveedores.
Tratamiento del riesgo dentro de acuerdos con proveedores	
	i) Establecer estrategias para facilitar o habilitar la obtención o acceso a datos.
	ii) Categorizar la información conforme al sistema de clasificación de la Municipalidad Distrital de Amarilis
	iii) Evaluar los requisitos legales y normativos, incluyendo la salvaguardia de información confidencial, derechos de propiedad intelectual y derechos de autor, junto con una descripción de los métodos para asegurar el cumplimiento de estos requisitos.
	iv) Formular directrices de seguridad de la información pertinentes al contrato con el proveedor.
	v) Poseer el derecho de llevar a cabo auditorías de los procedimientos y controles implementados por el proveedor en relación con el acuerdo.
	vi) Exigir que el proveedor entregue de manera periódica un reporte independiente sobre la efectividad de los mecanismos de control y los términos de servicio establecidos en el contrato.

Objetivos de Control: Gestión de la prestación del servicio por parte de los proveedores		
Supervisión y revisión de los servicios prestados por terceros		
	i) Supervisar el rendimiento del servicio y realizar una comparación con los acuerdos de conformidad.	
	ii) Programar encuentros y analizar los informes derivados del desempeño del servicio proporcionado por terceros.	
	iii) Suministrar datos acerca de los incidentes de seguridad de la información y efectuar revisiones periódicas según lo requerido.	
	iv) Resolver y administrar cualquier inconveniente identificado.	
	v) Evaluar los aspectos relativos a la seguridad de la información junto al proveedor.	
	vi) Verificar que el proveedor mantenga una capacidad de servicio adecuada para garantizar los niveles de continuidad.	
Gestión de cambios de los servicios prestados por terceros		
	i) Administrar modificaciones en los acuerdos con los proveedores de manera que no sean detectadas por un sistema de detección de similitudes.	
	ii) Supervisar las modificaciones efectuadas en la estructura organizativa con el fin de llevar a cabo:	
		- Optimizaciones en los servicios proporcionados.
		- El desarrollo de nuevas aplicaciones y sistemas.
		- Alteraciones o actualizaciones en las políticas y procedimientos de la Municipalidad Distrital de Amarilis.
		- La implementación de controles nuevos o ajustados con el propósito de abordar incidentes de seguridad de la información y reforzar la seguridad.
	iii) Gestionar las transformaciones en los servicios del proveedor con el objetivo de poner en marcha:	
		- Alteraciones realizadas y mejoras en las infraestructuras de red.
		- La adopción de nuevas tecnologías.
		- La incorporación de nuevos productos o versiones.
		- La integración de herramientas novedosas y la adopción de entornos de desarrollo.
		- Cambios en la ubicación física de las instalaciones de prestación de servicios.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	PSIMDA – D12	

DOMINIO	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
OBJETIVO	Proteger la información de la Municipalidad Distrital de Amarilis y minimizar los riesgos relacionados con la seguridad de la información a través de una gestión eficiente de incidentes.

Objetivo de Control: Gestión de incidentes de seguridad de la información.	
Notificación de los eventos de seguridad de la información	
	i) Violación de la triada de seguridad de la información, que abarca la autenticidad, la confidencialidad y la disponibilidad.
	ii) Fallos de origen humano.
	iii) No cumplimiento de las directrices o políticas establecidas.
	iv) Incumplimiento de las normativas relacionadas con la salvaguarda de la seguridad física.
	v) Modificaciones no supervisadas en el entorno del sistema.
	vi) Disfunción en el software o el hardware.
	vii) Quebrantos en la seguridad de acceso.
Respuesta a los incidentes de seguridad de la información	
	i) Recopilar pruebas lo más pronto posible tras la ocurrencia.
	ii) Realizar análisis de seguridad de la información forense, conforme a lo requerido.
	iii) Garantizar que todas las actividades de respuesta sean debidamente registradas para su ulterior análisis.
	iv) Notificar la presencia del incidente de seguridad de la información o cualquier detalle pertinente.
	v) Abordar las vulnerabilidades de la seguridad de la información identificadas que causen o contribuyan al incidente.
	vi) Una vez que el incidente haya sido gestionado con éxito, proceder a su cierre formal y documentarlo.
Aprendizaje de los incidentes de seguridad de la información	
	i) Los datos adquiridos mediante la evaluación de los incidentes deben integrarse en una base de datos de conocimiento con el propósito de identificar cuáles son los incidentes más persistentes y definir estrategias para su resolución.
	ii) Elaborar un registro de la cantidad de incidentes categorizados por su tipología y de acuerdo con el tiempo requerido para su resolución.
	iii) Calcular el promedio de gastos asociados a cada incidente.
	iv) Calcular la frecuencia de ocurrencia de incidentes recurrentes.
	v) Evaluar la frecuencia con la que se presenta un incidente recurrente.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	**PSIMDA – D13**	

DOMINIO	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
OBJETIVO	Salvaguardar la información esencial de las Municipalidad Distrital de Amarilis mientras se garantiza que la organización pueda seguir funcionando de manera efectiva en situaciones adversas.

Objetivo de Control: Continuidad de la seguridad de la información		
Planificación de la continuidad de la seguridad de la información		
	i) El personal a cargo del área de innovación tecnológica y TIC's será nombrado como el supervisor de la continuidad de los servicios informáticos, encargado de la supervisión del procedimiento de concepción e implementación del plan de continuidad, así como de la protección del personal.	
	ii) Desarrollar la directriz para la continuidad de los servicios informáticos, definiendo los metas y el ámbito del plan, junto con las funciones y deberes correspondientes; un documento que establezca de manera integral los metas, ámbito y responsabilidades relacionadas con la gestión de la continuidad.	
Implantación de la continuidad de la seguridad de la información		
	i) Contar con un equipo de respuesta a incidentes debidamente facultado, con la competencia y autoridad necesaria para supervisar un evento adverso y salvaguardar la integridad de los datos.	
	ii) Elaborar documentos de planificación, así como procedimientos de respuesta y recuperación, donde se describa en detalle la manera en que la Municipalidad Distrital de Amarilis administrará eventos adversos y mantendrá el resguardo de la seguridad de la información en un nivel constante.	
	iii) Determinar el contenido y formato de los mensajes a ser emitidos en caso de una situación de desastre o de una vulneración de seguridad.	
Verificación, revisión y evaluación de la continuidad de la seguridad de la información		
	i) Llevar a cabo un examen de los procedimientos relacionados con la continuidad de la seguridad de la información en la Municipalidad Distrital de Amarilis, con el propósito de evaluar su operatividad y eficiencia en el contexto empresarial.	
	ii) Validar y verificar la efectividad de las directrices adoptadas para garantizar la continuidad de la seguridad de la información ante situaciones de desastre. Realizar pruebas como:	
		- Validez: someter el plan a un análisis crítico y una discusión exhaustiva.
		- Simulación: crear un escenario que permita poner a prueba la aplicabilidad del plan de continuidad.
		- Actividades críticas: realizar pruebas en un entorno controlado para las operaciones esenciales.
		- Prueba completa: llevar a cabo una interrupción real y aplicar el plan de continuidad en su totalidad.

	iii) Ejecutar de manera efectiva el plan de continuidad, implementando las estrategias y procesos previamente desarrollados.
	iv) La evaluación y revisión anual del plan de continuidad de La Municipalidad Distrital de Amarilis S.A. es una práctica necesaria.
Objetivo de Control: Redundancias	
Disponibilidad de instalaciones para el procesamiento de información	
	i) Identificar los requerimientos comerciales relacionados con la disponibilidad de los sistemas de información.
	ii) Se desaconseja la utilización de la estructura arquitectónica preexistente del sistema, especialmente en lo que respecta a componentes duplicados.
	iii) Es imperativo llevar a cabo pruebas exhaustivas en los sistemas de información redundantes con el fin de garantizar que los componentes operen de acuerdo a las especificaciones establecidas.
	iv) La inclusión de medidas redundantes en la implementación puede conllevar riesgos potenciales para la integridad y la confidencialidad de los datos, factores que deben ser debidamente considerados durante la fase de diseño de sistemas de información.

	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS	PSIMDA – D14	

DOMINIO	CUMPLIMIENTO
OBJETIVO	Garantizar que la Municipalidad Distrital de Amarilis cumpla con las leyes, regulaciones y normativas aplicables relacionadas con la seguridad de la información.
Objetivo de Control: Cumplimiento de los requisitos legales y contractuales	
Identificación de la legislación aplicable	
	i) Llevar a cabo un análisis exhaustivo de las regulaciones legales, normativas y acuerdos contractuales asociados con cada uno de los activos de información empleados por la Municipalidad Distrital de Amarilis, con el propósito de elaborar un inventario detallado.
	ii) Considerar las normas y leyes relacionadas a la seguridad de la información.
	- Ley 30999. Ley de ciberdefensa (27/08/2019).
	- Ley 30096. Ley de delitos informáticos (22/10/2013).
	- Ley 27309. Ley que incorpora los delitos informáticos al Código Penal (17/07/2000).
	- Decreto Supremo 050-2018-PCM. Aprueban la definición de seguridad digital en el ámbito nacional (15/05/2018).
	- Decreto Legislativo N°1412 que aprueba la Ley de Gobierno Digital del Estado Peruano
	- Resolución Ministerial Nº119-PCM que dispone la conformación de los Comités de Gobierno Digital en las instituciones públicas.
	- Resolución Ministerial 004-2016-PCM. Aprueban el uso obligatorio de la norma técnica peruana "ISO NTP/IEC 27001:2014 tecnología de la información. técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos 2a. Edición", en todas las entidades integrantes del sistema nacional de informática (08/01/2016).
	- Resolución Ministerial 129-2012-PCM. Aprueban el uso obligatorio de la norma técnica peruana "NTP ISO/IEC 27001:2008 EDI tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos" en todas las entidades integrantes del sistema nacional de informática (25/05/2012).
	- Resolución Ministerial 197-2011-PCM. Establecen fecha límite para que diversas entidades de la administración pública implementen el plan de seguridad de la información dispuesto en la norma técnica peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información" (21/07/2011)
	- Resolución Ministerial 0391-2009-AG. Aprueban e institucionalizan el documento "Política de Seguridad de la Información" del Ministerio (19/05/2009)

		- Resolución Ministerial 246-2007-PCM. Norma técnica peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del sistema nacional de informática (25/08/2007).
		- Decreto Supremo N°003 Ministerio de Justicia y derechos Humanos (marzo, 2013) Aprueban Reglamento de la Ley N° 29733, Ley de Protección de Datos personales
		- Decreto de Urgencia N°007-PCM (enero, 2020), Marco de Confianza Digital
		- Decreto de Urgencia N°006-PCM (enero, 2020), Crea el Sistema Nacional de Transformación Digital.
		- Resolución Ministerial N°087-PCM (marzo, 2019), Aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital. Asimismo, disponer que el Oficial de Seguridad de la Información de la entidad, transfiera al Comité de Gobierno Digital de la entidad, la documentación generada respecto a la implementación del SGSI.
		- Resolución Ministerial N°378-PCM (diciembre, 2017), Aprueba el Plan de Nacional de Gobierno Abierto 2017-2019.
		- Resolución Ministerial N°166-PCM (junio, 2017), Modifican el artículo 5 de la R.M. N°004- 2016-PCM referente al Comité de Gestión de Seguridad de la información
Derechos de propiedad intelectual		
	i) Obtener software a través de fuentes reconocidas y de alta reputación con el fin de garantizar el cumplimiento de los derechos de autor.	
	ii) Mantener conocimiento actualizado de las políticas destinadas a salvaguardar los derechos de propiedad intelectual y notificar cualquier violación para aplicar sanciones disciplinarias contra los infractores.	
	iii) Realizar inspecciones exhaustivas donde únicamente se instale software autorizado y productos debidamente licenciados.	
	iv) Considerar el límite máximo de usuarios permitido por la licencia de software correspondiente.	
	v) Acatar rigurosamente los términos y condiciones estipulados por el software.	
	vi) Abstenerse de replicar, total o parcialmente, códigos, libros, artículos u otros documentos no autorizados por el autor.	
	vii) Evitar la duplicación, conversión a formatos alternativos o la extracción de contenido de material con derechos de autor, salvo cuando esté permitido por las disposiciones legales de propiedad intelectual.	
Protección de los registros de la Municipalidad Distrital de Amarilis		
	i) Es necesario establecer directrices referentes a la preservación, almacenamiento, gestión y eliminación de documentos y datos.	
	ii) Se debe elaborar un calendario de retención que identifique de manera precisa los documentos y el lapso de tiempo durante el cual deben mantenerse en la Municipalidad Distrital de Amarilis.	
	iii) Es fundamental mantener un registro detallado de las fuentes de información clave.	

	iv) Debe implementarse un conjunto adecuado de medidas de control con el fin de salvaguardar los documentos contra la posible pérdida, destrucción o alteración de la información.
Objetivo de Control: Revisiones de la seguridad de la información	
Cumplimiento de las políticas y normas de seguridad	
	i) Determinar las razones detrás de la falta de cumplimiento.
	ii) Analizar la pertinencia de medidas destinadas a alcanzar la conformidad.
	iii) Ejecutar la medida correctiva adecuada.
	iv) Supervisar el cumplimiento de las regulaciones de seguridad con el propósito de evaluar su eficacia y detectar eventuales insuficiencias y vulnerabilidades.
	v) Aplicar las sanciones por incumplimiento de acuerdo al Reglamento de Aplicación de Sanciones Administrativas - RASA y la Tabla de Infracciones y Sanciones Administrativas - TISA de la Municipalidad Distrital de Amarilis.

4.7. Fase de Implementación de las Políticas de Seguridad

Para la implementación de las políticas de seguridad, en primer lugar, se hizo la presentación de dicha investigación con el documento **CARTA N°011-2023-LAVS** con fecha 29 de diciembre del 2023 que se encuentra adjunto en el Anexo 10, en este documento estaba adjunto la auditoría realizada con los resultados obtenidos y también el diseño de las políticas de seguridad denominado **"Manual de Políticas de Seguridad de la Información de la Municipalidad Distrital de Amarilis".**

Posteriormente el proyecto presentado se derivó a la Gerencia de Administración y Finanzas ya que este es responsable de garantizar que el proyecto se ejecute de manera eficiente y eficaz, dicha gerencia dio salida del expediente al área competente que sería la Sub Gerencia de Planificación y Modernización Institucional perteneciente a la Gerencia de Planeamiento y presupuesto con el **INFORME N°1280-2023-MDA-GAF** con fecha 29 de diciembre del 2023 que se encuentra adjunto en el Anexo 11.

Finalmente, la Sub Gerencia de Planificación y Modernización Institucional luego de realizar un análisis exhaustivo, **APROBÓ** las políticas de seguridad denominado **"Manual de Políticas de Seguridad de la Información de la Municipalidad Distrital de Amarilis"** y dio a **DISPOSICIÓN** del proyecto al Área Funcional de Tecnología de la Información para la respectiva **IMPLEMENTACIÓN Y PUBLICACIÓN** con el **INFORME N°162-2023-MDA/GPP/SGPMI** con fecha 29 de diciembre del 2023 que se encuentra adjunto en el Anexo 12.

4.8. Fase de Resultados Obtenidos de la Implementación de las Políticas de Seguridad

Para obtener los resultados de la implementación se realizó de nuevo la Auditoría de los procesos con la metodología COBIT 4.1 con la finalidad de poder llegar a la conclusión que las políticas de seguridad mejoran la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

Esta segunda auditoria se realizó del 29 de febrero al 04 de marzo del 2024 dando un lapso de 2 meses para recopilar los datos y ver si las políticas de seguridad mejoran la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis. Los resultados obtenidos son los siguiente.

4.8.1. Reporte General de Grados de Madurez de la segunda auditoría

Los niveles de madurez se hallaron de acuerdo a las fichas individuales que se adjuntan en el Anexo 13, se tienen los siguientes resultados.

Tabla 27: Reporte General de Grados de Madurez de la Segunda Auditoria

DOMINIO	PROCESO		NIVEL DE MADUREZ
PLANEAR Y ORGANIZAR	PO1	Definir un plan estrategia de TI	3
	PO2	Definir la arquitectura de la información	3
	PO3	Definir la dirección tecnológica	4
	PO4	Definir los procesos, organización y relaciones de TI	3
	PO5	Administrar la Inversión en TI	3
	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia	3
	PO7	Administrar Recursos Humanos de TI	2
	PO8	Administrar la Calidad	2
	PO9	Evaluar y administrar los riesgos TI	4
	P10	Administrar Proyectos	3
ADQUIRIR E IMPLEMENTAR	AI1	Identificar las soluciones automatizadas	3
	AI2	Adquirir y mantener software aplicativo	2
	AI3	Adquirir y mantener la infraestructura tecnológica	3
	AI4	Facilitar la operación y el uso	2
	AI5	Adquirir recursos de TI	4
	AI6	Administrar cambios	3
	AI7	Instalar y acreditar soluciones y cambios	2
ENTREGAR Y DAR SOPORTE	DS1	Definir y administra los niveles de servicio	3
	DS2	Administrar los Servicios de Terceros	4
	DS3	Administrar el desempeño capacidad	2
	DS4	Asegurar el servicio continuo	4
	DS5	Garantizar la seguridad de los sistemas	3

	DS6	**Identificar y asignar costos**	**3**
	DS7	**Educar y entrenar a los usuarios**	**2**
	DS8	**Administrar la mesa de servicio y los incidentes**	**2**
	DS9	**Administrar la configuración**	**2**
	DS10	**Administrar los problemas**	**3**
	DS11	**Administrar los datos**	**3**
	DS12	**Administrar el ambiente físico**	**2**
	DS13	**Administrar las operaciones**	**2**
MONITOREAR Y EVALUAR	**ME1**	**Monitoreo y evaluar el desempeño de TI**	**2**
	ME2	**Monitorear y evaluar el control interno**	**3**
	ME3	**Garantizar el cumplimiento regulatorio**	**2**
	ME4	**Proporcionar gobierno de TI**	**3**

4.8.2. Resumen de Procesos y criterios de información por impacto de la segunda auditoría

Mediante la propuesta dada por COSO, podemos dar un valor promedio al impacto de los criterios de información, con los promedios obtenidos, procedemos a asignar como se muestra en la Tabla 24*Tabla 24.*

A continuación, se muestra la tabla con todos los valores de grado de impacto.

Tabla 28: Resumen de Procesos y Criterios de Información por Impacto de la Segunda Auditoria

OBJETIVOS DE CONTROL COBIT		NIVEL DE MADUREZ	CRITERIO DE INFORMACION DE COBIT							RECURSOS DE TI COBIT			
			EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	PERSONAS	INFORMACION	APLICACIÓN	INFRAESTRUCTURA
PLANEAR Y ORGANIZAR													
PO 1	**Definir un plan estrategia de TI**		0.86	0.63	-	-	-	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	1.89	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	12.90	9.45	-	-	-	-	-				
PO 2	**Definir la arquitectura de la información**		0.63	0.86	0.63	0.86	-	-	-		X	X	
	Total Real (Impacto * Nivel Real)	**3**	1.89	2.58	1.89	2.58	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	9.45	12.90	9.45	12.90	-	-	-				
PO 3	**Definir la dirección tecnológica**		0.86	0.86	-	-	-	-	-			X	X
	Total Real (Impacto * Nivel Real)	**4**	3.44	3.44	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
PO 4	**Definir los procesos, organización y relaciones de TI**		0.86	0.86	-	-	-	-	-	X			
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
PO 5	**Administrar la Inversión en TI**		0.86	0.86	-	-	-	-	0.63	X		X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	-	-	-	-	1.89				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	3.15				
PO 6	**Comunicar las Aspiraciones y la Dirección de la Gerencia**		0.86	-	-	-	-	0.63	-		X		X
	Total Real (Impacto * Nivel Real)	**3**	2.58	-	-	-	-	1.89	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	-	-	-	-	3.15	-				
PO 7	**Administrar Recursos Humanos de TI**		0.86	0.86	-	-	-	-	-				X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
PO 8	**Administrar la Calidad**		0.86	0.86	-	0.63	-	-	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	1.26	-	-	1.26				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	3.15	-	-	3.15				
PO 9	**Evaluar y administrar los riesgos TI**		0.63	0.63	0.86	0.86	0.86	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**4**	2.52	2.52	3.44	3.44	3.44	2.52	2.52				
	Total Ideal (Impacto * Nivel Ideal)	**5**	3.15	3.15	4.30	4.30	4.30	3.15	3.15				
PO 10	**Administrar Proyectos**		0.86	0.86	-	-	-	-	-	X		X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
ADQUIRIR E IMPLEMENTAR													
AI1	**Identificar las soluciones automatizadas**		0.86	0.63	-	-	-	-	-			X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	1.89	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	-	-	-	-				
AI2	**Adquirir y mantener software aplicativo**		0.86	0.86	-	-	0.63	-	0.63			X	
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	-	1.26	-	1.26				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	3.15	-	3.15				

AI3	**Adquirir y mantener la infraestructura tecnológica**		0.63	0.86	-	0.63	0.63	-	-				X
	Total Real (Impacto * Nivel Real)	**3**	1.89	2.58	-	1.89	1.89	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	3.15	4.30	-	3.15	3.15	-	-				
AI4	**Facilitar la operación y el uso**		0.86	0.86	-	0.63	0.63	0.63	0.63	X		X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	1.26	1.26	1.26	1.26				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	3.15	3.15	3.15	3.15				
AI5	**Adquirir recursos de TI**		0.63	0.86	-	-	-	0.63	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**4**	2.52	3.44	-	-	-	2.52	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	3.15	4.30	-	-	-	3.15	-				
AI6	**Administrar cambios**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	1.89	1.89	1.89	1.89	1.89				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
AI7	**Instalar y acreditar soluciones y cambios**		0.86	0.63	-	0.63	0.63	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.26	-	1.08	1.26	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	3.15	3.15	-	-				
ENTREGAR Y DAR SOPORTE													
DS1	**Definir y administra los niveles de servicio**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	1.89	1.89	1.89	1.89	1.89				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
DS2	**Administrar los Servicios de Terceros**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**4**	3.44	3.44	2.52	2.52	2.52	2.52	2.52				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
DS3	**Administrar el desempeño capacidad**		0.86	0.86	-	-	0.63	-	-			X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	-	1.26	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	3.15	-	-				
DS4	**Asegurar el servicio continuo**		0.86	0.63	-	-	0.86	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**4**	3.44	2.52	-	-	3.44	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	-	4.30	-	-				
DS5	**Garantizar la seguridad de los sistemas**		-	-	0.86	0.86	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	-	-	2.58	2.58	1.89	1.63	1.89				
	Total Ideal (Impacto * Nivel Ideal)	**5**	-	-	4.30	4.30	3.15	3.15	3.15				
DS6	**Identificar y asignar costos**		-	0.86	-	-	-	-	0.86	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	-	2.58	-	-	-	-	2.58				
	Total Ideal (Impacto * Nivel Ideal)	**5**	-	4.30	-	-	-	-	4.30				
DS7	**Educar y entrenar a los usuarios**		0.86	0.63	-	-	-	-	-	X			
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.26	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	-	-	-	-				
DS8	**Administrar la mesa de servicio y los incidentes**		0.86	0.86	-	-	-	-	-	X			X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	-	-	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	-	-	-				
DS9	**Administrar la configuración**		0.86	0.63	-	-	0.63	-	0.63		X	X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.26	-	-	1.26	-	1.26				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	3.15	-	-	3.15	-	3.15				
DS10	**Administrar los problemas**		0.86	0.86	-	-	0.63	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	-	-	1.89	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	-	3.15	-	-				
DS11	**Administrar los datos**		-	-	-	0.86	-	-	0.86		X		
	Total Real (Impacto * Nivel Real)	**3**	-	-	-	2.58	-	-	2.58				
	Total Ideal (Impacto * Nivel Ideal)	**5**	-	-	-	4.30	-	-	4.30				
DS12	**Administrar el ambiente físico**		-	-	-	0.86	0.86	-	-			X	
	Total Real (Impacto * Nivel Real)	**2**	-	-	-	1.72	1.72	-	-				

	Total Ideal (Impacto * Nivel Ideal)	**5**	-	-	-	4.30	4.30	-	-				
DS13	**Administrar las operaciones**		0.86	0.86	-	0.63	0.63	-	-	X	X	X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	-	1.26	1.26	-	-				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	-	3.15	3.15	-	-				
MONITOREAR Y EVALUAR													
ME1	**Monitoreo y evaluar el desempeño de TI**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**2**	1.72	1.72	1.26	1.26	1.26	1.26	1.26				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
ME2	**Monitorear y evaluar el control interno**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	1.89	1.89	1.89	1.89	1.89				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	3.15	3.15	3.15	3.15	3.15				
ME3	**Garantizar el cumplimiento regulatorio**		-	-	-	-	-	0.86	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**2**	-	-	-	-	-	1.72	1.26				
	Total Ideal (Impacto * Nivel Ideal)	**5**	-	-	-	-	-	4.30	3.15				
ME4	**Proporcionar gobierno de TI**		0.86	0.86	0.63	0.63	0.63	0.63	0.63	X	X	X	X
	Total Real (Impacto * Nivel Real)	**3**	2.58	2.58	1.89	1.89	1.89	1.89	1.89				
	Total Ideal (Impacto * Nivel Ideal)	**5**	4.30	4.30	3.15	3.15	3.15	3.15	3.15				

4.8.3. Resultados finales del impacto sobre los criterios de información de la segunda auditoria

A continuación, se muestra los resultados finales del impacto sobre los criterios de información y el porcentaje promedio obtenido de los criterios de información es de **52.53%,** de acuerdo a la *Tabla 5: Calificación COSO*, este resultado obtenido se encuentra en el nivel **MEDIO,** significa que la Municipalidad Distrital de Amarilis ha alcanzado un nivel razonable en los criterios de la información COBIT que son la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad, pero aún hay un margen de mejora.

Tabla 29: Resultados Finales del Impacto sobre los Criterios de Información de la Segunda Auditoria

	Efectividad	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	
Total Real (Impacto * Nivel Real)	66.44	65.06	19.25	30.99	33.17	22.88	29.10	
Total Ideal (Impacto * Nivel Ideal)	135.00	131.55	36.95	64.75	60.15	38.95	52.70	
Porcentaje Alcanzado	49.21%	49.46%	52.10%	47.87%	55.15%	58.73%	55.22%	**52.53%**

4.8.3.1 Resultados finales del impacto sobre los criterios de información

El objetivo de esto es alcanzar el 100% en cada criterio de información para poder decir con certeza que la información sea efectiva, eficiente, confidencial, integra, disponible, cumplimiento y confiable.

Los criterios de información se encuentran en el siguiente porcentaje todos sobre el 100%.

La efectividad consiste en que la información relevante sea entregada de forma oportuna, correcta, consistente y utilizable, este criterio tiene un promedio del 49.21%, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 5, se muestra el resultado en la siguiente ilustración.

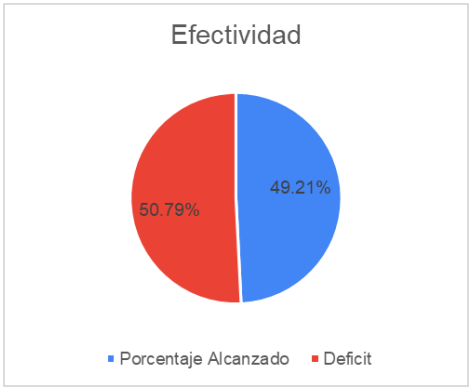


Ilustración 12: Resultado final del impacto sobre el criterio de información EFECTIVIDAD en la segunda auditoría

La eficiencia consiste en que la información debe ser generada optimizando los recursos, este criterio tiene un promedio del 49.46%, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 6, se muestra el resultado en la siguiente ilustración.

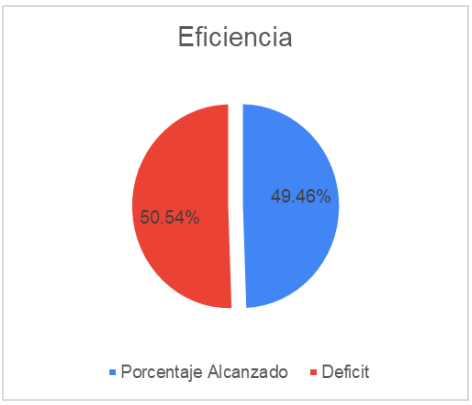


Ilustración 13: Resultado final del impacto sobre el criterio de información EFICIENCIA en la segunda auditoría.

La confidencialidad consiste en que la información vital sea protegida contra la revelación no autorizada, este criterio tiene un promedio del 52.10%, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 7, se muestra el resultado en la siguiente ilustración.

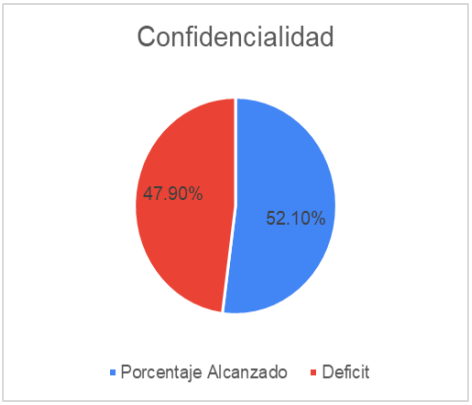


Ilustración 14: Resultado final del impacto sobre el criterio de información CONFIDENCIALIDAD en la segunda auditoría.

La integridad consiste en que la información debe ser precisa, completa y valida, este criterio tiene un promedio del 47.87 %, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 8, se muestra el resultado en la siguiente ilustración.

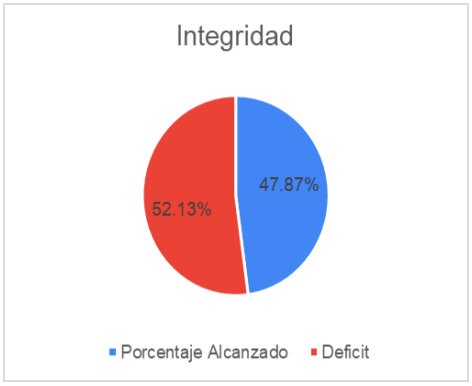


Ilustración 15: Resultado final del impacto sobre el criterio de información INTEGRIDAD en la segunda auditoría.

La disponibilidad consiste en que la información esté disponible cuando esta sea requerida por parte de las áreas del negocio en cualquier momento, este criterio tiene un promedio del 55.15%, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 9, se muestra el resultado en la siguiente ilustración.

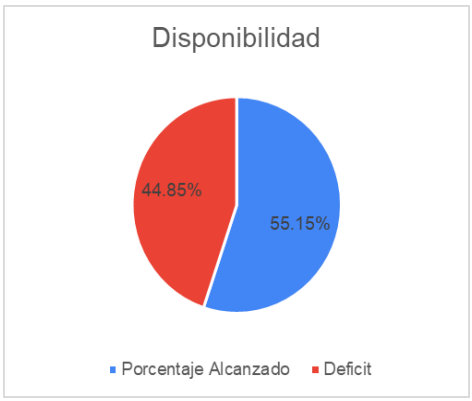


Ilustración 16: Resultado final del impacto sobre el criterio de información DISPONIBILIDAD en la segunda auditoría.

El cumplimiento consiste en que se debe respetar las leyes, reglamentos y acuerdos contractuales a los que está sujeta el proceso del negocio, como políticas internas, este criterio tiene un promedio del 58.73%, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 10, se muestra el resultado en la siguiente ilustración.

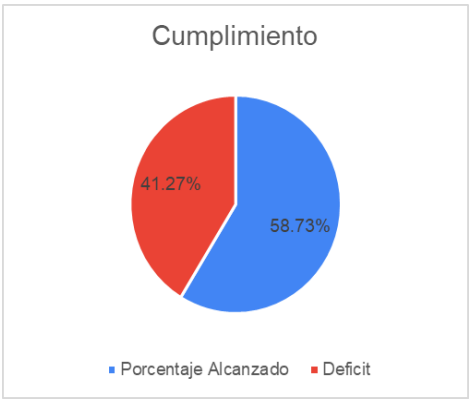


Ilustración 17: Resultado final del impacto sobre el criterio de información CUMPLIMIENTO en la segunda auditoría.

La confiabilidad consiste en que se debe respetar proporcionar la información apropiada, con el fin de que la Gerencia General administre la entidad, este criterio tiene un promedio del 55.22%, en este criterio hubo una mejora significativa a la primera auditoria que se puede ver en la Ilustración 11, se muestra el resultado en la siguiente ilustración.

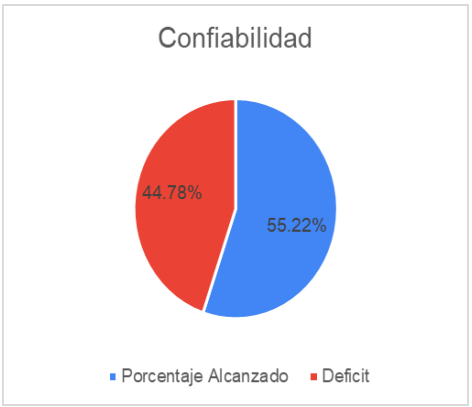


Ilustración 18: Resultado final del impacto sobre el criterio de información CONFIABILIDAD en la segunda auditoría.

CAPITULO V
DISCUSION

Para realizar este proyecto, resultó fundamental analizar las tesis y proyectos relacionados con el tema de investigación. Se evaluaron los métodos empleados por los autores y los resultados que perseguían. Algunos de ellos se llevaron a cabo mediante auditorías, otros a través de proyectos informáticos y algunos desde la perspectiva de los temas de investigación en sí. A pesar de las diferencias, se identificaron numerosas similitudes entre los enfoques del presente proyecto y los de los autores revisados. En última instancia, convergen hacia un resultado común: la afirmación de la aplicabilidad de las políticas de seguridad.

En relación con el proyecto que estamos abordando, incluye 7 fases de las cuales las primeras 3 fases compete a la metodología Magerit versión 3.0 y las ultimas 4 fases le compete a la metodología COBIT 4.1. Se comenzó con la Fase de Identificación de los escenarios de riesgos TI que abarca las siguientes actividades; la identificación y clasificación de los activos de TI, la valoración de criticidad de los activos de TI, la identificación de amenazas por activo e identificación de vulnerabilidades de cada activo de TI. Con esta Fase se pudo recopilar y analizar la información sobre los riesgos potenciales, teniendo en cuenta factores como las amenazas internas y externas, las vulnerabilidades del sistema y las posibles consecuencias de cada riesgo.

En la segunda Fase de valoración de los escenarios de TI que abarca las siguientes actividades de acuerdo a la metodología Magerit versión 3.0; estimación del impacto de los escenarios de riesgo, estimación de la probabilidad de ocurrencia de los escenarios de riesgo, cálculo de los niveles de exposición a los riesgos y la determinación del apetito y tolerancia del riesgo. En esta fase se pudo cuantificar y cualificar los impactos y las probabilidades asociadas a cada riesgo, con el fin de determinar su nivel de riesgo global. En otras palabras, la finalidad es valorar la importancia y magnitud de los riesgos para que la Municipalidad Distrital de Amarilis

pueda tomar decisiones informadas sobre la gestión y mitigación de estos riesgos en el entorno de Tecnologías de la Información para salvaguardar la información.

En la tercera Fase de tratamiento del riesgo que abarca la actividad según la metodología Magerit versión 3.0 es la identificación de los controles/salvaguardas de seguridad y Definición de la estrategia de implementación de controles/salvaguardas. En esta fase se pudo identificar medidas concretas (controles/salvaguardas) para mitigar los riesgos previamente identificados y establecer una estrategia clara para su gestión continua en el ámbito de las Tecnologías de la Información para salvaguardar la información en la Municipalidad Distrital de Amarilis.

En la cuarta Fase de auditoría de procesos según la metodología COBIT 4.1 que nos permite evaluar el control interno, garantizar el cumplimiento, optimización y mejora continua; y la gestión de riesgos bajo los dominios Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte; y Monitorear y Evaluar en relación a los criterios de COBIT. En esta fase se pudo obtener luego de la auditoría un resultado de nivel BAJO con 15.82% que se encuentra en la Tabla 26, esto significa que los criterios de la información COBIT que son la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad corren un mayor riesgo de sufrir una violación de datos, lo que puede tener un impacto significativo en su reputación, sus finanzas y sus operaciones.

En la quinta Fase de diseño de las políticas de seguridad de acuerdo a los datos obtenidos en la Tabla 26 de la auditoría de procesos bajo la metodología COBIT 4.1, Se pudo hacer un análisis y se diseñó de un manual de cada política de seguridad de la Municipalidad distrital de Amarilis con la finalidad de proporcionar un conjunto de directrices y normas que establecen cómo se deben manejar y proteger los activos de información para el resguardo de la información.

En la sexta Fase de implementación de las políticas de seguridad, previamente a la presentación formal de la auditoría realizada y la propuesta de las políticas de seguridad, se hizo

una coordinación para hacerles ver en qué estado se encontraban y se presentó la propuesta de mejora “Las políticas de seguridad” para poder resguardar la información en la entidad, los participantes fueron el Gerente Municipal, el Jefe de Informática, el Gerente de Administración y finanzas, el Gerente de Planeamiento y Presupuesto; y el Sub Gerente de Planificación y Modernización Institucional. Los participantes anteriormente mencionados, tomaron conciencia y estuvieron de acuerdo con el proyecto y se procedió con la presentación formal y documentada a la entidad el día 29 de diciembre del 2023, el mismo día se APROBÓ y se puso el proyecto a DISPOSICIÓN a la oficina de informática para su IMPLEMENTACIÓN y PUBLICACIÓN.

En la séptima Fase de Resultados Obtenidos de la implementación de las Políticas de Seguridad se realizó una segunda auditoría de procesos mediante la metodología COBIT 4.1, cabe recalcar que el periodo de auditoría de procesos respecto a las tecnologías de información para el resguardo de información es mínimo cada 06 meses para que las políticas de seguridad se reajusten a la nueva realidad de la entidad. En este caso se realiza una segunda auditoría para poder llegar a la conclusión que las políticas de seguridad mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis. En esta fase se pudo obtener un resultado de nivel MEDIO con 52.53% significa que la Municipalidad Distrital de Amarilis ha alcanzado un nivel razonable en los criterios de la información COBIT que son la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad, pero aún hay un margen de mejora.

Haciendo una comparación con los resultados obtenidos en la primera y segunda auditoría podemos darnos cuenta que existe un aumento significativo en el Impacto sobre los Criterios de Información bajo la auditoria de procesos con la metodología COBIT 4.1 gracias a la implementación de las políticas de seguridad de la información en la Municipalidad Distrital de Amarilis, como se muestra en la siguiente tabla.

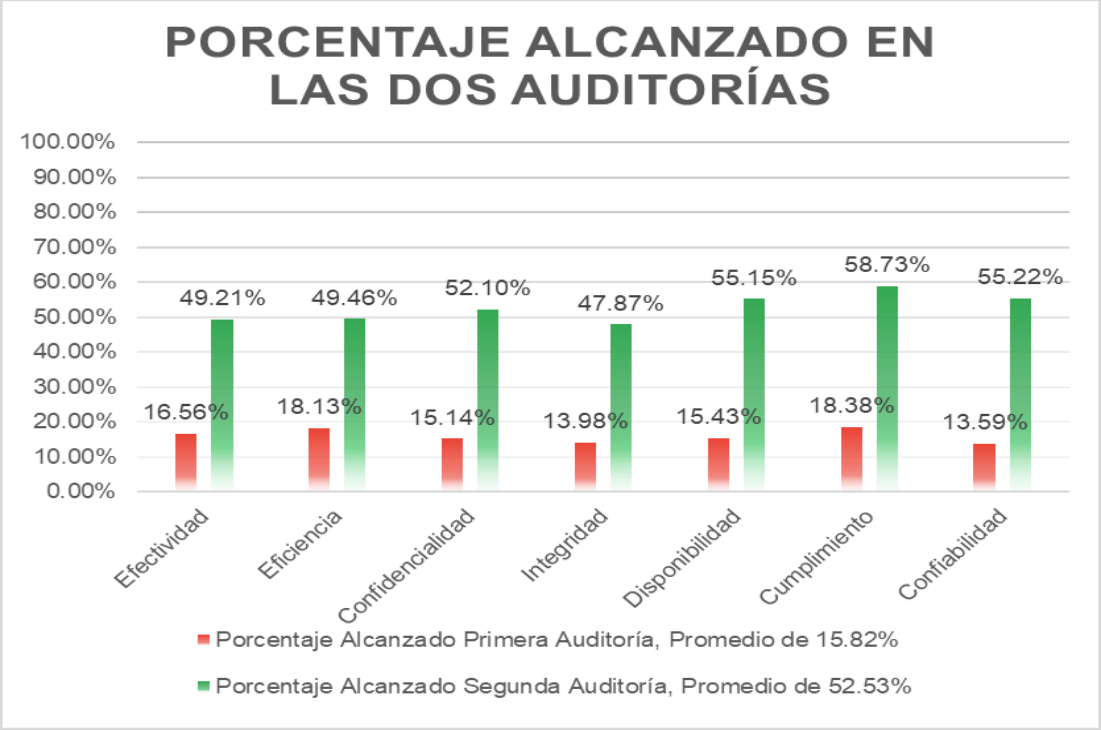


Ilustración 19: Comparativa de los resultados obtenidos en porcentajes en las dos Auditorías

CONCLUSIONES

A lo largo de esta investigación, se ha llevado a cabo un análisis exhaustivo para evaluar la influencia de la implementación de políticas de seguridad en la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.

Como primera conclusión tenemos; La hipótesis nula general que afirmaba que las políticas de seguridad mejorará la efectividad del resguardo de la información ha sido respaldada de manera concluyente por los resultados obtenidos por la auditoría de procesos de acuerdo la metodología COBIT 4.1, Se realizó 2 auditorias, la primera fue tal como se encontraba la Municipalidad Distrital de Amarilis y la segunda fue dos meses de haberse implementado la políticas de seguridad de la información y los datos obtenidos se pueden visualizar en la Ilustración 19, donde se encontraba en un NIVEL BAJO con un promedio de 15.82% y dos meses después de la implementación con un NIVEL MEDIO con un promedio de 52.83% sobre los criterios de información según la metodología COBIT 4.1, por esa razón podemos afirmar que las políticas de seguridad mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis que está enfocado a nuestro objetivo general del proyecto de investigación.

En segundo lugar, se concluye; La primera hipótesis específica sostenía que la identificación de los activos de sistemas de información mejorará la efectividad del resguardo de la información. Los resultados que se muestran en la Tabla 7 y Tabla 8 nos permite identificar los activos críticos en la entidad para conocer y gestionar de manera adecuada los recursos informáticos. Y posteriormente poder evaluarlos para la toma de decisiones respecto al resguardo de la información, por esa razón podemos afirmar que la identificación de los activos de sistemas de información mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis que está enfocado a nuestro primer objetivo específico del proyecto de investigación.

En tercer lugar, se concluye; La segunda hipótesis específica destacaba que la evaluación de amenazas, vulnerabilidades, impacto y riesgo de los sistemas de información contribuiría a mejorar la efectividad del resguardo de la información. La investigación confirma que una evaluación rigurosa de estos elementos que se muestran en el numeral 4.2 Fase de Identificación de los escenarios de riesgos de TI. y el numeral 4.3 Fase de Valoración de los Escenarios de Riesgos de TI. Estos proporcionan una base sólida para la toma de decisiones informadas en materia de seguridad, reduciendo la exposición a posibles riesgos, por esa razón podemos afirmar que la evaluación de las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis que está enfocado a nuestro segundo objetivo específico del proyecto de investigación.

En cuarto lugar, se concluye; La tercera hipótesis específica sugería que la evaluación de los modelos de madurez de los procesos de los sistemas de información incidiría positivamente en la efectividad del resguardo de la información. Los resultados indican que el análisis de la madurez de los procesos a evaluar como se muestra en el Anexo 09 nos permitió identificar el nivel de desarrollo y efectividad de los procesos de gobierno y gestión de TI en la entidad. Estos modelos permitió a la Municipalidad Distrital de Amarilis identificar áreas de mejora y establecer un plan para alcanzar un nivel de madurez más alto, no solo mejorar la eficiencia operativa, sino que también fortalecer la postura general de seguridad de la información en la entidad, por esa razón podemos afirmar que la evaluación de los modelos de madurez de los procesos de los sistemas de información mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis que está enfocado a nuestro tercer objetivo específico del proyecto de investigación.

En quinto lugar, se concluye; La cuarta hipótesis específica proponía que el diseño de las políticas de seguridad sería clave para mejorar la efectividad del resguardo de la información. La

investigación demuestra que un diseño meticuloso de las políticas de seguridad que se muestra en el numeral 4.6 Fase de Diseño de las Políticas de Seguridad, adaptado a las necesidades específicas de la Municipalidad, tiene un impacto significativo en la prevención de brechas de seguridad ya que estas políticas de seguridad permiten salvaguardar la integridad, confidencialidad y disponibilidad de la información que maneja la Municipalidad Distrital de Amarilis. Por esa razón podemos afirmar que el diseño de las políticas de seguridad mejora la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis que está enfocado a nuestro cuarto objetivo específico del proyecto de investigación.

Finalmente podemos concluir, En conjunto, los resultados de las hipótesis específicas y respaldan de manera contundente la hipótesis general, consolidando la premisa de que las políticas de seguridad desempeñan un papel fundamental en el fortalecimiento integral de la seguridad de la información en la Municipalidad Distrital de Amarilis. Estos hallazgos proporcionan una base sólida para recomendaciones prácticas y futuras iniciativas destinadas a optimizar la seguridad de la información en el ámbito municipal y han logrado cumplir con éxito los objetivos planteados.

RECOMENDACIONES Y SUGERENCIAS

A medida que se desarrollaba este proyecto, se hizo evidente la importancia de que la Municipalidad Distrital de Amarilis implementara políticas de seguridad para la efectividad del resguardo de la información, si bien es cierto que la entidad subió el nivel de impacto de los niveles de criterios de información que son efectividad, eficacia, cumplimiento, integridad, disponibilidad, cumplimiento, confiabilidad según COBIT 4.1, esto no significa que ha llegado a cierto punto de que la efectividad del resguardo de la información sea la más optima. Por Ende, se recomienda seguir el conjunto de reglas, normas y procedimientos que están plasmadas en las políticas de seguridad de la información implementadas en la entidad para así mejorar la efectividad del resguardo del respaldo de la información.

Se sugiere implementar un proceso de evaluación de riesgos de forma continua para identificar nuevas amenazas y vulnerabilidades. Esto permitirá una adaptación proactiva de las políticas de seguridad en respuesta a cambios en el entorno de amenazas.

Se recomienda desarrollar programas regulares de capacitación y concientización en seguridad de la información para todos los empleados de la Municipalidad. Una fuerza laboral informada y consciente es clave para fortalecer la seguridad desde el interior.

Se recomienda establecer un ciclo regular de revisión y actualización de las políticas de seguridad. Esto garantizará que las políticas estén alineadas con las últimas mejores prácticas y normativas de seguridad.

Se recomienda incluir mucho más a todo el personal de la Municipalidad Distrital de Amarilis en la definición de políticas de seguridad a través de procesos participativos. Esto asegurará una comprensión mutua de las necesidades de seguridad y construirá un sentido de responsabilidad compartida.

Estas recomendaciones y sugerencias buscan fortalecer la seguridad de la información en la Municipalidad Distrital de Amarilis, asegurando una mejor efectividad del respaldo de la información.

REFERENCIAS

Abalco Maila, D. E., & Ruilova Sandoval, R. R. (2015). *Elaboración del Plan de Seguridad de la Información para el Fondo de Cesantía y Jubilación del MDMQ.* ESCEULA POLITECNICA NACIONAL, Quito, Ecuador.

Aguilar, M. A. (2006). Sistema de gestión de seguridad de información para una institución financiera. *Sistema de gestión de seguridad de información para una institución financiera.* Pontificia Universidad Católica del Perú, Lima, Perú.

Altamirano de la Borda, K. J. (2020). La seguridad de la información en la administración pública. *Actas del III Congreso Internacional de Ingeniería de Sistemas*, (pág. 77).

Arguezo Ramirez, E. D. (2019). *PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL ÁREA DE INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO.* UNIVERSIDAD DE HUÁNUCO, Huánuco, Perú.

Avilés Arjimos, J. M., & Uyaguari Guartatanga, M. E. (2012). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA LA EMPRESA DE TELECOMUNICACIONES PUNTONET EN LA CIUDAD DE CUENCA, EN BASE A LAS NORMAS DE SEGURIDAD ISO 27001 Y 27011 COMO LÍNEAS BASE PARA LAS BUENAS PRÁCTICAS DE TRATAMIENTO Y SEGURIDAD DE LA INFORMACIÓN.* UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA, Cuenca, Ecuador.

Camapaza Quispe, A. A. (2019). *DISEÑO DEL PLAN DE SEGURIDAD INFORMATICA BASADO EN LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DEL CENTRO POBLADO DE SALCEDO - PUNO.* UNIVERSIDAD ANDINA DEL CUSCO, Cusco, Perú.

Enríquez Miranda, J. F. (2011). *POLÍTICAS DE SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DE LOS ENTORNOS WEB DE LA EMPRESA TURBOTECH DURANTE EL AÑO 2010.* UNIVERSIDAD TÉCNICA DE AMBATO, Ambato, Ecuador.

Gómez Vieites, Á. (2011). *SEGURIDAD INFORMATICA BASICA.*

HAIR JR., J. F., BLACK, W. C., BABIN, B. J., & ANDERSON, R. E. (2010). *MULTIVARIATE DATA ANALYSIS* (Vol. 7TH EDITION).

ISACA. (2009). *Manual de preparación, Asociación de Auditoria y Control de Sistemas de Información* . Lima.

ISO 27001. (2013). *ISO 27001.*

IT Governance Institute. (2007). *COBIT 4.1.*

MAGERIT. (2012). Metodología MAGERIT versión 3.

Martinez, J. (2022). *Seguridad Informática: La efectividad del resguardo de la información.*

Oñate Arboleda, A. (2021). *PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES.* UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, Bogota, Colombia.

Pilla Yanzapanta, J. C. (2019). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA., BASADO EN LA NORMA ISO/IEC 27002:2013.* UNIVERSIDAD INTERNACIONAL SEK, Quito, Ecuador.

Riveros Paraguay, J. K. (2019). *Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la Red en la Oficina Departamental de Estadística e Informática de Junín.* Universidad Nacional del Centro del Perú, Huancayo, Perú.

Sanchez Herrera, R. E. (2022). *POLÍTICAS DE SEGURIDAD Y RIESGOS DE LA INFORMACIÓN.* UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, Huaraz, Perú.

Torres Núñez, E. M. (2015). *Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.* UNIVERSIDAD TÉCNICA DE AMBATO, Ambato, Ecuador.

Vilcarromero Zubiate, L. L., & Vilchez Linares, E. (2018). *Propuesta de implementación de un modelo de gestión de ciberseguridad.* UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS, Lima, Perú.

Villadeza Romero, K. L., & Condor Simon, R. D. (2022). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TÉCNICA PERUANA -ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DISTRITAL DE HUÁCAR 2022.* UNIVERSIDAD NACIONAL HERMILIOVALDIZÁN, Huánuco, Perú.

Williams, H. R. (2019). *Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaria Región Huancavelica.* UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN, Huancavelica, Perú.

ANEXOS

Anexo 01: Matriz de Consistencia

<table>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPOTESIS</th><th>VARIABLES</th></tr>
<tr>
<td>Problema General:
¿De qué manera la implementación de las políticas de seguridad va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?</td>
<td>Objetivo general:
Implementar Políticas de seguridad para mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis</td>
<td>Hipótesis General
Ho: Las políticas de seguridad mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.
Ha: Las políticas de seguridad no mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.</td>
<td rowspan="4">
Variable Dependiente: (Y) Efectividad del resguardo de la información
<table>
<tr><th>DIMENSIONES</th><th>INDICADORES</th></tr>
<tr><td>Disponibilidad</td><td>% de resguardo de la información en la disponibilidad.</td></tr>
<tr><td>Integridad</td><td>% de resguardo de la información en la integridad.</td></tr>
<tr><td>Confidencialidad</td><td>% de resguardo de la información en la confidencialidad</td></tr>
<tr><td>Autenticidad</td><td>% de resguardo de la información en la autenticidad.</td></tr>
<tr><td>Trazabilidad</td><td>% de resguardo de la información en el Trazabilidad.</td></tr>
</table>
Variable Independiente: (X) Políticas de seguridad
<table>
<tr><th>DIMENSIONES</th><th>INDICADORES</th></tr>
<tr><td rowspan="7">Modelos de Madurez</td><td>% del impacto de los modelos de madurez en el criterio de información efectividad</td></tr>
<tr><td>% del impacto de los modelos de madurez en el criterio de información eficiencia</td></tr>
<tr><td>% del impacto de los modelos de madurez en el criterio de información disponibilidad.</td></tr>
<tr><td>% del impacto de los modelos de madurez en el criterio de información integridad.</td></tr>
<tr><td>% del impacto de los modelos de madurez en el criterio de información disponibilidad.</td></tr>
<tr><td>% del impacto de los modelos de madurez en el criterio de información cumplimiento.</td></tr>
<tr><td>% del impacto de los modelos de madurez en el criterio de información confiabilidad.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Problema específico:
• ¿De qué manera la identificación de los activos de sistemas de información va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?</td>
<td>Objetivos específicos:
• Identificar los activos de sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis distrital de amarilis basado en la metodología MAGERIT V.3.</td>
<td>Hipótesis Especifica:
• H1: La identificación de los activos de sistemas de información mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.</td>
</tr>
<tr>
<td>• ¿De qué manera la evaluación de las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?</td>
<td>• Evaluar las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de Amarilis basado en la metodología MAGERIT V.3.</td>
<td>• H2: La evaluación de las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.</td>
</tr>
<tr>
<td>• ¿De qué manera la evaluación de los modelos de madurez de los procesos de los sistemas de información va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?</td>
<td>• Evaluar los modelos de madurez para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de AMARILIS basado en la metodología COBIT 4.1.</td>
<td>• H3: La evaluación de los modelos de madurez de los procesos de los sistemas de información mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.</td>
</tr>
</table>

• ¿De qué manera el Diseño de las políticas de seguridad va a mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?	• Diseñar políticas de seguridad para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis basado en la metodología COBIT 4.1.	• **H4:** El diseño de las políticas de seguridad mejorará la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.	

Anexo 02: Encuesta sobre el conocimiento de las Políticas de Seguridad de la Información

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN: Son un conjunto de directrices, reglas y prácticas establecidas para proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Estas políticas son fundamentales para gestionar y mitigar los riesgos relacionados con la seguridad de la información, y generalmente se aplican a los activos digitales y sistemas de información.

APELLIDOS Y NOMBRES:

ÁREA:

CARGO:

N°	Pregunta	Marcar con una "X" en la opción que considere apropiada.		Observación o Comentario
		SI	NO	
1	¿Usted tenía conocimiento acerca de las políticas de seguridad de la información?			
2	¿Existe las Políticas de seguridad en Municipalidad Distrital de Amarilis?			
3	¿Cree que las políticas de seguridad mejorarán la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?			
4	¿Considera que existe información en el entorno laboral que requiere ser resguardada?			
5	Según sus responsabilidades laborales, ¿Ha participado en capacitación relacionada con la seguridad y resguardo de la información?			
6	¿Dispone de una computadora o portátil para llevar a cabo sus actividades diarias en el trabajo?			
7	¿La computadora o portátil pertenece a usted?			
8	¿Tiene acceso a algún sistema o aplicación donde introduce información relacionada con la Municipalidad Distrital de Amarilis?			
9	¿Cuándo deja su computadora o portátil sin supervisión, tiene activada la función de bloqueo de pantalla con contraseña para proteger la información?			

10	¿Ha enfrentado algún incidente de alteración o pérdida de información, ya sea por virus, acceso no autorizado, daño, extravío, u otras causas, en lo que va del año?			
11	¿Durante el transcurso del año, ha ocurrido algún incidente en el que se haya filtrado información sensible para la institución sin su autorización o conocimiento?			
12	¿Su computadora o laptop cuenta con antivirus actualizado?			
13	¿Hace backups (copias de información) como medida de protección para sus datos?			
14	¿Cree usted que su área está protegida de posibles amenazas externas o del entorno que podrían resultar en la pérdida de información?			
15	¿En caso de algún evento adverso en su computadora, portátil, equipo informático o sistema de información, se encarga de resolver el problema?			
16	¿En caso de algún suceso desfavorable en su computadora, portátil, equipo informático o sistema de información, busca asistencia ya sea de un colega, amigo dentro o fuera de la institución, de manera virtual o presencial?			
17	¿Hay algunas páginas web a las que se le ha limitado el acceso?			
18	En caso de algún incidente adverso en la computadora, portátil, equipo informático o sistema de información, ¿recibe asistencia rápida por parte del personal autorizado?			
19	¿Emplea dispositivos de almacenamiento personales como USB, discos externos, almacenaje en la nube, entre otros, para respaldar sus labores?			
20	¿Se documenta de manera detallada la evidencia de los eventos vinculados a la seguridad de la información?			

Anexo 03: Validación de Juicio por Expertos

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

NOMBRE DEL JUEZ	HILTON PEREZ SOLIS
ESPECIALIDAD	TECNOLOGIAS DE INFORMACION
EXPERIENCIA PROFESIONAL	25 AÑOS
CARGO	DOCENTE UNIVERSITARIO
"POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS"	
DATOS DEL TESISTA	
NOMBRES Y APELLIDOS	LUIS ARNOLD VILLA SANCHEZ
ESPECIALIDAD	INGENIERÍA DE SISTEMAS
INSTRUMENTO EVALUADO	ENCUESTA
OBJETIVOS DE LA INVESTIGACIÓN	GENERAL: Implementar Políticas de seguridad para mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.
	ESPECIFICAS: • Identificar los activos de sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis distrital de amarilis basado en la metodología MAGERIT V.3. • Evaluar las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de Amarilis basado en la metodología MAGERIT V.3. • Evaluar los modelos de madurez para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de AMARILIS basado en la metodología COBIT 4.1. • Diseñar politicas de seguridad para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis basado en la metodología COBIT 4.1.
EVALUÉ CADA ITEM DEL INSTRUMENTO CON LO QUE ESTOY DE ACUERDO QUE SE APLIQUE PARA DIAGNOSTICAR LA SITUACION ACTUAL EN LA MUNICIPALIDAD	
DETALLE DE LOS ITEMS DEL INSTRUMENTO	El instrumento consta de 20 ítems y ha sido construido teniendo en cuenta la revisión de la literatura y luego del juicio de expertos

DNI: 22521879

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

NOMBRE DEL JUEZ	Ines Eusebia Jesus Tolentino
ESPECIALIDAD	Dr. Gestion Empresarial
EXPERIENCIA PROFESIONAL	18 años
CARGO	Docente
"POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS"	
DATOS DEL TESISTA	
NOMBRES Y APELLIDOS	LUIS ARNOLD VILLA SANCHEZ
ESPECIALIDAD	INGENIERÍA DE SISTEMAS
INSTRUMENTO EVALUADO	ENCUESTA
OBJETIVOS DE LA INVESTIGACIÓN	**GENERAL:** Implementar Políticas de seguridad para mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis. **ESPECIFICAS:** • Identificar los activos de sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis distrital de amarilis basado en la metodología MAGERIT V.3. • Evaluar las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de Amarilis basado en la metodología MAGERIT V.3. • Evaluar los modelos de madurez para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de AMARILIS basado en la metodología COBIT 4.1. • Diseñar políticas de seguridad para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis basado en la metodología COBIT 4.1.
Evalué cada item del instrumento con lo que estoy totalmente en acuerdo que se aplique para diagnosticar la situación actual en la municipalidad distrital de Amarilis	
DETALLE DE LOS ITEMS DEL INSTRUMENTO	El instrumento consta de 20 ítems y ha sido construido teniendo en cuenta la revisión de la literatura y luego del juicio de expertos

DNI: 40346404

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

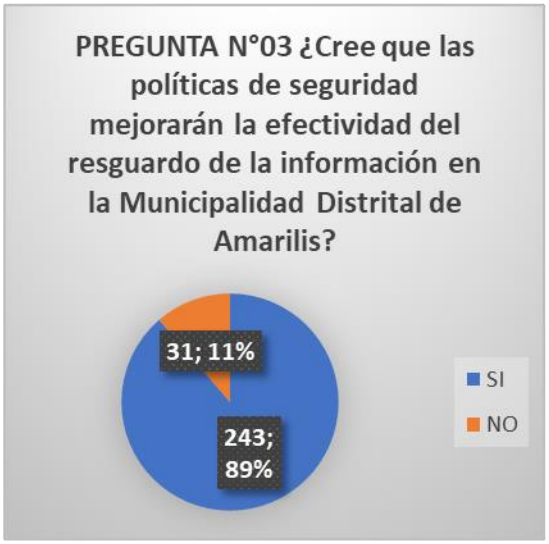
NOMBRE DEL JUEZ	JHONNY HENRY PIÑAN GARCIA.
ESPECIALIDAD	ING. INDUSTRIAL.
EXPERIENCIA PROFESIONAL	20 AÑOS.
CARGO	DOCENTE
"POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS"	
DATOS DEL TESISTA	
NOMBRES Y APELLIDOS	LUIS ARNOLD VILLA SANCHEZ
ESPECIALIDAD	INGENIERÍA DE SISTEMAS
INSTRUMENTO EVALUADO	ENCUESTA
OBJETIVOS DE LA INVESTIGACIÓN	GENERAL: Implementar Políticas de seguridad para mejorar la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis.
	ESPECIFICAS: • Identificar los activos de sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis distrital de amarilis basado en la metodología MAGERIT V.3. • Evaluar las amenazas, vulnerabilidades, impacto y el riesgo de los sistemas de información para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de Amarilis basado en la metodología MAGERIT V.3. • Evaluar los modelos de madurez para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis Distrital de AMARILIS basado en la metodología COBIT 4.1. • Diseñar políticas de seguridad para mejorar efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis basado en la metodología COBIT 4.1.
LAS PREGUNTAS DE LA ENCUESTA "CONOCIMIENTOS DE LOS POLITICAS DE LA SEGURIDAD DE LA INFORMACION" FUERON EVALUADOS Y ESTOY DE ACUERDO CON SU APLICACIÓN	
DETALLE DE LOS ITEMS DEL INSTRUMENTO	El instrumento consta de 20 ítems y ha sido construido teniendo en cuenta la revisión de la literatura y luego del juicio de expertos

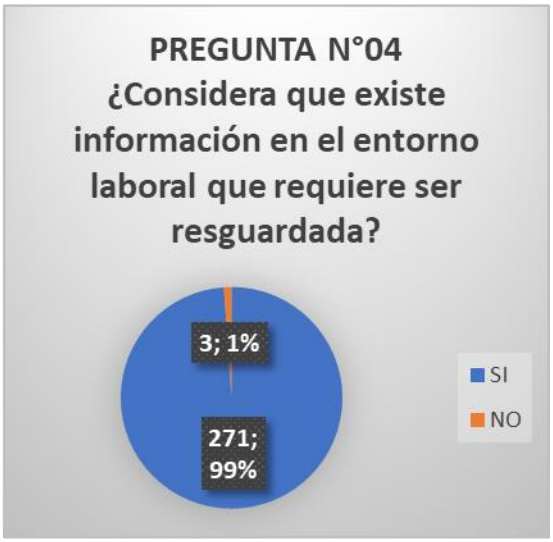
DNI: 10423397

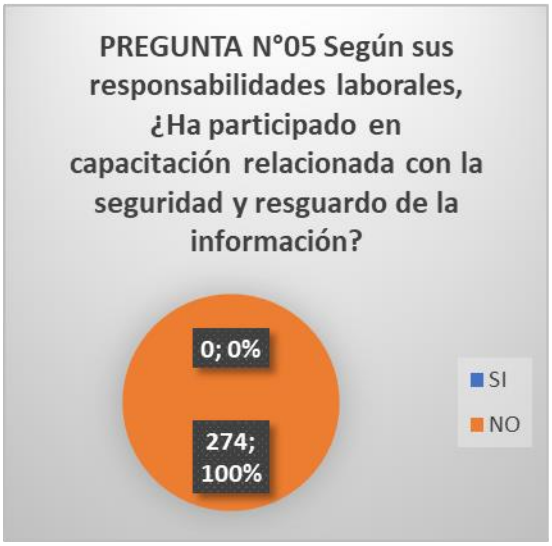
Anexo 4: Resultados Obtenidos de la Encuesta Realizada

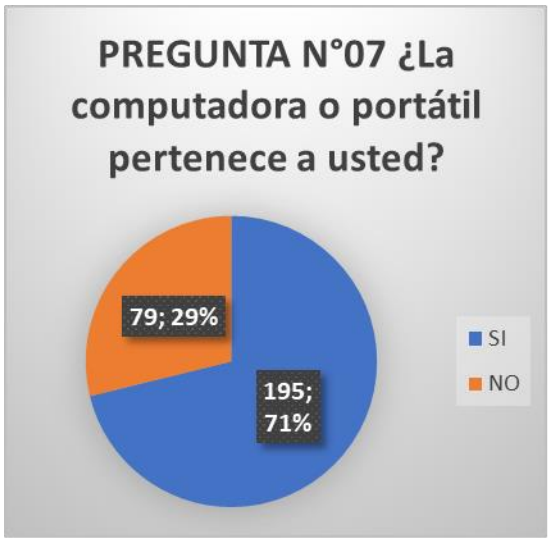
N°	Pregunta	Marcar con una "X" en la opción que considere apropiada.	
		SI	NO
1	¿Usted tenía conocimiento acerca de las políticas de seguridad de la información?	13	261
2	¿Existe las Políticas de seguridad en Municipalidad Distrital de Amarilis?	0	274
3	¿Cree que las políticas de seguridad mejorarán la efectividad del resguardo de la información en la Municipalidad Distrital de Amarilis?	243	31
4	¿Considera que existe información en el entorno laboral que requiere ser resguardada?	271	3
5	Según sus responsabilidades laborales, ¿Ha participado en capacitación relacionada con la seguridad y resguardo de la información?	0	274
6	¿Dispone de una computadora o portátil para llevar a cabo sus actividades diarias en el trabajo?	229	45
7	¿La computadora o portátil pertenece a usted?	195	79
8	¿Tiene acceso a algún sistema o aplicación donde introduce información relacionada con la Municipalidad Distrital de Amarilis?	190	84
9	¿Cuándo deja su computadora o portátil sin supervisión, tiene activada la función de bloqueo de pantalla con contraseña para proteger la información?	64	210
10	¿Ha enfrentado algún incidente de alteración o pérdida de información, ya sea por virus, acceso no autorizado, daño, extravío, u otras causas, en lo que va del año?	230	44
11	¿Durante el transcurso del año, ha ocurrido algún incidente en el que se haya filtrado información sensible para la institución sin su autorización o conocimiento?	255	19
12	¿Su computadora o laptop cuenta con antivirus actualizado?	2	272
13	¿Hace backups (copias de información) como medida de protección para sus datos?	11	263
14	¿Cree usted que su área está protegida de posibles amenazas externas o del entorno que podrían resultar en la pérdida de información?	32	242
15	¿En caso de algún evento adverso en su computadora, portátil, equipo informático o sistema de información, se encarga de resolver el problema?	21	253
16	¿En caso de algún suceso desfavorable en su computadora, portátil, equipo informático o sistema de información, busca asistencia ya sea de un colega, amigo dentro o fuera de la institución, de manera virtual o presencial?	111	163
17	¿Hay algunas páginas web a las que se le ha limitado el acceso?	0	274
18	En caso de algún incidente adverso en la computadora, portátil, equipo informático o sistema de información, ¿recibe asistencia rápida por parte del personal autorizado?	6	268
19	¿Emplea dispositivos de almacenamiento personales como USB, discos externos, almacenaje en la nube, entre otros, para respaldar sus labores?	44	230
20	¿Se documenta de manera detallada la evidencia de los eventos vinculados a la seguridad de la información?	0	274

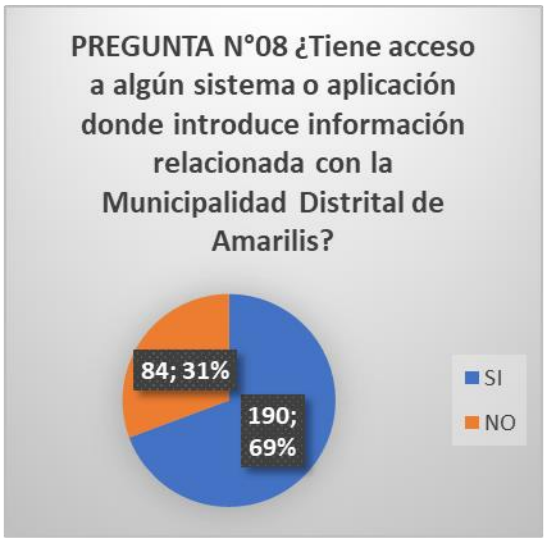
Anexo 05: Resultados Obtenidos Representados en Gráficos

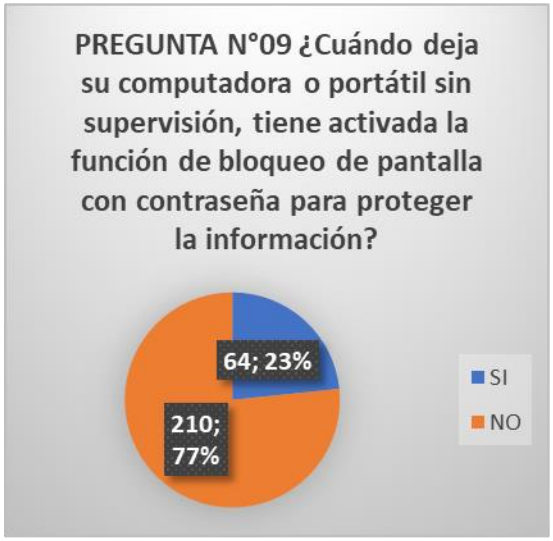


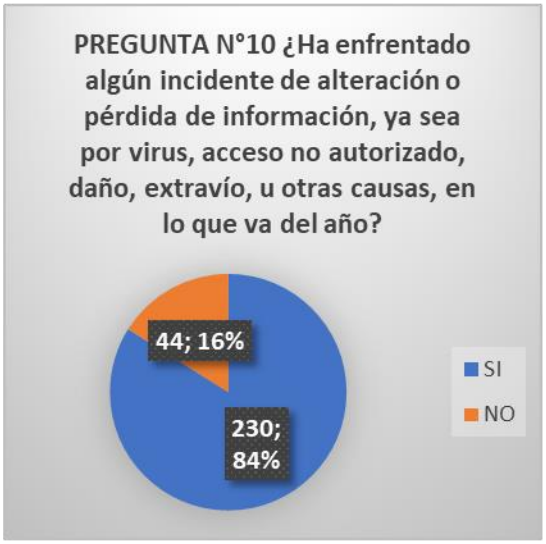


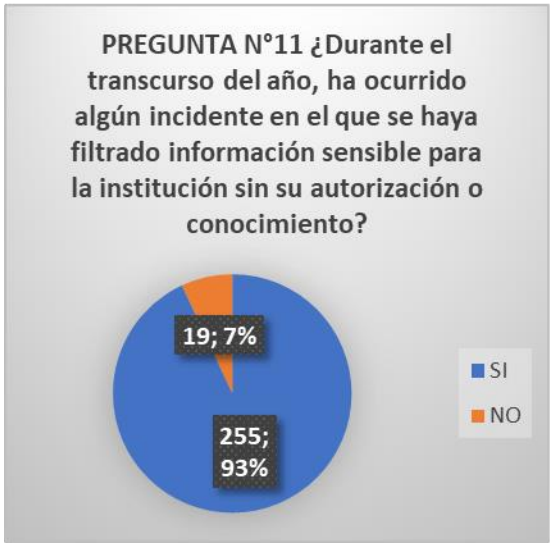


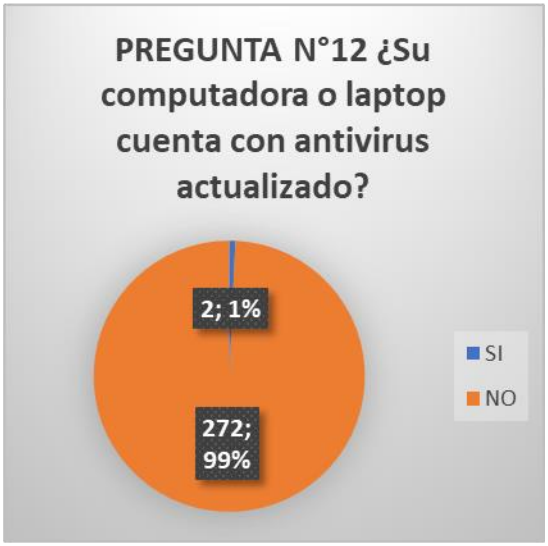

PREGUNTA N°07 ¿La computadora o portátil pertenece a usted?
79; 29%
195; 71%
SI
NO

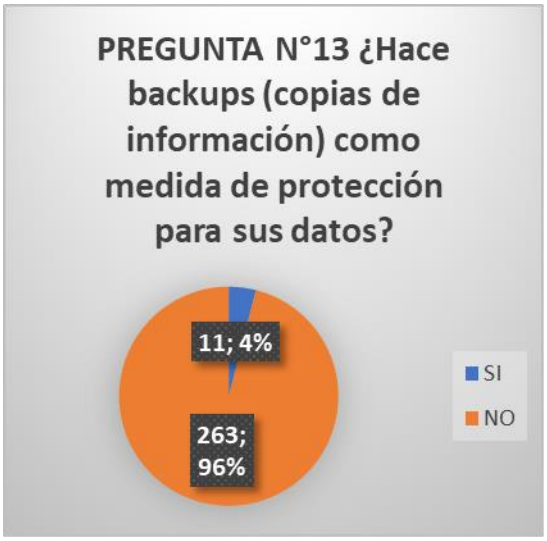

PREGUNTA N°08 ¿Tiene acceso a algún sistema o aplicación donde introduce información relacionada con la Municipalidad Distrital de Amarilis?
84; 31%
190; 69%
SI
NO

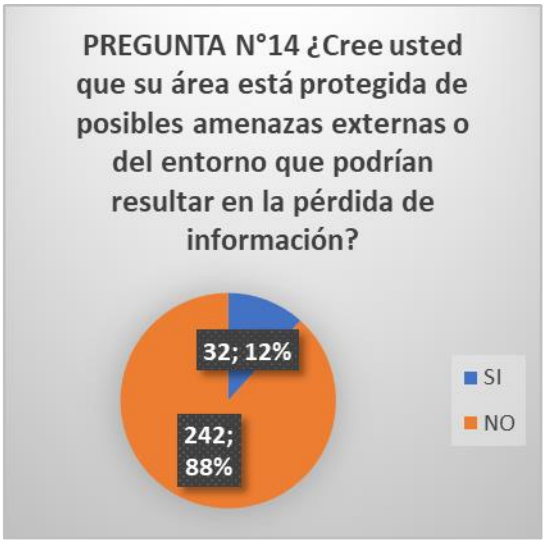

PREGUNTA N°09 ¿Cuándo deja su computadora o portátil sin supervisión, tiene activada la función de bloqueo de pantalla con contraseña para proteger la información?
64; 23%
210; 77%
SI
NO

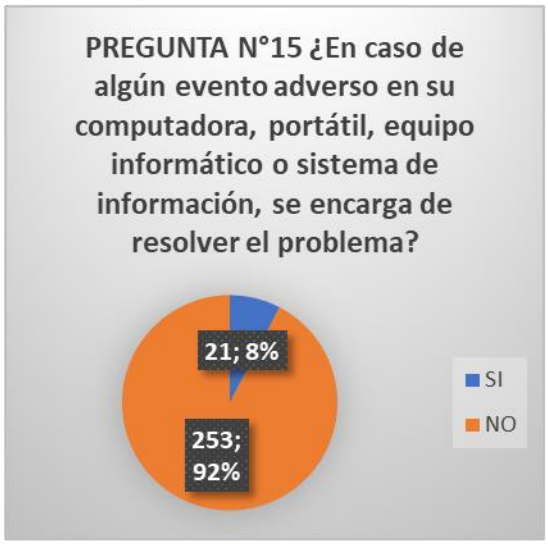

PREGUNTA N°10 ¿Ha enfrentado algún incidente de alteración o pérdida de información, ya sea por virus, acceso no autorizado, daño, extravío, u otras causas, en lo que va del año?
44; 16%
230; 84%
SI
NO

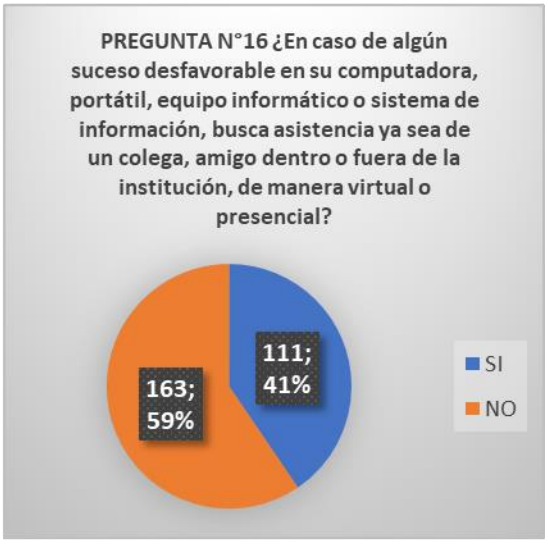

PREGUNTA N°11 ¿Durante el transcurso del año, ha ocurrido algún incidente en el que se haya filtrado información sensible para la institución sin su autorización o conocimiento?
19; 7%
255; 93%
SI
NO

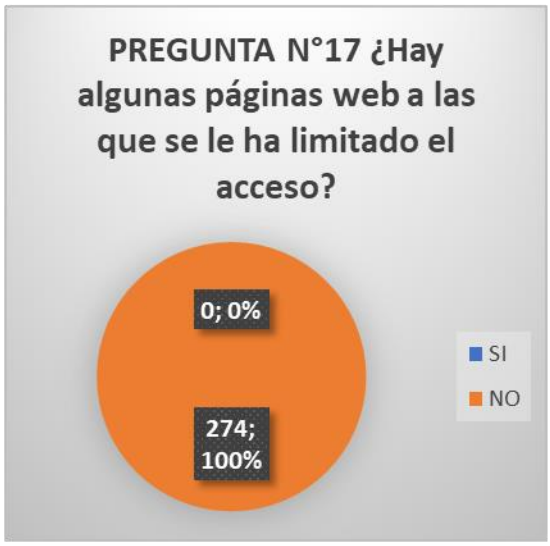

PREGUNTA N°12 ¿Su computadora o laptop cuenta con antivirus actualizado?
2; 1%
272; 99%
SI
NO

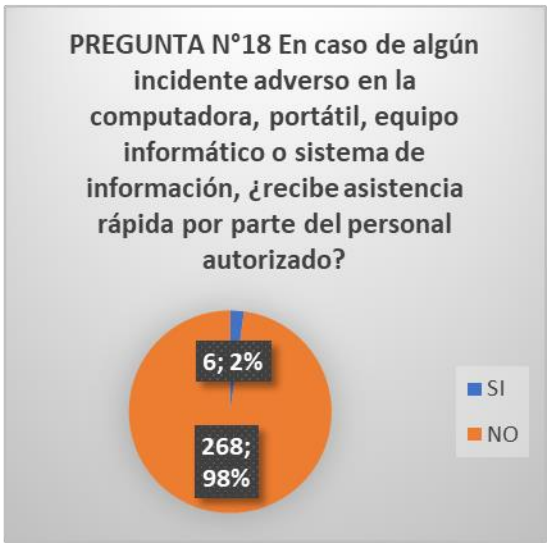

PREGUNTA N°13 ¿Hace backups (copias de información) como medida de protección para sus datos?
11; 4%
263; 96%
SI
NO

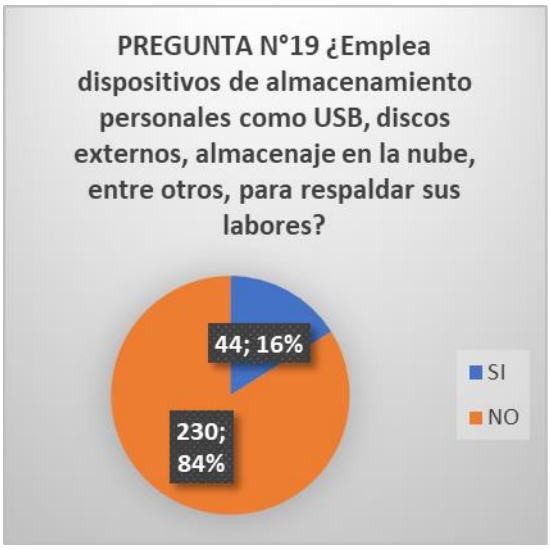

PREGUNTA N°14 ¿Cree usted que su área está protegida de posibles amenazas externas o del entorno que podrían resultar en la pérdida de información?
32; 12%
242; 88%
SI
NO

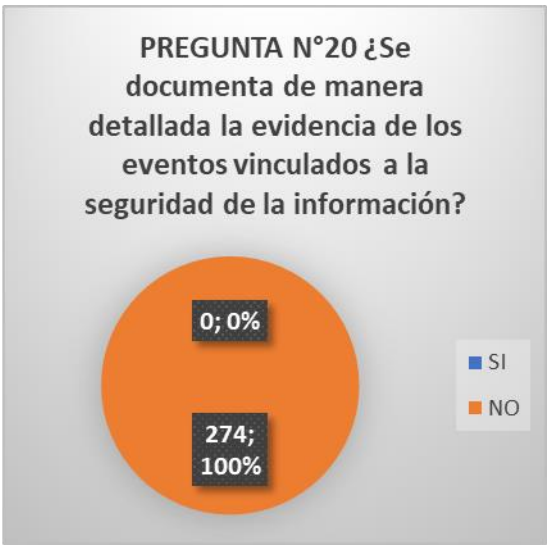

PREGUNTA N°15 ¿En caso de algún evento adverso en su computadora, portátil, equipo informático o sistema de información, se encarga de resolver el problema?
21; 8%
253; 92%
SI
NO


PREGUNTA N°16 ¿En caso de algún suceso desfavorable en su computadora, portátil, equipo informático o sistema de información, busca asistencia ya sea de un colega, amigo dentro o fuera de la institución, de manera virtual o presencial?
111; 41%
163; 59%
SI
NO


PREGUNTA N°17 ¿Hay algunas páginas web a las que se le ha limitado el acceso?
0; 0%
274; 100%
SI
NO


PREGUNTA N°18 En caso de algún incidente adverso en la computadora, portátil, equipo informático o sistema de información, ¿recibe asistencia rápida por parte del personal autorizado?
6; 2%
268; 98%
SI
NO


PREGUNTA N°19 ¿Emplea dispositivos de almacenamiento personales como USB, discos externos, almacenaje en la nube, entre otros, para respaldar sus labores?
44; 16%
230; 84%
SI
NO


PREGUNTA N°20 ¿Se documenta de manera detallada la evidencia de los eventos vinculados a la seguridad de la información?
0; 0%
274; 100%
SI
NO

Anexo 06: Tabla de referencia para la catalogación de activos de TI según Magerit versión 3

Tipo de activo		Sub clasificación		Descripción de aclaración
[info]	información	[adm]	datos de interés para la administración pública	
		[dv]	datos vitales (registros de la organización)	Información esencial para la supervivencia de la Organización. Su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar: - Aquellos que son imprescindibles para que la Organización supere una situación de emergencia - Aquellos que permiten desempeñar o reconstruir las misiones críticas - Aquellas de naturaleza legal o los derechos financieros de la Organización o sus usuarios.
		[per]	datos de carácter personal	Información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.
		[clasificado]	datos clasificados	Información sometida a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente relevante. La tipificación de qué datos deben ser clasificados y cuáles son las normas para su tratamiento, vienen determinadas por regulaciones gubernamentales, sectoriales, por acuerdos entre organizaciones o por normativa interna.
[dato]	Datos o documentos	[files]	ficheros	
		[backup]	copias de respaldo	
		[conf]	datos de configuración	Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información
		[int]	datos de gestión interna	Incluye la información referente a los niveles de acceso asignados a los distintos tipos de usuario según

				su función o puesto de trabajo
		[password]	credenciales	Claves de acceso a máquina asignada o a las aplicaciones
		[auth]	datos de validación de credenciales	Códigos de identificación de usuario
		[acl]	datos de control de acceso	
		[log]	registro de actividad	Los registros de actividad sustancian los requisitos de trazabilidad. Bitácoras o log.
		[source]	código fuente	
		[exe]	código ejecutable	
		[test]	datos de prueba	Generados en las pruebas de las aplicaciones o módulos antes de puesta en producción
[keys]	**Claves criptográficas**	[info]	protección de la información	Claves públicas o privadas de cifrado o descifrado de la información
		[com]	protección de las comunicaciones	Claves de cifrado del canal de comunicación, claves de autenticación
		[disk]	cifrado de soportes de información	Cifrado de soportes de información
[serv]	**Servicios**	[www]	acceso a Internet	
		[telnet]	acceso remoto a cuenta local	
		[email]	correo electrónico	Servidor de correo electrónico
		[file]	almacenamiento de ficheros	Servidor de datos
		[ftp]	transferencia de ficheros	
		[edi]	intercambio electrónico de datos	
		[dir]	servicio de directorio	Directorio activo. Localización de personas, permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado
		[idm]	gestión de identidades	Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización

		[ipm]	gestión de privilegios	Aplicación para definir niveles de acceso
[sw]	Aplicaciones	[prp]	desarrollo propio (in house)	
		[sub]	desarrollo a medida (subcontratado)	
		[browser]	navegador web	
		[app]	servidor de aplicaciones	
		[email_client]	cliente de correo electrónico	
		[email_server]	servidor de correo electrónico	
		[file]	servidor de ficheros	
		[dbms]	sistema de gestión de bases de datos	
		[office]	ofimática	
		[av]	anti virus	
		[os]	sistema operativo	
		[mv]	gestor de máquinas virtuales	
		[backup]	sistema de backup	
[hw]	Equipos informáticos	[host]	grandes equipos	Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente altos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción
		[mid]	equipos medios	Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción
		[pc]	informática personal	Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción
		[mobile]	informática móvil	Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son

				fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar
		[pda]	agendas electrónicas	
		[vhost]	equipo virtual	
		[backup]	equipamiento de respaldo	Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.
		[perife]	periféricos	Impresoras y servidores de impresión, escáneres
		[bp]	dispositivo de frontera	Son los equipos que se instalan entre dos zonas de confianza
		[network]	soporte de la red	Dícese de equipamiento necesario para transmitir datos: routers, módems, etc. Modems, conmutadores, routers, bridges, firewalls, wap (punto de acceso inalámbrico)
		[pabx]	centralita telefónica	
		[ipphone]	teléfono IP	
[com]	Comunicaciones	[PSTN]	red telefónica	
		[ISDN]	rdsi (red digital)	
		[X25]	X25 (red de datos)	
		[ADSL]	ADSL	
		[radio]	comunicaciones radio	
		[wifi]	red inalámbrica	
		[mobile]	telefonía móvil	
		[sat]	por satélite	
		[LAN]	red local	
		[MAN]	red metropolitana	
		[Internet]	Internet	
[media]	Soporte de información	[electro]	electrónicos	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo: discos, DVD, cintas, etc.
		[noelectro]	no electrónicos	Material impreso
[aux]	Equipamiento auxiliar	[power]	fuentes de alimentación	
		[ups]	sistemas de alimentación ininterrumpida	
		[gen]	generadores eléctricos	

		[ac]	equipos de climatización	
		[cabling_wire]	cable eléctrico	
		[cabling_utp]	cable de datos	
		[fiber]	fibra óptica	
		[supply]	suministros esenciales	Toner
		[furniture]	mobiliario: armarios, etc	
		[safe]	cajas fuertes	
[inmueb]	Intalaciones	[building]	edificio	
		[data]	Cuarto de procesamiento de datos	
		[backup]	instalaciones de respaldo	
[pers]	Personal	[ue]	usuarios externos	
		[ui]	usuarios internos	
		[op]	Operadores	
		[adm]	administradores de sistemas	
		[com]	administradores de comunicaciones	
		[dba]	administradores de BBDD	
		[sec]	administradores de seguridad	
		[des]	desarrolladores / programadores	
		[sub]	subcontratas	
		[prov]	proveedores	

Anexo 07: Tabla de descripción de las dimensiones de seguridad de la información que se tomarán en cuenta en la valoración de la criticidad de los activos de TI según Magerit versión 3

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Anexo 08: Catálogo de amenazas por activo y dimensión de seguridad de la información según Magerit versión 3.

AMENAZAS				
[AN]	**DESASTRES NATURALES**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[AN.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[AN.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[AN.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[AI]	**DE ORIGEN INDUSTRIAL**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[AI.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[AI.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[AI.*]	Desastres industriales	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información

		Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.		- [AUX] equipamiento auxiliar - [L] instalaciones
[AI.3]	Contaminación mecánica	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[AI.4]	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[AI.5]	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	[D] disponibilidad	- [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[AI.6]	Corte del suministro eléctrico	Cese de la alimentación de potencia	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información (electrónicos) - [AUX] equipamiento auxiliar
[AI.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[AI.8]	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	[D] disponibilidad	- [COM] redes de comunicaciones
[AI.9]	Interrupción de otros servicios y suministros esenciales	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante,	[D] disponibilidad	- [AUX] equipamiento auxiliar

[AI.10]	Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	- [Media] soportes de información
[AI.11]	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.	[C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] media - [AUX] equipamiento auxiliar - [L] instalaciones
[AE]	**ERRORES Y FALLOS NO INTENCIONADOS**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[AE.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [Media] soportes de información
[AE.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones - [Media] soportes de información
[AE.3]	Errores de monitorización *(log)*	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad (trazabilidad)	- [D.log] registros de actividad

[AE.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad	- [D.conf] datos de configuración
[AE.7]	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	[D] disponibilidad	- [P] personal
[AE.8]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	- [SW] aplicaciones (software)
[AE.9]	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	[C] confidencialidad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[AE.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[AE.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	
[AE.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[AE.18]	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo	[D] disponibilidad	- [D] datos / información

		se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.		- [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[AE.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	- [Media] soportes de información - [L] instalaciones - [P] personal (revelación)
[AE.20]	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[I] integridad [D] disponibilidad [C] confidencialidad	- [SW] aplicaciones (software)
[AE.21]	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	[I] integridad [D] disponibilidad	- [SW] aplicaciones (software)
[AE.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes electrónicos - [AUX] equipamiento auxiliar
[AE.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	- [S] servicios - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[AE.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento
[AE.28]	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	- [P] personal interno
[AA]	**ATAQUES INTENCIONADOS**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**

[AA.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	- [D.log] registros de actividad
[AA.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [A] disponibilidad	- [D.log] registros de actividad
[AA.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	[C] confidencialidad [A] autenticidad [I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[AA.6]	Abuso de privilegios de acceso	Cada usuario utiliza un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, puede ocasionar problemas.	[C] confidencialidad [I] integridad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[AA.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	- [SW] aplicaciones (software)
[AA.9]	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[AA.10]	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones

[AA.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[AA.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".	[C] confidencialidad	- [COM] redes de comunicaciones
[AA.13]	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	[I] integridad (trazabilidad)	- [S] servicios - [D.log] registros de actividad
[AA.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	- [COM] redes de comunicaciones
[AA.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[AA.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW)

				- [Media] soportes de información - [L] instalaciones
[AA.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[AA.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	- [SW] aplicaciones (software)
[AA.22]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	- [HW] equipos - [Media] soportes de información - [AUX] equipamiento auxiliar
[AA.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada (saturación del equipo informático)	[D] disponibilidad	- [S] servicios - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[AA.25]	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[AA.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información

		personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)		- [AUX] equipamiento auxiliar - [L] instalaciones
[AA.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	- [L] instalaciones
[AA.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	- [P] personal interno
[AA.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	- [P] personal interno
[AA.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	- [P] personal interno

Anexo 09: Fichas para la evaluación del nivel de madurez de la primera auditoría

Ficha 1: Nivel de Madurez del Proceso PO1: Definir el plan estratégico de Tecnología de la Información

<table>
<tr><th colspan="5">DOMINIO: PLANIFICAR Y ORGANIZAR</th></tr>
<tr><th colspan="5">PO1: Definir el plan estratégico de Tecnología de la Información</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>La dirección no muestra conciencia de la necesidad de la planificación estratégica de TI para respaldar los objetivos de la organización.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ
El proceso de Definir el Plan Estratégico de Tecnología Información está en el nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• Que no existe un plan estratégico de TI y estrategias de recursos de la Organización.
• No se realizan planes a largo plazo de TI, haciendo solo actualizaciones debido a los avances tecnológicos.</td></tr>
<tr><td>NIVEL 1</td><td>En las reuniones de la dirección, se aborda ocasionalmente la planificación estratégica de TI.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>Las decisiones estratégicas se toman proyecto por proyecto, sin coherencia con una estrategia global de la organización.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>La planificación estratégica de TI sigue un enfoque estructurado, documentado y compartido con todo el equipo. Las estrategias de recursos humanos, técnicos y financieros de TI tienen una influencia creciente en la adquisición de nuevos productos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Hay procesos bien definidos para determinar el uso de recursos internos y externos necesarios en el desarrollo y las operaciones de los sistemas.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Se abordan y elaboran planes acordes a la realidad de la entidad a largo plazo de TI y la actualización de constante para mostrar los avances tecnológicos cambiantes y el progreso relacionado al negocio de la entidad.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso PO1 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Elaborar planes a largo plazo de TI para alcanzar los objetivos del proceso.</td></tr>
<tr><td colspan="5">• Analizar las alternativas para la toma de decisiones estratégicas.</td></tr>
<tr><td colspan="5">• Definir los recursos de los procesos internos y externos primarios y necesarios.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias: En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Analizar y evaluar el desempeño actual del proceso, es decir realizar una evaluación exhaustiva de los planes estratégicos existentes, así como de los SI (sistemas de información) y su impacto de los objetivos en la MDA</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Crear planes tácticos de TI (tecnología de información) a futuro, que resulten del plan estratégico de TI (tecnología de información), estos planes deben ser bien específicos y detallados previo un análisis exhaustivo para poder realizar la definición de planes proyectados.</td></tr>
</table>

Ficha 2: Nivel de Madurez del Proceso PO2: Definir la arquitectura de la información

DOMINIO: PLANIFICAR Y ORGANIZAR				
PO2: Definir la arquitectura de la información				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	En la organización, no se cuenta con el conocimiento, la experiencia ni las responsabilidades necesarias para llevar a cabo el desarrollo de esta arquitectura.	√		**GRADO DE MADUREZ** El proceso de Definir la Arquitectura de la Información está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • Que no se resolvió necesidades futuras del negocio realizando el proceso de la arquitectura de la información. • Aprovechar las habilidades personales para la construcción de la arquitectura de la información.
NIVEL 1	La dirección reconoce la necesidad de una arquitectura de información, aunque el desarrollo de algunos componentes ocurre de manera improvisada.	√		
NIVEL 2	Las habilidades del personal se adquieren mediante la construcción práctica de la arquitectura de información y la aplicación repetida de técnicas.		√	
NIVEL 3	Se establece formalmente una función de administración de datos que define estándares para toda la organización y comienza a informar sobre la implementación y uso de la arquitectura de información.		√	
NIVEL 4	El proceso de definición de la arquitectura de información es proactivo y se centra en resolver las necesidades futuras del negocio.		√	
NIVEL 5	El equipo de TI posee la experiencia y las habilidades necesarias para desarrollar y mantener una arquitectura de información robusta y sensible que refleje todos los requisitos del negocio.		√	
RECOMENDACIONES				
Para el proceso PO2 de COBIT estable los siguientes objetivos de control:				
• Estructurar y Desarrollar la arquitectura de la información para que el proceso sea mucho más ágil.				
• Comprender y tener bien en claro la definición proceso de la arquitectura de la información.				
• Ser partícipe de la construcción de la arquitectura de la información para incrementar sus habilidades por medio de la experiencia.				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias: En el Corto Plazo:				
• Establecer y desarrollar un modelo de arquitectura de la información para facilitar el desarrollo de aplicaciones y actividades de soporte a la toma de decisiones, este modelo será útil para la creación, uso y compartición óptimas de la información vital.				
En el Largo Plazo:				
• Definir e implementar procedimientos para brindar integridad y consistencia de todos los datos que se encuentran almacenados en formato electrónico, como bases de datos, almacenamiento de datos y archivos.				

Ficha 3: Nivel de Madurez del Proceso PO3: Determinar la dirección tecnológica

<table>
<tr><th colspan="5">DOMINIO: PLANIFICAR Y ORGANIZAR</th></tr>
<tr><th colspan="5">PO3: Determinar la dirección tecnológica</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>No se tiene consciencia acerca de la relevancia de la planificación de la infraestructura tecnológica para la entidad.</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de Determinar la Dirección Tecnología está en el nivel de madurez 1.

OBJETIVOS NO CUMPLIDOS • Desarrollar las habilidades para la elaboración del plan de la infraestructura tecnológica en la MDA. • Realizar un plan de infraestructura tecnológica.</td></tr>
<tr><td>NIVEL 1</td><td>La administración reconoce la importancia de planificar la infraestructura tecnológica, así como el desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes, pero lo hace de manera no sistemática y de forma aislada.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 2</td><td>La evaluación de los cambios tecnológicos se encomienda a individuos que siguen procesos intuitivos, aunque similares.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Actualmente hay un plan de infraestructura tecnológica definido, documentado y ampliamente difundido, pero su aplicación y ejecución es inconsistente.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>El departamento de informática cuenta con la experiencia y habilidades necesarias para elaborar un plan de infraestructura tecnológica.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>La dirección del plan de infraestructura tecnológica se guía por estándares y avances industriales e internacionales en lugar de depender de los proveedores de tecnología.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso PO3 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Definir, Plantear, evaluar y Elaborar un plan de infraestructura tecnológica que se adecúe a la MDA.</td></tr>
<tr><td colspan="5">• No dejar a cargo los cambios e innovaciones tecnológicas a personas aficionadas que no tienen la debida experiencia, sino identificar a los stakeholders (interesados) clave que puedan influir en la dirección tecnológica. Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Contar con personal con experiencia en transformación digital, es decir que estos puedan analizar las tecnologías existentes y emergentes, para tomar en cuenta cual dirección tecnológica es apropiada para lograr cumplir con las estrategias de TI, y la arquitectura de sistemas del negocio.</td></tr>
<tr><td colspan="5">• Capacitar y formar a los empleados para que estén preparados para las nuevas tecnologías que se implementarán. Esto incluye tanto a la alta dirección como al personal técnico.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
</table>

• Establecer un proceso continuo de evaluación y monitoreo de tendencias tecnológicas, para asegurarse de que las soluciones implementadas sigan siendo relevantes y eficientes en el tiempo, para de esta forma brindar directrices tecnológicas.

Ficha 4: Nivel de Madurez del Proceso PO4: Definir los procesos, la organización y las relaciones de TI

DOMINIO: PLANIFICAR Y ORGANIZAR				
PO4: Definir los procesos, la organización y las relaciones de TI				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La eficacia en la orientación hacia los objetivos empresariales no está correctamente establecida en la estructura de Tecnologías de la Información (TI).	√		**GRADO DE MADUREZ** El proceso de Definir los Procesos, la Organización y las Relaciones de TI está en el nivel 2 de madurez **OBJETIVOS NO CUMPLIDOS** • Formular las relaciones con terceros para la TI en la MDA. • No satisfacer los requerimientos de la MDA
NIVEL 1	La función de TI se percibe únicamente como un respaldo sin una visión global dentro de la organización.	√		
NIVEL 2	Aunque se reconoce la necesidad de una organización estructurada, las decisiones aún se basan en el conocimiento y habilidades de individuos clave.	√		
NIVEL 3	Las relaciones con terceros, como comités de dirección, auditoría interna y gestión de proveedores, están siendo establecidas.		√	
NIVEL 4	La respuesta proactiva al cambio y la influencia en todos los roles necesarios para cumplir con los requisitos organizativos son características de la organización de TI.		√	
NIVEL 5	La estructura organizacional de TI exhibe flexibilidad y adaptabilidad.		√	
RECOMENDACIONES				
Para el proceso PO4 de COBIT estable los siguientes objetivos de control:				
• Capacitación y desarrollo de personal, proporcionar capacitación y desarrollo continuo para el personal involucrado en los procesos de TI.				
• Seguimiento y medición de procesos, Implementar sistemas de seguimiento y medición para evaluar la eficacia y eficiencia de los procesos de TI para responder de forma proactiva a los requerimientos de la MDA				
• Formular relaciones con terceros como los individuos clave (personal profesional con amplia experiencia en TI) y personal que realice auditorías internas.				
Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias: En el Corto Plazo:				
• Realizar una evaluación inicial de los procesos de TI para identificar las áreas de mejora más críticas y desarrollar un plan de acción para abordar las deficiencias más urgentes.				
• Impartir evaluaciones permanentes al personal, para así asegurar que el personal involucrado en las TI comprendan su rol en la MDA.				
En el Largo Plazo:				

• Implementar un programa de gestión del cambio para asegurar que todos los miembros de la organización estén alineados con los nuevos procesos y estructuras de TI. Comunicar de manera efectiva los beneficios del cambio.

Ficha 5: Nivel de Madurez del Proceso PO5: Administrar la Inversión en TI.

DOMINIO: PLANIFICAR Y ORGANIZAR PO5: Administrar la Inversión en TI.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No hay supervisión ni seguimiento de las inversiones y gastos relacionados con la tecnología de la información (TI).	√		**GRADO DE MADUREZ** El proceso de Administrar la Inversión en TI está en el nivel 1 de madurez . **OBJETIVOS NO CUMPLIDOS** • Falta de alineación estratégica en la MDA. • Falta de transparencia en el gasto en TI en la MDA.
NIVEL 1	Se reconoce la importancia de gestionar las inversiones en TI, aunque esta necesidad se comunica de manera irregular.	√		
NIVEL 2	El cumplimiento depende de la iniciativa individual dentro de la organización. Se utilizan enfoques comunes para elaborar partes del presupuesto de TI. Las decisiones presupuestarias son reactivas y tácticas.		√	
NIVEL 3	El personal de TI posee la experiencia y habilidades necesarias para desarrollar el presupuesto de TI y recomendar inversiones adecuadas.		√	
NIVEL 4	Se realizan análisis formales de costos que abarcan tanto los costos directos como los indirectos de las operaciones existentes, así como propuestas de inversión que consideran todos los costos a lo largo del ciclo de vida. Se utiliza un proceso de presupuesto proactivo y estandarizado.		√	
NIVEL 5	Las decisiones de inversión toman en cuenta las tendencias de mejora de precio/desempeño. Se exploran y evalúan formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital de la organización, utilizando métodos de evaluación formales. Se realiza una identificación proactiva de las variaciones.		√	
RECOMENDACIONES				
Para el proceso PO5 de COBIT estable los siguientes objetivos de control:				

• Desarrollar y documentar políticas y procedimientos básicos para la gestión de inversiones en TI. Esto puede incluir la identificación de responsabilidades clave y la creación de un marco de toma de decisiones inicial.
• Definir un presupuesto inicial para las inversiones en TI, basado en las necesidades y prioridades de la organización.
• Implementar un proceso de seguimiento y control de los gastos relacionados con las inversiones en TI para asegurar que se adhieran al presupuesto establecido.
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias: En el Corto Plazo:
• Realizar una evaluación rápida de los riesgos asociados a las inversiones en TI en curso. Identificar los riesgos más críticos y tomar medidas inmediatas para mitigarlos.
• Implementar procesos básicos de gestión financiera de TI, como la elaboración de presupuestos, seguimiento de gastos y revisión de inversiones existentes. Esto ayudará a establecer una base sólida.
En el Largo Plazo:
• Invertir en la capacitación y el desarrollo del personal involucrado en la gestión de inversiones en TI. Esto asegurará que el equipo esté preparado para tomar decisiones informadas y estratégicas.
• A largo plazo, considera la implementación de herramientas de gestión financiera de TI y sistemas de apoyo decisional para facilitar la toma de decisiones basadas en datos.

Ficha 6: Nivel de Madurez del Proceso PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia

DOMINIO: PLANIFICAR Y ORGANIZAR				
PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La gestión no ha instaurado un entorno positivo para la supervisión de la información. No existe la conciencia de la necesidad de desarrollar un conjunto de políticas, procedimientos, estándares y procesos de conformidad.	√		**GRADO DE MADUREZ** El proceso de Comunicar las Aspiraciones y la Dirección de la Gerencia está en el nivel 0 de madurez. **OBJETIVOS NO CUMPLIDOS** • Falta de claridad en la visión en la MDA. • Comunicación ineficaz en la MDA. • Falta de compromiso en la MDA.
NIVEL 1	Los procedimientos relativos a la creación, comunicación y cumplimiento son informales e irregulares.		√	
NIVEL 2	Se ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la creación se deja a la discreción de los gerentes y áreas de negocio respectivas.		√	
NIVEL 3	La dirección ha concebido, documentado y comunicado un entorno integral de gestión de calidad y control de la información, que incorpora un marco para las políticas, procedimientos y estándares.		√	
NIVEL 4	La dirección asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad, asignando suficientes recursos para mantener el		√	

	entorno en consonancia con los cambios significativos.			
NIVEL 5	El entorno de control de la información se alinea con el marco estratégico de gestión y la visión, y se revisa, actualiza y mejora con frecuencia.		√	
RECOMENDACIONES				
Para el proceso PO6 de COBIT estable los siguientes objetivos de control:				
• Desarrollar mensajes clave que comuniquen las aspiraciones y la dirección de la gerencia de manera clara y coherente. Estos mensajes deben alinearse con los objetivos estratégicos de la MDA.				
• Asegurarse de que los mensajes se comprendan correctamente por parte de los stakeholders y que no haya malentendidos. Esto podría requerir capacitación en comunicación para los miembros del personal.				
• Fomentar la transparencia en la comunicación para ganar la confianza de los stakeholders y promover una cultura de apertura en la MDA.				
Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias: En el Corto Plazo:				
• Comienza por identificar a las partes interesadas clave en la organización, como la alta dirección, los empleados y los clientes. Comprender sus expectativas es fundamental para la comunicación efectiva.				
• Realiza reuniones internas de comunicación para presentar la declaración de aspiraciones y la dirección de la gerencia a los empleados. Asegúrate de explicar cómo esto impactará en su trabajo y en la organización en general.				
En el Largo Plazo:				
• Implementa programas de capacitación a largo plazo para mejorar las habilidades de comunicación en toda la MDA. Esto garantizará que la comunicación de las aspiraciones y la dirección de la gerencia sea efectiva y constante.				
• Fomentar una cultura de comunicación abierta y transparente en la MDA. Esto implica alentar a los empleados a compartir sus ideas y preocupaciones de manera regular.				

Ficha 7: Nivel de Madurez del Proceso PO7: Administrar los Recursos Humanos de TI.

DOMINIO: PLANIFICAR Y ORGANIZAR				
PO7: Administrar los Recursos Humanos de TI.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No hay conciencia acerca de la importancia de alinear la gestión de los recursos humanos en tecnología de la información con el proceso de planificación tecnológica en la organización.	√		**GRADO DE MADUREZ** El proceso de Administrar los Recursos Humanos de TI está en el nivel 1 de madurez. **OBJETIVOS NO CUMPLIDOS** • Falta de roles y responsabilidades claramente definidos para el personal de TI en la MDA. • Falta de planificación estratégica de recursos humanos de TI en la MDA
NIVEL 1	Se reconoce por parte de la dirección la necesidad de implementar una gestión de recursos humanos en tecnología de la información.	√		
NIVEL 2	Se adopta un enfoque táctico para la contratación y gestión del personal en tecnología de la información.		√	
NIVEL 3	Existe un proceso claramente definido y documentado para la gestión de los recursos humanos en tecnología de la información, respaldado por		√	

	un plan de gestión de recursos humanos.			
NIVEL 4	La organización utiliza métricas estandarizadas para identificar desviaciones respecto al plan de gestión de recursos humanos en tecnología de la información, con especial énfasis en el manejo del crecimiento y la rotación del personal.		√	
NIVEL 5	El plan de gestión de recursos humanos en tecnología de la información se actualiza de manera continua para satisfacer los cambiantes requisitos del negocio.		√	
RECOMENDACIONES				
Para el proceso PO7 de COBIT estable los siguientes objetivos de control:				
• Establecer roles y responsabilidades claros para el personal de TI, de modo que sepan qué se espera de ellos en términos de sus funciones y tareas				
• Desarrollar y comunicar políticas y procedimientos de recursos humanos específicos para el departamento de TI, que incluyan aspectos como la contratación, la formación y el desarrollo del personal.				
• Implementar un proceso de contratación que garantice la selección de candidatos calificados y adecuados para los puestos de TI.				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias: En el Corto Plazo:				
• Establecer procesos básicos para la gestión de recursos humanos, como la evaluación del desempeño, la gestión de capacitación y desarrollo, y la gestión de conflictos.				
• Proporcionar capacitación adicional a los miembros del equipo para mejorar sus habilidades técnicas y de gestión.				
En el Largo Plazo:				
• Implementar sistemas de gestión de recursos humanos de TI que faciliten la administración de datos y procesos, como sistemas de seguimiento de candidatos y sistemas de gestión del desempeño.				
• Identificar y retener talento clave, y también tener un plan para la sucesión en caso de cambios en el equipo.				

Ficha 8: Nivel de Madurez del Proceso PO8: Administrar la Calidad.

DOMINIO: PLANIFICAR Y ORGANIZAR				
PO8: Administrar la Calidad.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dirección ejecutiva y el equipo de Tecnologías de la Información no reconocen la imperativa necesidad de implementar un programa de calidad. La evaluación de la calidad en los proyectos y operaciones nunca se lleva a cabo.	√		**GRADO DE MADUREZ** El proceso de Administrar la Calidad está en el nivel 0 de madurez. **OBJETIVOS NO CUMPLIDOS** • No existen procesos claramente definidos ni documentados para las actividades relacionadas con la calidad en la MDA. • La MDA puede no estar prestando la debida
NIVEL 1	Existe una consciencia dentro de la dirección acerca de la importancia de un Sistema de Gestión de la Calidad (QMS, por sus siglas en inglés).		√	

NIVEL 2	Se ha iniciado un programa para definir y supervisar las actividades relacionadas con el Sistema de Gestión de la Calidad (QMS) dentro del ámbito de Tecnologías de la Información.		√	atención a las necesidades y expectativas de los servicios que brinda. • No se están tomando medidas sistemáticas para identificar y abordar las oportunidades de mejora en los procesos
NIVEL 3	La dirección ha comunicado un proceso claramente definido para el Sistema de Gestión de la Calidad (QMS) e implica a los equipos de Tecnologías de la Información y a la gerencia de los usuarios finales.		√	
NIVEL 4	El Sistema de Gestión de la Calidad (QMS) se encuentra integrado en todos los procesos, incluyendo aquellos que dependen de terceros. Se está estableciendo una base de conocimiento estandarizada para las métricas de calidad.		√	
NIVEL 5	El Sistema de Gestión de la Calidad (QMS) está completamente integrado y aplicado en todas las actividades de Tecnologías de la Información. Los procesos de QMS son flexibles y se adaptan a los cambios en el entorno de TI.		√	

RECOMENDACIONES
Para el proceso PO8 de COBIT estable los siguientes objetivos de control:
• Definir y documentar las políticas de calidad básicas de la organización para asegurarse de que todos los empleados las conozcan.
• Designar roles y responsabilidades relacionados con la gestión de calidad, como el nombramiento de un responsable de calidad.
• Identificar y definir los indicadores clave de calidad que se medirán en el futuro.
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias: En el Corto Plazo:
• Sumergirse y recabar información sobre un QMS (Sistema de Gestión de la Calidad).
• Establecer metas específicas y alcanzables a corto plazo para mejorar la gestión de calidad en tus proyectos. Esto podría incluir la reducción de defectos en los servicios que se brinda.
• Proporciona capacitación inmediata a tu equipo sobre los principios de gestión de calidad y cómo aplicarlos en su trabajo diario.
En el Largo Plazo:
• Fomenta una cultura organizacional que valore la calidad en todos los niveles. Esto implica promover la responsabilidad y la importancia de la calidad en la toma de decisiones.
• Implementar un QMS (Sistema de Gestión de la Calidad). basado en estándares reconocidos, como ISO 9001. Esto ayudará a estandarizar y mejorar continuamente los procesos de calidad.

Ficha 9: Nivel de Madurez del Proceso PO9: Evaluar y administrar los riesgos TI

<table>
<tr><th colspan="5">DOMINIO: PLANIFICAR Y ORGANIZAR</th></tr>
<tr><th colspan="5">PO9: Evaluar y administrar los riesgos TI</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>No se lleva a cabo una evaluación y gestión de los riesgos asociados a la tecnología de la información.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ
El proceso de Evaluar y administrar los riesgos TI está en el nivel 1 de madurez.

OBJETIVOS NO CUMPLIDOS
• Establecimiento del contexto del riesgo • Identificación de posibles eventos • Evaluación y respuesta de riesgos • Mantenimiento y monitoreo de un plan de acción de riesgos</td></tr>
<tr><td>NIVEL 1</td><td>Aunque se reconoce la necesidad de evaluar y gestionar los riesgos de TI, la comunicación de esta necesidad es inconsistente dentro de la organización.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 2</td><td>Existe un conocimiento implícito sobre la necesidad de evaluar y gestionar los riesgos de TI.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>El departamento de Informática establece los contextos de los riesgos y identifica los eventos (amenazas y vulnerabilidades).</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>El departamento de Informática realiza la evaluación de los riesgos identificados y también responde a ellos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>El departamento de Informática se rige bajo un plan de acción de riesgos para el mantenimiento preventivo y/o correctivo y monitoreo de los riesgos.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso PO9 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Establecer un inventario de todos los activos de TI en la MDA, incluyendo hardware, software y datos.</td></tr>
<tr><td colspan="5">• Realizar evaluaciones periódicas de vulnerabilidades en los sistemas de TI para identificar posibles puntos de debilidad.</td></tr>
<tr><td colspan="5">• Establecer políticas de seguridad claras que guíen las prácticas de gestión de riesgos y seguridad de TI en la organización.</td></tr>
<tr><td colspan="5">• Realizar evaluaciones de riesgos periódicas para identificar amenazas y evaluar su impacto en los activos de TI.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias: En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Identificar los activos de TI más críticos en la MDA y los riesgos asociados a ellos. Est permitirá establecer una base sólida para la gestión de riesgos.</td></tr>
<tr><td colspan="5">• Desarrollar e implementar políticas de seguridad de la información que aborden las áreas de mayor riesgo identificadas en la evaluación inicial.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Crea un plan integral de gestión de riesgos de TI que incluya procedimientos detallados para identificar, evaluar y mitigar riesgos de manera continua.</td></tr>
<tr><td colspan="5">• Invertir en la capacitación y concienciación de los empleados en cuanto a la gestión de riesgos. Esto ayudará a crear una cultura organizacional que valora la seguridad de la información.</td></tr>
</table>

Ficha 10: Nivel de Madurez del Proceso PO10: Administrar Proyectos.

<table>
<tr><th colspan="5">DOMINIO: PLANIFICAR Y ORGANIZAR</th></tr>
<tr><th colspan="5">PO10: Administrar Proyectos.</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>En la organización, no se emplean las técnicas de gestión de proyectos, y no se toma en consideración la repercusión empresarial asociada con la gestión deficiente de proyectos y los fallos en el desarrollo del proyecto.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ
El proceso de Administrar Proyectos está en el nivel 0 de madurez

OBJETIVOS NO CUMPLIDOS
• La MDA carece de procesos definidos para planificar, ejecutar y controlar proyectos de manera efectiva.
• Presencia de dificultades para asignar recursos de manera eficiente a proyectos, lo que puede resultar en la falta de recursos críticos en momentos importantes.
• La MDA no cuenta un enfoque estructurado para identificar y gestionar los riesgos asociados a los proyectos.</td></tr>
<tr><td>NIVEL 1</td><td>Hay una falta de compromiso por parte de la alta dirección hacia la propiedad y gestión de proyectos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>La alta dirección ha adquirido conciencia de la necesidad de gestionar proyectos de tecnologías de la información y ha comunicado esta conciencia.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>La alta dirección organizacional y de tecnologías de la información comienza a comprometerse y participar activamente en la gestión de proyectos de tecnologías de la información.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>La gerencia requiere la revisión de métricas y lecciones aprendidas de manera estandarizada y formal al concluir cada proyecto.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Se ha implementado una metodología de ciclo de vida de proyectos probada, la cual se refuerza y se incorpora de manera integral en la cultura de toda la organización.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso PO10 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Identificar los proyectos en curso y futuros.</td></tr>
<tr><td colspan="5">• Definir los roles y responsabilidades básicos para los participantes en los proyectos.</td></tr>
<tr><td colspan="5">• Iniciar un registro de proyectos básico para realizar un seguimiento de la información esencial.</td></tr>
<tr><td colspan="5">• Identificar y asignar recursos de manera ad hoc (adecuada) a los proyectos.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias: En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Realizar una revisión exhaustiva de los proyectos que actualmente están en marcha. Identificar áreas de mejora y posibles problemas en la gestión de proyectos existentes.</td></tr>
<tr><td colspan="5">• Proporcionar capacitación inmediata al equipo en las mejores prácticas de gestión de proyectos. Esto ayudará a mejorar la competencia y comprensión de los procesos.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Diseñar un plan estratégico de mejora continua que incluya metas claras y medibles para avanzar hacia niveles superiores de madurez en la gestión de proyectos.</td></tr>
<tr><td colspan="5">• Considerar la posibilidad de formar un equipo de gestión de proyectos dedicado que se enfoque en la mejora constante de los procesos y la capacitación del personal.</td></tr>
</table>

Ficha 11: Nivel de Madurez del Proceso AI1: Identificar Soluciones Automatizadas

<table>
<tr><th colspan="5">DOMINIO: ADQUIRIR E IMPLEMENTAR</th></tr>
<tr><th colspan="5">AI1: Identificar Soluciones Automatizadas</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>La entidad no encuentra necesario realizar la identificación de los requisitos funcionales y operativos para el desarrollo, implementación o modificación soluciones automatizadas.</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de Identificar Soluciones Automatizadas está en el nivel de madurez 2.

OBJETIVOS NO CUMPLIDOS
• Automatización incompleta en la MDA.
• Poca capacidad de la MDA para tomar decisiones informadas basadas en datos.</td></tr>
<tr><td>NIVEL 1</td><td>Se lleva a cabo una investigación o análisis mínimo y estructurado acerca de la tecnología disponible.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 2</td><td>El éxito de cada proyecto se encuentra vinculado a la experiencia de unos pocos individuos clave. La calidad de la documentación y la toma de decisiones presenta variaciones considerables.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 3</td><td>El proceso de determinación de soluciones de tecnología de la información se implementa en algunos proyectos basándose en factores como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requisito de negocio inicial.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>La documentación de los proyectos cuenta con una calidad destacada y cada fase es aprobada de manera apropiada.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Se respalda la metodología en bases de datos de conocimiento internas y externas que albergan material de referencia sobre soluciones tecnológicas.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso AI1 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Establecer un proceso documentado para la identificación de soluciones automatizadas, que incluya pasos claros y roles y responsabilidades definidos.</td></tr>
<tr><td colspan="5">• Identificar y evaluar diferentes soluciones automatizadas disponibles en el mercado o desarrolladas internamente que puedan abordar las necesidades identificadas.</td></tr>
<tr><td colspan="5">• Seleccionar las soluciones automatizadas más adecuadas y llevar a cabo su implementación de acuerdo con las mejores prácticas y estándares de seguridad de la información.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
</table>

• Realizar una evaluación exhaustiva de las capacidades actuales de la MDA en cuanto a la identificación de soluciones automatizadas. Identificar las áreas de mejora inmediata
• Proporcionar capacitaciones al equipo en inteligencia artificial y automatización. Puedes considerar cursos en línea, talleres o contratar consultores especializados.
En el Largo Plazo:
• Fomentar una cultura de innovación en la MDA. Animar al equipo a proponer ideas y soluciones automatizadas, y recompensa la creatividad.
• Buscar colaboraciones y alianzas con otras organizaciones o instituciones académicas que estén trabajando en áreas relacionadas con la IA. Esto puede acelerar el avance hacia el nivel de madurez 3.
• Implementar un proceso de gestión del cambio sólido para garantizar que las nuevas soluciones automatizadas sean adoptadas de manera efectiva en toda la organización.

Ficha 12: Nivel de Madurez del Proceso AI2: Adquirir y mantener software aplicativo

DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI2: Adquirir y mantener software aplicativo				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Por lo general, las aplicaciones se adquieren en función de las ofertas de los proveedores, el reconocimiento de la marca o la familiaridad del personal de TI con productos específicos, prestando escasa atención a los requisitos actuales.	√		**GRADO DE MADUREZ** El proceso de Adquirir y Mantener Software Aplicativo está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • Dar a conocer el proceso de adquisición y mantenimiento del Sistema de Información (software) y aplicaciones. • Determinar la metodología formal para la documentación del software en uso.
NIVEL 1	Hay una probabilidad que se hayan obtenido de forma independiente diversas soluciones individuales para necesidades específicas de la organización, lo que resulta en ineficiencias en el mantenimiento y soporte.	√		
NIVEL 2	Se observan diferencias en los procesos de adquisición y mantenimiento de aplicaciones, pero estos son similares en función de la experiencia dentro de la operación de TI.		√	
NIVEL 3	Hay un proceso claramente definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso está alineado con la estrategia de TI.		√	
NIVEL 4	Se cuenta con una metodología formal y bien entendida que incluye un proceso de diseño y especificación en criterios de adquisición, así como un proceso de prueba y requisitos para la documentación.		√	

NIVEL 5	El enfoque se amplía a todas las empresas. La metodología de adquisición y mantenimiento ha avanzado considerablemente, permitiendo un posicionamiento estratégico rápido y proporcionando un alto grado de capacidad de respuesta y flexibilidad para hacer frente a los cambiantes requisitos del negocio.		√	
RECOMENDACIONES				
Para el proceso AI2 de COBIT estable los siguientes objetivos de control:				
• Establecer una política clara para la adquisición de software que incluya procesos de revisión y aprobación				
• Mantener un inventario actualizado de todos los activos de software utilizados en la organización, incluyendo licencias y versiones.				
• Evaluar y seleccionar proveedores de software confiables y evaluar sus productos en función de los requisitos de la MDA				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				
• Realizar una evaluación exhaustiva de las necesidades actuales de software aplicativo en la MDA. Identificar las áreas críticas que requieren mejoras inmediatas.				
• Desarrollar un plan para adquirir software aplicativo que aborde las necesidades identificadas. Esto podría incluir la compra de soluciones listas para usar (software comercial) o el desarrollo de software personalizado (software a medida).				
• Asignar los recursos necesarios, como personal y presupuesto, para implementar las soluciones de software de manera eficiente y efectiva.				
En el Largo Plazo:				
• Implementar una política de gestión de activos de software sólida para garantizar que todas las licencias estén actualizadas y que se estén utilizando de manera eficiente.				
• Desarrollar un plan de mantenimiento preventivo para garantizar que el software aplicativo se mantenga actualizado y funcione correctamente a lo largo del tiempo.				

Ficha 13: Nivel de Madurez del Proceso AI3: Adquirir y Mantener Infraestructura Tecnológica

DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI3: Adquirir y Mantener Infraestructura Tecnológica				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se asigna la debida importancia a la gestión de la infraestructura tecnológica como una cuestión prioritaria que requiera atención.	√		**GRADO DE MADUREZ** El proceso de Adquirir y Mantener Infraestructura Tecnológica está en el nivel de madurez 1.
NIVEL 1	Se efectúan modificaciones en la infraestructura cada vez que surge una nueva aplicación, sin un plan integral. Las labores de mantenimiento responden a necesidades a corto plazo.	√		**OBJETIVOS NO CUMPLIDOS** • Definir y establecer una estrategia para la adquisición y mantenimiento de la

NIVEL 2	El mantenimiento y la adquisición de la infraestructura de TI carecen de una estrategia definida y no tienen en cuenta las exigencias de las aplicaciones organizativas que deben ser respaldadas.		√	infraestructura de TI. • Falta de alineación entre la tecnología y los objetivos de la MDA
NIVEL 3	Aunque el proceso respalda las necesidades de las aplicaciones críticas del negocio y se alinea con la estrategia de tecnología de la información, no se implementa de manera consistente.		√	
NIVEL 4	La infraestructura de TI respalda de manera adecuada las aplicaciones del negocio. El proceso está bien estructurado y adopta un enfoque preventivo.		√	
NIVEL 5	El proceso de mantenimiento y adquisición de la infraestructura tecnológica es de naturaleza preventiva y está estrechamente alineado con las aplicaciones críticas del negocio y la arquitectura tecnológica, garantizando una implementación coherente.		√	

RECOMENDACIONES
Para el proceso AI3 de COBIT estable los siguientes objetivos de control:
• Desarrollar y establecer una política formal de adquisición de tecnología que defina los procesos para la compra y adquisición de activos tecnológicos.
• Mantener un inventario actualizado de todos los activos tecnológicos de la organización, incluyendo hardware, software y recursos de red.
• Implementar un proceso formal de control de cambios para gestionar y documentar las modificaciones en la infraestructura tecnológica.
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Realizar un análisis detallado de las necesidades tecnológicas actuales de la MDA y determinar qué componentes de infraestructura tecnológica son prioritarios para mejorar o adquirir de inmediato.
• Investigar y seleccionar proveedores de tecnología confiables y competitivos en términos de calidad y costo. Esto facilitará la adquisición de equipos y servicios tecnológicos necesarios.
• Definir un presupuesto específico para la adquisición y mantenimiento de la infraestructura tecnológica en el corto plazo.
En el Largo Plazo:
• Desarrollar un plan estratégico a largo plazo para la infraestructura tecnológica, considerando las metas y objetivos de la organización en un horizonte temporal más amplio.
• Implementar un programa de mantenimiento preventivo para garantizar que la infraestructura tecnológica funcione de manera óptima a lo largo del tiempo y se eviten interrupciones costosas.
• Destinar recursos a la investigación y desarrollo de nuevas tecnologías que puedan brindar ventajas a servicio de la comunidad a la MDA a largo plazo.

Ficha 14: Nivel de Madurez del Proceso AI4: Facilitar la Operación y el Uso

<table>
<tr><th colspan="5">DOMINIO: ADQUIRIR E IMPLEMENTAR</th></tr>
<tr><th colspan="5">AI4: Facilitar la Operación y el Uso</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>No se ha implementado ningún procedimiento en relación con la generación de documentación para usuarios, manuales operativos y materiales de formación.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ
El proceso de Facilitar la Operación y el Uso está en el nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• No se proporciona soporte o herramientas que faciliten el uso de las TI por parte de los usuarios finales.
• No hay documentos, guías ni recursos que ayuden a comprender ni a utilizar las TI de manera efectiva.</td></tr>
<tr><td>NIVEL 1</td><td>Gran parte de la documentación y muchos de los procedimientos han alcanzado su fecha de caducidad. Los recursos de formación consisten en esquemas individuales con niveles de calidad variables.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>La creación de los materiales de formación recae en individuos o equipos de proyecto, y la calidad está sujeta a la participación de dichos individuos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Los procedimientos se archivan y gestionan en una biblioteca formal, siendo accesibles para aquellos que requieran consultarla.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Se han establecido controles para asegurar la adherencia a estándares y para el desarrollo y mantenimiento de procedimientos en todos los procesos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Los documentos de procedimiento y formación son considerados como una base de conocimiento en constante evolución, conservados electrónicamente y gestionados mediante herramientas actualizadas de gestión del conocimiento, flujo de trabajo y tecnologías de distribución, facilitando su acceso y mantenimiento.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso AI4 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Comenzar a elaborar una política de uso de las TI que establezca las directrices iniciales para su implementación y operación.</td></tr>
<tr><td colspan="5">• Designar a personas o equipos responsables de la gestión de las TI y su operación siguiendo los manuales de usuario.</td></tr>
<tr><td colspan="5">• Desarrollar un plan para realizar soluciones de operación el cual sirva para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
</table>

• Proporciona capacitación y formación rápida a tu equipo para comprender los conceptos básicos de las TI y cómo se aplica en la operación y el uso de la MDA.
En el Largo Plazo:
• Desarrolla una estrategia sólida para la gestión de datos, que incluya la recopilación, limpieza y almacenamiento de datos de alta calidad para alimentar tus proyectos de TI

Ficha 15: Nivel de Madurez del Proceso AI5: Adquirir recursos de TI

DOMINIO: PLANIFICAR Y ORGANIZAR				
AI5: Adquirir recursos de TI				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se ha implementado un procedimiento definido para la obtención de recursos de tecnología de la información (TI).	√		**GRADO DE MADUREZ** El proceso de Adquirir Recursos de TI está en el nivel de madurez 4. **OBJETIVOS NO CUMPLIDOS** • Continuar buscando formas de mejorar los procesos y la adquisición de recursos de TI. • Aunque se logra una alta eficiencia, puede haber áreas específicas que no estén completamente optimizadas.
NIVEL 1	Los contratos destinados a la obtención de recursos de TI son elaborados y gestionados por líderes de proyectos y otros profesionales que ejercen su juicio experto en lugar de adherirse estrictamente a procedimientos y políticas formales.	√		
NIVEL 2	Se establecen responsabilidades y rendición de cuentas para la gestión de la adquisición y contratos de TI en función de la experiencia específica del gerente de contrato.	√		
NIVEL 3	La adquisición de TI se incorpora en gran medida a los sistemas generales de adquisición del negocio.	√		
NIVEL 4	La adquisición de TI se integra ampliamente con los sistemas generales de adquisición de la organización, y se implementan estándares de TI para la obtención de recursos de TI.	√		
NIVEL 5	Se guarda relaciones sólidas con la mayoría de los proveedores y socios a lo largo del tiempo, y se monitorea y evalúa la calidad de estas relaciones. La gestión de relaciones se lleva a cabo de manera estratégica.		√	
RECOMENDACIONES				
Para el proceso AI5 de COBIT estable los siguientes objetivos de control:				
• Establecer criterios de evaluación para seleccionar proveedores de TI confiables y calificados que cumplan con los requisitos de la organización.				

• Implementar un sistema de gestión de contratos sólido para garantizar que los acuerdos sean claros, legales y se cumplan de manera adecuada.
• Supervisar de cerca los costos relacionados con la adquisición de recursos de TI, asegurándose de que se mantengan dentro del presupuesto establecido.
Para pasar al nivel de madurez 5 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Implementar políticas de TI para adquirir los recursos de TI.
En el Largo Plazo:
• Cumplir y hacer cumplir los derechos y obligaciones de ambas partes en los términos contractuales.

Ficha 16: Nivel de Madurez del Proceso AI6: Administrar Cambios

DOMINIO: PLANIFICAR Y ORGANIZAR				
AI6: Administrar Cambios				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No existe conciencia respecto a la posibilidad de que los cambios puedan generar interrupciones tanto para el individuo como para las operaciones comerciales, y tampoco se reconoce la importancia de una gestión efectiva del cambio.	√		**GRADO DE MADUREZ** El proceso de Administrar Cambios está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • Falta de estructura y procedimientos establecidos para gestionar cambios de manera efectiva. • No existe una evaluación de riesgos e impacto de los cambios antes de implementarlos.
NIVEL 1	Se admite la necesidad de gestionar y controlar los cambios, si bien las prácticas al respecto son diversas, lo que aumenta la probabilidad de que se realicen cambios sin la debida autorización.	√		
NIVEL 2	Se observa la presencia de un proceso informal de gestión del cambio, siendo este el enfoque principal para la mayoría de las modificaciones. Sin embargo, dicho proceso carece de estructura, es rudimentario y susceptible a errores.		√	
NIVEL 3	Se constata la existencia de un proceso formal definido para la gestión del cambio, que abarca la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y gestión de la liberación. Además, se observa un incipiente cumplimiento de este proceso.		√	
NIVEL 4	El proceso de gestión del cambio se desarrolla de manera sólida y uniforme para todas las modificaciones. La gerencia confía en que las excepciones son mínimas, y se destaca la eficiencia y efectividad del proceso.		√	

NIVEL 5	Se realiza una revisión periódica del proceso de gestión del cambio, actualizándolo para mantenerse alineado con las mejores prácticas del momento.		√	
RECOMENDACIONES				
Para el proceso AI6 de COBIT estable los siguientes objetivos de control:				
• Asegurarse de que todas las solicitudes de cambio estén claramente identificadas, incluyendo el nombre del solicitante y la justificación del cambio.				
• Realizar evaluaciones de impacto preliminares para determinar cómo los cambios propuestos afectarán a los procesos y a otros sistemas de TI relacionados.				
• Gestionar la implementación de cambios de manera controlada, siguiendo procedimientos definidos y minimizando riesgos.				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				
• Proporcionar capacitación al equipo sobre los conceptos básicos de la gestión de cambios y las prácticas recomendadas. Esto ayudará a crear una comprensión común.				
• Adquirir y desplegar herramientas de gestión de cambios que faciliten la planificación, ejecución y seguimiento de cambios.				
En el Largo Plazo:				
• Documentar y estandarizar los procesos de gestión de cambios para garantizar que se sigan las mejores prácticas de manera consistente.				
• Desarrollar estrategias para abordar la resistencia al cambio, como la capacitación en gestión de resistencia y la promoción de la participación activa de los empleados.				

Ficha 17: Nivel de Madurez del Proceso AI7: Instalar y Acreditar Soluciones y Cambios

DOMINIO: PLANIFICAR Y ORGANIZAR				
AI7: Instalar y Acreditar Soluciones y Cambios				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No existen procedimientos formales de instalación o acreditación, y tanto la alta dirección como el personal de tecnologías de la información no reconocen la necesidad de validar la idoneidad de las soluciones para su propósito previsto.	√		**GRADO DE MADUREZ** El proceso de Instalar y Acreditar Soluciones y Cambios está en el nivel de madurez 0. **OBJETIVOS NO CUMPLIDOS** • Falta de planificación adecuada para la instalación y acreditación de soluciones y cambios. • No existe la recopilación de evidencia necesaria para demostrar que las soluciones y cambios se han implementado de manera efectiva y cumplen con los requisitos establecidos.
NIVEL 1	Se reconoce la necesidad de verificar y confirmar que las soluciones implementadas son adecuadas para el propósito previsto, aunque no hay procesos formales de instalación o acreditación.		√	
NIVEL 2	Si bien hay cierta coherencia en los enfoques de prueba y acreditación, generalmente no se basan en ninguna metodología específica.		√	

NIVEL 3	Se ha establecido una metodología formal para la instalación, migración, conversión y aceptación. Los procesos de tecnologías de la información relacionados con la instalación y acreditación se integran en el ciclo de vida del sistema y se han automatizado en cierta medida.		√	
NIVEL 4	Los procedimientos son formales y han sido diseñados para ser organizados y prácticos, con entornos de prueba definidos y procesos de acreditación establecidos.		√	
NIVEL 5	Los procedimientos de instalación y acreditación han alcanzado un nivel de buenas prácticas, basándose en los resultados de la mejora continua y el refinamiento constante.		√	

RECOMENDACIONES
Para el proceso AI7 de COBIT estable los siguientes objetivos de control:
• Definir un proceso para identificar y documentar las necesidades de cambio de las TI.
• Realizar una evaluación inicial de los riesgos asociados con las soluciones y cambios propuestos.
• Definir un proceso de aprobación para los cambios propuestos, que incluya la revisión y aprobación por parte de las partes relevantes.
• Documentar el proceso de acreditación de soluciones, incluyendo los criterios y pruebas utilizados.
Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Evaluar dónde se encuentra la MDA en cuanto a la instalación y acreditación de soluciones y cambios. Esto ayudará a establecer una línea de base.
• Asignar roles específicos a las personas encargadas de instalar y acreditar soluciones y cambios. Asegúrate de que todos comprendan sus responsabilidades.
• Desarrollar procedimientos básicos para la instalación y acreditación de soluciones y cambios. Esto puede incluir la documentación de procesos y flujos de trabajo.
• Proporcionar capacitación a los empleados involucrados en el proceso. Asegúrate de que estén familiarizados con las mejores prácticas y las normativas relevantes.
En el Largo Plazo:
• Desarrollar políticas y estándares más sólidos para la instalación y acreditación de soluciones y cambios. Estos deben alinearse con los objetivos estratégicos de la MDA
• Fomentar una cultura de mejora continua en la MDA. Anima a los empleados a proponer mejoras y ajustes en los procesos.

Ficha 18: Nivel de Madurez del Proceso DS1: Definir y Administrar los Niveles de Servicio

<table>
<tr><th colspan="5">DOMINIO: ENTREGAR Y DAR SOPORTE</th></tr>
<tr><th colspan="5">DS1: Definir y Administrar los Niveles de Servicio</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>La dirección ejecutiva no muestra conciencia acerca de la importancia de instaurar un procedimiento que defina los estándares de atención al cliente.</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de definir y administrar los niveles de servicio está en nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• No hay una medición y Seguimiento de Niveles de Servicio
• No se realiza y genera reportes de servicio de forma completa y relevante.</td></tr>
<tr><td>NIVEL 1</td><td>No se ha establecido de manera clara la responsabilidad y la obligación de supervisar tanto la formulación como la gestión de los servicios.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>Los informes acerca de los estándares de servicio se presentan de manera incompleta, pudiendo resultar irrelevantes o incluso engañosos para los clientes. La calidad de estos informes depende exclusivamente de las habilidades y la iniciativa de los gestores de manera individual.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>El proceso de elaboración del acuerdo de niveles de servicio se encuentra en orden y cuenta con puntos de control destinados a evaluar tanto los niveles de atención al cliente como su satisfacción.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>La satisfacción del cliente se mide y evalúa de forma regular. Las métricas de rendimiento reflejan las necesidades del cliente en lugar de los objetivos de la tecnología de la información.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Todos los procesos y procedimientos relacionados con la gestión de niveles de servicio están sujetos a un constante proceso de mejora. La administración y supervisión de la satisfacción del cliente se llevan a cabo de forma continua.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso DS1 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Realizar un portafolio de servicios para Identificar sus niveles de servicio asociados.</td></tr>
<tr><td colspan="5">• Documentación de los acuerdos de nivel de servicio (SLA) o acuerdos operativos (OLA) según corresponda.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Comprender los requisitos y necesidades actuales de los clientes y partes interesadas en términos de niveles de servicio. Esto implica recopilar datos y realizar análisis para identificar las expectativas existentes en la MDA.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Diseñar un proceso formal para la definición y administración de niveles de servicio. Esto debe incluir la forma en que se recopilan datos, establecer los acuerdos de nivel de servicio (SLAs) y realizar revisiones periódicas.</td></tr>
</table>

Ficha 19: Nivel de Madurez del Proceso DS2: Administrar los Servicios de Terceros

<table>
<tr><th colspan="5">DOMINIO: ENTREGAR Y DAR SOPORTE</th></tr>
<tr><th colspan="5">DS2: Administrar los Servicios de Terceros</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>La ausencia de directrices formales en relación con la contratación de terceros es evidente.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ
El proceso de Administrar los Servicios de Terceros está en nivel de madurez 2.

OBJETIVOS NO CUMPLIDOS
• No hay una identificación proactiva de riesgos estratégicos de los servicios de terceros en la MDA.
• No hay una gestión de desempeño y cumplimiento, que incluye la supervisión continua y la mejora proactiva de los servicios de terceros.</td></tr>
<tr><td>NIVEL 1</td><td>La dirección reconoce la importancia de establecer políticas y procedimientos detallados para la gestión de servicios proporcionados por terceros, lo que incluye la formalización mediante la firma de contratos.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 2</td><td>La supervisión de proveedores de servicios externos, la evaluación de riesgos asociados y la prestación de servicios se lleva a cabo de manera no estructurada.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 3</td><td>Existen procedimientos exhaustivamente documentados para supervisar los servicios de terceros, con procesos transparentes para abordar y negociar con los proveedores.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Se definen criterios formales y estandarizados para especificar los términos de un acuerdo, abarcando aspectos como el alcance del trabajo, los servicios o entregables a proporcionar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>El seguimiento del cumplimiento de las condiciones operativas, legales y de control se realiza activamente, implementando medidas correctivas. Se emplean medidas de monitoreo para la detección temprana de posibles problemas relacionados con los servicios de terceros.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso DS2 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Asegurar que se establezcan contratos claros y detallados con proveedores de servicios de terceros, que incluyan términos y condiciones específicas, niveles de servicio y responsabilidades.</td></tr>
<tr><td colspan="5">• Evaluar y seleccionar proveedores de servicios de terceros de manera objetiva, considerando su capacidad para cumplir con los requisitos de la MDA.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Proporcionar capacitación al equipo sobre las mejores prácticas en la gestión de terceros y las políticas de la empresa. Esto ayudará a mejorar la colaboración y la comprensión de los procesos.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Considerar la adopción de herramientas de gestión de proveedores y servicios que faciliten el seguimiento y la supervisión continua de las operaciones de terceros.</td></tr>
</table>

Ficha 20: Nivel de Madurez del Proceso DS3: Administrar el Desempeño y la Capacidad

<table>
<tr><th colspan="5">DOMINIO: ENTREGAR Y DAR SOPORTE</th></tr>
<tr><th colspan="5">DS3: Administrar el Desempeño y la Capacidad</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>La dirección ejecutiva no admite la posibilidad de que los procesos críticos de la empresa puedan necesitar un rendimiento significativamente alto de las tecnologías de la información, o que los requisitos totales de servicios de TI para la empresa puedan superar la capacidad existente.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ
El proceso de Administrar el Desempeño y la Capacidad está en el nivel de madurez 1.

OBJETIVOS NO CUMPLIDOS
• La MDA no puede prever y gestionar eficazmente los recursos necesarios para satisfacer la demanda actual y futura.
• No se optimizan los recursos de TI de manera eficiente.</td></tr>
<tr><td>NIVEL 1</td><td>Ada procesos tiene un responsable y se muestran escaso interés en la importancia de llevar a cabo una planificación proactiva de la capacidad y el rendimiento. Las medidas para gestionar el rendimiento y la capacidad suelen adoptarse de manera reactiva.</td><td>√</td><td></td></tr>
<tr><td>NIVEL 2</td><td>Por lo general, se logra satisfacer las necesidades de rendimiento mediante evaluaciones de sistemas individuales y el respaldo de equipos de proyecto con conocimientos especializados.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Los pronósticos de capacidad y rendimiento se modelan mediante un proceso claramente definido, y se generan informes con estadísticas de rendimiento.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>La información actualizada está disponible, proporcionando estadísticas de rendimiento estandarizadas y alertando sobre incidentes derivados de insuficiencias en rendimiento o capacidad.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Se realizan evaluaciones regulares de la infraestructura de TI y la demanda empresarial para garantizar la consecución de una capacidad óptima con el menor costo posible.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso DS3 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Establecer la recopilación de datos de desempeño básica para comprender el comportamiento de los sistemas para los recursos de TI.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Establece procesos y procedimientos básicos para la gestión del desempeño y la capacidad, como la recopilación de datos, el monitoreo de sistemas y la gestión de incidentes.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Realizar un monitoreo continuo del desempeño y la capacidad de los recursos de TI.</td></tr>
</table>

Ficha 21: Nivel de Madurez del Proceso DS4: Garantizar la continuidad del servicio

<table>
<tr><th colspan="5">DOMINIO: PLANIFICAR Y ORGANIZAR</th></tr>
<tr><th colspan="5">DS4: Garantizar la continuidad del servicio</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>La falta de comprensión de los riesgos, vulnerabilidades y amenazas para las operaciones de Tecnologías de la Información es evidente.</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de Garantizar la Continuidad del Servicio está en el nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• Ausencia de Planificación de Continuidad del Servicio
• No hay procedimientos efectivos para manejar incidentes y problemas.</td></tr>
<tr><td>NIVEL 1</td><td>La responsabilidad en relación con la continuidad de los servicios es informal, y las autoridades para llevar a cabo estas responsabilidades son limitadas.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>Los informes sobre la disponibilidad son intermitentes, potencialmente incompletos y no consideran adecuadamente el impacto en las operaciones comerciales.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Existe una asignación y definición clara de responsabilidades para la planificación y las pruebas de la continuidad de los servicios.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Se asigna la responsabilidad de mantener un plan formalizado para la continuidad de los servicios.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Los procesos integrados para la continuidad del servicio incorporan referencias de la industria y adoptan las mejores prácticas externas.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso DS4 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Establecer un inventario de los servicios que son críticos para la MDA y que deben ser respaldados para garantizar la continuidad del servicio.</td></tr>
<tr><td colspan="5">• Desarrollar un plan de continuidad que incluya medidas específicas para mantener la operación de los servicios críticos en caso de interrupciones.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Desarrollar un plan de respuesta ante incidentes que incluya procedimientos claros para abordar interrupciones en el servicio. Asegurar que el equipo esté capacitado para ejecutar este plan de manera efectiva.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• Desarrollar un proceso formal de gestión de riesgos que incluya evaluaciones periódicas de amenazas y vulnerabilidades. Esto te ayudará a identificar áreas de mejora a lo largo del tiempo.</td></tr>
<tr><td colspan="5">• Implementar un enfoque de mejora continua en la gestión de la continuidad del servicio. Esto implica revisar regularmente los procedimientos, identificar debilidades y ajustar las prácticas en consecuencia.</td></tr>
</table>

Ficha 22: Nivel de Madurez del Proceso DS5: Garantizar la Seguridad de los Sistemas

<table>
<tr><th colspan="5">DOMINIO: ENTREGAR Y DAR SOPORTE</th></tr>
<tr><th colspan="5">DS5: Garantizar la Seguridad de los Sistemas</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>Las estrategias para respaldar la gestión de la seguridad de Tecnologías de la Información no han sido aplicadas. No se generan informes sobre la seguridad de TI ni se dispone de un procedimiento para abordar incidentes de seguridad en TI.</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de Garantizar la Seguridad de los Sistemas está en el nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• No se tiene accesos adecuados para proteger la información sensible
• Elaborar un plan de seguridad de TI.</td></tr>
<tr><td>NIVEL 1</td><td>La gestión de la seguridad de TI se realiza de manera reactiva. No se realiza una evaluación cuantitativa de la seguridad de TI. Los incidentes de seguridad en TI provocan respuestas con acusaciones personales debido a la falta de claridad en las responsabilidades. Las respuestas a los incidentes de seguridad en TI son impredecibles.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>La conciencia sobre la importancia de la seguridad está fragmentada y limitada. Aunque los sistemas generan información relevante sobre la seguridad, esta no se somete a un análisis adecuado.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Las responsabilidades en materia de seguridad de TI están asignadas y comprendidas, pero no se aplican de manera continua. Se cuenta con un plan de seguridad de TI y se implementan soluciones de seguridad basadas en un análisis de riesgos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Es obligatorio establecer métodos para fomentar la conciencia sobre la seguridad. La identificación, autenticación y autorización de usuarios siguen estándares establecidos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Los usuarios y clientes asumen cada vez más la responsabilidad de definir los requisitos de seguridad, y las funciones de seguridad se integran con las aplicaciones durante la fase de diseño.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso DS5 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Se debe promover la concienciación sobre la seguridad de la información entre los empleados y los usuarios de sistemas de información.</td></tr>
<tr><td colspan="5">• Realizar un plan de seguridad de TI.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Realizar una evaluación inicial de los riesgos de seguridad en tus sistemas. Identifica las vulnerabilidades y amenazas más críticas.</td></tr>
<tr><td colspan="5">• Establecer políticas y procedimientos de seguridad básicos y comunicar claramente a todo el equipo su importancia.</td></tr>
</table>

• Desarrolla un plan de mitigación de riesgos que priorice las amenazas críticas y establezca acciones correctivas.
En el Largo Plazo:
• Implementa prácticas de desarrollo seguro en el ciclo de vida del software, como pruebas de seguridad regulares y revisión de código.
• Establecer un proceso de mejora continua para la seguridad de los sistemas, basado en la retroalimentación de incidentes y evaluaciones de seguridad.
• Asegúrate de cumplir con las regulaciones y estándares de seguridad relevantes en la MDA.

Ficha 23: Nivel de Madurez del Proceso DS6: Identificar y Asignar Costos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS6: Identificar y Asignar Costos				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La conciencia y el control respecto a la identificación y asignación de costos vinculados a la tecnología de la información están ausentes.	√		**GRADO DE MADUREZ** El proceso de Identificar y Asignar Costos está en el nivel de madurez 0. **OBJETIVOS NO CUMPLIDOS** • La MDA no tendría una comprensión completa y transparente de los costos asociados a las actividades de TI. Esto significa que no se podrían identificar y asignar los costos de manera precisa.
NIVEL 1	En esta fase, se toman medidas de manera improvisada para identificar y asignar costos, sin contar con un enfoque coherente y documentado. Puede existir una carencia de recursos y procedimientos formales.		√	
NIVEL 2	Se inician procesos más formales para la identificación y asignación de costos. Aunque persisten inconsistencias, se están dando pasos hacia la estandarización del proceso.		√	
NIVEL 3	El proceso está completamente definido y documentado, con políticas y procedimientos claros para la identificación y asignación de costos. Se asignan responsabilidades y se realiza un seguimiento de manera más estructurada.		√	
NIVEL 4	Se introducen métricas y medidas para evaluar la efectividad del proceso DS6. La monitorización constante de los costos lleva a mejoras basadas en datos y resultados medibles.		√	
NIVEL 5	La optimización continua busca la máxima eficiencia y eficacia. Se exploran oportunidades de mejora y se aplican constantemente las mejores prácticas.		√	
RECOMENDACIONES				
Para el proceso DS6 de COBIT estable los siguientes objetivos de control:				
• Asegurar que se registren y se identifiquen adecuadamente todos los costos relacionados con los servicios de TI y los proyectos.				
• Establecer un proceso para asignar los costos de manera adecuada a los servicios y proyectos específicos, de manera que se pueda determinar el costo total de la provisión de servicios de TI.				
Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				

• Proporcionar capacitación a tu equipo sobre las mejores prácticas para identificar y asignar costos de manera adecuada. Esto puede incluir cursos, talleres o la contratación de expertos en contabilidad.
• Utilizar herramientas de software especializadas en contabilidad y gestión de costos para simplificar el proceso. Esto puede ayudar a automatizar tareas repetitivas y reducir errores.
En el Largo Plazo:
• Desarrollar políticas claras y procesos documentados para la identificación y asignación de costos. Asegúrate de que todos los miembros del equipo estén al tanto de estas políticas y las sigan rigurosamente.
• Implementar un sistema de seguimiento continuo de los costos para identificar cualquier desviación o tendencia a lo largo del tiempo. Esto te permitirá tomar medidas correctivas cuando sea necesario.

Ficha 24: Nivel de Madurez del Proceso DS7: Educar y entrenar a los usuarios

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS7: Educar y entrenar a los usuarios				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Existe una ausencia total de programas destinados al desarrollo y formación. La entidad no admite la existencia de un inconveniente relacionado con el entrenamiento, y no se produce ninguna comunicación referente a este problema.	√		**GRADO DE MADUREZ** El proceso de Educar y Entrenar a los usuarios está en el nivel de madurez 0. **OBJETIVOS NO CUMPLIDOS** • Identificación de necesidades de entrenamiento y educación • Impartición de entrenamiento y educación • Evaluación constante del entrenamiento recibido
NIVEL 1	Se observa que la entidad ha reconocido la importancia de implementar un programa de formación, aunque carece de procedimientos normalizados. Dado la falta de un proceso organizado, los empleados han optado por participar en cursos relacionados con ética laboral, conciencia de seguridad en sistemas y prácticas de seguridad de manera independiente. La gestión global presenta una falta de cohesión, y la comunicación sobre los problemas y enfoques para abordar la formación y educación es esporádica e inconsistente.		√	
NIVEL 2	Existe conciencia acerca de la necesidad de un programa de formación y educación, así como de los procesos asociados a nivel organizativo. La formación comienza a incorporarse en los planes de rendimiento individuales de los empleados. Los procesos han avanzado hasta el punto en el cual diversos instructores imparten formación informal, cubriendo temas similares desde diferentes perspectivas. Algunas clases tratan asuntos éticos y conciencia sobre prácticas y actividades de seguridad en sistemas. A pesar de depender en gran medida del conocimiento individual, hay comunicación coherente respecto a		√	

	los problemas globales y la necesidad de abordarlos.			
NIVEL 3	El programa de formación y educación se institucionaliza y comunica, con empleados y gerentes identificando y documentando las necesidades de formación. Los procesos de formación y educación se estandarizan y documentan.		√	
NIVEL 4	Se implementa un programa completo de formación y educación que arroja resultados medibles. Las responsabilidades se definen claramente, y se establece la propiedad sobre los procesos. La formación y educación se convierten en componentes fundamentales de los planes de carrera de los empleados. La gerencia brinda apoyo y participa en sesiones de formación y educación.		√	
NIVEL 5	La formación y educación generan mejoras en el rendimiento individual. Estos aspectos se convierten en elementos críticos de los planes de carrera de los empleados. Se asignan presupuestos, recursos, instalaciones e instructores suficientes para los programas de formación y educación. Los procesos se perfeccionan y se encuentran en constante mejora, aprovechando las mejores prácticas externas y los modelos de madurez de otras organizaciones.		√	

RECOMENDACIONES
Para el proceso DS7 de COBIT estable los siguientes objetivos de control:
• Se debe identificar las necesidades de entrenamiento y educación para así enfocarse y desarrollar lo que necesita el usuario
• Se debe realizar programas de entrenamiento y educación
Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Identificar las necesidades de entrenamiento y educación
En el Largo Plazo:
• Implementar un programa de entrenamiento y educación

Ficha 25: Nivel de Madurez del Proceso DS8: Administrar la Mesa de Servicio y los Incidentes.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS8: Administrar la Mesa de Servicio y los Incidentes.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La entidad carece de mecanismos para abordar las inquietudes y preguntas de los usuarios, evidenciando una ausencia total de procesos para la gestión de incidentes. La organización no muestra reconocimiento alguno de la existencia de problemas que requieran atención.	√		**GRADO DE MADUREZ** El proceso de Administrar la Mesa de Servicio y los Incidentes está en el nivel de madurez 0. **OBJETIVOS NO CUMPLIDOS** • Los problemas en la MDA pueden no ser abordados de manera eficiente y que no se siguen procedimientos predefinidos para su resolución. • No hay una mesa de servicio centralizada o que no esté funcionando de manera efectiva en la MDA.
NIVEL 1	La dirección reconoce la necesidad de implementar un proceso respaldado por herramientas y personal para atender las consultas de los usuarios y gestionar la resolución de incidentes. Sin embargo, este proceso carece de estandarización y se limita a brindar un respaldo reactivo. La gerencia no supervisa las consultas de los usuarios, los incidentes o las tendencias, y no hay un sistema de escalado para asegurar la resolución de problemas.		√	
NIVEL 2	Existe una conciencia organizativa sobre la importancia de establecer una mesa de servicio y un proceso de gestión de incidentes. La asistencia se brinda de manera informal a través de una red de expertos individuales, quienes cuentan con algunas herramientas comunes para ayudar en la resolución de incidentes. Aunque no hay capacitación formal, la comunicación sobre procedimientos estándar se delega al individuo.		√	
NIVEL 3	Se reconoce y acepta la necesidad de implementar una mesa de servicio y un proceso para la gestión de incidentes. Los procedimientos se estandarizan y documentan, aunque la capacitación sigue siendo informal. La responsabilidad de obtener capacitación y seguir los estándares recae en el individuo. Aunque se desarrollan guías de usuario y preguntas frecuentes (FAQs), estos recursos deben ser encontrados por los individuos y no necesariamente son seguidos.		√	
NIVEL 4	Los mecanismos, herramientas y técnicas se encuentran automatizadas mediante una base de conocimientos centralizada. El personal de la mesa de servicio trabaja estrechamente con el personal de administración de problemas.		√	

NIVEL 5	Tanto el proceso de gestión de incidentes como la función de mesa de servicio están sólidamente organizados y establecidos, adoptando un enfoque centrado en el servicio al cliente gracias a su experiencia y especialización.		√	
RECOMENDACIONES				
Para el proceso DS8 de COBIT estable los siguientes objetivos de control:				
• Establecer un procedimiento para registrar y documentar todos los incidentes reportados por los usuarios o detectados internamente.				
• Desarrollar un método simple para determinar la prioridad inicial de los incidentes, lo que ayuda a asignar recursos de manera adecuada.				
Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				
• Establecer procesos básicos para la gestión de incidentes, como la creación de tickets, el enrutamiento adecuado y la priorización.				
• Si no se dispone de herramientas de gestión de incidentes, considere implementar una solución de software para mejorar la eficiencia en la gestión de incidentes.				
En el Largo Plazo:				
• Desarrollar procesos más avanzados y personalizados para la gestión de incidentes que se adapten a las necesidades específicas de la MDA.				

Ficha 26: Nivel de Madurez del Proceso DS9: Administrar la configuración.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS9: Administrar la configuración.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La alta dirección no reconoce la importancia de contar con un sistema implementado que permita informar y gestionar las configuraciones de la infraestructura de tecnologías de la información (TI), tanto en términos de hardware como de software.	√		**GRADO DE MADUREZ** El proceso de Administrar la configuración está en el nivel de madurez 1.
NIVEL 1	Se comprende la necesidad de tener una gestión de configuración. Se llevan a cabo actividades básicas de administración de configuraciones, como mantener inventarios de hardware y software, pero de forma individual. No existen prácticas estandarizadas definidas.	√		**OBJETIVOS NO CUMPLIDOS** • Falta de identificación adecuada de los elementos de configuración en un sistema o proyecto. Esto significa que no se tienen registros claros y completos de los componentes y sus relaciones. • Los cambios pueden realizarse sin un proceso formal y sin una evaluación adecuada de su impacto. • No hay una revisión de Integridad de la Configuración
NIVEL 2	La dirección es consciente de la importancia de controlar las configuraciones de TI y reconoce los beneficios de mantener información completa y precisa sobre las configuraciones, aunque existe una dependencia implícita del conocimiento y la experiencia del personal técnico. Se emplean herramientas de administración de configuraciones hasta cierto punto, pero varían entre plataformas. Además, no se han establecido prácticas estandarizadas de trabajo.		√	

NIVEL 3	Los procesos, procedimientos y prácticas de trabajo han sido documentados, estandarizados y comunicados, pero la implementación y aplicación de estándares dependen del individuo. Asimismo, se han introducido herramientas similares de administración de configuraciones entre plataformas. Es poco probable identificar desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se realiza alguna automatización para rastrear cambios en el software o hardware. La información de configuración es empleada por procesos interrelacionados.		√	
NIVEL 4	En todos los niveles, áreas, departamentos de la organización se reconoce la necesidad de gestionar las configuraciones y las mejores prácticas continúan evolucionando. Los procedimientos y estándares se comunican e incorporan a la implementación, y las desviaciones son monitoreadas, rastreadas y reportadas.		√	
NIVEL 5	Todos los sistemas, activos de TI se gestionan en un sistema central de configuraciones que contiene información completa sobre los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Existe una integración completa de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los informes de auditoría de los puntos de referencia proporcionan información esencial sobre el software y hardware en términos de reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se promueven reglas para restringir la instalación de software no autorizado.		√	
RECOMENDACIONES				
Para el proceso DS5 de COBIT estable los siguientes objetivos de control:				
• Crear y mantener una biblioteca de configuración que contenga todos los elementos de configuración relevantes, como documentos, código fuente y otros recursos.				
• Identificar y etiquetar claramente los elementos de configuración para que se puedan rastrear y gestionar de manera efectiva.				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				
• Establecer políticas y procedimientos claros para la gestión de la configuración. Esto incluye la identificación de elementos de configuración, control de versiones, y documentación de cambios.				
• Implementar un plan de control de configuraciones				
En el Largo Plazo:				
• Buscar automatizar los procesos de gestión de configuración tanto como sea posible.				

Ficha 27: Nivel de Madurez del Proceso DS10: Administrar los problemas

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS10: Administrar los problemas				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La falta de conciencia sobre la necesidad de abordar problemas conduce a la indiferenciación entre problemas e incidentes. Como resultado, no se ha hecho ningún esfuerzo por identificar las causas fundamentales de los incidentes.	√		**GRADO DE MADUREZ** El proceso de Administrar los problemas está en el nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** • Identificación y clasificación de problemas • Rastreo y resolución de problemas • La evaluación de la gravedad y urgencia de los problemas puede ser subjetiva y no estar completamente alineada con los objetivos de la MDA. Puede haber margen para mejoras en la evaluación de la prioridad de los problemas.
NIVEL 1	Existe un reconocimiento de la importancia de gestionar los problemas y abordar sus causas fundamentales. Aunque algunos expertos proporcionan asesoramiento en sus áreas de especialización, no se asigna responsabilidad formal para la gestión de problemas. La falta de intercambio de información conduce a la generación de nuevos problemas y la pérdida de tiempo en la búsqueda de soluciones.	√		
NIVEL 2	La conciencia sobre la gestión de problemas en TI es amplia tanto en las áreas de negocio como en los servicios de información. Aunque ha habido una evolución en el proceso de resolución, solo unos pocos individuos clave son responsables de identificar y resolver problemas. La información se comparte de manera informal y reactiva, afectando la calidad del servicio al usuario debido a la falta de conocimiento estructurado disponible para el administrador de problemas.	√		
NIVEL 3	Se reconoce la necesidad de un sistema integral de gestión de problemas, respaldado por el apoyo de la gerencia y asignación de presupuesto. Se estandarizan los procesos de escalado y resolución de problemas, y la información se comparte de manera formal y proactiva. Aunque existen limitaciones en la revisión de incidentes y en el análisis de identificación y resolución de problemas, se evidencia un progreso.		√	

NIVEL 4	La comprensión del proceso de gestión de problemas se ha extendido a todos los niveles de la organización, con responsabilidades y propiedad claramente definidas. Los métodos y procedimientos están documentados, comunicados y evaluados para medir su eficacia. Se ha iniciado la identificación y resolución de la mayoría de los problemas, y la gestión de problemas se integra de manera efectiva con otros procesos relacionados. Se han establecido indicadores clave de rendimiento (KPIs) y objetivos clave de rendimiento (KGIs) para el proceso.		√	
NIVEL 5	El proceso de gestión de problemas ha evolucionado hacia una fase proactiva y preventiva, contribuyendo activamente a los objetivos de TI. Los problemas se anticipan y previenen mediante el mantenimiento regular del conocimiento sobre patrones de problemas pasados y futuros a través de contactos con proveedores y expertos. La gestión de problemas se encuentra completamente integrada con la administración de datos de configuración, y se mide de manera consistente mediante KPIs y KGIs. La mayoría de los sistemas cuentan con mecanismos automáticos de advertencia y detección, sujetos a una evaluación continua. Se realiza un análisis constante del proceso de gestión de problemas para buscar mejoras continuas basadas en los KPIs y KGIs, informando a las partes interesadas.		√	

RECOMENDACIONES
Para el proceso DS10 de COBIT estable los siguientes objetivos de control:
• Establecer y mantener un registro centralizado de problemas que incluya información básica sobre cada problema identificado.
• Clasificar y categorizar los problemas según su gravedad, impacto y urgencia para priorizar la resolución
• Establecer un sistema de comunicación para informar a las partes interesadas relevantes sobre los problemas identificados y las acciones tomadas para abordarlos.
• Implementar un proceso de seguimiento para garantizar que los problemas se estén abordando y resolviendo de manera efectiva.
Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Identificar los problemas más críticos que enfrenta tu organización en la gestión de problemas. Priorizar aquellos que tienen un impacto significativo en la operación y el rendimiento.
• Definir procedimientos iniciales para la gestión de problemas, como la recopilación de datos, la notificación de incidentes y la asignación de responsabilidades. Estos procedimientos deben ser claros y estar disponibles para todo el personal.
En el Largo Plazo:
• Implementar un proceso de mejora continua en la gestión de problemas. Revisar regularmente los procedimientos y políticas para identificar áreas de mejora.

Ficha 28: Nivel de Madurez del Proceso DS11: Administrar los datos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS11: Administrar los datos				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La identificación de datos no se vincula con los recursos ni los activos corporativos.	√		**GRADO DE MADUREZ** El proceso de Administrar la configuración está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • Administración, Respaldo y Restauración de Datos • Acuerdos de Almacenamiento y Conservación.
NIVEL 1	La entidad reconoce la importancia de gestionar adecuadamente la información, aunque la responsabilidad de dicha gestión no está claramente definida. Los procedimientos de respaldo y recuperación, así como los acuerdos relativos a la eliminación de datos, están debidamente establecidos.	√		
NIVEL 2	En un nivel superior, comienza a surgir la noción de propiedad o responsabilidad sobre los datos.		√	
NIVEL 3	Existe una comprensión y aceptación de la necesidad de gestionar los datos tanto en el ámbito de la tecnología de la información como en toda la organización.		√	
NIVEL 4	Se comprende la necesidad de la gestión de datos y se aceptan las acciones requeridas en toda la organización.		√	
NIVEL 5	La comprensión y aceptación de la necesidad de llevar a cabo todas las actividades necesarias para la gestión de datos está arraigada en toda la organización.		√	
RECOMENDACIONES				
Para el proceso DS11 de COBIT estable los siguientes objetivos de control:				
• Definir y documentar los tipos de datos críticos que la MDA maneja.				
• Asignar responsabilidades claras para la gestión de datos, asegurando que haya propietarios designados para los conjuntos de datos críticos.				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				
• Realizar una evaluación completa de los datos que la MDA maneja en la actualidad.				
• Crear una política de datos que establezca directrices claras para la recopilación, almacenamiento y uso de datos. Asegurar de que todos los miembros del equipo estén al tanto y la cumplan.				
En el Largo Plazo:				
• Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad. Requerimientos de Seguridad para la Administración de Datos				
• Invertir en tecnologías adecuadas para la gestión de datos, como sistemas de gestión de bases de datos, herramientas de análisis de datos y soluciones de seguridad cibernética.				
• Establecer un marco de gobernanza de datos que defina roles y responsabilidades en toda la MDA para garantizar la calidad y la integridad de los datos.				
• Asegurar que se cumpla con las regulaciones de privacidad de datos aplicables de acuerdo a las normas de la MDA.				

Ficha 29: Nivel de Madurez del Proceso DS12: Administración del Ambiente Físico

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS12: Administración del Ambiente Físico				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No existe conciencia acerca de la imperiosa necesidad de salvaguardar las instalaciones o invertir en recursos informáticos. Los aspectos medioambientales, como la protección contra incendios, polvo, suciedad, exceso de calor y humedad, no son objeto de control ni vigilancia.	√		**GRADO DE MADUREZ** El proceso de Administración del Ambiente Físico está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • Falta de políticas puede llevar a una gestión ineficiente y a la falta de estándares. • No se realizan evaluaciones adecuadas de los riesgos asociados a los activos físicos por los ambientes físicos.
NIVEL 1	La entidad reconoce la imperante necesidad de contar con un entorno físico que resguarde los recursos y el personal ante amenazas naturales y provocadas por el ser humano. La gestión de las instalaciones y equipos se basa en las habilidades de individuos clave. El personal puede desplazarse sin restricciones dentro de las instalaciones, y la administración no supervisa los controles medioambientales ni los movimientos del personal.	√		
NIVEL 2	La supervisión y aplicación de controles medioambientales recae en el personal de operaciones. La seguridad física es un proceso informal, llevado a cabo por un reducido grupo de empleados altamente comprometidos con la protección de las instalaciones. Los procedimientos de mantenimiento de las instalaciones carecen de una documentación detallada y dependen de las buenas prácticas de unos pocos individuos. Las metas de seguridad física no se basan en estándares formales, y la gerencia no garantiza el cumplimiento de los objetivos de seguridad.		√	
NIVEL 3	Existe una comprensión generalizada en toda la organización acerca de la necesidad de mantener un entorno informático bajo control. Los controles medioambientales, el mantenimiento preventivo y la seguridad física cuentan con un presupuesto autorizado y son supervisados por la gerencia. Se implementan restricciones de acceso, permitiendo el ingreso solo al personal autorizado. Los visitantes se registran y son acompañados según el individuo.		√	

NIVEL 4	El proceso de gestión del entorno físico se monitorea y mide. Se implementan mejoras continuas basadas en datos, buscando la eficiencia.		√	
NIVEL 5	La gestión del entorno físico es altamente eficiente y se mejora de manera constante. Se persigue la innovación y la excelencia en la administración del entorno físico.		√	
RECOMENDACIONES				
Para el proceso DS12 de COBIT estable los siguientes objetivos de control:				
• Asegurarse de que se haya asignado y establecido un lugar físico adecuado para llevar a cabo las actividades relacionadas con los procesos de la MDA.				
• Garantizar que solo las personas autorizadas tengan acceso al ambiente físico y los recursos relacionados con el proceso.				
• Mantener registros básicos relacionados con la administración del ambiente físico, como inventarios de equipos y registros de acceso.				
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:				
En el Corto Plazo:				
• Realiza una evaluación inicial del estado actual de la administración del ambiente físico de la MDA.				
• Desarrollar políticas y procedimientos relacionados con la gestión del ambiente físico. Asegurar de que todos los empleados estén al tanto de estas políticas.				
• Implementar medidas de control de acceso, como tarjetas de identificación y cerraduras de seguridad, para proteger las áreas críticas de tu entorno físico.				
• Realizar auditorías de seguridad periódicas para identificar y corregir posibles vulnerabilidades o incumplimientos de políticas.				
En el Largo Plazo:				
• Invertir en tecnología de seguridad avanzada, como sistemas de videovigilancia y alarmas, para fortalecer la protección de las instalaciones de la MDA.				
• Fomentar una cultura de seguridad en toda la organización, donde todos los empleados estén comprometidos con la protección de los recursos físicos.				
• Establecer un proceso de mejora continua para revisar y actualizar regularmente tus políticas y procedimientos de gestión del ambiente físico				

Ficha 30: Nivel de Madurez del Proceso DS13: Administración de Operaciones

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS13: Administración de Operaciones				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dedicación de la entidad a la configuración del respaldo básico de Tecnologías de la Información (TI) y a las actividades operativas es inexistente.	√		**GRADO DE MADUREZ** El proceso de Administración de Operaciones está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • No hay procedimientos e instrucciones de operación. • No hay programación de tareas en la MDA.
NIVEL 1	Se reconoce en la entidad la necesidad de estructurar las funciones de soporte de TI. Se implementan algunos procedimientos estándar, y las actividades operativas tienen un carácter reactivo. La mayoría de los procesos operativos se programan de manera informal, y la validación previa de las solicitudes no es habitual. La disponibilidad, interrupción o demora de las computadoras, sistemas y aplicaciones que respaldan los procesos de negocio es frecuente. Se pierde tiempo en la espera de recursos por parte de los empleados.	√		

NIVEL 2	La entidad está consciente del papel crucial de las actividades operativas de TI en el soporte de funciones de TI. Se asignan presupuestos para herramientas de manera selectiva. Las operaciones de soporte de TI son informales e intuitivas, con una fuerte dependencia de las habilidades individuales. Las instrucciones sobre qué hacer, cuándo y en qué orden no están documentadas de manera sistemática. Se brinda cierta capacitación al operador, y existen algunos estándares formales de operación.		√	
NIVEL 3	La necesidad de gestionar las operaciones informáticas es comprendida y aceptada en la entidad. Se asignan recursos y se proporciona capacitación durante las labores. Las funciones repetitivas se definen, estandarizan, documentan y comunican formalmente. Los resultados de las tareas completadas y de los eventos se registran, con informes limitados dirigidos a la gerencia. Se introduce el uso de herramientas de programación automatizada y otras para reducir la intervención del operador.		√	
NIVEL 4	Los procesos de gestión de operaciones se definen y documentan. La entidad opera de manera proactiva, siguiendo procedimientos predefinidos.		√	
NIVEL 5	Los procesos de gestión de operaciones se monitorean y miden para asegurar la consistencia y promover la mejora continua. Se emplean métricas y se gestiona eficazmente los riesgos.		√	

RECOMENDACIONES
Para el proceso DS13 de COBIT estable los siguientes objetivos de control:
• Documentar los procedimientos clave para la administración de operaciones, de modo que estén disponibles para el personal y se sigan de manera consistente.
• Asegurar que se identifiquen y se mantengan registros de los recursos críticos necesarios para las operaciones, como personal, equipo, y suministros.
• Establecer un proceso para el control de cambios en los procedimientos y recursos relacionados con las operaciones, asegurando que los cambios se realicen de manera planificada y controlada.
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• identificar los procesos clave de administración de operaciones que necesitan mejoras inmediatas.
• Evaluar las oportunidades de automatización en tus operaciones. La implementación de sistemas de software adecuados puede acelerar los procesos y reducir errores.
En el Largo Plazo:
• Desarrollar y documentar los procesos estandarizados para todas las áreas de administración de operaciones. Esto promoverá la consistencia y la eficiencia a lo largo del tiempo.
• Considerar la implementación de tecnologías avanzadas como la inteligencia artificial, el análisis de datos y la IoT para mejorar la toma de decisiones y la eficiencia en tiempo real.

Ficha 31: Nivel de Madurez del Proceso ME1: Monitorear y evaluar el desempeño de TI

<table>
<tr><th colspan="5">DOMINIO: PLANIFICAR Y ORGANIZAR</th></tr>
<tr><th colspan="5">ME1: Monitorear y evaluar el desempeño de TI</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>El monitoreo autónomo de proyectos o procesos no se lleva a cabo en TI. La ausencia de informes útiles, precisos y oportunos es evidente, y no se reconoce la necesidad de una comprensión clara de los objetivos de los procesos.</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de Monitorear y Evaluar el Desempeño de TI está en el nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• No se han establecido métricas claras ni estándares para medir el desempeño de los servicios de TI. Esto dificulta la evaluación efectiva. • No hay medidas para corregir problemas o deficiencias en el desempeño de TI.</td></tr>
<tr><td>NIVEL 1</td><td>La recolección y evaluación de procesos no han sido estandarizadas. La implementación del monitoreo y la resolución de métricas se realiza de manera adaptativa, según las necesidades específicas de proyectos de Tecnologías de la Información.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>La interpretación de los resultados del monitoreo se fundamenta en la experiencia de individuos clave.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Se han establecido mediciones para evaluar la contribución de la función de servicio de información al rendimiento organizacional, utilizando criterios financieros y operativos convencionales.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Existe una integración de métricas en todos los proyectos y procesos de TI. Los sistemas de informes de la administración de TI están formalizados.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>Las mediciones y métricas orientadas al negocio se emplean de manera regular para evaluar el rendimiento y se incorporan en marcos estratégicos, como el balanced scorecard.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso ME1 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Identificar los activos de TI críticos.</td></tr>
<tr><td colspan="5">• Establecer responsabilidades mínimas para la supervisión de TI.</td></tr>
<tr><td colspan="5">• Recopilar datos básicos de desempeño de TI.</td></tr>
<tr><td colspan="5">• Implementar procedimientos ad hoc para abordar problemas de desempeño de TI cuando surgen.</td></tr>
<tr><td colspan="5">Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:</td></tr>
<tr><td colspan="5">En el Corto Plazo:</td></tr>
<tr><td colspan="5">• Adquirir o configurar herramientas de monitoreo que permitan recopilar datos en tiempo real sobre el desempeño de TI. Esto te ayudará a obtener información inmediata.</td></tr>
<tr><td colspan="5">• Definir procedimientos para recopilar y registrar datos de manera consistente. Esto asegurará que información sea precisa para evaluar el desempeño.</td></tr>
<tr><td colspan="5">En el Largo Plazo:</td></tr>
<tr><td colspan="5">• implementar un sistema de gestión de calidad, como ISO 9001, que puede ayudar a estandarizar procesos y mejorar la eficiencia.</td></tr>
</table>

Ficha 32: Nivel de Madurez del Proceso ME2: Monitorear y Evaluar el Control Interno

<table>
<tr><th colspan="5">DOMINIO: MONITOREAR Y EVALUAR</th></tr>
<tr><th colspan="5">ME2: Monitorear y Evaluar el Control Interno</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>CUMPLE</th><th>NO CUMPLE</th><th>OBSERVACIONES</th></tr>
<tr><td>NIVEL 0</td><td>Lamentablemente, no se encuentran implementados los procedimientos de gestión interna para el control, lo cual refleja una carencia generalizada de conciencia respecto a la seguridad operativa y la garantía de control interno en el ámbito de Tecnologías de la Información (TI).</td><td>√</td><td></td><td rowspan="7">GRADO DE MADUREZ
El proceso de Monitorear y Evaluar el Control Interno está en el nivel de madurez 0.

OBJETIVOS NO CUMPLIDOS
• Establecer los procesos para la identificación, evaluación y aseguramiento del control interno.
• Utilizar herramientas integradas para la detección del control interno de TI.</td></tr>
<tr><td>NIVEL 1</td><td>La dirección de TI no ha formalizado la asignación de responsabilidades para supervisar la eficacia de los mecanismos de control internos.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 2</td><td>La gestión de servicios de información lleva a cabo revisiones periódicas de la eficacia de los controles internos que considera críticos. Aunque se están introduciendo metodologías y herramientas para evaluar estos controles, no se basan en un plan predefinido.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 3</td><td>Se ha implementado un programa de educación y formación orientado al monitoreo del control interno. Además, se ha establecido un proceso para autoevaluaciones y revisiones de aseguramiento del control interno, con roles específicos para los responsables tanto del negocio como de TI.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 4</td><td>Se han adoptado herramientas para estandarizar las evaluaciones y detectar automáticamente las excepciones de control. Asimismo, se ha constituido de manera formal una función especializada para el control interno de TI, integrando profesionales certificados que siguen un marco de trabajo de control respaldado por la alta dirección.</td><td></td><td>√</td></tr>
<tr><td>NIVEL 5</td><td>La organización utiliza mecanismos, herramientas integradas y actualizadas, cuando corresponde, que facilitan una evaluación eficaz de los controles críticos de TI y la detección ágil de incidentes relacionados con el control de TI.</td><td></td><td>√</td></tr>
<tr><td colspan="5">RECOMENDACIONES</td></tr>
<tr><td colspan="5">Para el proceso ME2 de COBIT estable los siguientes objetivos de control:</td></tr>
<tr><td colspan="5">• Identificar las áreas críticas o sensibles en los procesos de la MDA donde se requiere control interno.</td></tr>
<tr><td colspan="5">• Evaluar el conocimiento y la comprensión de los empleados sobre los controles internos y su importancia.</td></tr>
</table>

• Comenzar a recopilar información sobre los procesos y riesgos clave para futuras evaluaciones y mejoras.
Para pasar al nivel de madurez 1 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Documentar los procesos actuales de control interno. Esto te ayudará a comprender mejor tus flujos de trabajo y a identificar áreas de mejora donde involucre la administración de procesos, políticas y contratos de TI.
• Realizar auditorías internas periódicas para identificar brechas y áreas de mejora en los controles internos.
En el Largo Plazo:
• Diseñar políticas y procedimientos sólidos de control interno que estén alineados con los estándares y regulaciones aplicables de la MDA
• Realizar evaluaciones periódicas de los controles internos y ajusta tus estrategias según sea necesario.

Ficha 33: Nivel de Madurez del Proceso ME3: Garantizar el Cumplimiento Regulatorio

DOMINIO: MONITOREAR Y EVALUAR				
ME3: Garantizar el Cumplimiento Regulatorio				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Existe escasa conciencia acerca de los elementos externos que inciden en Tecnologías de la Información, careciendo de procedimientos orientados al cumplimiento de requisitos normativos, legales y contractuales.	√		**GRADO DE MADUREZ** El proceso de Garantizar el Cumplimiento Regulatorio está en el nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** • Brindar capacitación constante sobre requisitos legales y regulatorios externos a los que se rige la MDA. • No hay políticas, estándares, procedimientos y metodologías de TI para el regulamiento legal y regulatorio.
NIVEL 1	Se implementan procedimientos informales para asegurar el cumplimiento, pero únicamente en casos emergentes relacionados con nuevos proyectos o en respuesta a auditorías y evaluaciones.	√		
NIVEL 2	Aunque no se sigue un enfoque estandarizado, se confía en el conocimiento y la responsabilidad de los individuos, admitiendo la posibilidad de errores.		√	
NIVEL 3	Se imparte formación sobre los requisitos legales y normativos externos que afectan a la organización, junto con instrucciones sobre los procesos de cumplimiento establecidos.		√	
NIVEL 4	Las responsabilidades están claramente definidas, y se comprende la potenciación de los procesos. El procedimiento incluye una revisión del entorno para identificar requisitos externos y cambios recurrentes.		√	
NIVEL 5	Existe un amplio conocimiento de los requisitos externos aplicables, abarcando tanto sus tendencias futuras como los cambios anticipados, así como la necesidad de nuevas soluciones.		√	
RECOMENDACIONES				

Para el proceso ME3 de COBIT estable los siguientes objetivos de control:
• Identificar y documentar las regulaciones relevantes que se aplican en la MDA y sus actividades.
• Asegurar de que los empleados estén conscientes de las regulaciones que afectan a sus responsabilidades y actividades laborales.
Para pasar al nivel de madurez 2 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Identificar todas las regulaciones que afectan a la MDA y priorizar aquellas que son más críticas y urgentes.
• Evaluar la situación actual en relación con los requisitos regulatorios. Identificar las brechas y áreas de mejora que deben abordarse de inmediato.
En el Largo Plazo:
• Establecer políticas y procedimientos iniciales para cumplir con las regulaciones aplicables.

Ficha 34: Nivel de Madurez del Proceso ME4: Proporcionar Gobierno de TI

DOMINIO: MONITOREAR Y EVALUAR				
ME4: Proporcionar Gobierno de TI				
NIVEL DE MADUREZ		**CUMPLE**	**NO COMPLE**	**OBSERVACIONES**
NIVEL 0	Se observa una ausencia total de cualquier estructura discernible para la administración de Tecnologías de la Información (TI). La entidad no ha reconocido la existencia de un problema por resolver, lo que resulta en una falta de comunicación al respecto.	√		**GRADO DE MADUREZ** El proceso de Proporcionar Gobierno de TI está en el nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** • No hay una comunicación por parte de la Gerencia los procedimientos estandarizados.
NIVEL 1	La gestión adopta un enfoque reactivo y la comunicación acerca de los problemas y las estrategias para abordarlos es esporádica e inconsistente.	√		
NIVEL 2	Aunque la administración ha identificado mediciones fundamentales para la gobernanza de TI, así como métodos y técnicas de evaluación, aún no se ha implementado el proceso a nivel organizacional.	√		
NIVEL 3	La dirección ha difundido procedimientos estandarizados y ha establecido programas de formación. Se han señalado herramientas para respaldar la supervisión de la gobernanza de TI.		√	
NIVEL 4	Los procedimientos y procesos de TI y la gobernanza de TI están alineados e integrados con la estrategia corporativa de TI. La mejora de los procesos de TI se basa principalmente en un conocimiento cuantitativo y es posible monitorear y medir la conformidad con procedimientos y métricas de procesos.		√	

NIVEL 5	La implementación de las políticas de TI ha conducido a una organización ágil y procesos que se adaptan rápidamente, brindando un respaldo completo a los requisitos de gobernanza de TI. Todos los problemas y desviaciones se analizan a través de las técnicas de causa raíz, y se identifican e implementan eficientemente medidas correctivas.		√	

RECOMENDACIONES
Para el proceso ME4 de COBIT estable los siguientes objetivos de control:
• Identificación de roles y responsabilidades clave en el proceso de gobierno de TI.
• Desarrollar políticas y procedimientos que guíen el gobierno de TI en la MDA. Estos deben ser claros y estar alineados con los objetivos estratégicos.
• Comunicar de manera efectiva el marco de gobierno de TI a todas las partes interesadas relevantes dentro de la MDA. Esto garantiza que todos estén al tanto de las políticas y procedimientos.
Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias:
En el Corto Plazo:
• Establecer roles y responsabilidades claros dentro del equipo de TI para garantizar una gestión eficaz.
• Crear políticas y procedimientos básicos que aborden los aspectos críticos del Gobierno de TI, como la gestión de riesgos, la seguridad de la información y el cumplimiento normativo.
En el Largo Plazo:
• Adoptar un marco reconocido, como COBIT o ITIL, para guiar la gestión de TI y asegurarte de que estás siguiendo las mejores prácticas.
• Invertir en la capacitación y desarrollo del personal de TI para mejorar sus habilidades y conocimientos en áreas clave de Gobierno de TI.

Anexo 10: Carta para la presentación de la propuesta de Policías de seguridad de la información en la Municipalidad Distrital de Amarilis

CARTA N° 011-2023-LAVS

PARA : MUNICIPALIDAD DISTRITAL DE AMARILIS

ATENCIÓN : SUB GERENCIA DE PLANIFICACIÓN Y MODERNIZACIÓN INSTITUCIONAL

ASUNTO : PRESENTACIÓN DE LA PROPUESTA DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIAPLIDAD DISTRITAL DE AMARILIS PARA SU IMPLEMENTACIÓN

FECHA : AMARILIS, 29/12/2023

Mediante el presente me dirijo a su despacho, para saludarlo cordialmente y comunicar que mi persona **LUIS ARNOLD VILLA SANCHEZ**, identificado con **DNI N° 70910102**, domiciliado en el Jr. San Martin #1543, **egresado de la Escuela Profesional de Ingeniería de Sistemas perteneciente a la Facultad de Ingeniería Industrial y Sistemas de la Universidad Nacional Hermilio Valdizan** con código universitario **N° 2017230005.** Estando en proceso de desarrollo mi proyecto de tesis como ámbito geográfico la Municipalidad Distrital de Amarilis, titulado **"POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS"**.

Habiendo finalizado el análisis y diseño de las políticas de seguridad de la información del proyecto de tesis, se le hace presente la propuesta de este denominado **"MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS"** que tiene como objetivo proporcionar una directriz, reglas y procedimientos que permita solventar los problemas de seguridad de la información en la Municipalidad Distrital de Amarilis de acuerdo con las leyes y regulaciones vigentes en la que se encuentra la seguridad de la información.

Para su implementación este documento lo debe disponer el responsable de la oficina de informática de la Municipalidad Distrital de Amarilis que deberá ser aprobado por el área responsable para luego ser publicado y comunicado a los empleados y partes externas relacionadas con las áreas involucradas.

Por lo expuesto se remite el documento denominado **"Manual de Políticas de Seguridad de la información de la Municipalidad Distrital de Amarilis"** para su **APROBACIÓN E IMPLEMENTACIÓN** con la finalidad de mitigar los problemas de seguridad de la información que se presentan en la entidad.

Es todo cuanto informo para su conocimiento y atención.

.....

VILLA SANCHEZ LUIS ARNOLD

DNI: 70910102

Anexo 11: Informe emitido por la Gerencia de Administración y Finanzas para que se remita a la Sub Gerencia de Planificación y Modernización Institucional

Municipalidad Distrital de **Amarilis**

Digital ecológico y emprendedor.

"Año de la unidad, la paz y el desarrollo"

GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
29 DIC. 2023
REG. N° 5259 HORA 5:10PM
FOLIO 03 FIRMA

INFORME N°1280-2023-MDA-GAF

A	:	**C.P.C. SERGIO H. BERROSPI AGUILAR** Gerente de Planeamiento y Presupuesto
ASUNTO	:	**REMITIR AL ÁREA COMPETENTE LA PROPUESTA DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS PARA SU APROBACIÓN E IMPLEMENTACIÓN**
REFERENCIA	:	CARTA N° 011-2023-LAVS
FECHA	:	Amarilis, 29 de diciembre del 2023

Es grato dirigirme a usted, para saludarlo cordialmente y **remitir la PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS** para que sea derivado al área competente para su **APROBACIÓN E IMPLEMENTACIÓN.** Elaborado por el **BACH. LUIS ARNOLD VILLA SANCHEZ**, egresado de la Escuela Profesional de Ingeniería de Sistemas perteneciente a la Facultad de Ingeniería Industrial y Sistemas de la Universidad Nacional Hermilio Valdizan.

I. ANTECEDENTES

- De acuerdo a la **CARTA N° 011-2023-LAVS**, el **BACH. LUIS ARNOLD VILLA SANCHEZ** presentó la **PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS,** Encontrándose en proceso de desarrollo de proyecto de tesis como ámbito geográfico la Municipalidad Distrital de Amarilis, titulado **"POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS".**

MUNICIPALIDAD DISTRITAL DE AMARILIS – GERENCIA DE ADMINISTRACIÓN Y FINANZAS

II. ANALISIS

- El documento presentado denominado **"Manual de Políticas de Seguridad de la Información de la Municipalidad Distrital de Amarilis"** tiene como objetivo proporcionar una directriz, reglas y procedimientos que permita solventar los problemas de seguridad de la información en la Municipalidad Distrital de Amarilis de acuerdo con las leyes y regulaciones vigentes en la que se encuentra la seguridad de la información.

III. CONCLUSIONES Y RECOMENDACIONES

- Por ende, se remite el documento a su despacho para que se derive al área competente **"Sub gerencia de Planificación y Modernización Institucional".**

- Se sugiere y recomienda que el documento adjuntado se revise y de ser

"Año de la unidad, la paz y el desarrollo"

favorable continuar con su trámite **APROBACIÓN E IMPLEMENTACIÓN** del **"Manual de Políticas de Seguridad de la información de la Municipalidad Distrital de Amarilis".**

- Se adjunta los siguientes documentos:
  - CARTA N° 011-2023-LAVS
  - "Manual de Políticas de Seguridad de la información de la Municipalidad Distrital de Amarilis"

Es todo cuanto informo para su conocimiento y fines pertinentes

Atentamente

MUNICIPALIDAD DISTRITAL DE AMARILIS

CPC. Bonnie Verónica Cayo Chaupis
GERENTE DE ADMINISTRACIÓN Y FINANZAS

Anexo 12: APROBACIÓN de las políticas de seguridad mediante informe emitido por la Sub Gerencia de Planificación y Modernización Institucional y se DISPONE a la Oficina de Informática para su IMPLEMENTACIÓN y PUBLICACIÓN

Municipalidad Distrital de **Amarilis**

Digital ecológico y emprendedor.

"Año de la unidad, la paz y el desarrollo"

MUNICIPALIDAD DISTRITAL DE AMARILIS HUÁNUCO GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
29 DIC. 2023
REG. N° 5260 HORA 5:30 PM
FOLIO 45 FIRMA

INFORME Nº162-2023-MDA-GPP/SGPMI

A	:	**CPC. SERGIO H. BERROSPI AGUILAR** Gerencia de Planeamiento y Presupuesto
DE	:	**CPC. WALTER ESPINOZA EVARISTO** Sub Gerente de Planificación y Modernización Institucional
ATENCIÓN	:	**ÁREA FUNCIONAL DE TECNOLOGÍA DE LA INFORMACIÓN**
ASUNTO	:	**DISPONER EL "MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS" PARA SU IMPLEMENTACIÓN Y PUBLICACIÓN**
REFERENCIA	:	- INFORME N°1280-2023-MDA-GAF - CARTA N°11-2023-LAVS - MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS
FECHA	:	Amarilis, 29 de diciembre del 2023

Es grato dirigirme a usted, para saludarlo cordialmente y a la vez **disponer** mediante su despacho disponer el documento **"Manual de Políticas de Seguridad de la Información de la Municipalidad Distrital De Amarilis"** para su **implementación y publicación** al Área Funcional de Tecnología de la Información.

I. ANTECEDENTES

- De acuerdo a la **CARTA N° 011-2023-LAVS**, el **BACH. LUIS ARNOLD VILLA SANCHEZ** presentó la **PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE AMARILIS,** Encontrándose en proceso de desarrollo de proyecto de tesis como ámbito geográfico la Municipalidad Distrital de Amarilis, titulado **"POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS".**

II. ANALISIS

- El documento presentado denominado **"Manual de Políticas de Seguridad de la información de la Municipalidad Distrital de Amarilis"** teniendo como:
  - **Objetivo:** Proporcionar una directriz, reglas y procedimientos que permita solventar los problemas de seguridad de la información en la Municipalidad Distrital de Amarilis
  - **Finalidad:** Proteger la confidencialidad, integridad y disponibilidad de la información en la Municipalidad Distrital de Amarilis
  - **Alcance:** Municipalidad Distrital de Amarilis

"Año de la unidad, la paz y el desarrollo"

Todo bajo las leyes y regulaciones vigentes en la que se encuentra la seguridad de la información

- Viendo que este proyecto teniendo como producto denominado **"Manual de Políticas de Seguridad de la información de la Municipalidad Distrital de Amarilis"** es beneficioso para la entidad ya que va a permitir mitigar los problemas de seguridad de la información que presenta la entidad.

III. CONCLUSIONES Y RECOMENDACIONES

- En conclusión, se **APRUEBA** el proyecto denominado **"Manual de Políticas de Seguridad de la información de la Municipalidad Distrital de Amarilis"** y se **DISPONE** a su despacho para su respectiva **IMPLEMENTACIÓN Y PUBLICACIÓN PILOTO** desde el Área Funcional de Tecnología de la Información.

Es cuanto informo para su conocimiento, trámite correspondiente y demás fines que estime conveniente.

Atentamente,

CPC. Walter Espinoza Evaristo
Sub Gerente de Planificación y Modernización Institucional

Anexo 13: Fichas para la evaluación del nivel de madurez de la segunda auditoría

Ficha 35: Nivel de Madurez del Proceso PO1: Definir el plan estratégico de Tecnología de la Información de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO1: Definir el plan estratégico de Tecnología de la Información**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dirección no muestra conciencia de la necesidad de la planificación estratégica de TI para respaldar los objetivos de la organización.	√		**GRADO DE MADUREZ** El proceso de Definir el Plan Estratégico de Tecnología Información está en el nivel de madurez 3. - La MDA ya desarrolló y aprobó su plan de gobierno digital denominado "Plan de Gobierno Digital 2024-2026 de la Municipalidad Distrital de Amarilis"
NIVEL 1	En las reuniones de la dirección, se aborda ocasionalmente la planificación estratégica de TI.	√		
NIVEL 2	Las decisiones estratégicas se toman proyecto por proyecto, sin coherencia con una estrategia global de la organización.	√		
NIVEL 3	La planificación estratégica de TI sigue un enfoque estructurado, documentado y compartido con todo el equipo. Las estrategias de recursos humanos, técnicos y financieros de TI tienen una influencia creciente en la adquisición de nuevos productos.	√		
NIVEL 4	Hay procesos bien definidos para determinar el uso de recursos internos y externos necesarios en el desarrollo y las operaciones de los sistemas.		√	
NIVEL 5	Se abordan y elaboran planes acordes a la realidad de la entidad a largo plazo de TI y la actualización de constante para mostrar los avances tecnológicos cambiantes y el progreso relacionado al negocio de la entidad.		√	

Ficha 36: Nivel de Madurez del Proceso PO2: Definir la arquitectura de la información de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO2: Definir la arquitectura de la información**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	En la organización, no se cuenta con el conocimiento, la experiencia ni las responsabilidades necesarias para llevar a cabo el desarrollo de esta arquitectura.	√		**GRADO DE MADUREZ** El proceso de Definir la Arquitectura de la Información está en el nivel de madurez 3. - La MDA desarrolló un plan de trabajo para adquisición de equipos tecnológicos con el fin de mejorar la infraestructura tecnológica para la administración de
NIVEL 1	La dirección reconoce la necesidad de una arquitectura de información, aunque el desarrollo de algunos componentes ocurre de manera improvisada.	√		

NIVEL 2	Las habilidades del personal se adquieren mediante la construcción práctica de la arquitectura de información y la aplicación repetida de técnicas.	√		datos y para estén debidamente estandarizados.
NIVEL 3	Se establece formalmente una función de administración de datos que define estándares para toda la organización y comienza a informar sobre la implementación y uso de la arquitectura de información.	√		
NIVEL 4	El proceso de definición de la arquitectura de información es proactivo y se centra en resolver las necesidades futuras del negocio.		√	
NIVEL 5	El equipo de TI posee la experiencia y las habilidades necesarias para desarrollar y mantener una arquitectura de información robusta y sensible que refleje todos los requisitos del negocio.		√	

Ficha 37: Nivel de Madurez del Proceso PO3: Determinar la dirección tecnológica de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO3: Determinar la dirección tecnológica**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se tiene consciencia acerca de la relevancia de la planificación de la infraestructura tecnológica para la entidad.	√		**GRADO DE MADUREZ** El proceso de Determinar la Dirección Tecnología está en el nivel de madurez 4. - La MDA reforzó el área de informática; Personal competente al rubro con la habilidad de desarrollar y ejecutar planes concernientes a la infraestructura tecnológica
NIVEL 1	La administración reconoce la importancia de planificar la infraestructura tecnológica, así como el desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes, pero lo hace de manera no sistemática y de forma aislada.	√		
NIVEL 2	La evaluación de los cambios tecnológicos se encomienda a individuos que siguen procesos intuitivos, aunque similares.	√		
NIVEL 3	Actualmente hay un plan de infraestructura tecnológica definido, documentado y ampliamente difundido, pero su aplicación y ejecución es inconsistente.	√		
NIVEL 4	El departamento de informática cuenta con la experiencia y habilidades necesarias para elaborar un plan de infraestructura tecnológica.	√		

NIVEL 5	La dirección del plan de infraestructura tecnológica se guía por estándares y avances industriales e internacionales en lugar de depender de los proveedores de tecnología.		√	

Ficha 38: Nivel de Madurez del Proceso PO4: Definir los procesos, la organización y las relaciones de TI de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO4: Definir los procesos, la organización y las relaciones de TI**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La eficacia en la orientación hacia los objetivos empresariales no está correctamente establecida en la estructura de Tecnologías de la Información (TI).	√		**GRADO DE MADUREZ** El proceso de Definir los Procesos, la Organización y las Relaciones de TI está en el nivel 3 de madurez. - La MDA realiza reuniones y coordinaciones con proveedores clave para la implementación de una ciudad inteligente en el distrito de Amarilis y cada reunión queda documentado en un acta de mesa de trabajo.
NIVEL 1	La función de TI se percibe únicamente como un respaldo sin una visión global dentro de la organización.	√		
NIVEL 2	Aunque se reconoce la necesidad de una organización estructurada, las decisiones aún se basan en el conocimiento y habilidades de individuos clave.	√		
NIVEL 3	Las relaciones con terceros, como comités de dirección, auditoría interna y gestión de proveedores, están siendo establecidas.	√		
NIVEL 4	La respuesta proactiva al cambio y la influencia en todos los roles necesarios para cumplir con los requisitos organizativos son características de la organización de TI.		√	
NIVEL 5	La estructura organizacional de TI exhibe flexibilidad y adaptabilidad.		√	

Ficha 39: Nivel de Madurez del Proceso PO5: Administrar la Inversión en TI de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO5: Administrar la Inversión en TI.**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No hay supervisión ni seguimiento de las inversiones y gastos relacionados con la tecnología de la información (TI).	√		**GRADO DE MADUREZ** El proceso de Administrar la Inversión en TI está en el nivel 1 de madurez. - La MDA cuenta con personal competente a la TI con la capacidad de desarrollar una estructura
NIVEL 1	Se reconoce la importancia de gestionar las inversiones en TI, aunque esta necesidad se comunica de manera irregular.	√		

NIVEL 2	El cumplimiento depende de la iniciativa individual dentro de la organización. Se utilizan enfoques comunes para elaborar partes del presupuesto de TI. Las decisiones presupuestarias son reactivas y tácticas.	√		de costos y fomentar proyectos de inversión concernientes a las TIC's
NIVEL 3	El personal de TI posee la experiencia y habilidades necesarias para desarrollar el presupuesto de TI y recomendar inversiones adecuadas.	√		
NIVEL 4	Se realizan análisis formales de costos que abarcan tanto los costos directos como los indirectos de las operaciones existentes, así como propuestas de inversión que consideran todos los costos a lo largo del ciclo de vida. Se utiliza un proceso de presupuesto proactivo y estandarizado.		√	
NIVEL 5	Las decisiones de inversión toman en cuenta las tendencias de mejora de precio/desempeño. Se exploran y evalúan formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital de la organización, utilizando métodos de evaluación formales. Se realiza una identificación proactiva de las variaciones.		√	

Ficha 40: Nivel de Madurez del Proceso PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La gestión no ha instaurado un entorno positivo para la supervisión de la información. No existe la conciencia de la necesidad de desarrollar un conjunto de políticas, procedimientos, estándares y procesos de conformidad.	√		**GRADO DE MADUREZ** El proceso de Comunicar las Aspiraciones y la Dirección de la Gerencia está en el nivel 3 de madurez. - Gerencia Municipal elaboró un documento para la publicación de las políticas de seguridad de la información diseñadas en este proyecto de investigación.
NIVEL 1	Los procedimientos relativos a la creación, comunicación y cumplimiento son informales e irregulares.	√		
NIVEL 2	Se ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la creación se deja a la discreción de los gerentes y áreas de negocio respectivas.	√		

NIVEL 3	La dirección ha concebido, documentado y comunicado un entorno integral de gestión de calidad y control de la información, que incorpora un marco para las políticas, procedimientos y estándares.	√		
NIVEL 4	La dirección asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad, asignando suficientes recursos para mantener el entorno en consonancia con los cambios significativos.		√	
NIVEL 5	El entorno de control de la información se alinea con el marco estratégico de gestión y la visión, y se revisa, actualiza y mejora con frecuencia.		√	

Ficha 41: Nivel de Madurez del Proceso PO7: Administrar los Recursos Humanos de TI de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO7: Administrar los Recursos Humanos de TI.**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No hay conciencia acerca de la importancia de alinear la gestión de los recursos humanos en tecnología de la información con el proceso de planificación tecnológica en la organización.	√		**GRADO DE MADUREZ** El proceso de Administrar los Recursos Humanos de TI está en el nivel 2 de madurez. - La Gerencia de Administración y finanzas actualizó su directiva de contrataciones del estado.
NIVEL 1	Se reconoce por parte de la dirección la necesidad de implementar una gestión de recursos humanos en tecnología de la información.	√		
NIVEL 2	Se adopta un enfoque táctico para la contratación y gestión del personal en tecnología de la información.	√		
NIVEL 3	Existe un proceso claramente definido y documentado para la gestión de los recursos humanos en tecnología de la información, respaldado por un plan de gestión de recursos humanos.		√	
NIVEL 4	La organización utiliza métricas estandarizadas para identificar desviaciones respecto al plan de gestión de recursos humanos en tecnología de la información, con especial énfasis en el manejo del crecimiento y la rotación del personal.		√	

NIVEL 5	El plan de gestión de recursos humanos en tecnología de la información se actualiza de manera continua para satisfacer los cambiantes requisitos del negocio.		√	

Ficha 42: Nivel de Madurez del Proceso PO8: Administrar la Calidad de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **PO8: Administrar la Calidad.**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dirección ejecutiva y el equipo de Tecnologías de la Información no reconocen la imperativa necesidad de implementar un programa de calidad. La evaluación de la calidad en los proyectos y operaciones nunca se lleva a cabo.	√		**GRADO DE MADUREZ** El proceso de Administrar la Calidad está en el nivel 2 de madurez. - La MDA realizó un convenio con la Facultad de Ingeniería de Sistemas e Informática de la Universidad de Huánuco para impulsar la Transformación Digital en la entidad y dentro de ese convenio incluye la implementación de un Sistema de Gestión de Calidad.
NIVEL 1	Existe una consciencia dentro de la dirección acerca de la importancia de un Sistema de Gestión de la Calidad (QMS, por sus siglas en inglés).	√		
NIVEL 2	Se ha iniciado un programa para definir y supervisar las actividades relacionadas con el Sistema de Gestión de la Calidad (QMS) dentro del ámbito de Tecnologías de la Información.	√		
NIVEL 3	La dirección ha comunicado un proceso claramente definido para el Sistema de Gestión de la Calidad (QMS) e implica a los equipos de Tecnologías de la Información y a la gerencia de los usuarios finales.		√	
NIVEL 4	El Sistema de Gestión de la Calidad (QMS) se encuentra integrado en todos los procesos, incluyendo aquellos que dependen de terceros. Se está estableciendo una base de conocimiento estandarizada para las métricas de calidad.		√	
NIVEL 5	El Sistema de Gestión de la Calidad (QMS) está completamente integrado y aplicado en todas las actividades de Tecnologías de la Información. Los procesos de QMS son flexibles y se adaptan a los cambios en el entorno de TI.		√	

Ficha 43: Nivel de Madurez del Proceso PO9: Evaluar y administrar los riesgos TI de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR PO9: Evaluar y administrar los riesgos TI				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se lleva a cabo una evaluación y gestión de los riesgos asociados a la tecnología de la información.	√		**GRADO DE MADUREZ** El proceso de Evaluar y administrar los riesgos TI está en el nivel 4 de madurez. - La Oficina de Informática analiza y evalúa los riesgos que se identificaron en este proyecto de investigación, se encuentra en la tabla 18 y 21.
NIVEL 1	Aunque se reconoce la necesidad de evaluar y gestionar los riesgos de TI, la comunicación de esta necesidad es inconsistente dentro de la organización.	√		
NIVEL 2	Existe un conocimiento implícito sobre la necesidad de evaluar y gestionar los riesgos de TI.	√		
NIVEL 3	El departamento de Informática establece los contextos de los riesgos y identifica los eventos (amenazas y vulnerabilidades).	√		
NIVEL 4	El departamento de Informática realiza la evaluación de los riesgos identificados y también responde a ellos.	√		
NIVEL 5	El departamento de Informática se rige bajo un plan de acción de riesgos para el mantenimiento preventivo y/o correctivo y monitoreo de los riesgos.		√	

Ficha 44: Nivel de Madurez del Proceso PO10: Administrar Proyectos de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR PO10: Administrar Proyectos.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	En la organización, no se emplean las técnicas de gestión de proyectos, y no se toma en consideración la repercusión empresarial asociada con la gestión deficiente de proyectos y los fallos en el desarrollo del proyecto.	√		**GRADO DE MADUREZ** El proceso de Administrar Proyectos está en el nivel 3 de madurez. - Gerencia Municipal realiza mesas de trabajo continuamente para administrar los proyectos de TI con las áreas involucradas Comité de Transformación Digital, Gerencia de Planeamiento y Presupuesto; y Gerencia de Administración y Finanzas; cada reunión queda documentado en un acta de mesa de trabajo.
NIVEL 1	Hay una falta de compromiso por parte de la alta dirección hacia la propiedad y gestión de proyectos.	√		
NIVEL 2	La alta dirección ha adquirido conciencia de la necesidad de gestionar proyectos de tecnologías de la información y ha comunicado esta conciencia.	√		

NIVEL 3	La alta dirección organizacional y de tecnologías de la información comienza a comprometerse y participar activamente en la gestión de proyectos de tecnologías de la información.	√		
NIVEL 4	La gerencia requiere la revisión de métricas y lecciones aprendidas de manera estandarizada y formal al concluir cada proyecto.		√	
NIVEL 5	Se ha implementado una metodología de ciclo de vida de proyectos probada, la cual se refuerza y se incorpora de manera integral en la cultura de toda la organización.		√	

Ficha 45: Nivel de Madurez del Proceso AI1: Identificar Soluciones Automatizadas de la segunda auditoría de procesos

DOMINIO: ADQUIRIR E IMPLEMENTAR **AI1: Identificar Soluciones Automatizadas**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La entidad no encuentra necesario realizar la identificación de los requisitos funcionales y operativos para el desarrollo, implementación o modificación soluciones automatizadas.	√		**GRADO DE MADUREZ** El proceso de Identificar Soluciones Automatizadas esta en el nivel de madurez 3. - El personal de TI identifica deficiencias en los proyectos y propone soluciones para regular y optimizar el proyecto en los factores de decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original.
NIVEL 1	Se lleva a cabo una investigación o análisis mínimo y estructurado acerca de la tecnología disponible.	√		
NIVEL 2	El éxito de cada proyecto se encuentra vinculado a la experiencia de unos pocos individuos clave. La calidad de la documentación y la toma de decisiones presenta variaciones considerables.	√		
NIVEL 3	El proceso de determinación de soluciones de tecnología de la información se implementa en algunos proyectos basándose en factores como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requisito de negocio inicial.	√		
NIVEL 4	La documentación de los proyectos cuenta con una calidad destacada y cada fase es aprobada de manera apropiada.		√	
NIVEL 5	Se respalda la metodología en bases de datos de conocimiento internas y externas que albergan		√	

	material de referencia sobre soluciones tecnológicas.			

Ficha 46: Nivel de Madurez del Proceso AI2: Adquirir y mantener software aplicativo de la segunda auditoría de procesos

DOMINIO: ADQUIRIR E IMPLEMENTAR **AI2: Adquirir y mantener software aplicativo**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Por lo general, las aplicaciones se adquieren en función de las ofertas de los proveedores, el reconocimiento de la marca o la familiaridad del personal de TI con productos específicos, prestando escasa atención a los requisitos actuales.	√		**GRADO DE MADUREZ** El proceso de Adquirir y Mantener Software Aplicativo está en el nivel de madurez 2. - El área de informática elaboró un plan de trabajo para la adquisición de licencias y softwares que requiere la MDA, donde involucra la estandarización de softwares para todos los usuarios, adquisición de licencias originales, fechas de caducidad, fechas de renovación, cada uno con su respectivo presupuesto para su adquisición.
NIVEL 1	Hay una probabilidad que se hayan obtenido de forma independiente diversas soluciones individuales para necesidades específicas de la organización, lo que resulta en ineficiencias en el mantenimiento y soporte.	√		
NIVEL 2	Se observan diferencias en los procesos de adquisición y mantenimiento de aplicaciones, pero estos son similares en función de la experiencia dentro de la operación de TI.	√		
NIVEL 3	Hay un proceso claramente definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso está alineado con la estrategia de TI.		√	
NIVEL 4	Se cuenta con una metodología formal y bien entendida que incluye un proceso de diseño y especificación en criterios de adquisición, así como un proceso de prueba y requisitos para la documentación.		√	
NIVEL 5	El enfoque se amplía a todas las empresas. La metodología de adquisición y mantenimiento ha avanzado considerablemente, permitiendo un posicionamiento estratégico rápido y proporcionando un alto grado de capacidad de respuesta y flexibilidad para hacer frente a los cambiantes requisitos del negocio.		√	

Ficha 47: Nivel de Madurez del Proceso AI3: Adquirir y Mantener Infraestructura Tecnológica de la segunda auditoría de procesos

DOMINIO: ADQUIRIR E IMPLEMENTAR AI3: Adquirir y Mantener Infraestructura Tecnológica				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se asigna la debida importancia a la gestión de la infraestructura tecnológica como una cuestión prioritaria que requiera atención.	√		**GRADO DE MADUREZ** El proceso de Adquirir y Mantener Infraestructura Tecnológica esta en el nivel de madurez 3. - Existe un plan de trabajo que está en proceso de ejecución para la implementación de Sistemas Administrativos para optimizar los procesos en la entidad.
NIVEL 1	Se efectúan modificaciones en la infraestructura cada vez que surge una nueva aplicación, sin un plan integral. Las labores de mantenimiento responden a necesidades a corto plazo.	√		
NIVEL 2	El mantenimiento y la adquisición de la infraestructura de TI carecen de una estrategia definida y no tienen en cuenta las exigencias de las aplicaciones organizativas que deben ser respaldadas.	√		
NIVEL 3	Aunque el proceso respalda las necesidades de las aplicaciones críticas del negocio y se alinea con la estrategia de tecnología de la información, no se implementa de manera consistente.	√		
NIVEL 4	La infraestructura de TI respalda de manera adecuada las aplicaciones del negocio. El proceso está bien estructurado y adopta un enfoque preventivo.		√	
NIVEL 5	El proceso de mantenimiento y adquisición de la infraestructura tecnológica es de naturaleza preventiva y está estrechamente alineado con las aplicaciones críticas del negocio y la arquitectura tecnológica, garantizando una implementación coherente.		√	

Ficha 48: Nivel de Madurez del Proceso AI4: Facilitar la Operación y el Uso de la segunda auditoría de procesos

DOMINIO: ADQUIRIR E IMPLEMENTAR AI4: Facilitar la Operación y el Uso				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se ha implementado ningún procedimiento en relación con la generación de documentación para usuarios, manuales operativos y materiales de formación.	√		**GRADO DE MADUREZ** El proceso de Facilitar la Operación y el Uso está en el nivel de madurez 2. - El nuevo personal de TI cuenta con la capacidad de brindar soporte; y capacitar el uso y buen
NIVEL 1	Gran parte de la documentación y muchos de los procedimientos	√		

	han alcanzado su fecha de caducidad. Los recursos de formación consisten en esquemas individuales con niveles de calidad variables.			funcionamiento de los sistemas que aloja la entidad.
NIVEL 2	La creación de los materiales de formación recae en individuos o equipos de proyecto, y la calidad está sujeta a la participación de dichos individuos.	√		
NIVEL 3	Los procedimientos se archivan y gestionan en una biblioteca formal, siendo accesibles para aquellos que requieran consultarla.		√	
NIVEL 4	Se han establecido controles para asegurar la adherencia a estándares y para el desarrollo y mantenimiento de procedimientos en todos los procesos.		√	
NIVEL 5	Los documentos de procedimiento y formación son considerados como una base de conocimiento en constante evolución, conservados electrónicamente y gestionados mediante herramientas actualizadas de gestión del conocimiento, flujo de trabajo y tecnologías de distribución, facilitando su acceso y mantenimiento.		√	

Ficha 49: Nivel de Madurez del Proceso AI5: Adquirir recursos de TI de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **AI5: Adquirir recursos de TI**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No se ha implementado un procedimiento definido para la obtención de recursos de tecnología de la información (TI).	√		**GRADO DE MADUREZ** El proceso de Adquirir Recursos de TI está en el nivel de madurez 4. - Existe un plan de trabajo de equipamiento de infraestructura tecnológica que están bajo las normas que lo rigen, como no tener más de 2 años de antigüedad y con las ultimas características en el mercado.
NIVEL 1	Los contratos destinados a la obtención de recursos de TI son elaborados y gestionados por líderes de proyectos y otros profesionales que ejercen su juicio experto en lugar de adherirse estrictamente a procedimientos y políticas formales.	√		
NIVEL 2	Se establecen responsabilidades y rendición de cuentas para la gestión de la adquisición y contratos de TI en función de la experiencia específica del gerente de contrato.	√		
NIVEL 3	La adquisición de TI se incorpora en gran medida a los	√		

	sistemas generales de adquisición del negocio.			
NIVEL 4	La adquisición de TI se integra ampliamente con los sistemas generales de adquisición de la organización, y se implementan estándares de TI para la obtención de recursos de TI.	√		
NIVEL 5	Se guarda relaciones sólidas con la mayoría de los proveedores y socios a lo largo del tiempo, y se monitorea y evalúa la calidad de estas relaciones. La gestión de relaciones se lleva a cabo de manera estratégica.		√	

Ficha 50: Nivel de Madurez del Proceso AI6: Administrar Cambios de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **AI6: Administrar Cambios**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No existe conciencia respecto a la posibilidad de que los cambios puedan generar interrupciones tanto para el individuo como para las operaciones comerciales, y tampoco se reconoce la importancia de una gestión efectiva del cambio.	√		**GRADO DE MADUREZ** El proceso de Administrar Cambios está en el nivel de madurez 3. - Cada cambio que se realiza en un proceso se documenta para que quede registro y se haga su cumplimiento y tiene que ser aprobado por el área competente.
NIVEL 1	Se admite la necesidad de gestionar y controlar los cambios, si bien las prácticas al respecto son diversas, lo que aumenta la probabilidad de que se realicen cambios sin la debida autorización.	√		
NIVEL 2	Se observa la presencia de un proceso informal de gestión del cambio, siendo este el enfoque principal para la mayoría de las modificaciones. Sin embargo, dicho proceso carece de estructura, es rudimentario y susceptible a errores.	√		
NIVEL 3	Se constata la existencia de un proceso formal definido para la gestión del cambio, que abarca la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y gestión de la liberación. Además, se observa un incipiente cumplimiento de este proceso.	√		
NIVEL 4	El proceso de gestión del cambio se desarrolla de manera sólida y uniforme para todas las modificaciones. La gerencia confía en que las excepciones son mínimas, y se destaca la		√	

	eficiencia y efectividad del proceso.			
NIVEL 5	Se realiza una revisión periódica del proceso de gestión del cambio, actualizándolo para mantenerse alineado con las mejores prácticas del momento.		√	

Ficha 51: Nivel de Madurez del Proceso AI7: Instalar y Acreditar Soluciones y Cambios de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR **AI7: Instalar y Acreditar Soluciones y Cambios**				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No existen procedimientos formales de instalación o acreditación, y tanto la alta dirección como el personal de tecnologías de la información no reconocen la necesidad de validar la idoneidad de las soluciones para su propósito previsto.	√		**GRADO DE MADUREZ** El proceso de Instalar y Acreditar Soluciones y Cambios está en el nivel de madurez 2. - Las soluciones y cambios nacen del personal de TI más no existe una metodología para realizarlo, estas soluciones propuestas se coordinan con el área responsable para realizar pruebas y acreditaciones.
NIVEL 1	Se reconoce la necesidad de verificar y confirmar que las soluciones implementadas son adecuadas para el propósito previsto, aunque no hay procesos formales de instalación o acreditación.	√		
NIVEL 2	Si bien hay cierta coherencia en los enfoques de prueba y acreditación, generalmente no se basan en ninguna metodología específica.	√		
NIVEL 3	Se ha establecido una metodología formal para la instalación, migración, conversión y aceptación. Los procesos de tecnologías de la información relacionados con la instalación y acreditación se integran en el ciclo de vida del sistema y se han automatizado en cierta medida.		√	
NIVEL 4	Los procedimientos son formales y han sido diseñados para ser organizados y prácticos, con entornos de prueba definidos y procesos de acreditación establecidos.		√	
NIVEL 5	Los procedimientos de instalación y acreditación han alcanzado un nivel de buenas prácticas, basándose en los resultados de la mejora continua y el refinamiento constante.		√	

Ficha 52: Nivel de Madurez del Proceso DS1: Definir y Administrar los Niveles de Servicio de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS1: Definir y Administrar los Niveles de Servicio				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dirección ejecutiva no muestra conciencia acerca de la importancia de instaurar un procedimiento que defina los estándares de atención al cliente.	√		**GRADO DE MADUREZ** El proceso de definir y administrar los niveles de servicio está en nivel de madurez 3. - El nivel de servicio se mide con pequeñas encuestas al usuario y acorde a eso se hace los controles necesarios para la mejora del servicio.
NIVEL 1	No se ha establecido de manera clara la responsabilidad y la obligación de supervisar tanto la formulación como la gestión de los servicios.	√		
NIVEL 2	Los informes acerca de los estándares de servicio se presentan de manera incompleta, pudiendo resultar irrelevantes o incluso engañosos para los clientes. La calidad de estos informes depende exclusivamente de las habilidades y la iniciativa de los gestores de manera individual.	√		
NIVEL 3	El proceso de elaboración del acuerdo de niveles de servicio se encuentra en orden y cuenta con puntos de control destinados a evaluar tanto los niveles de atención al cliente como su satisfacción.	√		
NIVEL 4	La satisfacción del cliente se mide y evalúa de forma regular. Las métricas de rendimiento reflejan las necesidades del cliente en lugar de los objetivos de la tecnología de la información.		√	
NIVEL 5	Todos los procesos y procedimientos relacionados con la gestión de niveles de servicio están sujetos a un constante proceso de mejora. La administración y supervisión de la satisfacción del cliente se llevan a cabo de forma continua.		√	

Ficha 53: Nivel de Madurez del Proceso DS2: Administrar los Servicios de Terceros de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS2: Administrar los Servicios de Terceros				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La ausencia de directrices formales en relación con la contratación de terceros es evidente.	√		**GRADO DE MADUREZ** El proceso de Administrar los Servicios

NIVEL 1	La dirección reconoce la importancia de establecer políticas y procedimientos detallados para la gestión de servicios proporcionados por terceros, lo que incluye la formalización mediante la firma de contratos.	√		de Terceros está en nivel de madurez 4. - La gerencia de Administración y Finanzas actualizó la directiva de contrataciones del estado, incluye la modificación de los términos de referencia, la descripción del servicio, actividades a realizar, garantía, requisitos mínimos que debe cumplir el contratista, productos y/o entregables, plazo de ejecución del servicio, conformidad del servicio, forma de pago, penalidades; y cláusulas de confidencialidad, responsabilidad por vicios ocultos y anticorrupción.
NIVEL 2	La supervisión de proveedores de servicios externos, la evaluación de riesgos asociados y la prestación de servicios se lleva a cabo de manera no estructurada.	√		
NIVEL 3	Existen procedimientos exhaustivamente documentados para supervisar los servicios de terceros, con procesos transparentes para abordar y negociar con los proveedores.	√		
NIVEL 4	Se definen criterios formales y estandarizados para especificar los términos de un acuerdo, abarcando aspectos como el alcance del trabajo, los servicios o entregables a proporcionar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades.	√		
NIVEL 5	El seguimiento del cumplimiento de las condiciones operativas, legales y de control se realiza activamente, implementando medidas correctivas. Se emplean medidas de monitoreo para la detección temprana de posibles problemas relacionados con los servicios de terceros.		√	

Ficha 54: Nivel de Madurez del Proceso DS3: Administrar el Desempeño y la Capacidad de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS3: Administrar el Desempeño y la Capacidad				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dirección ejecutiva no admite la posibilidad de que los procesos críticos de la empresa puedan necesitar un rendimiento significativamente alto de las tecnologías de la información, o que los requisitos totales de servicios de TI para la empresa puedan superar la capacidad existente.	√		**GRADO DE MADUREZ** El proceso de Administrar el Desempeño y la Capacidad está en el nivel de madurez 2. - En la MDA se estableció objeticos y expectativas claras, se proporciona la retroalimentación y coaching, se realiza capacitaciones, se recompensa el buen desempeño y se gestiona el bajo desempeño.
NIVEL 1	Ada procesos tiene un responsable y se muestran escaso interés en la importancia de llevar a cabo una planificación proactiva de la capacidad y el rendimiento. Las medidas para gestionar el rendimiento y la capacidad suelen adoptarse de manera reactiva.	√		

NIVEL 2	Por lo general, se logra satisfacer las necesidades de rendimiento mediante evaluaciones de sistemas individuales y el respaldo de equipos de proyecto con conocimientos especializados.	√		
NIVEL 3	Los pronósticos de capacidad y rendimiento se modelan mediante un proceso claramente definido, y se generan informes con estadísticas de rendimiento.		√	
NIVEL 4	La información actualizada está disponible, proporcionando estadísticas de rendimiento estandarizadas y alertando sobre incidentes derivados de insuficiencias en rendimiento o capacidad.		√	
NIVEL 5	Se realizan evaluaciones regulares de la infraestructura de TI y la demanda empresarial para garantizar la consecución de una capacidad óptima con el menor costo posible.		√	

Ficha 55: Nivel de Madurez del Proceso DS4: Garantizar la continuidad del servicio de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR				
DS4: Garantizar la continuidad del servicio				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La falta de comprensión de los riesgos, vulnerabilidades y amenazas para las operaciones de Tecnologías de la Información es evidente.	√		**GRADO DE MADUREZ** El proceso de Garantizar la Continuidad del Servicio está en el nivel de madurez 4. - En la MDA se designó responsabilidades al personal de TI ante cualquier inconveniente o problema del hardware o software para la continuidad de los servicios.
NIVEL 1	La responsabilidad en relación con la continuidad de los servicios es informal, y las autoridades para llevar a cabo estas responsabilidades son limitadas.	√		
NIVEL 2	Los informes sobre la disponibilidad son intermitentes, potencialmente incompletos y no consideran adecuadamente el impacto en las operaciones comerciales.	√		
NIVEL 3	Existe una asignación y definición clara de responsabilidades para la planificación y las pruebas de la continuidad de los servicios.	√		
NIVEL 4	Se asigna la responsabilidad de mantener un plan formalizado para la continuidad de los servicios.		√	
NIVEL 5	Los procesos integrados para la continuidad del servicio incorporan referencias de la industria y adoptan las mejores prácticas externas.		√	

Ficha 56: Nivel de Madurez del Proceso DS5: Garantizar la Seguridad de los Sistemas de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS5: Garantizar la Seguridad de los Sistemas				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Las estrategias para respaldar la gestión de la seguridad de Tecnologías de la Información no han sido aplicadas. No se generan informes sobre la seguridad de TI ni se dispone de un procedimiento para abordar incidentes de seguridad en TI.	√		**GRADO DE MADUREZ** El proceso de Garantizar la Seguridad de los Sistemas está en el nivel de madurez 3. - La MDA gracias a las políticas de seguridad de la información propuesta por este proyecto de investigación, pueden controlar la accesibilidad, la designación de responsabilidades y sanciones por el incumplimiento.
NIVEL 1	La gestión de la seguridad de TI se realiza de manera reactiva. No se realiza una evaluación cuantitativa de la seguridad de TI. Los incidentes de seguridad en TI provocan respuestas con acusaciones personales debido a la falta de claridad en las responsabilidades. Las respuestas a los incidentes de seguridad en TI son impredecibles.	√		
NIVEL 2	La conciencia sobre la importancia de la seguridad está fragmentada y limitada. Aunque los sistemas generan información relevante sobre la seguridad, esta no se somete a un análisis adecuado.	√		
NIVEL 3	Las responsabilidades en materia de seguridad de TI están asignadas y comprendidas, pero no se aplican de manera continua. Se cuenta con un plan de seguridad de TI y se implementan soluciones de seguridad basadas en un análisis de riesgos.	√		
NIVEL 4	Es obligatorio establecer métodos para fomentar la conciencia sobre la seguridad. La identificación, autenticación y autorización de usuarios siguen estándares establecidos.		√	
NIVEL 5	Los usuarios y clientes asumen cada vez más la responsabilidad de definir los requisitos de seguridad, y las funciones de seguridad se integran con las aplicaciones durante la fase de diseño.		√	

Ficha 57: Nivel de Madurez del Proceso DS6: Identificar y Asignar Costos de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS6: Identificar y Asignar Costos				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La conciencia y el control respecto a la identificación y asignación de costos vinculados a la tecnología de la información están ausentes.	√		**GRADO DE MADUREZ** El proceso de Identificar y Asignar Costos está en el nivel de madurez 3. - La gerencia de Administración y Finanzas Actualizó su directiva de contrataciones del estado, incluye los procedimientos para la estructuración de costos de quipos tecnológicos de la información, se designó responsabilidades a los cotizadores del área.
NIVEL 1	En esta fase, se toman medidas de manera improvisada para identificar y asignar costos, sin contar con un enfoque coherente y documentado. Puede existir una carencia de recursos y procedimientos formales.	√		
NIVEL 2	Se inician procesos más formales para la identificación y asignación de costos. Aunque persisten inconsistencias, se están dando pasos hacia la estandarización del proceso.	√		
NIVEL 3	El proceso está completamente definido y documentado, con políticas y procedimientos claros para la identificación y asignación de costos. Se asignan responsabilidades y se realiza un seguimiento de manera más estructurada.	√		
NIVEL 4	Se introducen métricas y medidas para evaluar la efectividad del proceso DS6. La monitorización constante de los costos lleva a mejoras basadas en datos y resultados medibles.		√	
NIVEL 5	La optimización continua busca la máxima eficiencia y eficacia. Se exploran oportunidades de mejora y se aplican constantemente las mejores prácticas.		√	

Ficha 58: Nivel de Madurez del Proceso DS7: Educar y entrenar a los usuarios de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS7: Educar y entrenar a los usuarios				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Existe una ausencia total de programas destinados al desarrollo y formación. La entidad no admite la existencia de un inconveniente relacionado con el entrenamiento, y no se produce ninguna comunicación referente a este problema.	√		**GRADO DE MADUREZ** El proceso de Educar y Entrenar a los usuarios está en el nivel de madurez 2. - El entrenamiento y educación a los usuarios es de manera informal y

NIVEL 1	Se observa que la entidad ha reconocido la importancia de implementar un programa de formación, aunque carece de procedimientos normalizados. Dado la falta de un proceso organizado, los empleados han optado por participar en cursos relacionados con ética laboral, conciencia de seguridad en sistemas y prácticas de seguridad de manera independiente. La gestión global presenta una falta de cohesión, y la comunicación sobre los problemas y enfoques para abordar la formación y educación es esporádica e inconsistente.	√		lo hace el personal de TI cuando surge alguna circunstancia sin tener algún plan de entrenamiento, pero Gerencia Municipal es consciente de que se necesita implementar un plan de entrenamiento y educación con cronograma de fechas y temas.
NIVEL 2	Existe conciencia acerca de la necesidad de un programa de formación y educación, así como de los procesos asociados a nivel organizativo. La formación comienza a incorporarse en los planes de rendimiento individuales de los empleados. Los procesos han avanzado hasta el punto en el cual diversos instructores imparten formación informal, cubriendo temas similares desde diferentes perspectivas. Algunas clases tratan asuntos éticos y conciencia sobre prácticas y actividades de seguridad en sistemas. A pesar de depender en gran medida del conocimiento individual, hay comunicación coherente respecto a los problemas globales y la necesidad de abordarlos.	√		
NIVEL 3	El programa de formación y educación se institucionaliza y comunica, con empleados y gerentes identificando y documentando las necesidades de formación. Los procesos de formación y educación se estandarizan y documentan.		√	
NIVEL 4	Se implementa un programa completo de formación y educación que arroja resultados medibles. Las responsabilidades se definen claramente, y se establece la propiedad sobre los procesos. La formación y educación se convierten en componentes fundamentales de los planes de carrera de los empleados. La gerencia brinda apoyo y participa en sesiones de formación y educación.		√	

NIVEL 5	La formación y educación generan mejoras en el rendimiento individual. Estos aspectos se convierten en elementos críticos de los planes de carrera de los empleados. Se asignan presupuestos, recursos, instalaciones e instructores suficientes para los programas de formación y educación. Los procesos se perfeccionan y se encuentran en constante mejora, aprovechando las mejores prácticas externas y los modelos de madurez de otras organizaciones.		√	

Ficha 59: Nivel de Madurez del Proceso DS8: Administrar la Mesa de Servicio y los Incidentes de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS8: Administrar la Mesa de Servicio y los Incidentes.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La entidad carece de mecanismos para abordar las inquietudes y preguntas de los usuarios, evidenciando una ausencia total de procesos para la gestión de incidentes. La organización no muestra reconocimiento alguno de la existencia de problemas que requieran atención.	√		**GRADO DE MADUREZ** El proceso de Administrar la Mesa de Servicio y los Incidentes está en el nivel de madurez 2. - La solución de incidencias se realiza de manera informal por el personal de TI experta en el tema, están en coordinación de desarrollan de procedimientos para la administración de incidencias.
NIVEL 1	La dirección reconoce la necesidad de implementar un proceso respaldado por herramientas y personal para atender las consultas de los usuarios y gestionar la resolución de incidentes. Sin embargo, este proceso carece de estandarización y se limita a brindar un respaldo reactivo. La gerencia no supervisa las consultas de los usuarios, los incidentes o las tendencias, y no hay un sistema de escalado para asegurar la resolución de problemas.	√		
NIVEL 2	Existe una conciencia organizativa sobre la importancia de establecer una mesa de servicio y un proceso de gestión de incidentes. La asistencia se brinda de manera informal a través de una red de expertos individuales, quienes cuentan con algunas herramientas comunes para ayudar en la resolución de incidentes. Aunque no hay capacitación formal, la comunicación sobre procedimientos estándar se delega al individuo.	√		

NIVEL 3	Se reconoce y acepta la necesidad de implementar una mesa de servicio y un proceso para la gestión de incidentes. Los procedimientos se estandarizan y documentan, aunque la capacitación sigue siendo informal. La responsabilidad de obtener capacitación y seguir los estándares recae en el individuo. Aunque se desarrollan guías de usuario y preguntas frecuentes (FAQs), estos recursos deben ser encontrados por los individuos y no necesariamente son seguidos.		√	
NIVEL 4	Los mecanismos, herramientas y técnicas se encuentran automatizadas mediante una base de conocimientos centralizada. El personal de la mesa de servicio trabaja estrechamente con el personal de administración de problemas.		√	
NIVEL 5	Tanto el proceso de gestión de incidentes como la función de mesa de servicio están sólidamente organizados y establecidos, adoptando un enfoque centrado en el servicio al cliente gracias a su experiencia y especialización.		√	

Ficha 60: Nivel de Madurez del Proceso DS9: Administrar la configuración de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS9: Administrar la configuración.				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La alta dirección no reconoce la importancia de contar con un sistema implementado que permita informar y gestionar las configuraciones de la infraestructura de tecnologías de la información (TI), tanto en términos de hardware como de software.	√		**GRADO DE MADUREZ** El proceso de Administrar la configuración está en el nivel de madurez 2. - Toda configuración de los equipos tecnológicos de la información se realizan de manera informal por el personal de TI con experiencia técnica en ciertos temas específicos, todas estas configuraciones no se documentan. Gerencia Municipal y el Comité de
NIVEL 1	Se comprende la necesidad de tener una gestión de configuración. Se llevan a cabo actividades básicas de administración de configuraciones, como mantener inventarios de hardware y software, pero de forma individual. No existen prácticas estandarizadas definidas.	√		

NIVEL 2	La dirección es consciente de la importancia de controlar las configuraciones de TI y reconoce los beneficios de mantener información completa y precisa sobre las configuraciones, aunque existe una dependencia implícita del conocimiento y la experiencia del personal técnico. Se emplean herramientas de administración de configuraciones hasta cierto punto, pero varían entre plataformas. Además, no se han establecido prácticas estandarizadas de trabajo.	√		Transformación digital están en coordinación para la implementación de procedimientos de administración de configuración para mejorar la seguridad, mejorar la eficiencia operativa y la reducción de riesgos.
NIVEL 3	Los procesos, procedimientos y prácticas de trabajo han sido documentados, estandarizados y comunicados, pero la implementación y aplicación de estándares dependen del individuo. Asimismo, se han introducido herramientas similares de administración de configuraciones entre plataformas. Es poco probable identificar desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se realiza alguna automatización para rastrear cambios en el software o hardware. La información de configuración es empleada por procesos interrelacionados.		√	
NIVEL 4	En todos los niveles, áreas, departamentos de la organización se reconoce la necesidad de gestionar las configuraciones y las mejores prácticas continúan evolucionando. Los procedimientos y estándares se comunican e incorporan a la implementación, y las desviaciones son monitoreadas, rastreadas y reportadas.		√	
NIVEL 5	Todos los sistemas, activos de TI se gestionan en un sistema central de configuraciones que contiene información completa sobre los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Existe una integración completa de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los informes de auditoría de los puntos de referencia proporcionan información esencial sobre el software y hardware en términos de reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se promueven reglas para restringir la instalación de software no autorizado.		√	

Ficha 61: Nivel de Madurez del Proceso DS10: Administrar los problemas de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS10: Administrar los problemas				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La falta de conciencia sobre la necesidad de abordar problemas conduce a la indiferenciación entre problemas e incidentes. Como resultado, no se ha hecho ningún esfuerzo por identificar las causas fundamentales de los incidentes.	√		**GRADO DE MADUREZ** El proceso de Administrar los problemas está en el nivel de madurez 3. - La MDA realizó un convenio con la facultad de Ingeniería de sistemas e informática de la Universidad de Huánuco la cual incluye, la implementación de un sistema integrado de gestión de incidencias para reducir el tiempo de resolución, Evitar incidentes costosos, Aumentar la productividad y Promover la continuidad del servicio.
NIVEL 1	Existe un reconocimiento de la importancia de gestionar los problemas y abordar sus causas fundamentales. Aunque algunos expertos proporcionan asesoramiento en sus áreas de especialización, no se asigna responsabilidad formal para la gestión de problemas. La falta de intercambio de información conduce a la generación de nuevos problemas y la pérdida de tiempo en la búsqueda de soluciones.	√		
NIVEL 2	La conciencia sobre la gestión de problemas en TI es amplia tanto en las áreas de negocio como en los servicios de información. Aunque ha habido una evolución en el proceso de resolución, solo unos pocos individuos clave son responsables de identificar y resolver problemas. La información se comparte de manera informal y reactiva, afectando la calidad del servicio al usuario debido a la falta de conocimiento estructurado disponible para el administrador de problemas.	√		
NIVEL 3	Se reconoce la necesidad de un sistema integral de gestión de problemas, respaldado por el apoyo de la gerencia y asignación de presupuesto. Se estandarizan los procesos de escalado y resolución de problemas, y la información se comparte de manera formal y proactiva. Aunque existen limitaciones en la revisión de incidentes y en el análisis de identificación y resolución de problemas, se evidencia un progreso.	√		
NIVEL 4	La comprensión del proceso de gestión de problemas se ha extendido a todos los niveles de la organización, con responsabilidades y propiedad claramente definidas. Los métodos y procedimientos están documentados, comunicados y evaluados para medir su eficacia.		√	

	Se ha iniciado la identificación y resolución de la mayoría de los problemas, y la gestión de problemas se integra de manera efectiva con otros procesos relacionados. Se han establecido indicadores clave de rendimiento (KPIs) y objetivos clave de rendimiento (KGIs) para el proceso.			
NIVEL 5	El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.		√	

Ficha 62: Nivel de Madurez del Proceso DS11: Administrar los datos de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS11: Administrar los datos				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La identificación de datos no se vincula con los recursos ni los activos corporativos.	√		**GRADO DE MADUREZ** El proceso de Administrar la configuración está en el nivel de madurez 3. - Gerencia Municipal y el comité de Transformación Digital realizaron una mesa de trabajo para poder cumplir con las políticas de seguridad de la información propuesta por este proyecto de investigación que incluye la administración de los datos para estandarizar y se aplican a la recopilación, el almacenamiento, el procesamiento y la eliminación de los datos,
NIVEL 1	La entidad reconoce la importancia de gestionar adecuadamente la información, aunque la responsabilidad de dicha gestión no está claramente definida. Los procedimientos de respaldo y recuperación, así como los acuerdos relativos a la eliminación de datos, están debidamente establecidos.	√		
NIVEL 2	En un nivel superior, comienza a surgir la noción de propiedad o responsabilidad sobre los datos.	√		
NIVEL 3	Existe una comprensión y aceptación de la necesidad de gestionar los datos tanto en el ámbito de la tecnología de la información como en toda la organización.	√		

NIVEL 4	Se comprende la necesidad de la gestión de datos y se aceptan las acciones requeridas en toda la organización.		√	Determinar quién tiene acceso a qué tipo de datos y qué tipos de datos están bajo administración, para Analizar e integrar los datos para obtener inteligencia empresarial destinada a la planificación estratégica.
NIVEL 5	La comprensión y aceptación de la necesidad de llevar a cabo todas las actividades necesarias para la gestión de datos está arraigada en toda la organización.		√	

Ficha 63: Nivel de Madurez del Proceso DS12: Administración del Ambiente Físico de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS12: Administración del Ambiente Físico				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	No existe conciencia acerca de la imperiosa necesidad de salvaguardar las instalaciones o invertir en recursos informáticos. Los aspectos medioambientales, como la protección contra incendios, polvo, suciedad, exceso de calor y humedad, no son objeto de control ni vigilancia.	√		**GRADO DE MADUREZ** El proceso de Administración del Ambiente Físico está en el nivel de madurez 2. - El mantenimiento de la infraestructura física de la entidad se realiza de manera informal por el personal experto de la Sub Gerencia de Patrimonio y Servicios Generales, Gerencia municipal está en coordinación con la Gerencia de Administración y Finanzas para implementar procedimientos de mantenimiento de instalaciones bien documentados.
NIVEL 1	La entidad reconoce la imperante necesidad de contar con un entorno físico que resguarde los recursos y el personal ante amenazas naturales y provocadas por el ser humano. La gestión de las instalaciones y equipos se basa en las habilidades de individuos clave. El personal puede desplazarse sin restricciones dentro de las instalaciones, y la administración no supervisa los controles medioambientales ni los movimientos del personal.	√		
NIVEL 2	La supervisión y aplicación de controles medioambientales recae en el personal de operaciones. La seguridad física es un proceso informal, llevado a cabo por un reducido grupo de empleados altamente comprometidos con la protección de las instalaciones. Los procedimientos de mantenimiento de las instalaciones carecen de una documentación detallada y dependen de las buenas prácticas de unos pocos individuos. Las metas de seguridad física no se basan en estándares formales, y la gerencia no garantiza el cumplimiento de los objetivos de seguridad.	√		

NIVEL 3	Existe una comprensión generalizada en toda la organización acerca de la necesidad de mantener un entorno informático bajo control. Los controles medioambientales, el mantenimiento preventivo y la seguridad física cuentan con un presupuesto autorizado y son supervisados por la gerencia. Se implementan restricciones de acceso, permitiendo el ingreso solo al personal autorizado. Los visitantes se registran y son acompañados según el individuo.		√	
NIVEL 4	El proceso de gestión del entorno físico se monitorea y mide. Se implementan mejoras continuas basadas en datos, buscando la eficiencia.		√	
NIVEL 5	La gestión del entorno físico es altamente eficiente y se mejora de manera constante. Se persigue la innovación y la excelencia en la administración del entorno físico.		√	

Ficha 64: Nivel de Madurez del Proceso DS13: Administración de Operaciones de la segunda auditoría de procesos

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS13: Administración de Operaciones				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	La dedicación de la entidad a la configuración del respaldo básico de Tecnologías de la Información (TI) y a las actividades operativas es inexistente.	√		**GRADO DE MADUREZ** El proceso de Administración de Operaciones está en el nivel de madurez 2. - Gerencia Municipal y el comité de Transformación Digital están realizando mesas de trabajo para el desarrollo e implementación de los procedimientos para la administración de operaciones y con el convenio realizado con la facultad de ingeniería de sistemas e informática la cual incluye sistemas integrados de Administración de operaciones.
NIVEL 1	Se reconoce en la entidad la necesidad de estructurar las funciones de soporte de TI. Se implementan algunos procedimientos estándar, y las actividades operativas tienen un carácter reactivo. La mayoría de los procesos operativos se programan de manera informal, y la validación previa de las solicitudes no es habitual. La disponibilidad, interrupción o demora de las computadoras, sistemas y aplicaciones que respaldan los procesos de negocio es frecuente. Se pierde tiempo en la espera de recursos por parte de los empleados.	√		

NIVEL 2	La entidad está consciente del papel crucial de las actividades operativas de TI en el soporte de funciones de TI. Se asignan presupuestos para herramientas de manera selectiva. Las operaciones de soporte de TI son informales e intuitivas, con una fuerte dependencia de las habilidades individuales. Las instrucciones sobre qué hacer, cuándo y en qué orden no están documentadas de manera sistemática. Se brinda cierta capacitación al operador, y existen algunos estándares formales de operación.	√		
NIVEL 3	La necesidad de gestionar las operaciones informáticas es comprendida y aceptada en la entidad. Se asignan recursos y se proporciona capacitación durante las labores. Las funciones repetitivas se definen, estandarizan, documentan y comunican formalmente. Los resultados de las tareas completadas y de los eventos se registran, con informes limitados dirigidos a la gerencia. Se introduce el uso de herramientas de programación automatizada y otras para reducir la intervención del operador.		√	
NIVEL 4	Los procesos de gestión de operaciones se definen y documentan. La entidad opera de manera proactiva, siguiendo procedimientos predefinidos.		√	
NIVEL 5	Los procesos de gestión de operaciones se monitorean y miden para asegurar la consistencia y promover la mejora continua. Se emplean métricas y se gestiona eficazmente los riesgos.		√	

Ficha 65: Nivel de Madurez del Proceso ME1: Monitorear y evaluar el desempeño de TI de la segunda auditoría de procesos

DOMINIO: PLANIFICAR Y ORGANIZAR				
ME1: Monitorear y evaluar el desempeño de TI				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	El monitoreo autónomo de proyectos o procesos no se lleva a cabo en TI. La ausencia de informes útiles, precisos y oportunos es evidente, y no se reconoce la necesidad de una comprensión clara de los objetivos de los procesos.	√		**GRADO DE MADUREZ** El proceso de Monitorear y Evaluar el Desempeño de TI esta en el nivel de madurez 2. - El monitoreo y desempeño de las TI lo realiza el personal de TI de manera informal y no documentada.
NIVEL 1	La recolección y evaluación de procesos no han sido estandarizadas. La implementación del monitoreo y la resolución de métricas se realiza de manera adaptativa, según las necesidades específicas de proyectos de Tecnologías de la Información.	√		
NIVEL 2	La interpretación de los resultados del monitoreo se fundamenta en la experiencia de individuos clave.	√		
NIVEL 3	Se han establecido mediciones para evaluar la contribución de la función de servicio de información al rendimiento organizacional, utilizando criterios financieros y operativos convencionales.		√	
NIVEL 4	Existe una integración de métricas en todos los proyectos y procesos de TI. Los sistemas de informes de la administración de TI están formalizados.		√	
NIVEL 5	Las mediciones y métricas orientadas al negocio se emplean de manera regular para evaluar el rendimiento y se incorporan en marcos estratégicos, como el balanced scorecard.		√	

Ficha 66: Nivel de Madurez del Proceso ME2: Monitorear y Evaluar el Control Interno de la segunda auditoría de procesos

DOMINIO: MONITOREAR Y EVALUAR				
ME2: Monitorear y Evaluar el Control Interno				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Lamentablemente, no se encuentran implementados los procedimientos de gestión interna para el control, lo cual refleja una carencia generalizada de conciencia respecto a la seguridad operativa y la garantía de control interno en el ámbito de Tecnologías de la Información (TI).	√		**GRADO DE MADUREZ** El proceso de Monitorear y Evaluar el Control Interno esta en el nivel de madurez 2. - Gerencia Municipal y el comité de Transformación digital desarrollaron un plan de entrenamiento y designación de roles a cada miembro del comité para la realización de autoevaluaciones y revisiones de aseguramiento del control interno.
NIVEL 1	La dirección de TI no ha formalizado la asignación de responsabilidades para supervisar la eficacia de los mecanismos de control internos.	√		
NIVEL 2	La gestión de servicios de información lleva a cabo revisiones periódicas de la eficacia de los controles internos que considera críticos. Aunque se están introduciendo metodologías y herramientas para evaluar estos controles, no se basan en un plan predefinido.	√		
NIVEL 3	Se ha implementado un programa de educación y formación orientado al monitoreo del control interno. Además, se ha establecido un proceso para autoevaluaciones y revisiones de aseguramiento del control interno, con roles específicos para los responsables tanto del negocio como de TI.		√	
NIVEL 4	Se han adoptado herramientas para estandarizar las evaluaciones y detectar automáticamente las excepciones de control. Asimismo, se ha constituido de manera formal una función especializada para el control interno de TI, integrando profesionales certificados que siguen un marco de trabajo de control respaldado por la alta dirección.		√	
NIVEL 5	La organización utiliza mecanismos, herramientas integradas y actualizadas, cuando corresponde, que facilitan una evaluación eficaz de los controles críticos de TI y la detección ágil de incidentes relacionados con el control de TI.		√	

Ficha 67: Nivel de Madurez del Proceso ME3: Garantizar el Cumplimiento Regulatorio de la segunda auditoría de procesos

DOMINIO: MONITOREAR Y EVALUAR				
ME3: Garantizar el Cumplimiento Regulatorio				
NIVEL DE MADUREZ		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
NIVEL 0	Existe escasa conciencia acerca de los elementos externos que inciden en Tecnologías de la Información, careciendo de procedimientos orientados al cumplimiento de requisitos normativos, legales y contractuales.	√		**GRADO DE MADUREZ** El proceso de Garantizar el Cumplimiento Regulatorio está en el nivel de madurez 2. - La Entidad confía en la capacidad del personal de TI con capacidad y experiencia para poder garantizar el cumplimiento regulatorio.
NIVEL 1	Se implementan procedimientos informales para asegurar el cumplimiento, pero únicamente en casos emergentes relacionados con nuevos proyectos o en respuesta a auditorías y evaluaciones.	√		
NIVEL 2	Aunque no se sigue un enfoque estandarizado, se confía en el conocimiento y la responsabilidad de los individuos, admitiendo la posibilidad de errores.	√		
NIVEL 3	Se imparte formación sobre los requisitos legales y normativos externos que afectan a la organización, junto con instrucciones sobre los procesos de cumplimiento establecidos.		√	
NIVEL 4	Las responsabilidades están claramente definidas, y se comprende la potenciación de los procesos. El procedimiento incluye una revisión del entorno para identificar requisitos externos y cambios recurrentes.		√	
NIVEL 5	Existe un amplio conocimiento de los requisitos externos aplicables, abarcando tanto sus tendencias futuras como los cambios anticipados, así como la necesidad de nuevas soluciones.		√	

Ficha 68: Nivel de Madurez del Proceso ME4: Proporcionar Gobierno de TI de la segunda auditoría de procesos

DOMINIO: MONITOREAR Y EVALUAR				
ME4: Proporcionar Gobierno de TI				
NIVEL DE MADUREZ		**CUMPLE**	**NO COMPLE**	**OBSERVACIONES**
NIVEL 0	Se observa una ausencia total de cualquier estructura discernible para la administración de Tecnologías de la Información (TI). La entidad no ha reconocido la existencia de un problema por resolver, lo que resulta en una falta de comunicación al respecto.	√		**GRADO DE MADUREZ** El proceso de Proporcionar Gobierno de TI está en el nivel de madurez 3. La entidad está aplicando las políticas de seguridad propuestas por este proyecto de investigación y así conseguir el gobierno digital que hace referencia al uso de las tecnologías digitales como parte integral de las estrategias de modernización de la entidad con el fin de crear valor público.
NIVEL 1	La gestión adopta un enfoque reactivo y la comunicación acerca de los problemas y las estrategias para abordarlos es esporádica e inconsistente.	√		
NIVEL 2	Aunque la administración ha identificado mediciones fundamentales para la gobernanza de TI, así como métodos y técnicas de evaluación, aún no se ha implementado el proceso a nivel organizacional.	√		
NIVEL 3	La dirección ha difundido procedimientos estandarizados y ha establecido programas de formación. Se han señalado herramientas para respaldar la supervisión de la gobernanza de TI.	√		
NIVEL 4	Los procedimientos y procesos de TI y la gobernanza de TI están alineados e integrados con la estrategia corporativa de TI. La mejora de los procesos de TI se basa principalmente en un conocimiento cuantitativo y es posible monitorear y medir la conformidad con procedimientos y métricas de procesos.		√	
NIVEL 5	La implementación de las políticas de TI ha conducido a una organización ágil y procesos que se adaptan rápidamente, brindando un respaldo completo a los requisitos de gobernanza de TI. Todos los problemas y desviaciones se analizan a través de las técnicas de causa raíz, y se identifican e implementan eficientemente medidas correctivas.		√	

NOTA BIOGRÁFICA

Luis Arnold Villa Sanchez, nacido en el Distrito de Huánuco Provincia de Huánuco del Departamento de Huánuco en el año 2000, demostró un temprano interés por la tecnología. Durante su paso por la Universidad, se ha destacado por su compromiso con el estudio, su capacidad para colaborar en equipo y su incansable curiosidad por ampliar sus conocimientos en su área de especialización.

Realizó sus estudios universitarios de pregrado en la Universidad Nacional Hermilio Valdizán, llegando a egresar y obtener el grado académico de Bachiller en Ingeniería Sistemas y aspirando posteriormente al título profesional y grados académicos superiores, Actualmente cursando el grado de maestría en Ingeniería de Sistemas en la Universidad Nacional Hermilio Valdizán mención en Tecnología de Información y Comunicación.

Complementa sus estudios con especializaciones en administración de base de datos, Análisis de datos, Inteligencia Artificial aplicada a proyectos, Big data, Realidad virtual y aumentada, Internet de las cosas y Seguridad de la Información.

Poseyendo una mente curiosa y un firme compromiso con la calidad, siente entusiasmo por proseguir su trayecto en el ámbito de la ingeniería, aspirando a realizar aportes relevantes y generar impacto en la sociedad mediante la aplicación innovadora de sus capacidades y saberes.

UNHEVAL
UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
DECANATO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL

En la ciudad universitaria de Cayhuayna, siendo las 8:00 a.m. horas del día 02 de mayo del 2024 nos reunimos en la Sala de sustentaciones de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, los miembros integrantes del Jurado Evaluador:

Dr. FRANCISCO PAREDES ABIMAEL ADAM	**PRESIDENTE**
Dra. JESUS TOLENTINO INES EUSEBIA	**SECRETARIO**
Mg. BALDEON CANCHAYA WALTER TEOFILO	**VOCAL**

Acreditados mediante Resolución Nº **0168-2024-UNHEVAL/FIIS-D,** de fecha **15 de abril del 2024**, de la tesis titulada: **POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS,** presentado por el titulando: **VILLA SANCHEZ Luis Arnold,** con el asesoramiento del docente **Mg. FLORES VIDAL JIMMY GROVER**, se procedió a dar inicio el acto de sustentación para optar el **Título Profesional de Ingeniero de Sistemas**.

Concluido el acto de sustentación, cada miembro del Jurado Evaluador procedió a la evaluación del titulando, teniendo presente los siguientes criterios:

1. Presentación
2. Exposición y dominio del tema
3. Absolución de preguntas

Nombres y Apellidos del Titulando	Jurado Evaluador			Promedio Final
	Presidente	Secretario	Vocal	
VILLA SANCHEZ Luis Arnold	18	18	18	18

Obteniendo en consecuencia el titulando: **VILLA SANCHEZ Luis Arnold** la nota de DIECIOCHO (10), equivalente a MUY BUENO por lo que se declara APROBADO

Calificación que se realiza de acuerdo con el Art. 78° del Reglamento General de Grados y Títulos Modificado de la UNHEVAL.

Se da por finalizado el presente acto, siendo las 9:15 a.m. horas, del día 02 de mayo del 2024 firmando en señal de conformidad.

PRESIDENTE
DNI Nº 22498088

SECRETARIO
DNI Nº 40396404

VOCAL
DNI Nº 72512084

Leyenda:
19 a 20: Excelente
17 a 18: Muy Bueno
14 a 16: Bueno
0 a 13: Desaprobado

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN"

Licenciada con Resolución del Consejo Directivo N° 099-2019-SUNEDU/CD

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE SIMILITUD N° 05-2024 SOFTWARE ANTIPLAGIO TURNITIN-FIIS-UNHEVAL.

La Unidad de Investigación de la Facultad de Ingeniería Industrial y de Sistemas, emite la presente constancia de Antiplagio, aplicando el Software TURNITIN, la cual reporta un 7% de similitud, correspondiente a los interesados (a) **VILLA SANCHEZ, LUIS ARNOLD.** Del trabajo de investigación ***POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS***, considerado como asesor(a) al Mg. Flores Vidal, Jimmy Grover.

DECLARANDO (APTO)

Se expide la presente, para los trámites pertinentes

Pillco Marca, 3 de mayo 2024

Dr. (a) Guadalupe Ramírez Reyes
Director(a) de la Unidad de Investigación
de la Facultad de Ingeniería Industrial y de Sistemas
UNHEVAL

Reporte de similitud

NOMBRE DEL TRABAJO

POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS

AUTOR

LUIS ARNOLD VILLA SANCHEZ

RECUENTO DE PALABRAS

106295 Words

RECUENTO DE CARACTERES

590336 Characters

RECUENTO DE PÁGINAS

386 Pages

TAMAÑO DEL ARCHIVO

14.2MB

FECHA DE ENTREGA

May 3, 2024 11:19 AM GMT-5

FECHA DEL INFORME

May 3, 2024 11:24 AM GMT-5

7% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 6% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 2% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 15 palabras)

7% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 6% Base de datos de Internet
- Base de datos de Crossref
- 2% Base de datos de trabajos entregados
- 1% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.unprg.edu.pe Internet	3%
2	docshare.tips Internet	1%
3	nanopdf.com Internet	<1%
4	Centro Europeo de Postgrado - CEUPE on 2023-08-14 Submitted works	<1%
5	Corporación Universitaria Minuto de Dios, UNIMINUTO on 2024-02-24 Submitted works	<1%
6	bibdigital.epn.edu.ec Internet	<1%
7	scribd.com Internet	<1%
8	qdoc.tips Internet	<1%

9	Cedeño, Eugenio Vallejo. "La Integración de la fe en el Proceso de Ense... Publication	<1%
10	slideshare.net Internet	<1%
11	docslide.us Internet	<1%
12	hdl.handle.net Internet	<1%
13	Centro Europeo de Postgrado - CEUPE on 2023-08-14 Submitted works	<1%
14	Centro Europeo de Postgrado - CEUPE on 2023-08-14 Submitted works	<1%
15	Centro Europeo de Postgrado - CEUPE on 2023-08-14 Submitted works	<1%
16	Carrera Torres, Olger | Prasshak Quiza, John Edgard | Quispe Vergaray,... Publication	<1%
17	Centro Europeo de Postgrado - CEUPE on 2023-08-14 Submitted works	<1%
18	Universidad Privada del Norte on 2024-01-26 Submitted works	<1%
19	docplayer.es Internet	<1%
20	Santos Castellanos, Weimar. "Impact of the Information Technology (I... Publication	<1%

21	Matallana, Doris Roxana Flores | Cahui, Joao Alejandro Tunque | Busto... Publication	<1%
22	unsaac on 2024-02-04 Submitted works	<1%
23	Avilez Farfan, Jose Antonio. "Planeamiento estrategico del distrito de ... Publication	<1%
24	Leonel Hernández Collante, Yamith Escobar, Freddy Acosta, Andri Pran... Crossref	<1%
25	dspace.ups.edu.ec Internet	<1%
26	UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ. "VI CONGRESO INTERN... Crossref	<1%

UNHEVAL UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN | VICERRECTORADO DE INVESTIGACIÓN | DIRECCIÓN DE INVESTIGACIÓN

AUTORIZACIÓN DE PUBLICACIÓN DIGITAL Y DECLARACIÓN JURADA DEL TRABAJO DE INVESTIGACIÓN PARA OPTAR UN GRADO ACADÉMICO O TÍTULO PROFESIONAL

1. Autorización de Publicación: *(Marque con una "X")*

Pregrado	X	Segunda Especialidad		Posgrado:	Maestría		Doctorado	

Pregrado (*tal y como está registrado en **SUNEDU***)

Facultad	INGENIERÍA INDUSTRIAL Y DE SISTEMAS
Escuela Profesional	INGENIERÍA DE SISTEMAS
Carrera Profesional	INGENIERÍA DE SISTEMAS
Grado que otorga	----------
Título que otorga	INGENIERO DE SISTEMAS

Segunda especialidad (*tal y como está registrado en **SUNEDU***)

Facultad	----------
Nombre del programa	----------
Título que Otorga	----------

Posgrado (*tal y como está registrado en **SUNEDU***)

Nombre del Programa de estudio	----------
Grado que otorga	----------

2. Datos del Autor(es): *(Ingrese todos los **datos** requeridos **completos**)*

Apellidos y Nombres:	VILLA SANCHEZ LUIS ARNOLD							
Tipo de Documento:	**DNI**	X	**Pasaporte**		**C.E.**		**Nro. de Celular:**	980073532
Nro. de Documento:	70910102						**Correo Electrónico:**	luisvillasanchez123@gmail.com

Apellidos y Nombres:								
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**Nro. de Celular:**	
Nro. de Documento:							**Correo Electrónico:**	

Apellidos y Nombres:								
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**Nro. de Celular:**	
Nro. de Documento:							**Correo Electrónico:**	

3. Datos del Asesor: *(Ingrese todos los **datos** requeridos **completos según DNI**, no es necesario indicar el Grado Académico del Asesor)*

¿El Trabajo de Investigación cuenta con un Asesor?: *(marque con una "X" en el recuadro del costado, según corresponda)*							**SI**	X	**NO**	
Apellidos y Nombres:	FLORES VIDAL JIMMY GROVER					**ORCID ID:**	https://orcid.org/ 0000-0001-8116-2340			
Tipo de Documento:	**DNI**	X	**Pasaporte**		**C.E.**		**Nro. de documento:**	22527461		

4. Datos del Jurado calificador: *(Ingrese solamente los **Apellidos y Nombres completos según DNI**, no es necesario indicar el Grado Académico del Jurado)*

Presidente:	FRANCISCO PAREDES ABIMAEL ADAM
Secretario:	JESUS TOLENTINO INES EUSEBIA
Vocal:	BALDEON CANCHAYA WALTER TEOFILO
Vocal:	
Vocal:	
Accesitario	

5. Declaración Jurada: *(Ingrese todos los **datos** requeridos **completos**)*

a) **Soy Autor (a) (es) del Trabajo de Investigación Titulado:** *(Ingrese el título tal y como está registrado en el **Acta de Sustentación**)*
POLÍTICAS DE SEGURIDAD PARA LA EFECTIVIDAD DEL RESGUARDO DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE AMARILIS
b) **El Trabajo de Investigación fue sustentado para optar el Grado Académico ó Título Profesional de:** *(tal y como está registrado en **SUNEDU**)*
TITULO PROFESIONAL DE INGENIERO DE SISTEMAS
c) El Trabajo de investigación no contiene plagio (ninguna frase completa o párrafo del documento corresponde a otro autor sin haber sido citado previamente), ni total ni parcial, para lo cual se han respetado las normas internacionales de citas y referencias.
d) El trabajo de investigación presentado no atenta contra derechos de terceros.
e) El trabajo de investigación no ha sido publicado, ni presentado anteriormente para obtener algún Grado Académico o Título profesional.
f) Los datos presentados en los resultados (tablas, gráficos, textos) no han sido falsificados, ni presentados sin citar la fuente.
g) Los archivos digitales que entrego contienen la versión final del documento sustentado y aprobado por el jurado.
h) Por lo expuesto, mediante la presente asumo frente a la Universidad Nacional Hermilio Valdizan (en adelante LA UNIVERSIDAD), cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido del Trabajo de Investigación, así como por los derechos de la obra y/o invención presentada. En consecuencia, me hago responsable frente a LA UNIVERSIDAD y frente a terceros de cualquier daño que pudiera ocasionar a LA UNIVERSIDAD o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causas en la tesis presentada, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello. Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudieran derivarse para LA UNIVERSIDAD en favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del trabajo de investigación. De identificarse fraude, piratería, plagio, falsificación o que el trabajo haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Nacional Hermilio Valdizan.

6. Datos del Documento Digital a Publicar: *(Ingrese todos los **datos** requeridos **completos**)*

Ingrese solo el año en el que sustentó su Trabajo de Investigación: *(Verifique la Información en el **Acta de Sustentación**)*						2024	
Modalidad de obtención del Grado Académico o Título Profesional: *(Marque con **X** según Ley Universitaria con la que inició sus estudios)*	**Tesis**	**X**	**Tesis Formato Artículo**		**Tesis Formato Patente de Invención**		
	Trabajo de Investigación		**Trabajo de Suficiencia Profesional**		**Tesis Formato Libro, revisado por Pares Externos**		
	Trabajo Académico		**Otros** *(especifique modalidad)*				

Palabras Clave: *(solo se requieren 3 palabras)*	Políticas de seguridad de la información	metodología MAGERIT versión 3	metodología COBIT 4.1

Tipo de Acceso: *(Marque con **X** según corresponda)*	**Acceso Abierto**	**X**	**Condición Cerrada (*)**		
	Con Periodo de Embargo (*)		**Fecha de Fin de Embargo:**		

¿El Trabajo de Investigación, fue realizado en el marco de una Agencia Patrocinadora? *(ya sea por financiamientos de proyectos, esquema financiero, beca, subvención u otras; marcar con una "**X**" en el recuadro del costado según corresponda):*	**SI**		**NO**	**X**
Información de la Agencia Patrocinadora:				

El trabajo de investigación en digital y físico tienen los mismos registros del presente documento como son: Denominación del programa Académico, Denominación del Grado Académico o Título profesional, Nombres y Apellidos del autor, Asesor y Jurado calificador tal y como figura en el Documento de Identidad, Titulo completo del Trabajo de Investigación y Modalidad de Obtención del Grado Académico o Título Profesional según la Ley Universitaria con la que se inició los estudios.

7. **Autorización de Publicación Digital:**

A través de la presente. Autorizo de manera gratuita a la Universidad Nacional Hermilio Valdizán a publicar la versión electrónica de este Trabajo de Investigación en su Biblioteca Virtual, Portal Web, Repositorio Institucional y Base de Datos académica, por plazo indefinido, consintiendo que con dicha autorización cualquier tercero podrá acceder a dichas páginas de manera gratuita pudiendo revisarla, imprimirla o grabarla siempre y cuando se respete la autoría y sea citada correctamente. Se autoriza cambiar el contenido de forma, más no de fondo, para propósitos de estandarización de formatos, como también establecer los metadatos correspondientes.

Firma:		
Apellidos y Nombres:	VILLA SANCHEZ LUIS ARNOLD	**Huella Digital**
DNI:	70910102	
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Fecha: 01/06/2024		

Nota:

- ✓ No modificar los textos preestablecidos, conservar la estructura del documento.
- ✓ Marque con una **X** en el recuadro que corresponde.
- ✓ Llenar este formato de forma digital, con tipo de letra **calibri, tamaño de fuente 09**, manteniendo la alineación del texto que observa en el modelo, sin errores gramaticales *(recuerde las mayúsculas también se tildan si corresponde).*
- ✓ La información que escriba en este formato debe coincidir con la información registrada en los demás archivos y/o formatos que presente, tales como: DNI, Acta de Sustentación, Trabajo de Investigación (PDF) y Declaración Jurada.
- ✓ Cada uno de los datos requeridos en este formato, es de carácter obligatorio según corresponda.