UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERIA DE SISTEMAS

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

LÍNEA DE INVESTIGACIÓN: INGENIERÍA Y TECNOLOGÍA

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

TESISTAS:

VILLADEZA ROMERO, KAREN LUCILA.

CONDOR SIMON, REYNALDO DAVID.

ASESOR:

MG. FLORES VIDAL, JIMMY GROVER

HUÁNUCO – PERÚ

2022

Dedicatoria

A Dios por darme la vida y estar siempre a mi lado más en este momento tan importante de mi formación profesional.

A mis padres que me han educado con valores y buenos sentimientos que me han ayudado a salir adelante en los momentos más difíciles.

A mis hermanos por el apoyo moral e incondicional durante mi etapa universitaria.

Bachiller Karen Lucila Villadeza Romero

Dedicatoria

Al Dios que me dio la valentía y fortaleza para levantarme día a día para continuar cuando estuve por derrumbarme.

A mi madre por demostrarme siempre su cariño incondicional y estar siempre a mi lado.

A mis hermanos que siempre están presentes para mi y por su apoyo desde que inicie esta aventura de convertirme en un profesional

A mi padre porque, aunque no estemos juntos y sé que está presente en cada paso. Estoy seguro que estarías orgulloso por mis logros.

Bachiller Reynaldo David Cóndor Simón

Agradecimiento

Agradecemos en primer lugar a Dios por habernos brindado fuerza y valor para dar por concluido este proyecto de tesis.

A nuestro asesor el Ingeniero Jimmy Flores Vidal por la colaboración y orientación brindada durante la elaboración de este proyecto.

A cada uno de los ingenieros de la facultad ya que nos guiaron de la mejor manera con sus amplios conocimientos.

Resumen

El proyecto descrito en este documento parte de la 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 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.

Para el desarrollo del SGSI, usamos la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT en la versión 3 para el análisis y gestión de riesgos de los activos, primero empezamos con el análisis de la evaluación del estado inicial de la organización, para luego planificar y diseñar el SGSI. Con los resultados del análisis de los activos que definimos con el MAGERIT V3 iniciamos el tratamiento de riesgos para luego continuar con la elaboración de los controles de seguridad asociados a la NTP – ISO/IEC 27001:2014 y así realizar el diseño de la declaración de aplicabilidad de acuerdo a sus lineamientos y proponer políticas de seguridad de información alineados al contexto de la municipalidad distrital de Huácar.

los resultados evidencian la carencia de la seguridad de la información en la municipalidad a lo que en la documentación que se les va a proporcionar usamos los controles más adecuados para la posterior implementación de este SGSI en sus áreas y procesos.

Palabras clave: Norma Técnica Peruana NTP – ISO/IEC 27001:2014, SGSI, metodología MAGERIT en la versión 3, Sistema de Gestión de Seguridad de la Información, Seguridad de la información, riesgos, controles, políticas de seguridad, activos,

Summary

The project described in this document is based on the problems of the District Municipality of Huácar related to the requirement of the implementation of the Peruvian technical standard NTP-ISO/IEC 27001:2014 in state institutions, for this reason it is necessary to perform an assessment of this entity, developing an Information Security Management System (ISMS) to evaluate how safe our systems are, quantifying the assets and their characteristics of greater value, so that later when an implementation is carried to reduce or eliminate risks and increase productivity and effectiveness in it.

For the development of the ISMS, we used the methodology of Analysis and Risk Management of Information Systems - MAGERIT in version 3 for the analysis and risk management of assets, first we started with the analysis of the evaluation of the initial state of the organization, and then plan and design the ISMS. With the results of the analysis of the assets that we defined with MAGERIT V3 we started the risk treatment to then continue with the development of security controls associated with the NTP - ISO/IEC 27001:2014 and thus make the design of the statement of applicability according to its guidelines and propose information security policies aligned to the context of the district municipality of Huácar.

The results show the lack of information security in the municipality to what in the documentation that will be provided to them we use the most appropriate controls for the subsequent implementation of this ISMS in their areas and processes.

Key words: Peruvian Technical Standard NTP - ISO/IEC 27001:2014, ISMS, MAGERIT methodology in version 3, Information Security Management System, Information Security, risks, controls, security policies, assets,

Introducción

Cada día aumentan las amenazas que dañan a la seguridad de la información siendo esto un riesgo para los activos más vulnerables dentro de las organizaciones. La seguridad de la información, se entiende cómo aquellas técnicas preventivas que las organizaciones adquieren para resguardar y proteger sus activos y mantener la confidencialidad, integridad y disponibilidad de los mismos.

Este proyecto se diseña un sistema de gestión de la seguridad de la información (SGSI) en la Municipalidad Distrital de Huácar (MDH) involucrando a la norma técnica peruana NTP ISO/IEC 27001:2014 para reducir los riesgos existentes en los activos de la entidad.

La investigación se estructuró de la siguiente manera para describir dicho modelo:

En el capítulo I, la investigación se inicia con la problemática, objetivos, justificación, limitaciones y variables.

En el capítulo II, dentro del marco teórico se muestra la revisión bibliográfica del tema principal y también se menciona los trabajos de investigación que tengan relación.

En el capítulo III, detalla la metodología que usaremos como guía para la realización del SGSI para la MDH, además se describe el diseño de la investigación y muestra de la población.

En el capítulo IV, desarrolla el diseño del SGSI propuesto.

En el capítulo V, Finalmente se describe la discusión y se muestra las conclusiones de la investigación, ya finalizando se enumera las recomendaciones que aportaran enormemente cuando decidan realizar la implementación del sistema en la MDH.

Índice de tablas

Índice de gráficos

Contenido

Capítulo I. Problema de investigación

1.1. Fundamentación del problema de investigación

Actualmente el valor más alto e importante en comparación de otros activos en una organización es la información, las organizaciones están sujetas a una serie de amenazas mientras no garanticen un entorno completamente seguro para sus datos, ya que éstos se han convertido en la base fundamental para la consecución de sus objetivos y su existencia.

El gobierno peruano ha establecido como objetivo principal de su estrategia de ciberseguridad lo siguiente: Garantizar la privacidad, integridad, disponibilidad, legalidad y confiabilidad de la información, salvaguardar la infraestructura de información, los datos y la información del Estado, así como la tecnología utilizada para su procesamiento, frente a amenazas internas o externas intencionadas o no. Las presentes normas establecen la aplicación requerida de la Norma Técnica Peruana-ISO/IEC 27001:2014 para la municipalidad distrital de Huácar como resultado del alcance de esta política que se implementa en todas las entidades de la administración pública.

Estas son las razones por las que se realizó una evaluación a la municipalidad distrital de Huácar, con el fin de realizar un SGSI apoyándonos de la metodología MAGERIT v3 para identificar, valorar y diagnosticar qué tan seguros están nuestros activos de información, para luego con la NTP – ISO/IEC 27001:2014 realizar el diseño de la declaración de aplicabilidad de acuerdo a sus lineamientos, para así más adelante disminuir o eliminar los riesgos e incrementar la productividad y efectividad en el mismo.

1.2. Formulación del problema de investigación

1.2.1. Problema General

¿De qué manera un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 mejoraría la seguridad de la información en la Municipalidad Distrital de Huácar 2022?

1.2.2. Problema Específico

- ¿Qué requisitos de la Norma Técnica Peruana – ISO/IEC 27001:2014 aplicar para diagnosticar el nivel y situación actual de la seguridad de la información en la municipalidad distrital de Huácar?
- ¿De qué manera la identificación de los riesgos contribuye con el Sistema de Gestión de la seguridad de la información de la municipalidad distrital de Huácar?
- ¿Influye la propuesta de políticas de seguridad de la Norma Técnica Peruana – ISO/IEC 27001:2014 en la reducción de los riesgos a los que está expuesto los activos de la municipalidad distrital de Huácar?

1.3. Formulación de objetivos generales y específicos

1.3.1. Objetivo General

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.

1.3.2. Objetivos Específicos

- Aplicar los requisitos 4 y 5 de la Norma Técnica Peruana ISO/IEC 27001:2014 para diagnosticar el nivel y situación actual de la municipalidad distrital de Huácar.
- Identificar los riesgos de la seguridad de la información usando MAGERIT V3 para contribuir con el SGSI de la municipalidad distrital de Huácar.
- Proponer políticas de seguridad basadas en la Norma Técnica Peruana ISO/IEC 27001:2014 para reducir el estado de riesgos de seguridad de la información en la municipalidad distrital de Huácar.

1.4. Justificación

En la actualidad la dependencia de las TICS en las organizaciones es más constante ya que su usa en sus actividades diarias, inclusive se incrementó más la dependencia con la crisis actual provocada por el COVID – 19, llevando a todas las organizaciones adaptarse forzosamente a una situación de entorno online y la utilización de las TIC, y al no estar familiarizados con estos medios tecnológicos pueden tener amenazas en la seguridad de activos informáticos.

Por lo expuesto previamente acerca de la información como activo esencial de las organizaciones sostiene el desarrollo del presente estudio, por cuanto diseñar un sistema de gestión de la seguridad de la información basado en la Norma Técnica Peruana ISO/IEC 27001:2014 y usando la metodología MAGERIT V3 permitió a la municipalidad distrital de Huácar gestionar los riesgos que tienen actualmente todos los activos, además permitió la toma de decisiones de acuerdo a sus resultados.

En la municipalidad distrital de Huácar no se encontraron estudios sobre el tema, lo que indica que allí no se implementó una gestión de riesgos. En consecuencia, se presentaron fallas en la conexión de la red, falta de estándares de seguridad, listas de activos desactualizadas y fallas encontradas por el personal de la entidad que comprometen la seguridad de los datos.

Es así como la municipalidad distrital de Huácar se benefició con el diseño de un SGSI basado en la Norma Técnica Peruana ISO/IEC 27001:2014 y su implementación a futuro, porque cuando las políticas de seguridad estén definidas se podrá proponer controles que ayudarán a manejar los riesgos a que se expone sus activos de información.

1.5. Limitaciones

Como limitación se tiene:

- La información de la municipalidad algunas son de carácter privado y restringido.
- la falta de estudios previos de investigación sobre el tema de investigación en la municipalidad distrital de Huácar.
- Desinterés en la entidad de aplicar controles que establece la NTP-ISO 27001:2014.
- Escasez de conocimientos sólidos acerca de la NTP-ISO/IEC 27001:2014 por parte del personal que trabaja en la entidad y no tienen un plan presupuestal para este.
- La falta de un área responsable en tecnologías de información en la municipalidad distrital de Huácar.

1.6. Formulación de hipótesis

1.6.1. Hipótesis General

En la investigación la formulación de hipótesis no se realizará puesto que tiene el alcance de estudio exploratorio, y también un enfoque cuantitativo.

Al final de la investigación se mostrará una solución al problema encontrado.

1.7. Variables

- **VI:** Sistema de Gestión de la Seguridad de la información basado en la NTP-ISO/IEC 27001:2014**.**
- **VD** Nivel de riesgo de los activos de información en la Municipalidad Distrital de Huácar.

1.8. Definición teórica y operacionalización de variables

1.8.1. Dimensiones:

- **Variable independiente:** Controles de seguridad, análisis de riesgo y el diagnóstico.
- **Variable dependiente:** Disponibilidad, integridad, confidencialidad, autenticidad y No repudio.

1.8.2. Indicadores:

- **Variable independiente:** % de requisitos completamente implementados, % de requisitos parcialmente implementados, % de requisitos diseñados, % de requisitos parcialmente diseñados, % de requisitos no diseñados, riesgos identificados, probabilidad de impacto de riesgo, criterios de aceptación de riesgos, número de políticas de seguridad.
- **Variable dependiente:** % riesgo en la disponibilidad, % riesgo en la integridad, % riesgo en la confidencialidad, % riesgo en la autenticidad y % riesgo en el no repudio.

1.8.3. Operacionalización de las variables

Tabla 1: ***Operacionalización de la variable independiente.***

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
Sistema de Gestión de la Seguridad de la información basado en la NTP-ISO/IEC 27001:2014	El Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma NTP ISO/IEC 27001:2014 permite a una organización evaluar la gestión de la seguridad de la información, tanto de la confidencialidad como de la integridad, para aplicar los controles necesarios que ayuden a reducir o eliminar los riesgos a los que están expuestos los activos de información.	● Diagnóstico. ● Análisis de riesgo. ● Controles de seguridad.	● % de requisitos completamente implementados. ● % de requisitos parcialmente implementados. ● % de requisitos diseñados. ● % de requisitos parcialmente diseñados. ● % de requisitos no diseñados. ● Riesgos identificados. ● Probabilidad de impacto de riesgo. ● Criterios de aceptación de riesgos. ● Número de políticas de seguridad.

Tabla 2: ***Operacionalización de la variable dependiente.***

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
Nivel de riesgo de los activos de información en la Municipalidad Distrital de Huácar.	un conjunto de medidas de seguridad proactivas y reactivas, o de directrices y precauciones de uso que repercuten en el tratamiento de los datos por parte de una organización.	● Disponibilidad ● Integridad ● Confidencialidad ● Autenticidad ● No repudio.	● % riesgo en la disponibilidad. ● % riesgo en la integridad. ● % riesgo en la confidencialidad. ● riesgo en la autenticidad. ● % riesgo en el no repudio.

Capítulo II. Marco teórico

2.1 Antecedentes

2.1.1. Antecedentes Internacionales

(Medina Balseca & Meza Castillo, 2019), en su investigación “el objetivo principal fue facilitar la gestión de identificación, análisis y remediación de vulnerabilidades existentes en la Empresa de Telecomunicaciones en la cuidad de Quito”.

En la estructura de su tesis lo primero que realizaron fue la investigación de la problemática dentro de la organización ya que la empresa está en constante crecimiento se tomó la decisión de adquirir nuevos equipos informáticos para satisfacer las necesidades de los clientes con esto aumentan los riesgos de seguridad de la información. El autor describió la identificación de los riesgos que tienen en la empresa en cuanto seguridad de la información para luego proponer en un marco de referencias.

(Fernández Villacrés, Martínez Campaña, & Aguilar Carrión, 2017), La tesis tuvo como “objetivo realizar un plan de seguridad informática basado en estándar ISO- IEC 27001 para proteger la información y activos del Gad Cantona de Pastaza, el punto de partida fue diagnosticar la situación actual del área informática del GAD Cantonal de Pastaza para conocer sus fortalezas y debilidades y con este resultado poder realizar un plan de seguridad que permitan mejorar la seguridad de activos e información”.

en sus conclusiones el autor describió que todo sistema siempre estará expuesto a las amenazas que están constantes en el entorno de la organización y con el plan de seguridad que planteo se pobra mitigar esos riesgos.

(Chicaiza Castillo & Torres Chango, 2020), sostuvo en su tesis como objetivo “elaborar una propuesta de plan de seguridad informática utilizando la norma ISO 27001 en la empresa Megaprofer S.A., por lo tanto, estudiar el proceso de verificación del cumplimiento de políticas ya establecidas dentro de la empresa, realizar el diagnóstico de la seguridad de la información del Departamento de TICS, integrar los beneficios que ofrece la norma 27001 para la protección ante cualquier amenaza que pueda poner en peligro o riesgo a la empresa, elaborar un plan de seguridad informática”.

Al finalizar el proyecto se aplicaron controles adecuados dentro lo sus procedimientos y se desarrolló la implementación del plan de seguridad.

(Dosa-Castro & Guevara-Gamboa, 2019), “En la investigación se tuvo como conclusión que a información es el activo más importante para cualquier organización, por lo tanto, es importante proteger los datos frente a la perdida de la disponibilidad, integridad y confidencialidad, El inventario de activos de información permite a las organizaciones realizar la identificación y clasificación de los activos de información que son de vital importancia dentro del Core del negocio, determinando su nivel de criticidad, Las organizaciones deben adoptar una metodología que permita realizar la identificación, análisis y evaluación los riesgos a los que se encuentran expuestos los activos de información, permitiendo mitigar el impacto en los procesos críticos de la organización, En el diagnóstico inicial del presente proyecto, se pudo evidenciar que, aunque en la empresa WI-SAT Comunicaciones S.A.S cuenta con medidas y controles de protección estos no son suficientes para salvaguardar los activos de información, de acuerdo a lo anterior la empresa se ve en la necesidad de implementar controles y medidas que permitan mitigar el impacto de los riesgos en los procesos críticos de la organización, Para la gestión de riesgos, se tomó como referencia la Guía para la administración del riesgo y el diseño de controles desarrollados por el DAFP, se realizó la identificación, de los activos de información, se realizó la estimación del nivel de los riesgos de acuerdo a los criterios de confidencialidad, integridad, disponibilidad de la seguridad de la información. Se evidenció una alta probabilidad de materialización de vulnerabilidades relacionadas con ausencia en el control de acceso, fallos en el sistema, mal funcionamiento del software de administración de copias de respaldo de la base de datos, dichas amenazas pueden ser mitigadas por medio de la implementación de las políticas propuestas en el presente proyecto y Se puede concluir que después de realizar el diagnostico de controles la estructuración de políticas de seguridad de la información con base en la metodología de gestión de riesgos del DAFP, es altamente viable la implementación de la NTC-ISO-IEC 27001:2013 en la empresa, permitiendo implementar el Sistema de Gestión de Seguridad de la información lo que permite la mejora continua en sus procesos, ahorraría costos por la reducción de incidentes, adopta y alinea los controles a todas las áreas de la empresa, genera confianza a sus clientes y proveedores con los mejores estándares y prácticas en materia de seguridad de la información, entre otras ventajas”.

(Chacón-Monroy & Molina-Montaña, 2022), “En este documento se presenta un análisis de riesgos basado en la norma ISO/IEC 27005 del 2018 e ISO/IEC 27002 del 2013 para el área de front digital de la compañía Xorex de Colombia S.A.S, que permita identificar de forma clara los riesgos a los que se encuentra expuesta la compañía y una serie de recomendaciones y procedimientos que garantizan el buen uso de la información, estableciendo las debidas restricciones, controles y demás procedimientos que nos ayuden a custodiar la información. De acuerdo al cumplimiento de los lineamientos constitucionales a los que hace referencia la ley estatutaria Ley 1341 o Ley de TIC, la ley 1581 de 2012 art 17 y art 18 sobre obligaciones, deberes y derechos de todos los actores para la protección de datos personales, normativa ISO/IEC 27005 del 2018 entre otras disposiciones donde brindaremos un enfoque de investigación y análisis sobre los riesgos de la seguridad de la información, así como procedimientos para la protección de datos y evitar pérdida de dicho activo, garantizando la disponibilidad, integridad, confidencialidad y buen uso. Debido a que el front digital es un proyecto bajo una licitación presentada por telefónica los criterios que debemos considerar para el análisis del riesgo se debe establecer bajo el objeto que presenta telefónica y para ello se comparten los siguientes criterios: la naturaleza y el tipo de riesgo, medición de la probabilidad y el impacto de los riesgos, la forma en que se determina el nivel de riesgo”.

2.1.2. Antecedentes Nacionales

(Huamán Monzón, 2014), enfoca su investigación con el fin “de establecer un modelo riguroso para el desarrollo de los planes de seguridad de la información de las mismas, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) publicó la normativa que declara la obligatoriedad del uso de las Normas Técnicas Peruanas NTP-ISO/IEC 27001:2008 y NTP-IEC 17799:2007 a un listado de empresas estatales peruanas que pertenecen y/o están involucradas en la Administración Pública. Como parte del proceso de implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 para mejorar la gestión de la seguridad de la información, esta investigación también tiene como objetivo establecer un procedimiento de auditoría de cumplimiento de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las instituciones estatales peruanas basado en el marco de trabajo COBIT 5.0”.

(Talavera Álvarez, 2015), con el fin “de asegurar el buen uso y protección de la información crucial que manejan, ya sea de clientes o de información estratégica interna, busca desarrollar el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud, el Instituto Nacional Materno Perinatal, sujeto al cumplimiento de la normativa vigente en materia de Seguridad de la Información, la Norma Técnica NTP ISO/IEC 27001. El uso de la Norma Técnica Peruana NTP ISO/IEC 27001, que obliga a las entidades públicas a crear un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con sus directrices y procedimientos, establece la conexión entre la investigación y esta norma”.

(Quispe Barreto, 2018), El objetivo principal del estudio fue “establecer la aplicabilidad de la NTP - IEC27001:2014 para prevenir accidentes en la Dirección Regional de Transportes y Comunicaciones de la Subdirección de Licencias de Conducir de Ancash, así como sugerir las mejores prácticas de seguridad de la información para el proceso de emisión de maletines. Se tomó en cuenta la NTP - ISO/IEC 27001:2014 y sus anexos, que incluyen los controles de seguridad, así como las teorías de la técnica de la elipsis y la gestión de riesgos. El estudio fue de carácter no experimental, descriptivo, correlacional y transversal, con una muestra compuesta por empleados y usuarios. Se utilizaron métodos de encuesta y se creó el instrumento utilizado en el siguiente cuestionario para el tratamiento y análisis de los datos con el fin de contrastar la hipótesis. Se determinó proponer la declaración de aplicabilidad, el apoyo de la alta dirección es esencial porque aumenta la conciencia y asigna la responsabilidad a los miembros del personal que participan en el proceso de solicitud de la licencia de conducir, que proporcionaron una visión inestimable durante la evaluación de los activos de información”.

(Sánchez Palacios, 2020), “La presente investigación desarrollada bajo la línea de investigación en evaluación y propuestas de implementación de normas o estándares, tuvo como objetivo realizar el análisis para la seguridad informática basado en la norma ISO 27001 que permita mejorar la gestión en los activos de información en la DRET. La investigación es no experimental, descriptiva porque tiene como finalidad examinar, desarrollando un análisis de la seguridad informática, de nivel aplicativo; pues se dirige a la aplicación inmediata. Se trabajó con una población de 52 trabajadores, con una muestra de 46 trabajadores. Utilizando el instrumento cuestionario y la técnica encuesta obtuvimos los siguientes resultados: En lo que concierne a la primera dimensión, en la Tabla Nro. 4: sobre políticas y procedimientos de seguridad, se

determina que el 100 % de los trabajadores, manifiestan que No saben de la existencia de políticas y/o procesos de seguridad de la información, en la segunda dimensión de seguridad de la información, en la Tabla Nro. 22: sobre análisis de seguridad informática, los trabajadores manifestaron que el 100% de los trabajadores encuestados manifiestan que SI consideran que se debe realizar un análisis de la seguridad informática para conocer cómo se lleva a cabo este proceso para mantener a salvo los activos de la institución. Lo que nos lleva a analizar que la seguridad informática es aprobada por parte de los trabajadores quienes creen que si se debería realizar un análisis de las amenazas hacia los activos de la información de la DRET".

(Lara Morales, 2018), "Esta tesis fue desarrollada bajo la línea de investigación en tecnología de la información y comunicación para la mejora continua de las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote Sede en Piura. La investigación tuvo como objetivo realizar la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, permitirá mejorar la gestión en los activos de información. La investigación tuvo un diseño de tipo no experimental porque los datos no se manipularán y de corte transversal porque se realiza en un determinado tiempo; la población de esta investigación fue de 28 empleados de los cuales se tomó en conciencia que esta investigación no se delimitará debido a que se verán beneficiados en su totalidad de empleados, a quien se les aplicó el instrumentos donde se lograron obtener los siguientes resultados: En la dimensión 01: Situación actual; que el 61% de los trabajadores encuestados opinaron que la situación actual NO cuenta con la adecuada gestión en los procesos de la clínica Simedic Diagnóstica S.A.C, mientras que el 39% SI está conforme con la situación actual de la clínica. Y en la dimensión 02: seguridad de información; se observó que el 68% de los trabajadores encuestados opinaron que, SI están de acuerdo con la que se debería realizar la propuesta para la seguridad informática para la clínica Simedic Diagnóstica S.A.C, mientras que el 32% NO cree necesario la propuesta para la seguridad informática. Se concluyó la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, para la seguridad de información queda aceptada en su totalidad para brindar mayor seguridad en la clínica, trabajadores y clientes".

2.1.3. Antecedentes Locales

(Argüezo Ramirez, 2019), el autor dentro de sus conclusiones “determino que en la investigación se identificó y evaluaron los riegos a lo que los activos están expuestos también sostuvo que el desarrollo de las políticas de seguridad es de gran utilidad para la protección de los activos y con ellos se podrá prevenir y mitigar los riesgos de los activos”.

(Pajuelo Godoy & Velásquez Gudiño, 2019), en esta investigación el objetivo principal “fue determinar la incidencia de la aplicación de la metodología Magerit v3 en la seguridad de información de la municipalidad Distrital de Pillco Marca. A lo que en sus conclusiones describieron el valor de significancia y realce que tuvo su tesis”.

(Tacza Valverde, 2018), “El estudio tuvo como objetivo determinar el cumplimiento de la norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur. El estudio básico descriptivo y correlacional se realizó con una muestra de 80 trabajadores con acceso a la información de la Universidad Nacional Tecnológica de Lima Sur. Se localizaron las fuentes de información como bibliografía, revistas, Internet, asociaciones de profesionales, de egresados, investigaciones de campo, tesis, etc. Del resultado de la hipótesis principal obtenido se infiere que existe relación significativa del plan de seguridad de información y la norma ISO/IEC). Por tanto, es necesario adaptarse a la Norma ISO 27001:2005 y plantear un plan de aseguramiento de la información. Se concluye, que la UNTELS no ha cumplido la implementación adecuada de un plan de seguridad de la información, según lo normado por al ONGEI, por tanto, dicha institución está en grave riesgo y constante amenaza con respecto a la gestión adecuada de sus repositorios de información, así como los mecanismos y políticas que enmarcan dichos procesos. Palabras clave: seguridad de la información, sistema de seguridad de la información, ISO 27000, plan de seguridad de la información, riesgos en seguridad de información, disponibilidad de información, distribución de información, diagnóstico de la seguridad de la información, condiciones de la seguridad de la información”.

2.2 Bases teóricas

2.2.1. Sistema de gestión de seguridad de la información

(Alvarado, 2022), “Un Sistema de gestión de seguridad de la información (SGSI) es básicamente, un conjunto de políticas de administración de la información. Para entender más a profundidad en qué consiste un SGSI debemos partir de la definición dada por el estándar internacional ISO/IEC 27000”.

“Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. A continuación, hablaremos de qué significan cada uno de estos términos en relación con la información:” (Alvarado, 2022).

- **Confidencialidad**: “la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Es necesario acceder a la información mediante autorización y control” (Alvarado, 2022).

- **Integridad**: “debe mantenerse la exactitud y completitud de la información y sus métodos de proceso. Su objetivo es prevenir modificaciones no autorizadas de la información” (Alvarado, 2022).

- **Disponibilidad:** “Garantizar el acceso y la utilización de la información y los sistemas de tratamiento de la misma, por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Su objetivo es prevenir interrupciones no autorizadas de los recursos informáticos” (Alvarado, 2022).

- .

Gráfico N.º 1, Sistema de Gestión de Seguridad de la información

(Alvarado, 2022), “Para lograr esta protección de los activos se debe establecer, implantar, mantener y mejorar un SGSI, el cual puede desarrollarse según el conocido enfoque de mejora continua denominado Ciclo de Deming. Este enfoque está constituido por cuatro pasos: **Planificar:** es una fase de diseño del SGSI en la que se evalúan los riesgos de seguridad de la información y se seleccionan los controles adecuados, **Hacer:** es una fase que envuelve la implantación y operación de los controles, **Verificar:** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI y **Actuar:** en esta fase se realizan cambios periódicamente para mantener el SGSI al máximo rendimiento”.

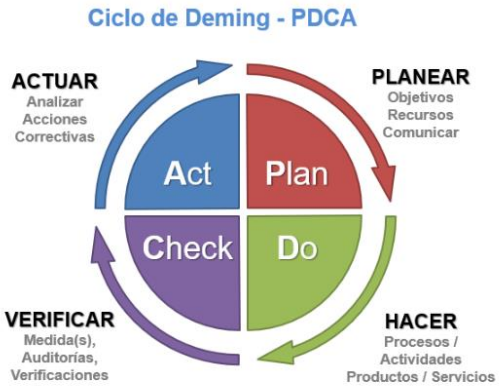

Gráfico N.º 2, Ciclo de Deming - PDCA

(Alvarado, 2022)

2.2.2. Ruta de implementación y mejoramiento continuo

- **Apoyo de la alta dirección**

(Alvarado, 2022), “Debido a que el Sistema de Gestión de Seguridad de la Información afecta a la gestión del negocio, requiere que todas las acciones futuras y las decisiones que se tomen sólo puedan ser desarrolladas por la alta dirección de la organización”.

(Alvarado, 2022), “Es un error común que el SGSI sea considerado una cuestión meramente tecnológica o técnica de los niveles operativos de la empresa. El compromiso de la alta dirección en la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información se evidencia con las siguientes iniciativas: Desarrollar una política de seguridad de la información, Garantizar el cumplimiento de planes y objetivos del Sistema de Gestión de Seguridad de la Información, Constituir roles y responsabilidades de seguridad de la información, Informar a la empresa la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad, Designar todos los recursos necesarios para llevar a cabo el SGSI, Determinar todos los criterios de aceptación de riesgos y sus correspondientes niveles, Asignar los recursos suficientes para todas las fases del SGSI y Garantizar que se realizan todas las auditorías internas”.

- **Alcance del SGSI**

(Alvarado, 2022), “El alcance del SGSI aclara cuáles son sus límites en función del contexto, la importancia y la ubicación de los activos críticos de información de la organización (por ejemplo: unidades, ubicaciones o departamentos) y los riesgos propios o externos asociados (por ejemplo: leyes y reglamentos, obligaciones contractuales, estrategias y políticas impuestas por organismos centrales)”.

“Se deben tener en cuenta los problemas internos y externos (análisis del contexto de la organización) y los requisitos y expectativas procedentes de las partes interesadas, que se relacionan con las actividades esenciales, es decir, aquellas que permiten cumplir con la misión y los objetivos generales de la organización” (Alvarado, 2022).

(Alvarado, 2022), “También se deben definir los procesos a incluir en el alcance y sus relaciones, esto debe hacerse teniendo en cuenta no solo los procesos de seguridad de la información sino todos los procesos que se aplican a su negocio y que impactan o pueden ser impactados por la seguridad de la información”.

- **Inventario de activos de información**

(Alvarado, 2022), “Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización. Para realizar este inventario se recomienda hacer una clasificación. Una clasificación recomendada por expertos es la siguiente”.

“Activos de información pura: **Datos digitales** (Bases de datos, Unidades lógicas y Copias de seguridad), **Activos tangibles(**Personales, Financieros y Legales), **Activos intangibles(**Conocimiento, Relaciones y Secretos comerciales), **Software de aplicación (**Propietario desarrollo por la organización, Herramientas de bases de datos, Aplicaciones de comercio electrónico y Middleware), **Sistemas operativos (**Servidores, Dispositivos de red y Dispositivos de mano e incrustados)” (Alvarado, 2022).

(Alvarado, 2022), “Activos físicos: **Infraestructura de TI** (Edificios, Centros de datos y Habitaciones de equipos y servidores), **Controles de entorno de TI** (Equipos de alarma, Supresión contra incendio y Sistemas de alimentación ininterrumpida), **Hardware de TI** (Dispositivos de almacenamiento, Ordenadores de mesa, Estaciones de trabajo y Ordenadores portátiles), **Activos de servicios de TI** (Servicios de autenticación de usuario, Administración de procesos y Enlaces)”.

“Activos humanos: **Empleados** (Personal y directivos, Participan quienes tienen roles de gestión como, por ejemplo, altos cargos y Arquitectos de software y desarrolladores), **Externos (**Trabajadores temporales**,** Consultores externos **y** Asesores especialistas)” (Alvarado, 2022).

(Alvarado, 2022), “Todos los activos de información deben ser propiedad de una parte designada de la organización. En este sentido, el propietario del activo definirá y garantizará los controles para la adecuada protección del activo. Adicionalmente, los activos de información

en este inventario deben clasificarse en términos de confidencialidad, integridad y disponibilidad".

- **Evaluación de riesgos**

(Alvarado, 2022), "Cada organización debe determinar el proceso más apropiado para evaluar los riesgos teniendo en cuenta las guías ISO/IEC 27005 e ISO 31000".

"Este proceso debe ser estructurado y repetible, es decir, un procedimiento documentado de evaluación de riesgos que explique cómo se identifican, analizan (por ejemplo, en base a posibles consecuencias y probabilidades de ocurrencia), evalúan (por ejemplo, aplicando criterios específicos para la aceptación del riesgo) y priorizan los riesgos relacionados con los activos de información más relevantes del alcance (por ejemplo, en atención a niveles de riesgo definidos)" (Alvarado, 2022).

"Las revisiones y las actualizaciones periódicas, o por cambios sustanciales que afronta la organización, son requeridas para evidenciar los cambios en los riesgos antes de que se produzcan y así mantener un enfoque preventivo y de anticipación en acciones mitigadoras o de control. El análisis de riesgo informático es un proceso relevante y es crucial su implementación para poder tener una perspectiva preventiva y no reactiva" (Alvarado, 2022).

- **Declaración de aplicabilidad**

(Alvarado, 2022), "Una vez evaluados los riesgos, se bebe hacer una verificación para determinar cuáles de los controles recomendados en el Anexo A de ISO/IEC 27001 están siendo aplicados o deben aplicarse en la organización. Para esto se puede hacer una referencia cruzada directa con la guía de implementación ISO/IEC 27002 y con cualquier otra fuente alternativa o suplementaria de información".

"La función esencial de este documento es evidenciar que los controles recomendados en el Anexo A de ISO/IEC 27001 se aplican cuando están dentro del alcance y son apropiados para su organización o, por el contrario, dejar claro cuando no se justifica el esfuerzo de su aplicación por motivos de gestión estratégica o de coste/efectividad, esto motivos que deben

ser formalmente registrados y justificados para evidenciar ante los auditores que no se los ha descuidado, ignorado o excluido arbitrariamente o porque hayan pasado inadvertidos" (Alvarado, 2022).

- **Tratamiento de riesgos**

"En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información. Esta definición debe alinearse con la disponibilidad, confidencialidad e integridad del mismo y con la política definida por la dirección. En este punto, se seleccionan las acciones adecuadas para cada riesgo, las cuales irán orientados a:" (Alvarado, 2022).

- "Asumir el riesgo: se trata de no hacer nada. Simplemente, sabemos que no tenemos cómo evitarlo y debemos convivir con él. Las organizaciones deciden aceptar un riesgo cuando la probabilidad de que ocurra es muy baja" (Alvarado, 2022).

- "Reducir el riesgo: Se usa cuando eliminar completamente el riesgo resulta mucho más costoso que asumir las consecuencias negativas de que este llegara a materializarse" (Alvarado, 2022).

- "Eliminar el riesgo: Se implementan las acciones para hacer que las condiciones o los factores que pueden generar el riesgo desaparezcan y con ellos el riesgo. Esta es una opción para aquellos casos de alta probabilidad de ocurrencia, con un muy alto impacto negativo" (Alvarado, 2022).

- "Transferir el riesgo: Significa que pasamos el problema a alguien más. La forma más usual de transferir un riesgo es contratar una póliza de seguros que indemnice a la organización en caso de que se presente el problema" (Alvarado, 2022).

Gráfico N.º 3, Respuesta de riesgos

(Alvarado, 2022)

2.2.3. Norma Técnica Peruana ISO/ IEC 27001: 2014

(INDECOPI, 2014), “Esta Norma Técnica Peruana ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo”.

“Es importante que el sistema de gestión de la seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información. Se espera que la implementación de un sistema de gestión de seguridad de la información crezca a escala en concordancia con las necesidades de la organización” (INDECOPI, 2014).

2.2.4. Metodologías para análisis y gestión de riesgos

Existen muchas metodologías para evaluar los riesgos en un proyecto, algunas de las metodologías son COBIT (Control Objetives for Information and Related Technology), MAGERIT y ITIL (Information Technology Infrastructure Library), las cuales nos brindaran herramientas para poder tomar decisiones e implementar controles para prevenir y mitigar los riesgos a los que están vulnerables los activos.

- **Metodología Control Objetives for Information and Related Technology (COBIT)**

(GlobalSuit Solutions, 2022), "La metodología COBIT Es un marco de trabajo (framework) para el gobierno y la gestión de las tecnologías de la información (TI) empresariales y dirigido a toda la empresa. La TI empresarial significa toda la tecnología y procesamiento de la información que una empresa utiliza para lograr sus objetivos, independientemente de dónde ocurra dentro de la empresa. En otras palabras, la TI empresarial no se limita al Depto. de TI de una organización. Su función es hacer un mapeo de procesos IT".

- **Metodología *Information Technology Infrastructure Library* ITIL**

(Freshservice, 2021), se define como "El conjunto de buenas prácticas que ayudan a mejorar la prestación de un servicio, en particular un servicio de TI (Tecnología de la Información) Permite a las organizaciones y a los individuos ofrecer una gestión de servicios de TI rentable, alinear su gestión con la visión, la estrategia y el crecimiento de la empresa, y actuar como un punto único de contacto entre el proveedor de servicios y los usuarios finales. Mientras que la gestión de servicios de TI (ITSM) ayuda a las empresas a lograr su misión gracias a una combinación de procesos, tecnología y personas adecuadas, el marco de trabajo ITIL expone la forma en la que hay que gestionar y prestar los servicios. Las buenas prácticas incluidas en la metodología ITIL sirven de guía para las iniciativas de tecnología y transformación digital. Las empresas que la adoptan pueden lograr sus beneficios empresariales más rápidamente gracias a tener unos procesos bien definidos y asequibles".

- **Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT V3)**

(Administrativa, 2012), Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista”.

2.3 Bases conceptuales

- **Activo de información:** Son los elementos que contienen la parte más valiosa de una organización que es la información.
- **Análisis de riesgo:** Parte de la metodología que identifica a los activos que son vulnerables a fugas de información.
- **Impacto:** Cuantifica el daño de un activo e identifica nivel de las amenazas.
- **Políticas de Seguridad:** Documentación que establece normas dentro de la organización para proteger y prevenir los riesgos.
- **Riesgo:** nivel de ocurrencia probable.
- **Amenazas:** Aprovechar los fallos de seguridad o los errores que pueden afectar a la funcionalidad de un sistema con el objetivo de sacar beneficio.
- **Equipos informáticos:** Son dispositivos tecnológicos que tienen en un entorno laboral.
- **Valoración de activos:** Definida para puntuar el valor de cada activo de acuerdo al criterio personal o expertos.
- **Seguridad de la información:** Normas que ayudan a prevenir riesgos

2.4 Bases epistemológicas o bases filosóficas o bases antropológicas

(Gomez Vieites, 2011), “En este libro se pretende abordar desde un punto de vista global la problemática de la Seguridad Informática y la Protección de Datos, contemplando tanto los aspectos técnicos, como los factores humanos y organizativos, así como el cumplimiento del entorno legal. Para ello, el contenido de esta obra se ha estructurado en siete grandes bloques: La primera parte presenta los principios básicos de la Seguridad de la Información en las organizaciones y en las redes de ordenadores, describiendo los elementos de las Políticas, Planes y procedimientos de Seguridad, el análisis y gestión de riesgos, así como la certificación según estándares como los de la familia ISO/IEC 27000, en la segunda parte se estudian las vulnerabilidades de los sistemas y redes informáticas, las amenazas y los tipos de ataques más frecuentes. También se analizan los Planes de Respuesta a Incidentes y de Continuidad del Negocio, una tercera parte se dedica a los aspectos relacionados con la identificación y autenticación de los usuarios en los sistemas informáticos, incluyendo el estudio de los más novedosos sistemas biométricos, en la cuarta parte se describen los principales sistemas y técnicas criptográficos, así como algunas de sus aplicaciones para mejorar la seguridad de los sistemas informáticos y de los servicios de Internet, analizando las características del DNI electrónico o de la factura electrónica, la quinta parte se centra en los aspectos técnicos para implantar las medidas de seguridad en las redes de ordenadores, analizando el papel de dispositivos como los cortafuegos (firewalls), sistema s de detección de intrusiones (IDS) o servidores proxy. Así mismo, se aborda el estudio de la seguridad en las redes privadas virtuales y en las redes inalámbricas, en la sexta parte del libro se presentan los aspectos relacionados con la seguridad en el uso de los principales servicios de Internet, el desarrollo de los medios de pago on-line, as í como la forma de afrontar problemas como el spam, el phishing o la protección de la privacidad de los ciudadanos en Internet y por último, en la séptima parte se analizan diversos aspectos relacionados con e l entorno legal y normativo que afectan a la Seguridad Informática: la lucha contra los Delitos Informáticos, la protección de los Datos Personales o el Control de Contenidos, entre otros”.

(Avenía Delgado, 2017), “El autor Carlos Arturo Avenía Delgado, en su libro Fundamentos de seguridad informática, la Seguridad de TI es minimizar los riesgos asociados con el acceso y el uso de cierta información del sistema de forma no autorizada y, en general maliciosamente.

Este punto de vista de la seguridad implica la necesidad de una gestión, sobre todo la gestión de riesgos. Para ello, debe evaluar y cuantificar los activos a proteger (información), y en base a estos análisis, aplicar medidas preventivas y correctivas para eliminar los riesgos asociados o para reducirlos a niveles que pueda transmitir o tomar el riesgo.”

Capítulo III. Metodología

3.1 Ámbito

Esta investigación se realizó en la Municipalidad Distrital de Huácar.

3.2 Población

En la presente investigación la población incluye todo los activos y personal de la municipalidad distrital de Huácar.

Tabla 3: ***Universo población de estudio***

Gerencia general de la municipalidad	2
Sub gerencia de contabilidad, patrimonio y RHH.	3
Sub gerencia de logística, servicios generales y almacén	2
Sub gerencia de tesorería y recaudación tributaria	2
Oficina de secretaria general, registro civil y archivo	4
Oficina de asesoría jurídica	1
Gerencia de planificación y presupuesto	5
Gerencia de infraestructura y desarrollo urbano rural	5
Gerencia de desarrollo social y comunal	21
Oficina de alcaldía	2
Total	47

Nota. Fuente: Elaboración propia

3.3 Muestra

En esta investigación, serian un total de 47 ya que la cantidad de activos son la misa que el número de población y como son igual de importante no se puede dejar a ninguna de lado.

3.4 Tipo de estudio

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

- **Según el tipo de investigación:**

Garay, Hilario, Flores, (2021), “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 de un SGSI de acuerdo a la norma técnica peruana ISO-27001:2014, que aborda la gestión de riesgos de los activos informáticos, mejora la seguridad de la información y proporciona herramientas de gestión de riesgos en la información, se propone aplicar los conocimientos para resolver el problema cuya solución beneficiará a la municipalidad distrital de Huácar.

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, 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 Huácar.

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 4: ***Técnicas de recolección de datos***

Revisión de documentos: Los documentos de la Municipalidad de Huácar que fueron revisados son el inventario de activos, y documentos referentes a la organización proporcionados por el subgerente de contabilidad y patrimonio.	• Documentos administrativos.
Observación: La observación se realizó para valorar los activos de información a criterio de los tesistas.	• Fichas de observación. • Fotografías.
Encuesta: Se realizó este instrumento para recolectar	• Formularios

información inicial sobre el estado actual de la entidad.	
Entrevista: El conversatorio con fines de investigación que se tendrá con los encargados de la municipalidad.	• Apuntes

Nota. Elaboración propia

3.7 Validación y confidencialidad del instrumento

La validez y la confidencialidad del instrumento se realizó por tres expertos en el tema, lo que permitió valorar las diferentes opiniones y validar si el contenido de los formularios 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 confidencialidad se realizó el análisis con el alfa de Cronbach, dando como resultado 0.930 a lo que se interpretó que el valor indica que el instrumento tiene un excelente nivel de confidencialidad.

Los expertos emitieron su juicio en un instructivo diseñado para tal fin (ver **ANEXO K**). Las observaciones recibidas contribuyen a la edición definitiva del cuestionario (ver **ANEXO B**) y a la operacionalización de las variables.

3.8 Procedimiento

Una vez terminada la recopilación de datos de los activos de información, se llevaron al Excel y se organizaron por modelos según la metodología MAGERIT V3, esto nos ayudó a hacer el análisis de los activos y para conocer la situación de la Municipalidad Distrital de Huácar en cuanto a su seguridad informática se realizó una encuesta de conocimientos previos.

Con los resultados obtenidos del MAGERIT V3 se podrá hacer del diseño de la declaración de aplicabilidad de los controles y políticas de acuerdo a la norma técnica peruana ISO/IEC 27001:2014.

3.9 Tabulación y análisis de datos

Se trasladaron los datos obtenidos por el formulario “Encuesta sobre el conocimiento de un Sistema de Gestión de Seguridad de la Información (SGSI)” a una tabla de doble entrada

conformada por filas y columnas, donde se calcularon el porcentaje de conocimiento al SGSI y con los resultados diagnosticar la situación actual de la Municipalidad Distrital de Huácar.

3.10 Consideraciones éticas

En la encuesta de conocimientos previos para diagnosticar la situación actual en la Municipalidad de Huácar (MDH) estas fueron las consideraciones éticas:

- Se protegió la privacidad de los participantes.
- Los participantes fueron informados acerca de la investigación.
- La investigación busca mejorar el conocimiento.
- Los participantes fueron el personal contratado de la MDH.
- Las preguntas fueron concisas y de tipo dicotómicas.

Capítulo IV. Resultado

4.1. Diagnóstico de la situación actual de municipalidad distrital de Huácar.

En esta fase se presentan diagnósticos que se desarrolló con la finalidad de conocer la situación inicial de la municipalidad distrital de Huácar considerando la implementación de un SGSI basado en la NTP-ISO/IEC 27001:2014.

4.1.1. Evaluación inicial de la municipalidad distrital de Huácar en relación con los requisitos de la Norma técnica peruana ISO/IEC 27001:2014

Para evaluar el cumplimiento inicial de los criterios de la NTP-ISO/IEC 27001:2014 por parte de la municipalidad, se idearon dos métodos de presentación de resultados: uno descriptivo y otro cuantificable. Este método se basa en la clasificación del estado de los requisitos mediante una escala Liker con cinco posibilidades, ordenadas de menor a mayor.

Tabla 5: ***Evaluación por criterio del estado actual de la MDH en referencia a los requisitos de la NTP- ISO/IEC 27001:2014.***

CRITERIO PARA CALIFICAR	***VALORACIÓN***
NO DISEÑADO: Las acciones/procedimientos muestran que el requisito no existe o no se especifica su aplicación.	**0%**
PARCIALMENTE DISEÑADO: Las acciones/procedimientos muestran que la norma está definida pero no es totalmente conforme a la NTP-ISO/IEC 27001:2014.	**25%**
DISEÑADO: Los procedimientos están en línea con el estándar de la NTP- ISO/IEC 27001:2014 de NTP, pero no hay pruebas de que se hayan utilizado.	**50%**

PARCIALMENTE IMPLEMENTADO: Hay algunos indicios de que las actividades y los procesos se adhieren a los requisitos de la norma ISO/IEC 27001 de NTP, pero no existe poca evidencia.	**75%**
COMPLETAMENTE IMPLEMENTADO: Las acciones/procedimientos se adhieren a los requisitos de la NTP- ISO/IEC 27001:2014, y su aplicación está permanentemente documentada.	**100%**

Nota. *Adaptado de* (BAZAN, 2019)

Iniciamos elaborando el SGSI con los requisitos y controles de la NTP-ISO/IEC 27001:2014; realizamos la evaluación de la manera siguiente:

- Cada requisito fue evaluado.
- Se organizó la evidencia/sugerencia respecto al cumplimiento de la NTP-ISO/IEC 27001:2014 en base al puntaje obtenido.

A través de la tabla 6 se pueden ver los resultados de la evaluación del cumplimiento inicial de la municipalidad distrital de Huácar con respecto a los requisitos de la NTP-ISO/IEC 27001:2014.

(En el ANEXO H se detalla la tabla completa).

Tabla 6: ***Estado inicial de la municipalidad distrital de Huácar respecto a la NTP-ISO/IEC 27001:2014***

SECCIÓN	REQUISITOS DE LA NTP-ISO/IEC 27001:2014.	ESTADO	EVIDENCIA Y/O SUGERENCIA (¿DE QUE MANERA SE CUMPLE? / ¿QUE MEJORAR PARA EL CUMPIMIENTO ?)	VALORACION
4	ORGANIZACIÓN Y SU CONTEXTO	No diseñado	La sugerencia es realizar el análisis del contexto de la MDH para entender aspectos internos como externos, los interesados relevantes al SGSI para después elaborar y	6%

			documentar cual será el alcance del SGSI".	
4.1	Entender el contexto de la organización y esta misma. La municipalidad debe decidir los factores internos y externos que son importantes para alcanzar este objetivo y que afectan a su capacidad para lograr los resultados deseados de este SGSI.	Parcialmente diseñado	El MDH dispone de documentos fácilmente accesibles que describen su misión, visión, matriz FODA y estrategias. Sin embargo, no considera explícitamente las cuestiones de seguridad de la información. Se sugiere crear políticas de seguridad de la información que estén en línea con los objetivos estratégicos de la organización.	25%
4.2	Comprender las necesidades y expectativas de las partes interesadas. La organización debe determinar las partes interesadas y los requisitos de las mismas.	No diseñado	Se sugiere identificar a las partes interesadas y comprender sus requisitos y expectativas en lo que respecta a seguridad de la información.	0%
4.3	Determinar el alcance del SGSI.	No diseñado	Sugerencia: Tener determinado cual será el alcance del SGSI teniendo en cuenta los factores mencionados, probar con documentos y que este a disposición de las partes interesadas.	0%
4.4	Sistema de Gestión de Seguridad de la información. La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta	No diseñado	Sugerencia: Desarrollar un plan de mejora continua del SGSI de acuerdo con la NTP – ISO/IEC 27001:2014 vigente.	0%

	NTP-ISO 27001:2014.			
5	LIDERAZGO	No diseñado	El líder de la entidad debe actuar con iniciativa y dedicación hacia el SGSI. Además, debe procurar que los puestos relacionados con la seguridad de la información tengan poder y responsabilidades. En consecuencia, es esencial definir las normas de seguridad de la información y sus objetivos de acuerdo con la misión de la organización.	0%
5.1	Liderazgo y compromiso. “La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI”.	No diseñado	“El titular de la entidad debe mostrar liderazgo y compromiso”.	0%
5.2	Política	No diseñado	Crear políticas de seguridad de información, que esté en consonancia con los objetivos de la municipalidad, incluya los objetivos de seguridad de la información, sea accesible y se comparta con toda la organización.	0%
5.3	Roles, responsabilidades y autoridades organizacionales.	No diseñado	De acuerdo con la alta dirección, se debe asignar y transferir la responsabilidad y la autoridad de las tareas relacionadas con la seguridad de la información.	0%
PUNTUACIÓN TOTAL DE LA EVALUACIÓN DE REQUISITOS DE LA NTP-ISO/IEC 27001:2014.				2%

Nota. Adaptado de (Sandoval Alania, 2020)

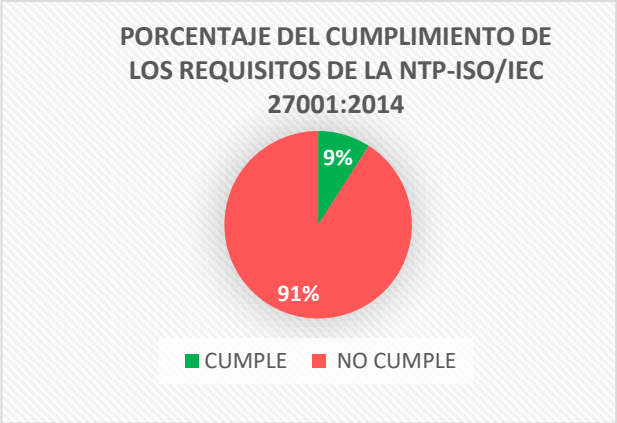

Gráfico Nº 4: Porcentaje de cumplimiento de los requisitos de la NTP- ISO/IEC 27001:2014.

Nota. *Elaboración propia*

Por medio de este análisis se determinó que la municipalidad distrital de Huácar comprende los beneficios de un SGSI y su importancia y tiene una iniciativa del control, planificación y evaluación de riesgos; sin embargo, aún no existe un proceso o análisis sistemático de los riesgos informáticos y de cómo abordarlos, y no hay documentación requerida por la NTP-ISO/IEC 27001:2014.

- **Resultados de la evaluación inicial de la municipalidad distrital de Huácar en relación con los requisitos de la NTP ISO/IEC 27001:2014**

La evaluación reveló que la municipalidad distrital de Huácar recibió un puntaje total de 2%, lo que significa que no cuenta con un SGSI y se encuentra en la etapa inicial (no diseñado), de un total de 100% de los requisitos de la NTP-ISO/IEC 27001:2014 que debe cumplir.

El resultado anterior también demuestra que la municipalidad no gestiona la seguridad de la información, y que el diseño e implementación del SGSI requerirá más trabajo y dependerá de la dedicación y disponibilidad del personal de la municipalidad distrital de Huácar.

- **Diagnóstico inicial de la seguridad de la información y probabilidad de aceptación del SGSI.**

Para la recoger datos se utilizó una encuesta que se muestra en el **ANEXO C** de esta investigación. Con el fin de evaluar las actitudes, perspectivas y la situación fundamental de la seguridad de la información dentro de la municipalidad distrital de Huácar, se realizó una encuesta que comprende de 20 preguntas básicas. Esto con el fin de verificar la situación actual de la municipalidad con respecto a la seguridad de la información y la probabilidad de que el diseño del SGSI sea aceptado.

4.2. Contexto de la organización.

4.2.1. Comprender el contexto de la organización.

La necesidad de comprender el contexto de la organización se menciona en el requisito 4 de la NTP-ISO/IEC 27001:2014: “Contexto de la organización”. Esto se refiere a los factores internos y externos que son importantes para el desarrollo del SGSI, así como la determinación del alcance del SGSI y entender de las demandas y expectativas de las partes interesadas.

- **Contexto externo:** En este punto se examinaron los factores externos significativos que inciden en la implementación del SGSI de la Municipalidad Distrital de Huácar. La municipalidad debe hacer frente a los nuevos retos tecnológicos, lo que significa que debe reorganizar sus procesos e incluir el uso nuevas tecnologías para poder cumplir con sus funciones. Por un lado, tenemos influencias como del estado, el gobierno regional, los municipios, los sindicatos, la sociedad, etc. De otro lado, tenemos la actualidad del país y su situación como resultado de la pandemia por la COVID-19.

Para esto utilizamos la técnica de análisis PEST – (Factores políticos, Legales, económicos, socioculturales y tecnológicos

.

Tabla 7: ***Análisis PEST***

Político legal	▪ Interés en seguridad de la información por parte del estado y de todas las organizaciones" (la PCM a través de ONGEI, auditorías realizadas por la contraloría). ▪ Asistencia de ONGEI para establecer el SGSI. ▪ A través de las gerencias regionales de control, los organismos de control institucional (OCI) y las empresas de auditoría (SOA), la Contraloría de la República observa y confirma la correcta aplicación de las políticas públicas y el uso de los recursos del Estado.
Económico	▪ Elevado costo en contratar consultores para establecer el SGSI ▪ Presupuesto escaso.
Socio – cultural	▪ Sociedad con más conocimiento en tecnología. ▪ Sociedad con mayor interés y preocupación en el tema de seguridad de la información
Tecnológico	▪ Descubrimiento e innovación de tecnologías de la información. ▪ Vulnerabilidades y amenazas en la seguridad de la información. ▪ Necesidades de implementar nuevas tecnologías

Para asegurarse de que se tienen en cuenta los objetivos y las inquietudes de las partes externas al crear los criterios de riesgo, es crucial comprender el contexto externo.

- **Contexto interno:** Los factores internos incluyen la resistencia al cambio, el mal mantenimiento de los recursos tecnológicos, la utilización inadecuada de los recursos tecnológicos y el uso inadecuado de los permisos de trabajo por parte del personal, entre otras.

La cultura, los procedimientos, la estructura y la estrategia de la organización deben estar alineados con el SGSI.

- **Naturaleza de la entidad:** Huácar, durante el Gobierno de don Ramón Castilla fue creado como distrito por Ley del 9 de febrero de 1,861, en donde pertenecía Ambo. Y, en el Gobierno de don Guillermo Billinghurts, es delimitado su territorio, para nacer la Provincia de Ambo por Ley N.º 1598 de 21 de octubre de 1,912.

  Para el mejor cumplimiento de sus objetivos, la Municipalidad Distrital de Huácar elabora, autoriza, ejecuta, evalúa, supervisa y regula los planes de desarrollo local en cumplimiento de los planes de desarrollo nacional y regional.

- **Misión:** Brindar un servicio inteligente, humano y democrático, con calidad oportuna y transparente en beneficio del ciudadano, promoviendo a la vez el desarrollo integral y sostenible del distrito, a través de una gestión tecnológica y/o eficiente, transparente y participativa.

- **Visión:** Todos aquí trabajan en busca de una mejor condición de vida de los habitantes, promover la historia y nuestra cultura para lograr un turismo sostenido, e invirtiendo en Educación, Salud y Medio Ambiente, con infraestructura para alcanzar ser un pueblo con desarrollo productivo y moderno.

- **Valores Institucionales.**

  Responsabilidad: En Huácar las funciones y normas se cumplen, predispuestos a asumir retos y también sus consecuencias de las decisiones que puedan existir.

  Honestidad: Nuestra labor diaria debe ser con esmero y honestidad, teniendo una conducta recta y de confianza, dentro la ética y la moral.

  Compromiso: Todos están comprometidos en dar un buen servicio, así como superándose constantemente.

  Respeto: En Huácar prima el respeto y buen trato, entre todos los trabajadores, vecinos y proveedores; en la misma forma con el medio ambiente y su entorno social.

  Transparencia: Todos los actos de la gestión deben proceder con veracidad, informándose de manera abierta y oportuna.

- **Aspectos técnicos:** La Municipalidad Distrital de Huácar dispone de una red de área local (LAN), formado por un total de 16 oficina, 2 salas de reuniones, 1 servidor y correo corporativo Gmail para sus usuarios, no cuenta con un área de informática.

  El hardware informático, el servidor y el acceso a la red, junto con todos los datos necesarios para el funcionamiento de los sistemas, están centralizados, y se crean copias de seguridad que se guardan en USB y PC. Hay una línea de fibra óptica para la salida de los sistemas de información. Es importante señalar que todos los activos de la Municipalidad Distrital de Huácar son vulnerables a las amenazas que pueden comprometer su integridad, disponibilidad y confidencialidad. El cableado de la red está desorganizado y expuesto al suelo en algunos lugares.

  La Municipalidad Distrital de Huácar carece de un área de cómputo, pero cuenta con una red de área local (LAN) con 16 oficinas, 2 salas de reuniones, 1 servidor y correo corporativo Gmail para sus usuarios.

  Además de dar acceso a la red de la entidad y centralizar toda la información necesaria para el funcionamiento del sistema, también se crean copias de seguridad que se guardan en Pc y unidades USB. Existe una línea de fibra óptica para la salida de los sistemas de información. Es importante señalar que todos los activos de la Municipalidad Distrital de Huácar son vulnerables a las amenazas que pueden comprometer su integridad, disponibilidad y confidencialidad. El cableado de la red está desorganizado y expuesto al suelo en algunos lugares.

- **Sistemas que manejan la municipalidad distrital de Huácar.**

  DATAS: Según gob.pe, (2020), “El sistema nacional de información se encarga de recopilar, analizar y difundir información específica sobre los servicios de saneamiento en los núcleos de población rurales.”

SIAF: Según gianeca.blogspo, (2022), “Se trata de una tecnología para agilizar la gestión administrativa de las Administraciones Locales, sistematizar sus requisitos de información y reducir el tiempo de conciliación.”

SIGA: (Sistema Integrado de Gestión Administrativa) es una herramienta tecnológica que automatiza y simplifica los procesos administrativos dentro de una institución estatal, respetando las normas establecidas por los organismos que supervisan los sistemas administrativos estatales.

RUB PVL: registro único de beneficiarios del programa del vaso de leche (RUBPVL), que contiene la información nominal de los usuarios del Programa.

SISFOH: Es una herramienta esencial para satisfacer las necesidades de información social. A este objetivo sirve su Registro General de Hogares, un sistema de información sobre las características socioeconómicas de los hogares (PGH).

SRG: Sistema de Registro Civil.

GESMUN: Sistema de abastecimiento y almacén

4.2.2. Comprender las necesidades y expectativas de las partes interesadas.

- **Partes interesadas externas.**

- **Contraloría de la república:** Es la autoridad más alta del Sistema Nacional de Control. Supervisa, confirma y valida la correcta aplicación de las políticas públicas, así como la utilización efectiva de los bienes y recursos del Estado. Para el adecuado cumplimiento de sus funciones, cuenta con autonomía administrativa, funcional, económica y financiera.

- **Gobierno (ONGEI-PCM):** Los proyectos, normas y diversas actividades del Estado en materia de gobierno electrónico son supervisados por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), que actúa como órgano rector del sistema informático nacional y es un organismo técnico especializado directamente dependiente de la Presidencia del consejo de ministros (PCM). Algunas de sus actividades en curso son la creación de

proyectos ilustrativos en el ámbito de las tecnologías de la información y la comunicación (TIC), el asesoramiento técnico e informático a las entidades públicas, la formación y la difusión de información en materia de gobierno electrónico, y la modernización y descentralización del Estado.

- **Usuarios:** Comprende a la comunidad Huacarina, personas naturales, los trabajadores de la municipalidad, estudiantes, etc.

- **Partes interesadas internas.**

- **Alta dirección – gerencia general y alcaldía:** Debe mostrar liderazgo y dedicación en relación con el SGSI, asegurándose de que los objetivos fijados son coherentes para la planificación estratégica de la municipalidad, y aplicando políticas.

- **Responsable administrativo:** Encargado del sistema de información antes, durante y después de la contratación de empleados.

- **Responsable de informática:** Es el encargado de mantener la seguridad tecnológica e informativa de la organización.

- **Trabajadores de la organización:** Plenamente cumpliendo de las normas y reglamentos de seguridad de la municipalidad, responsable de garantizar la seguridad de los activos de información de la organización.

Tabla 8: ***Requisitos de las partes interesadas***

PARTES INTERESADAS	*REQUISITOS*
Alta dirección	• Dirigir las acciones y proyectos del encargado de informática relacionados con la seguridad de la información. • Encargado de dar el ejemplo en lo que concierna sobre liderazgo y compromiso.
Responsable de informática	• Anunciar las no aprobaciones en lo que concierne a seguridad de la información.

	• Los empleados deben recibir formación en materia de seguridad de la información por parte de este.
Responsable administrativo	• Monitorear que se cumpla con la seguridad de la información antes, durante y después de la contratación de los empleados.
Trabajadores de la municipalidad distrital de Huánuco.	• Tener conocimiento en las normas y políticas en temas de seguridad de la información. • Protección de su información personal. • Cuidar y proteger cada activo de información de la municipalidad distrital de Huácar. • Participar en capacitaciones en temas de seguridad de la información.

4.3. Alcance y límite del SGSI

Este documento, que es relevante para todos los trámites relacionados con el SGSI, tiene por objeto definir el alcance y los límites de la planificación del SGSI en la municipalidad distrital de Huácar.

4.3.1. Propósito y alcance de los usuarios.

Los miembros del comité de seguridad de la información y los empleados autorizados de la municipalidad distrital de Huácar son los únicos usuarios que tienen acceso a este documento.

4.3.2. Alcance del SGSI

Sólo los procedimientos de gestión de los activos de la información y de gestión de los riesgos para la seguridad de la información, que forman parte de la gestión integrada de la seguridad de la información y están relacionados con la planificación del SGSI, están incluidos en el ámbito del SGSI.

4.3.3. Documentos de referencia.

- NTP-ISO/IEC 27001:2014, requisito 4.3.

- Documentación legal: Con fecha 8 de enero de 2016, RM N.º 004-2016-PCM aprobó la adopción de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014" como requisito obligatorio.

4.3.4. Sistema de gestión de la seguridad de la información

- **Definición del alcance del SGSI**

Para salvaguardar sus recursos informáticos que dan soporte a la institución, la municipalidad distrital de Huácar se definió los límites de la planificación del SGSI. La municipalidad distrital de Huácar está representada en esta fase de planificación del SGSI en toda su extensión (Se incluyen el personal que labora, sus activos y la infraestructura de la municipalidad).

- **Análisis diferencial.**

La norma NTP-ISO/IEC 27001:2014 estipula que el Sistema de Gestión de la Seguridad de la Información (SGSI) de una organización debe establecerse, ponerse en marcha, mantenerse y mejorarse con el tiempo.

Para determinar si la municipalidad distrital de Huácar cumple actualmente con la norma NTPISO/IEC 27001:2014, se realizó un análisis diferencial de los requisitos 4 al 10 (Requisitos de la norma NTP-ISO/IEC 27001:2014) y el anexo A (controles de seguridad). Se creó un plan de mejora de acuerdo con los objetivos de seguridad deseados, evaluando las condiciones actuales para identificar las deficiencias y el grado de cumplimiento de la norma.

- **Requisitos de la Norma NTP-ISO/IEC 27001:2014.**

Ninguna de las especificaciones enumeradas en los puntos 4 a 10 debe ser ignorada para que una organización cumpla con NTPISO/IEC 27001:2014.

En el **ANEXO H**, se pueden ver los resultados del nivel de conformidad y cumplimiento de estos requisitos.

Este Análisis Diferencial ha demostrado que la municipalidad distrital de Huácar cuenta con el liderazgo necesario para poner en marcha un SGSI. Sin embargo, aún no se ha elaborado el documento requerido por la NTP-ISO/IEC 27001:2014 ni una metodología sistemática para

el análisis, evaluación y tratamiento de los riesgos. Sin embargo, se reconoce que el SGSI debe estar a la altura de los avances tecnológicos dentro de la municipalidad.

4.4. Liderazgo, roles Y responsabilidades.

4.4.1. Liderazgo y compromiso

Para adoptar con éxito un SGSI, la dirección debe estar a bordo y proporcionar liderazgo; en este ejemplo, sería el alcalde de la municipalidad. Dado que el cambio de cultura necesario para adoptar un SGSI sería difícil de lograr sin el apoyo continuo de la alta dirección, este apartado se incluye en la norma. El alcalde tiene que demostrar su dedicación, entre otras cosas, proporcionando los recursos necesarios (humanos y financieros) y establecer políticas y objetivos de seguridad de la información en línea con los objetivos estratégicos, comunicando la importancia de gestionar eficazmente la seguridad de la información y apoyando la mejora continua, entre otras cosas.

Con el fin de garantizar que el SGSI cumpla con la NTP ISO 27001:2014 y para proporcionar a la alta dirección informes de rendimiento, este requisito también exige la formación de funciones, deberes y autoridad de la organización.

- **Objetivos de la seguridad de la información**

Los objetivos del sistema de gestión de seguridad de la información son los siguientes:

- Proteger la confidencialidad de la información que se encuentra almacenada en sus sistemas.
- La información sensible de la municipalidad debe estar asegurada en el aspecto de confidencialidad, disponibilidad e integridad.
- Maximizar la calidad y disponibilidad de los servicios ofrecidos a la población del distrito de Huácar.
- Garantizar que nuestras actividades y procedimientos presentes y futuros se ajusten a las leyes y reglamentos pertinentes en materia de seguridad de la información.

- Reducir la exposición de la municipalidad distrital de Huácar a niveles aceptables de riesgo de seguridad de la información.
- Emitir y extender la Política de Seguridad a través de cada responsable de área.
- Llevar a cabo una mejora continua mientras se evalúa el rendimiento del SGSI.

- **Requisitos legales**

El principal requisito que se deben cumplir para implementar y certificar un SGSI es el cumplimiento de la legislación peruana vigente. La entidad está protegida de los peligros externos e internos gracias a su cumplimiento, que además permite respetar los derechos del personal administrativo, proveedores y residentes de la región de Huácar, al tiempo que se evitan las infracciones involuntarias y los costos asociados. La municipalidad distrital de Huácar está sujeta a las leyes y normas que se enumeran a continuación en lo que concierne sobre seguridad de la información.

- Norma de Control Interno de las Entidades del Estado
- Ley de Protección de Datos Personales
- Ley 30096.- Ley de Delitos Informáticos
- Ley N° 30171.- Ley que modifica la Ley 30096, ley de Delitos
- Informáticos

- **Comité de seguridad de la información.**

La alta dirección se asegurará de que se asignen y comuniquen las responsabilidades y la autoridad de los puestos relevantes para la seguridad de la información, de acuerdo con el requisito 5.3 Funciones, responsabilidades y autoridades de la organización de NTP ISO/IEC 27001:2014.

De acuerdo con el requisito 5.3 de la NTP ISO/IEC 27001:2014, el artículo 5 de la RM Nº 004-2016-PCM también ordena la formación del comité de gestión de la seguridad de la información. Los miembros de este comité de gestión de la seguridad de la información serán:

- Alta dirección - alcalde.
- Gerente general.
- Responsable de asesoría jurídica.
- Responsable de informática.

4.4.2. Roles, responsabilidades y autoridades organizacionales.

Las funciones y responsabilidades sugeridas se describen en los párrafos siguientes. La alta dirección evaluará estas funciones y deberes junto con la necesidad de cualquier autoridad adicional en colaboración con el comité de seguridad de la información.

Es importante señalar que este criterio será mejorado continuamente de acuerdo a los requerimientos de la municipalidad distrital de Huácar.

- **Alta dirección – alcalde:** Establezca las funciones y responsabilidades vinculadas a la seguridad de la información en los niveles de gerencia y sub gerencia, apruebe la política de seguridad de la información y transmítala a todos los empleados municipales. También debe hacer cumplir las normas de seguridad de la información dentro del municipio.

- **Gerente General:** La política de seguridad de la información de un municipio debe proponerse al alcalde, revisarse a intervalos regulares o siempre que se produzcan cambios significativos en la legislación sobre seguridad, y debe mantenerse en observación el éxito del municipio en materia de seguridad de la información.

- **Responsable de asesoría jurídica:** Mantener un registro actualizado de las leyes y reglamentos vigentes en materia de seguridad de la información, y evaluar el cumplimiento de dichas leyes y reglamentos por parte de la entidad.

- **Responsable de informática:** El gerente y el alcalde deben ser informados sobre los componentes del SGSI, la disponibilidad y funcionalidad de los equipos informáticos del municipio, la creación de los mecanismos necesarios de gestión y administración de riesgos, la capacitación del personal en estos temas, y la existencia de metodologías para el tratamiento de riesgos y oportunidades, políticas de SI, así como los documentos requeridos por la NTP ISO/IEC 27001:2014.

4.5. Planificación

4.5.1. Propósito, alcance y usuarios

De acuerdo con la NTP ISO/IEC 2001:2014, el objetivo de este documento es definir la metodología de análisis y evaluación de riesgos, evaluar el informe de evaluación de riesgos elaborado por la municipalidad distrital de Huácar, e identificar los riesgos que suponen una mayor amenaza para esta misma.

"El análisis de riesgos abarca todo el sistema de gestión de la seguridad de la información, incluidos todos los activos inventariados que puedan tener un impacto en la seguridad de la información. Todo el personal administrativo que participan en el proceso de análisis y evaluación de riesgos son los usuarios previstos de este documento" (BAZAN, 2019).

- **Metodología de análisis y evaluación de riesgos y reporte de evaluación de riesgos**

  - **Metodología magerit**

    El CSAE (Consejo Superior de Administración Electrónica) ha desarrollado MAGERIT, una metodología de análisis y gestión de riesgos de los sistemas de información, que asume los beneficios evidentes del empleo de las tecnologías de la información, al tiempo que gestiona los riesgos asociados a las mismas. Actualmente se encuentra en la versión 3. De acuerdo con las Dimensiones de

Seguridad sugeridas, el objetivo principal de MAGERIT es asegurar los activos de TI para ayudar al cumplimiento de la misión de una organización.

Tabla 9: ***Dimensiones de la seguridad para la identificación y valoración de amenazas en MAGERIT***

NOMENCLATURA	DEFINICION	DIMENSIONES DE SEGURIDAD
[D]	Los recursos están disponibles siempre que se necesiten.	Disponibilidad
[I]	La información no puede modificarse durante el proceso de envío.	Integridad
[C]	Asegurar el secreto de las comunicaciones.	Confidencialidad
[A]	Enviado por la persona que se hace pasar por emisor.	Autenticidad
[N_R]	No puede discutir la autoría del mensaje enviado	No Repudio

Nota. *Adaptado de* (Sandoval Alania, 2020)

El Análisis de Riesgos y el Tratamiento de Riesgos son las dos (2) principales responsabilidades que MAGERIT considera para el proceso de Gestión de Riesgos.

Calculando las implicaciones de los riesgos (análisis cuantitativo) o juzgando su importancia relativa, el análisis de riesgos busca categorizar los riesgos presentes (análisis cualitativo). Para estimar el impacto y el riesgo al que está expuesto cada activo, así como su impacto en el nivel de seguridad de la información en una organización, este proceso de análisis implica la identificación de los activos, sus riesgos y los controles de seguridad sugeridos. Las acciones emprendidas para modificar la circunstancia o la cantidad de riesgo están comprendidas en el tratamiento del riesgo.

Dado que MAGERIT es una metodología sistemática, la gestión de riesgos implica los siguientes pasos:

1. Inventario de Activos: Los activos del sistema de información son aquellas partes o características que son vulnerables a un ataque intencionado o a un ataque con repercusiones para una organización. Además, son los componentes que necesita una organización para procesar la información. Los activos se dividen en las siguientes categorías por MAGERIT:

Tabla 10: ***Clasificación de los tipos de activos informáticos en MAGERIT***

TIPO DE ACTIVO	NOMENCLATURA	DEFINICION
Activos esenciales	[Essential]	Son aquellos que son cruciales para la supervivencia de la organización, y su pérdida o daño tendría un impacto negativo en su capacidad de continuar. Suelen llevar a cabo misiones importantes.
Servicios	[S]	Son aquellos que satisfacen las necesidades de los usuarios. Son activos que cubren las necesidades de los usuarios.
Software/aplicaciones informáticas	[SW]	Son los que se encargan del procesamiento de datos y de la entrega de información para la prestación de servicios.
Hardware/equipamiento informático	[HW]	Son los soportes reales donde se almacenan los datos y ofrecen servicios directa o indirectamente.
Redes de comunicación	[COM]	Sirven como medio de transporte de los datos.
Soporte de información	[Media]	Son dispositivos físicos que permiten el almacenamiento temporal

		o a largo plazo de los datos.
Equipamiento auxiliar	[Aux]	Son los equipos que dan soporte a los sistemas de información sin tener ninguna conexión con los datos.
Instalaciones	[L]	Los sistemas de información y comunicación se alojan en estos lugares.
Personal	[P]	Son las personas que manejan los sistemas de información.

Nota. Adaptado de (ESCALANTE CORONEL, 2019).

1. **Valoración de los Activos:** Los activos que aportan valor son los que hay que salvaguardar, y cada activo tiene un nivel de importancia diferente dentro de la municipalidad. MAGERIT define dos tipos de valoraciones: cualitativa y cuantitativa. La primera determina el valor de un activo en función de la influencia potencial que tendrá en la empresa (incluyendo el coste de compra, reparación, configuración, mantenimiento, etc.). A diferencia de la cuantitativa, permite determinar órdenes de magnitud (MA [Muy Alto], A [Alto], M [Medio], B [Bajo] y MB [Muy Bajo]) y no genera valores numéricos, la Cuantitativa sí permite calcular el costo y/o valor monetario.

Tabla 11: ***Criterio para la valoración de activos.***

CRITERIO	VALOR	
Daño muy grave a la municipalidad.	*Muy alto*	*10*
Daño grave a la municipalidad.	*Alto*	*7-9*
Daño importante a la municipalidad.	*Medio*	*4-6*
Daño menor a la municipalidad.	*Bajo*	*1-3*
Despreciable	*Despreciable*	*0*

Nota. Adaptado de (Dirección General de Modernización Administrativa, 2012)

Cuestionario para determinar la criticidad del activo de información.

Tabla 1: ***Preguntas para determinar la criticidad de un activo.***

DIMENSIONES	ASPECTO	PREGUNTA
Disponibilidad [D]	Económico.	
	Legal.	
	Imagen.	
Integridad [I]	Económico.	
	Legal.	
	Imagen.	
Confidencialidad [C]	Económico.	
	Legal.	
	Imagen.	
Autenticidad [A]	Económico.	
	Legal.	
	Imagen.	
No Repudio [N_R]	Económico.	
	Legal.	
	Imagen.	

Nota. Adaptado de (Escalante Coronel, 2019, pág. 43)

En el **ANEXO D**: Ficha de observación para la valoración de activos se encuentran detalladas dichas preguntas

A continuación, se aplicaron los criterios de la tabla 12 para calcular el nivel de criticidad del activo valorado. En este enfoque, el proceso de gestión de la infraestructura tecnológica se utilizó para determinar la importancia de los activos de información.

Tabla 2: ***Niveles de criticidad de los activos de información***

CRITERIO DE VALORACION	VALOR	NIVEL
El activo de información pone en peligro el alto nivel de integridad, confidencialidad y/o disponibilidad de la información.	$7 < VF \leq 10$	Alto
El activo de información compromete la disponibilidad, confidencialidad y/o integridad de la información en un grado medio.	$4 < VF \leq 7$	Medio
Los niveles integridad, confidencialidad y/o disponibilidad de la información están comprometidos en un nivel bajo por el activo de información.	$0 < VF \leq 4$	bajo

Nota. Elaboración propia

El resultado de la evaluación de los activos y su nivel de criticidad se muestran en el **ANEXO I**. Esta evaluación refleja el valor medio de los cinco factores: disponibilidad, integridad, confidencialidad, autenticidad y no repudio que contribuyen a la seguridad del activo.

Los activos de información con un nivel de criticidad alto y medio se eligieron después de valorar los activos de información.

2. **Identificación y Valoración de Amenazas:** Para definir los criterios de valoración de cada dimensión de seguridad, MAGERIT establece cinco (5) Dimensiones de Seguridad (D [Disponibilidad], I [Integridad], C [Confidencialidad], A [Autenticidad] y NR [No Repudio]). Estos valores y/o criterios son comparables a los establecidos en la tabla de valoración cualitativa de los activos informáticos de MAGERIT.

    - **Identificación de Amenazas:** Los eventos que le ocurren a un activo y que tienen el potencial de dañar a una organización se denominan amenazas. MAGERIT emplea una lista de peligros potenciales para los activos de un sistema de información que se clasifican de la siguiente manera:

Tabla 3: ***Catálogo de Amenazas sobre los activos informáticos en MAGERIT***

TIPO DE AMENAZA	NOMENCLATURA	DEFINICION
Desastres naturales	[N]	Sucesos que pueden ocurrir sin intervención humana, ya sea directa o indirectamente.
De origen industrial	[I]	Sucesos accidentales que pueden ocurrir como resultado de la actividad humana industrial. Estos peligros pueden ser involuntarios o intencionados.
Errores y fallos no intencionados	[E]	Errores involuntarios que las personas cometen.
Ataques intencionados	[A]	errores intencionados de las personas.

Nota. Elaboración propia.

La lista de amenazas potenciales para un activo y las dimensiones potenciales del impacto se encuentran en el **ANEXO J.**

El **ANEXO K** contiene información sobre la identificación, valoración y criticidad de los activos.

- **Valoración de Amenazas:** Se debe conocer la probabilidad de ocurrencia para valorar las amenazas. Las probabilidades en MAGERIT son las siguientes:

Tabla 4: Probabilidad de ocurrencia de las amenazas en MAGERIT

PROBABILIDAD DE OCURRENCIA	RANGO
Muy raro	1
Improbable	2
Posible	3
Probable	4

Prácticamente segura	5

Nota. (MarcadorDePosición1)

Los riesgos se han clasificado por activos de información, ya que no todas las amenazas afectan a todos los activos, pero existe una correlación entre el tipo de activo y lo que puede ocurrirle.

Por último, la degradación de los activos fue valorados según los criterios de la tabla 16.

Tabla 5: ***Criterio para valorar la degradación de un activo***

CRITERIO	VALOR	
Muy alto	90%	100%
Alto	70%	80%
Medio	40%	60%
Bajo	20%	30%
Despreciable	0%	10%

Nota. (MarcadorDePosición1)

Para este proyecto, hemos evaluado el deterioro de los activos críticos de nivel alto y medio. Estos activos se deterioran gradualmente con el tiempo.

Los activos elegidos, la probabilidad de que la amenaza se materialice y la degradación en cada una de sus dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y no repudio). se muestran en el **ANEXO L.**

3. Cálculo de impacto. En este caso, el impacto se calculó utilizando el valor del activo y la degradación que la amenaza, en caso de materializarse, causaría. Los criterios y la valoración para este fin se desarrollaron en las tablas 16 y 17.

Tabla 6: ***Criterios para calcular el valor de un activo***

VALOR DEL IMPACTO	IMPACTO

VALOR	CRITERIO	VALOR	CRITERIO
10	Muy alto	9 – 10	Desastroso
7 – 9	Alto	7 – 8	Mayor
4 – 6	Medio	4 – 6	Moderado
1 – 3	Bajo	2 – 3	Menor
0	Despreciable	0 – 1	Insignificante

Fuente: (MarcadorDePosición1).

Tabla 7: ***Matriz de evaluación del impacto***

Degradación de un activo		Despreciable		Bajo		Medio			Alto		Muy alto	
		0%	*10%*	*20%*	*30%*	*40%*	*50%*	*60%*	*70%*	*80%*	*90%*	*100%*
Muy alto	10	0	1	2	3	4	5	6	7	8	9	10
	9	0	1	2	3	4	5	5	6	7	8	9
Muy alto	8	0	1	2	2	3	4	5	6	6	7	8
	7	0	1	1	2	3	4	4	5	6	6	7
	6	0	1	1	2	2	3	4	4	5	5	6
	5	0	1	1	2	2	3	3	4	4	5	5
Medio	4	0	0	1	1	2	2	2	3	3	4	4
	3	0	0	1	1	1	2	2	2	2	3	3
Bajo	2	0	0	0	1	1	1	1	1	2	2	2
	1	0	0	0	0	0	1	1	1	1	1	1
Despreciable	0	0	0	0	0	0	0	0	0	0	0	0
Valor de un activo												

Fuente: (MarcadorDePosición1).

Hay que destacar que para determinar esta valoración no se han tenido en cuenta las posibles medidas de seguridad existentes en la actualidad. El riesgo máximo de cada activo se determina de este modo.

La tabla 19 muestra el impacto en los activos de información como resultado.

Tabla 8: ***Resultado del impacto de los activos***

ACTIVO	PROBABILIDAD	DIMENSIONES				
		[D]	[I]	[C]	[A]	[N_R]
Computadora de escritorio	4	7	7	5	0	0
Laptop	4	7	8	5	0	0
Router	4	7	6	2	0	0
Servidor	4	9	7	6	0	0

Nota. Fuente: Elaboración propia.

El **ANEXO M** contiene la tabla completa de valoración del impacto de los activos.

4. **Cálculo de riego.** En función de la probabilidad de que la amenaza se materialice, así como del impacto que tendría en el activo, se calcula el riesgo.

   Esta comparación permite tener en cuenta la necesidad de tratamiento, así como las decisiones que deben tomarse de acuerdo con las leyes, los reglamentos y otros factores.

   La decisión de no tratar el riesgo de forma diferente a los controles que ya pueden estar en marcha en la organización también puede provenir de la evaluación del riesgo. El siguiente criterio fue diseñado para el presente proyecto para evaluar el nivel de riesgo de los activos.

Tabla 9: ***Criterio para calcular el nivel de riesgo***

CRITERIO	VALOR	
Controlable	0	1
Aceptable	2	5
Tolerable	6	16
Intolerable	17	30
Extremo	31	50

Fuente: (MarcadorDePosición1).

Tabla 10: ***Matriz de evaluación de riesgo***

IMPACTO						
Muy alto	*10*	*10*	*20*	*30*	*40*	*50*
Alto	*9*	*9*	*18*	*27*	*36*	*45*
	8	*8*	*16*	*24*	*32*	*40*
	7	*7*	*14*	*21*	*28*	*35*
Medio	*6*	*6*	*12*	*18*	*24*	*30*
	5	*5*	*10*	*15*	*20*	*25*
	4	*4*	*8*	*12*	*16*	*20*
Bajo	*3*	*3*	*6*	*9*	*12*	*15*
	2	*2*	*4*	*6*	*8*	*10*
	1	*1*	*2*	*3*	*4*	*5*
Despreciable	*0*	*0*	*0*	*0*	*0*	*0*
PROBABILIDAD DE OCURRENCIA		1	2	3	4	5
		Muy raro	Improbable	Posible	Probable	Prácticamente segura

Fuente: (MarcadorDePosición1).

El resultado de los riesgos en los activos se muestra en la tabla 22.

Tabla 11: ***Resultado del riesgo de los activos***

ACTIVO	PROBABILIDAD	DIMENSIONES				
		[D]	[I]	[C]	[A]	[N_R]
Computadora de escritorio	4	28	28	20	0	0
Laptop	4	28	32	20	0	0
Router	4	28	24	8	0	0
Servidor	4	36	28	24	0	0

Fuente: (MarcadorDePosición1).

El **ANEXO N** muestra el cuadro completo de la valoración del riesgo de los activos.

En este momento, la municipalidad distrital de Huácar no ha determinado cuánto riesgo está dispuesta a asumir, ni qué cantidad de riesgo se considera aceptable. Dada esta circunstancia, se sugirió que: Dado que se sabe que la organización en la que se desarrolla el proyecto tiene una calificación de gran empresa, el nivel de riesgo que estarían dispuestos a aceptar serían los riesgos aceptables y los riesgos tolerables, mientras que los riesgos intolerables deberían ser objeto de seguimiento y control continuos.

Por último, nunca deben tolerarse los riesgos extremos, sino que hay que vigilarlos de cerca y controlarlos rápidamente.

Gráfico N° 5: Apetito de riesgo para el tratamiento de riesgos

Nota.: (Escalante Coronel, 2019)

5. **Propietarios del riesgo:** En este punto se identificó al responsable de los riesgos, que es el encargado de aprobar los planes de tratamiento de los riesgos y los riesgos excedentes (para reducir los riesgos a un nivel aceptable). Para este proyecto, se decidió que el comité de seguridad, formado por la alta dirección - alcaldía, incluidos el gerente general, el asesor jurídico y el responsable de informática, es el único grupo responsable de la gestión de riesgos.

6. **Tratamiento de riesgos:** Las opciones para su tratamiento pueden ser minimizarlos, compartirlos o transferirlos, eliminarlos o aceptarlos, según el tipo de riesgo.

Tabla 12: ***Opciones de mitigación en el tratamiento de riesgos***

TRATAMIENTO	DESCRIPCION
Reducir	Esto implica poner en marcha las medidas preventivas o correctivas necesarias para disminuir la probabilidad de que un riesgo pueda ocurrir o tener un efecto adverso.
Transferir	Esta opción se refiere a la obtención de algún tipo de seguro para cubrir las repercusiones financieras de una pérdida o degradación de los datos.
Eliminar	La organización debe hacer todo lo posible para tratar de erradicar el riesgo si es tan grave que puede poner en peligro la propia continuidad de la organización. De este modo, se garantizará que no haya ninguna posibilidad de que la amenaza se materialice.
Aceptar	Conviene considerar la opción de aceptar el riesgo y aminorar sus efectos cuando los costes de tomar las medidas necesarias para erradicarlo superan los efectos previstos de la ocurrencia del incidente.

Nota. Elaboración propia.

A partir de los valores y niveles de riesgo obtenidos se determinó el riesgo máximo asumible es el nivel tolerable. Para todos los riesgos que presentaban niveles intolerables o extremos, se implantaron controles que ayudaran a reducir los riesgos causados por los peligros hasta un nivel aceptable en las dimensiones afectadas.

Se dio prioridad al tratamiento de riesgos de nivel intolerable y extremo, y se tomaron todas las precauciones de seguridad. También es importante señalar que se vigilaron los peligros de nivel aceptable para garantizar que su impacto y probabilidad no aumentaran con el tiempo.

- **Identificación de controles según la norma técnica peruana ISO/IEC 27001**

(Gimenez Albacete, 2014) ”La elección de los controles es una decisión de la empresa basada en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo, la estrategia general de gestión del riesgo de la organización, así como las leyes y reglamentos locales, nacionales e internacionales”.

Sobre la base de las amenazas identificadas, en esta sección se destacaron las medidas que ayudaron a reducir los riesgos a un nivel tolerable. Los controles para disminuir los riesgos de los activos de la municipalidad distrital de Huácar se muestran en la tabla 23.

Tabla 13: ***Plan de tratamiento de riesgos***

Identificación del riesgo		Evaluación del riesgo			Tratamiento de riesgo					
		Nivel de riesgo								
Nombre del activo	Amenaza	Disponibilidad	integridad	Confidencialidad	Estrategia de	Plan de contingencia	Tipo de control	Cláusula de la NTP-	Control de la ISO/IEC	Responsable

Nota. Elaboración propia.

En el **ANEXO O** de este documento se encuentra detallado y de forma completa el plan de tratamiento de riesgos.

- **Declaración de aplicabilidad**

Por último, pero no menos importante, la declaración de aplicabilidad se creó de acuerdo con la NTP-ISO/IEC 27001:2014; contiene todos los controles necesarios que se identificaron, así como la justificación de su inclusión o exclusión.

Tabla 14: ***Declaración de aplicabilidad***

CONTROL DE LA NTP ISO/IEC27001:2014	OBJETIVO CONTROL	ESTADO	JJUSTIFICACION

En el **ANEXO P** de este documento se encuentra detallado y de forma completa la declaración de la aplicabilidad de la tabla 25.

4.6. Propuesta de políticas de seguridad de los activos de información del sistema de gestión de seguridad de la información

La política de seguridad de la información de la municipalidad se estableció en este apartado (en cumplimiento con la NTP - ISO/IEC 27001:2014 requisito 5.2).

Dado que pueden producirse cambios organizativos importantes, como el cese y la contratación de empleados, las modificaciones de la infraestructura tecnológica de la organización, la creación de nuevos servicios, etc., la política de seguridad debe ser autorizada por la alta dirección y evaluada manualmente.

Objetivo: Con el fin de proporcionar un marco de gestión de los objetivos de seguridad de la información a la municipalidad distrital de Huácar, la dirección general y los principios operativos, respaldada por normas nacionales en una política de ciberseguridad.

Finalidad: Establecer normas para la creación y aplicación de prácticas y procesos de gestión para salvaguardar la seguridad de la información y reducir el impacto de posibles

amenazas o sucesos desafortunados en el funcionamiento continuo de la municipalidad distrital de Huácar.

Alcance: Toda la municipalidad distrital de Huácar, incluyendo todos sus activos y todas las operaciones internas y externas relacionadas con la entidad a través de contratos u otros acuerdos con terceros, está cubierta por estas políticas.

Responsabilidad de su cumplimiento: Independientemente de su condición, todos los funcionarios, trabajadores, subdirectores y personal técnico están obligados a respetar estas Políticas como parte de sus funciones.

Tabla 15: ***Propuestas de políticas de seguridad***

SECCION	DOMINIO	CONTROL	PROPUESTA DE TESISTAS
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACION**		
	Objetivo: Proporcionar directrices de gestión de seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones		

Nota. *Elaboración propia.*

En el **ANEXO Q** de este documento se encuentra detallado y de forma completa la declaración de la aplicabilidad de la tabla 26.

La tabla 26 es el planteamiento de las políticas de seguridad de la información propuestas a través del estándar de la norma técnica peruana NTP ISO/IEC 27001:2014. En ella se presenta el formato, así como las sugerencias en las diferentes categorías, que, de acuerdo a los requerimientos de la entidad, se basan en un análisis de riesgos, y que nos permitió estimar los riesgos a los que están expuestos los activos. Estos datos nos permitieron comprender el contexto, realizar un análisis de correlación y determinar si las políticas de seguridad de la información propuestas son adecuadas.

De acuerdo con los requisitos de seguridad de la información, la siguiente tabla tiene la función de estimar los controles de seguridad necesarios. Estos controles se definen a partir de la Sección - Dominio de la normativa, se asigna una Prioridad, que indica si son aplicables en la entidad, y la propia propuesta de política de seguridad está en la última columna.

Capítulo V. Discusión

Para llevar a cabo este proyecto fue importante evaluar las tesis y los proyectos relacionados con el tema de esta investigación. Se examinaron los métodos de los autores y los resultados que buscaban; algunos de ellos se llevaron a cabo desde el punto de vista de las auditorías, otros desde el de los proyectos informáticos y otros desde el de los temas de investigación propiamente dichos. Sin embargo, hay muchas áreas en las que los enfoques del presente proyecto y de los autores revisados son similares porque, al final, se llega al mismo resultado, que es la declaración de la aplicabilidad y la presentación de políticas de seguridad.

Para el proyecto que nos ocupa, comenzamos de acuerdo con las recomendaciones de la NTP-ISO/IEC 27001:2014, que establece que la postura de seguridad de la información de una organización debe ser evaluada inicialmente. Esto establece el grado de aceptación que tendrá el SGSI dentro de la empresa.

Los preparativos para el SGSI comenzaron con un análisis del contexto interno y externo de la organización, seguido de la definición del alcance, los objetivos y el comité de seguridad del SGSI de acuerdo con las directrices de la NTP-ISO/IEC 27001:2014 de NTP y, por último, la propuesta de políticas de seguridad.

Para el presente proyecto, se utilizó la metodología MAGERIT en su versión 3 porque proporciona una visión más estructurada de cómo se realizará el proceso de análisis y gestión de riesgos hasta llegar al tratamiento de los riesgos encontrados.

El siguiente paso consistió en diseñar los controles y la declaración de aplicabilidad de acuerdo con los requisitos de la NTP - ISO/IEC 27001:2014; sin embargo, aunque ésta fue la conclusión a la que llegaron la mayoría de los autores, otros optaron por aplicarla en sus organizaciones. Este resultado es variable porque cada organización o entidad es única, aunque pertenezca a la misma categoría.

El último paso fue realizar las propuestas de políticas de seguridad de los activos basados en la NTP-ISO/IEC 27001:2014. Que a diferencia de los otros autores los propusimos al final viendo el estado de riesgo en el cual se encontraban los activos.

Este proyecto puede tener el inconveniente de que sólo ha llegado a la fase de diseño y no se ha puesto en práctica, pero sienta las bases para esta última porque, además de estar en consonancia

con la NTP-ISO/IEC 27001:2014, proporciona a la organización una documentación en la que se describen las amenazas a la seguridad de la información a las que se enfrenta y cómo gestionarlas eficazmente.

Aunque la seguridad de la información es un tema que se discute con frecuencia, no se utiliza en el contexto de la organización. El resultado del desarrollo actual del proyecto acerca a la municipalidad distrital de Huácar al tema. Una vez desarrollados los resultados y presentados a la empresa, se prevé que ésta implemente procedimientos sólidos de seguridad en todos sus procesos para salvaguardar sus activos más valiosos de posibles peligros y amenazas.

Conclusiones

La primera conclusión es que municipalidad distrital de Huácar se encontraba en una etapa inicial (no diseñada), con un 2% de cumplimiento de los requisitos, y en una situación actual en la que la organización entendía el significado y los beneficios de un SGSI y tenía el liderazgo para poder llevarlo a cabo. Sin embargo, no se habían establecido estrategias o metodologías para la evaluación y tratamiento de los riesgos esto gracias a la aplicación de los requisitos cuatro y cinco de la NTP-ISO/IEC 27001:2014.

En segundo lugar, se concluye que el uso de la metodología MAGERIT para el análisis y gestión de riesgos en su versión 3 permitió observar los peligros internos y externos a los que está sometida la municipalidad, así como sus efectos y peligros asociados. La investigación determinó que la municipalidad del distrito de Huácar había alcanzado un nivel intolerable, ya que la mayoría de sus activos estaban fuera de la tolerancia al riesgo.

En tercer lugar, se puede decir que la creación de el PLAN DE TARTAMIETO DE RIESGOS ayudó a la municipalidad distrital de Huácar a establecer contramedidas a las amenazas previamente identificadas en los activos. y reducirlas. Además, se completó el desarrollo de la DECLARACION DE APLICABILIDAD que permitió registrar los controles de seguridad que eran aplicables y si estaban en funcionamiento, y finalmente, las POLITICAS DE SEGURIDAD basadas en la NTP-ISO/IEC 27001:2014.

Recomendaciones o sugerencias

A medida que se desarrollaba este proyecto, se hizo evidente la necesidad de que la municipalidad distrital de Huácar adoptara el SGSI y contara con documentos de gestión relativos a la seguridad de la información. Por ende, se recomienda contratar primero a un consultor que ayude a la municipalidad, y luego reservar fondos para la implementación del SGSI. También es necesario seguir estos pasos para tener éxito: primero hay que contar con el apoyo del alcalde como de la alta gerencia, luego seguir con el diseño del SGSI, que se ha desarrollado a lo largo de este proyecto, y después concienciar a todos los empleados sobre el SGSI. Como consecuencia del cambio y de los posibles problemas de aplicación, es posible que este elemento no se realice de inmediato.

Es práctico proporcionar formación continua a los empleados de la municipalidad antes de la implementar el SGSI, y explicarles dentro de estos la situación actual en la que se encuentra el municipio en cuanto a seguridad informática, así como las funciones y responsabilidades que tendrá cada persona en cuanto a seguridad informática. Asimismo, atender las inquietudes que tengan los empleados para crear una cultura de seguridad dentro de la organización.

Es aconsejable establecer el cargo de responsable de la seguridad de la información, también denominado CISO (Chief Information Security Officer), que se encargará de planificar, presupuestar y medir el rendimiento de los componentes de la seguridad de la información, así como de llevar a cabo una gestión de riesgos adecuada para la toma de decisiones, y que, junto con los demás responsables del sistema de información, ayudará a los empleados en un futuro proceso de implementación.

Referencias

(s.f.).

Administrativa, D. G. (2012). versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En M. A. Director, *versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (pág. 7). Madrid: Ministerio de Hacienda y Administraciones Públicas. Obtenido de https://repository.udistrital.edu.co/

Alvarado, C. (2022). *PENSEMOS*. Obtenido de Sistema de gestión de seguridad de la información: qué es y sus etapas: https://gestion.pensemos.com/

Argüezo 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. *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. Obtenido de http://repositorio.udh.edu.pe/123456789/2084

Avenía Delgado, C. A. (2017). *Fundamentos de seguridad informática.* Bogotá, Colombia: Areandino Editorial. Obtenido de repositorio.unesum.edu.ec

BAZAN, E. L. (2019). Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC27001:2014 para la dirección general de informática y estadistica de la Universidad Nacional Daniel Alcides Carrión . En E. A. BAZAN, *Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC27001:2014 para la dirección general de informática y estadistica de la Universidad Nacional Daniel Alcides Carrión .* Pasco - Perú.

Chacón-Monroy, N. C., & Molina-Montaña, A. V. (2022). Análisis de riesgos de seguridad de la información en el área de front digital de la empresa Xorex de Colombia. *Análisis de riesgos de seguridad de la información en el área de front digital de la empresa Xorex de Colombia.* Universidad Católica de Colombia, Bogotá, Colombia. Obtenido de https://hdl.handle.net/10983/27642

Chicaiza Castillo, D. V., & Torres Chango, C. D. (2020). Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A. *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* Universidad Técnica de Ambato, Ambato, Ecuador. Obtenido de ttps://repositorio.uta.edu.ec/jspui/handle/123456789/30690

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Dosa-Castro, E. J., & Guevara-Gamboa, N. F. (2019). Estructuración de políticas de seguridad informática para la empresa WI-SAT Comunicaciones S.A.S. *Estructuración de políticas de seguridad informática para la empresa WI-SAT Comunicaciones S.A.S.* Universidad Católica de Colombia, Bogotá, Colombia. Obtenido de https://hdl.handle.net/10983/23384

Escalante Coronel, D. (2019). "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas. *(Tesis).* Universidad Nacional Jose Maria Arguedas, Chincheros.

ESCALANTE CORONEL, D. M. (2019). DISEÑO DE UN SISEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BAJO EL ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS – CHINCHEROS . En D. M. ESCALANTE CORONEL, *DISEÑO DE UN SISEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BAJO EL*

ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS – CHINCHEROS (pág. 31). ANDAHUAYLAS.

Fernández Villacrés, G. E., Martínez Campaña, C. E., & Aguilar Carrión, M. R. (2017). lan de seguridad informática basado en estándares Iso-Iec 27001 para proteger la información y activos del GAD cantonal de Pastaza. *Plan de seguridad informática basado en estándares Iso-Iec 27001 para proteger la información y activos del GAD cantonal de Pastaza.* Uniandes Ambato, Ambato. Obtenido de ttp://dspace.uniandes.edu.ec/handle/123456789/6508

Freshservice. (2021). Obtenido de Freshservice: https://freshservice.com

Gimenez Albacete, J. F. (2014). *Seguridad en equipos informáticos (Primera ed.).* Malaga España: Antequera, Málaga, España.

GlobalSuit Solutions. (25 de Enero de 2022). Obtenido de GlobalSuit Solutions: https://www.globalsuitesolutions.com/es/que-es-cobit/

Gomez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática. 2ª Edición.* Madrid, España: RA - MA.

Huamán Monzón, F. M. (2014). Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano. *Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano.* Pontifica Universidad Católica del Perú, Lima, Perú. Obtenido de http://hdl.handle.net/20.500.12404/5582

INDECOPI, C. d. (2014). Portal INDECI. *Norma Técnica Peruana NTP-ISO/IEC 27001: 2014.* INDECOPI, Lima, Perú. Obtenido de https://portal.indeci.gob.pe/images/contenido/NTP-ISO-IEC_27001_2014_Original_SelloINDECI_4ziAt.pdf

Lara Morales, K. S. (2018). Propuesta para la seguridad informática basado en la norma Iso/Iec 27001 en la clínica Simedic diagnóstica S.A.C – Piura; 2018. *Propuesta para la seguridad informática basado en la norma Iso/Iec 27001 en la clínica Simedic diagnóstica S.A.C – Piura; 2018.* ULADECH CATÓLICA, Piura, Perú. Obtenido de https://hdl.handle.net/20.500.13032/7882

Medina Balseca, J. L., & Meza Castillo, A. L. (2019). Diseño de un marco de referencia para el análisis de vulnerabilidades a un segmento de la red corporativa de una empresa de telecomunicaciones en Quito basado en las principales metodologías de pruebas de seguridad informática. *Diseño de un marco de referencia para el análisis de vulnerabilidades a un segmento de la red corporativa de una empresa de telecomunicaciones en Quito basado en las principales metodologías de pruebas de seguridad informática.* Universidad Internacional SEK, Quito, Ecuador. Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/3348

Pajuelo Godoy, P., & Velásquez Gudiño, S. B. (2019). La metodología Magerit V3 y su incidencia en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019. *La metodología Magerit V3 y su incidencia en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019.* Universidad Nacional Hermilio Valdizán, Huánuco, Perú. Obtenido de https://hdl.handle.net/20.500.13080/5250

Quispe Barreto, J. A. (2018). Declaración de aplicabilidad mediante la NTP-ISO/IEC27001:2014 para mitigar los siniestros de la información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, 2018. *Declaración de aplicabilidad mediante la NTP-ISO/IEC27001:2014 para mitigar los siniestros de la información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, 2018.* Universidad Nacional Santiago Antúnez de Mayolo, Ancash, Perú. Obtenido de ttp://repositorio.unasam.edu.pe/handle/UNASAM/2883

Sánchez Palacios, E. S. (2020). Análisis para la seguridad informática basado en la norma ISO/IEC 27001 en el área de cómputo de la dirección regional de educación – Tumbes; 2020. *Análisis para la seguridad informática basado en la norma ISO/IEC 27001 en el área de cómputo de la dirección regional de educación – Tumbes; 2020.* ULADECH CATÓLICA, Tumbes, Perú. Obtenido de https://hdl.handle.net/20.500.13032/19763

Sandoval Alania, J. C. (2020). PROPUESTA DE DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTPISO/IEC 27001 PARA LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO – HUÁNUCO. En J. C. Sandoval Alania, *PROPUESTA DE DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTPISO/IEC 27001 PARA LA DIRECCIÓN REGIONAL DE TRABAJO Y PROMOCIÓN DEL EMPLEO – HUÁNUCO* (pág. 94). Huánuco - Perú.

Tacza Valverde, I. R. (2018). Cumplimiento del plan de seguridad de la información con relación a la norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur. año 2017. *Cumplimiento del plan de seguridad de la información con relación a la norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur. año 2017.* Universidad Nacional Hermilio Valdizán, Huánuco, Perú. Obtenido de https://hdl.handle.net/20.500.13080/2952

Talavera Álvarez, V. R. (2015). Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013.* Pontifica Universidad Católica del Perú, LIma, Perú. Obtenido de http://hdl.handle.net/20.500.12404/6092

Anexos

ANEXO A: Matriz de consistencia.

TITULO	FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES y = f(x)	DIMENSIONES	INDICADORES	DISEÑO DE LA INVESTIGACIÓN
"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTP-ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DISTRITAL DE HUÁCAR 2022"	**PROBLEMA GENERAL** ¿De qué manera un SGSI basado en la NTP-ISO/IEC 27001:2014 mejoraría la seguridad de la información en la Municipalidad Distrital de Huácar 2022?	**OBJETIVO GENERAL:** 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	**HIPOTESIS PRINCIPAL:** Para la presente investigación no se realizará una formulación de hipótesis dado que tiene un alcance de estudio exploratorio, y a su vez un enfoque cuantitativo. Al finalizar el presente proyecto no se afirmará o refutará nada, se presentará una solución al problema encontrado.	**VARIABLE DEPENDIENTE (y):** Nivel de riesgo de los activos de información en la Municipalidad Distrital de Huácar	**VARIABLE DEPENDIENTE (y):** Disponibilidad Integridad Confidencialidad Autenticidad No repudio	**VARIABLE DEPENDIENTE (y):** % riesgo en la disponibilidad de los activos informáticos % riesgo en la integridad de los activos informáticos % riesgo en la confidencialidad de los activos informáticos, % riesgo en la autenticidad de los activos informáticos % riesgo en el no repudio de los activos informáticos.	Investigación no experimental – transeccional descriptivo.
PROBLEMAS ESPECÍFICOS:		**OBJETIVOS ESPECÍFICOS:**		**VARIABLE INDEPENDIENTE (x):**	**VARIABLE INDEPENDIENTE (x):**	**VARIABLE INDEPENDIENTE (x):**	

b) ¿Qué requisitos de la Norma Técnica Peruana – ISO/IEC 27001:2014 aplicar para diagnosticar el nivel y situación actual de la seguridad de la información en la municipalidad distrital de Huácar?	a) Aplicar los requisitos 4 y 5 de la Norma Técnica Peruana ISO/IEC 27001:2014 para diagnosticar el nivel y situación actual de la municipalidad distrital de Huácar.		Sistema de Gestión de la Seguridad de la información basado en la NTP-ISO/IEC 27001:2014	Diagnóstico	* % de requisitos completamente implementados. * % de requisitos parcialmente implementados. * % de requisitos diseñados. * % de requisitos parcialmente diseñados. * % de requisitos no diseñados.	
a) ¿De qué manera la identificación de los riesgos contribuye con el Sistema de Gestión de la seguridad de la información de la municipalidad distrital de Huácar??	b) Identificar los riesgos de la seguridad de la información usando MAGERIT V3 para contribuir con el SGSI de la municipalidad distrital de Huácar.			Análisis de riesgo	* Riesgos identificados * probabilidad de impacto de riesgo	
c) ¿Influye la propuesta de políticas de seguridad de la Norma Técnica Peruana ISO/IEC 27001:2014 en la reducción de los riesgos a los que está expuesto los activos de la municipalidad distrital de Huácar?	c) Proponer políticas de seguridad basadas en la Norma Técnica Peruana ISO/IEC 27001:2014 para reducir el estado de riesgos de seguridad de la información en la municipalidad distrital de Huácar.			controles de seguridad	* Criterios de aceptación de riesgos. * Numero de políticas de seguridad.	

ANEXO B: Consentimiento informado.

CARTA N° 08-2022-SGCPRH-MDH.

Huácar, 10 de mayo de 2022.

Señor:

DECANO DE LA CARRERA PROFESIONAL INGENIERIA DE SISTEMAS UNIVERSIDAD NACIONAL HERMILIO VALDIZAN.

Presente:

Asunto : Autorización para realización de trabajo de investigación.

Referencia : Solicitud de fecha 09 de mayo de 2022.

De mi mayor consideración.

Por medio del presente, expreso mi saludo cordial y a su vez en referencia a la solicitud presentada de fecha 09 de mayo de 2022, se comunica la autorización para la realización de trabajo de investigación a los bachilleres **VILLADEZA ROMERO KAREN LUCILA** y **CONDOR SIMON REYNALDO DAVID** para realización del proyecto de tesis **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.**

Para cualquier coordinación y/o solicitud adicional de información realizar a través de la subgerencia de contabilidad, patrimonio y recursos humanos.

Sin más que decir, reiterar mis saludos, aprovecho la oportunidad para expresarle las muestras de mi especial consideración y respeto.

Atentamente,

MUNICIPALIDAD DISTRITAL DE HUACAR
AMBO - HUÁNUCO
C.P.C. Orlando Alex Falcón Ambrosio
Subgerente de Contabilidad, Patrimonio y RR.HH
DNI. N° 47895642

ANEXO C: Encuesta sobre el conocimiento de un SGSI.

SGSI: Sistema de Gestión de Seguridad de la Información, es una guía que permite a las instituciones evaluar los riesgos y definir las aplicaciones de control necesarias para poder eliminar o minimizar consecuencias negativas en un activo.

APELLIDOS Y NOMBRES:

AREA:

Pregunta	Responder con una "X" en una de ellas donde le parezca conveniente		Observación o Comentario
	SI	NO	
1. ¿Existe un SGSI en Municipalidad Distrital de Huácar?			
2. ¿Cree que el diseño de un SGSI permitirá aumentar la seguridad de la información en el Distrito Municipal de Huácar?			
3. ¿Usted tiene conocimiento acerca de políticas de seguridad de la información?			
4. ¿Cree que hay información en el trabajo que debe ser protegida?			
5. De acuerdo con su función laboral, ¿ha recibido formación sobre seguridad de la información?			
6. ¿Cuenta usted con una computadora o laptop para realizar sus funciones?			
7. ¿El computador o laptop es propio?			
8. ¿Cuenta usted con acceso a algún sistema u aplicación donde ingresa información sobre la Municipalidad Distrital de Huácar?			
9. Cuando su computadora o laptop esta desatendido ¿Está activado el bloqueo de pantalla con contraseña para salvaguardar los datos?			
10. ¿Ha experimentado alguna alteración o pérdida de información como consecuencia de virus, acceso no autorizado, deterioro, pérdida, etc. en lo que va de año?			
11. ¿En lo que va del año se produjo casos de filtración de información sensible para la institución sin su autorización o conocimiento?			
12. ¿Su computadora o laptop cuenta con antivirus actualizado?			
13. ¿Realiza usted backups (copias de información) para proteger su información?			

14. ¿Cree que su área está a salvo de los peligros del exterior o del entorno que podrían provocar la pérdida de información?			
15. ¿Ante algún acontecimiento negativo en la computadora, laptop, equipo informático o sistema de información, usted soluciona el problema?			
16. ¿Ante algún acontecimiento negativo en la computadora, laptop, equipo informático o sistema de información, usted pide ayuda a un compañero, o amigo dentro o fuera de la institución de forma virtual o presencial?			
17. ¿Tiene acceso restringido a algunas páginas web?			
18. Ante algún acontecimiento negativo en la computadora, laptop, equipo informático, o sistema de información, ¿el personal autorizado le asiste rápidamente?			
19. ¿Usted usa dispositivos de almacenamiento (usb, disco externo, etc.) personales para apoyarse en sus funciones?			
20. ¿Se guarda evidencia (informe detallado) de los sucesos relacionados con la seguridad de la información?			

ANEXO D: Ficha de verificación de valoración de activos.

FICHA DE OBSERVACIÓN PARA VALORACIÓN DE ACTIVOS MDH 2022

Observador: Bach. Ing. Reynaldo David Condor Simón.

Bach. Ing. Villadeza Romero, Karen Lucila.

Fecha: 22/08/2022

Activo: Sistema Integrado para la gestión de operaciones de focalización.

INDICACIONES:

Se presenta una escala de valoración logarítmica, cuyo objetivo es hacer valoración cualitativa respondiendo a valoraciones subjetivas por parte del personal.

Valor		Criterio
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	despreciable	Irrelevante a efectos prácticos

PREGUNTAS PARA DETERMINAR LA CRITICIDAD DE LOS ACTIVOS

DIMENSIONES	ASPECTO	PREGUNTA	
Disponibilidad [D]	**Económico**	¿Puede la entidad sufrir pérdidas financieras si el activo o los datos que controla no están disponibles?	
	Legal	¿Pueden las entidades de control imponer un castigo legal si el activo o los datos manejados a través de él no están disponibles?	
	Imagen	¿Puede verse afectada la imagen de la entidad si el activo o la información gestionada a través de él no están disponibles?	
Integridad [I]	**Económico**	Si el activo o la información controlada a través de él se actualiza sin autorización, ¿podría causar daños financieros a la entidad?	
	Legal	¿Pueden las entidades de control imponer sanciones si el activo o la información gestionada a través de él se modifica sin permiso?	
	Imagen	¿Se puede perjudicar la imagen de la entidad si se modifica el activo o la información gestionada a través de él sin permiso?	
Confidencialidad [C]	**Económico**	¿Una revelación ilegal de información confidencial de la empresa, necesaria para la toma de decisiones estratégicas y financieras, podría acarrear pérdidas financieras?	
	Legal	¿Podría la publicación no autorizada tener un impacto en el cumplimiento de las normas o la legislación establecida por los organismos reguladores?	
	Imagen	¿Podría la reputación de la entidad verse perjudicada por una divulgación no autorizada?	

Autenticidad [A]	**Económico**	¿Puede la entidad sufrir pérdidas financieras si el activo o la información controlada a través de él no se autentifica?	
	Legal	¿Pueden las entidades de control imponer sanciones legales si el activo o los datos gestionados a través de él no están autentificados?	
	Imagen	¿Se puede perjudicar la imagen de la entidad si no se autentifica el activo o la información que se gestiona a través de él?	
No Repudio [N_R]	**Económico**	¿Puede la entidad sufrir pérdidas financieras si el activo o la información que controla no puede impugnar quién entregó el mensaje?	
	Legal	¿Pueden las entidades de control imponer consecuencias legales si el activo o la información que se maneja a través de él no puede impugnar quién entregó el mensaje?	
	Imagen	¿Puede verse perjudicada la imagen de la entidad si el activo o la información que se controla a través de él no puede impugnar quién ha emitido el mensaje?	

ANEXO E: validación por juicio de expertos.

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

NOMBRE DEL JUEZ	Mary Fernanda Huamán Sobrado
ESPECIALIDAD	Ingeniera de Sistemas
EXPERIENCIA PROFESIONAL	8 años
CARGO	SOFTWARE ENGINEER III & ARQUITECTA DE SOFTWARE AWS ACIDLABS CENCOCUD(CHILE)
"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TECNICA PERUANA -ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DISTRITAL DE HUÁCAR 2022"	
DATOS DE TESISTAS	
NOMBRES Y APELLIDOS	REYNALDO DAVID CONDOR SIMON KAREN LUCILA VILLADEA ROMERO
ESPECIALIDAD	INGENIERIA DE SISTEMAS
INTRUMENTO EVALUADO	ENCUESTA
OBJETIVOS DE LA INVESTIGACION	GENERAL: Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2014, para la Municipalidad Distrital de Huácar 2022.
	ESPECIFICAS: - Aplicar los requisitos 4 y 5 de la Norma Técnica Peruana ISO/IEC 27001:2014 para diagnosticar el nivel y situación actual de la municipalidad distrital de Huácar. -Identificar los riesgos de la seguridad de la información usando MAGERIT V3 para contribuir con el SGSI de la municipalidad distrital de Huácar. -Proponer políticas de seguridad basadas en la Norma Técnica Peruana ISO/IEC 27001:2014 para reducir el estado de riesgos de seguridad de la información en la municipalidad distrital de Huácar.
EVALUÉ CADA ITEM DEL INSTRUMENTO CON LO QUE ESTOY TOTALMENTE EN ACUERDO QUE SE APLIQUE PARA DIAGNOSTICAR LA SITUACIÓN ACUTAL EN LA MUNICIPALIDAD.	
DETALLE DE LOS ITEMS DEL INTRUMENTO	El instrumento consta de 20 ítems y ha sido construido teniendo en cuenta la revisión de la literatura y luego del juicio de expertos.

Ing. Sist. Mary Fernanda Huamán Sobrado
CIP 217070

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

NOMBRE DEL JUEZ	Brayan Murphy Crespo Espinoza
ESPECIALIDAD	Ingeniería de Sistemas
EXPERIENCIA PROFESIONAL	5 años
CARGO	CONSULTOR DE SOPORTE INFORMÁTICO
"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TECNICA PERUANA -ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DISTRITAL DE HUÁCAR 2022"	
DATOS DE TESISTAS	
NOMBRES Y APELLIDOS	REYNALDO DAVID CONDOR SIMON KAREN LUCILA VILLADEA ROMERO
ESPECIALIDAD	INGENIERIA DE SISTEMAS
INTRUMENTO EVALUADO	ENCUESTA
OBJETIVOS DE LA INVESTIGACION	GENERAL: Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2014, para la Municipalidad Distrital de Huácar 2022.
	ESPECIFICAS: - Aplicar los requisitos 4 y 5 de la Norma Técnica Peruana ISO/IEC 27001:2014 para diagnosticar el nivel y situación actual de la municipalidad distrital de Huácar. -Identificar los riesgos de la seguridad de la información usando MAGERIT V3 para contribuir con el SGSI de la municipalidad distrital de Huácar. -Proponer políticas de seguridad basadas en la Norma Técnica Peruana ISO/IEC 27001:2014 para reducir el estado de riesgos de seguridad de la información en la municipalidad distrital de Huácar.
LAS PREGUNTAS DE LA ENCUESTA "CONOCIMIENTOS SOBRE EL SGSI" FUERON EVALUADOS POR MI PERSONA Y ESTOY DE ACUERDO CON SU APLICACIÓN AL PERSONAL DE LA MUNICIPALIDAD.	
DETALLE DE LOS ITEMS DEL INTRUMENTO	El instrumento consta de 20 ítems y ha sido construido teniendo en cuenta la revisión de la literatura y luego del juicio de expertos.

Ing. Sist. Brayan Murphy Crespo Espinoza

INSTRUMENTO DE VALIDACIÓN POR JUICIO DE EXPERTOS

NOMBRE DEL JUEZ	Yossary Darill Bravo Taboada
ESPECIALIDAD	GESTION PUBLICA
EXPERIENCIA PROFESIONAL	10 años
CARGO	DOCENTE UNIVERSITARIA DE LA ESCUELA DE POST GRADO DE LA UNIVERSIDAD HERMILIO VALDIZAN (PERU)
"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TECNICA PERUANA -ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DISTRITAL DE HUÁCAR 2022"	
DATOS DE TESISTAS	
NOMBRES Y APELLIDOS	REYNALDO DAVID CONDOR SIMON KAREN LUCILA VILLADEA ROMERO
ESPECIALIDAD	INGENIERIA DE SISTEMAS
INTRUMENTO EVALUADO	ENCUESTA
OBJETIVOS DE LA INVESTIGACION	GENERAL: Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2014, para la Municipalidad Distrital de Huácar 2022. ESPECIFICAS: - Aplicar los requisitos 4 y 5 de la Norma Técnica Peruana ISO/IEC 27001:2014 para diagnosticar el nivel y situación actual de la municipalidad distrital de Huácar. -Identificar los riesgos de la seguridad de la información usando MAGERIT V3 para contribuir con el SGSI de la municipalidad distrital de Huácar. -Proponer políticas de seguridad basadas en la Norma Técnica Peruana ISO/IEC 27001:2014 para reducir el estado de riesgos de seguridad de la información en la municipalidad distrital de Huácar.
EVALUÉ CADA ITEM DEL INSTRUMENTO CON LO QUE ESTOY TOTALMENTE EN ACUERDO QUE SE APLIQUE PARA DIAGNOSTICAR LA SITUACIÓN ACUTAL EN LA MUNICIPALIDAD.	
DETALLE DE LOS ITEMS DEL INTRUMENTO	El instrumento consta de 20 ítems y ha sido construido teniendo en cuenta la revisión de la literatura y luego del juicio de expertos.

Dr. Yossary Darill Bravo Taboada
DNI. 42816455

ANEXO F: Constancia de exclusividad

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" DE HUÁNUCO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE EXCLUSIVIDAD DEL TEMA

De acuerdo al Reglamento General de Grados y Títulos Modificado de la Universidad Nacional Hermilio Valdizán de Huánuco aprobado con Resolución del Consejo Universitario N° 0734-2022-UNHEVAL, de fecha 07 de marzo de 2022, considerando el Art. 24. Art 35 y en atención a lo solicitado y el informe de conformidad y Originalidad del tema de investigación de parte del señor Asesor, se hace Constar que:

La investigación titulada:

"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"

Tesista:

BACH. VILLADEZA ROMERO, KAREN LUCILA.
BACH. CONDOR SIMON, REYNALDO DAVID.

Presenta ORIGINALIDAD respecto al tema de investigación.

Huánuco, 24 de octubre de 2022

Nérida del Carmen Pastrana Díaz
Directora de Investigación - FIIS

ANEXO G: Hoja de progresión de asesor de tesis.

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN – HUÁNUCO
VICERRECTORADO ACADÉMICO
DIRECCIÓN DE ASUNTOS Y SERVICIOS ACADÉMICOS

ANEXO N° 03

HOJA DE PROGRESIÓN DE ASESORÍA DE TESIS

ESPECIALIDAD: INGENIERÍA DE SISTEMAS

1. DATOS PERSONALES

NOMBRE DEL BACHILLER:
REYNALDO DAVID CONDOR SIMON
KAREN LUCILA VILLADEZA ROMERO

NOMBRE DEL DOCENTE: MG. JIMMY GROVER FLORES VIDAL

TEMA DE INVESTIGACIÓN:
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

MES: DEL 03 DE JUNIO AL 20 DE OCTUBRE

LUGAR DE ASESORAMIENTO HUÁNUCO

2. SESIONES DE ASESORAMIENTO.

FECHA	HORA INICIO	ASUNTO TEMÁTICO	HORA DE TÉRMINOS	FIRMA DEL ASESOR	FIRMA DEL BACHILLER
13/06/2022	10 am	Formulacion de objetivos	11:30 am		
11/07/2022	5 pm	operacionalizacion de variables	6 pm		
08/08/2022	5 pm	marco teorico y metodologia	7 pm		
05/09/2022	8 am	analisis de riesgos en MAGERIT	10 am		
20/10/2022	9 am	propuesta de politicas de seguridad	11 am		

Ciudad Universitaria, 20 de OCTUBRE DEL 2022

ASESOR

BACHILLER

ANEXO H: Situación actual de la organización

SECCIÓN	REQUISITOS DE LA NTP-ISO/IEC 27001:2014.	ESTADO	EVIDENCIA Y/O SUGERENCIA (¿DE QUE MANERA SE CUMPLE? / ¿QUE MEJORAR PARA EL CUMPIMIENTO ?)	VALORACION
4	ORGANIZACIÓN Y SU CONTEXTO	No diseñado	La sugerencia seria realizar el análisis del contexto de la MDH para entender aspectos internos como externos, los interesados relevantes al SGSI para después elaborar y documentar cual será el alcance del SGSI".	6%
4.1	Entender el contexto de la organización y esta misma. La municipalidad debe decidir los factores internos y externos que son importantes para alcanzar este objetivo y que afectan a su capacidad para lograr los resultados deseados de este SGSI.	Parcialmente diseñado	El MDH dispone de documentos fácilmente accesibles que describen su misión, visión, matriz FODA y estrategias. Sin embargo, no considera explícitamente las cuestiones de seguridad de la información. Se sugiere crear políticas de seguridad de la información que estén en línea con los objetivos estratégicos de la organización.	25%
4.2	Comprender las necesidades y expectativas de las partes interesadas. La organización debe determinar las partes interesadas y los requisitos de las mismas.	No diseñado	Se sugiere identificar a las partes interesadas y comprender sus requisitos y expectativas en lo que respecta a seguridad de la información.	0%
4.3	Determinar el alcance del SGSI.	No diseñado	Sugerencia: Tener determinado cual será el alcance del SGSI teniendo en cuenta los factores mencionados, probar con documentos y que este a disposición de las partes interesadas.	0%

4.4	Sistema de Gestión de Seguridad de la información. La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta NTP-ISO 27001:2014.	No diseñado	Sugerencia: Desarrollar un plan de mejora continua del SGSI de acuerdo con la NTP – ISO/IEC 27001:2014 vigente.	0%
5	LIDERAZGO	No diseñado	El líder de la entidad debe actuar con iniciativa y dedicación hacia el SGSI. Además, debe procurar que los puestos relacionados con la seguridad de la información tengan poder y responsabilidades. En consecuencia, es esencial definir las normas de seguridad de la información y sus objetivos de acuerdo con la misión de la organización.	0%
5.1	Liderazgo y compromiso. “La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI”.	No diseñado	“El titular de la entidad debe mostrar liderazgo y compromiso”.	0%
5.2	Política	No diseñado	Crear políticas de seguridad de información, que esté en consonancia con los objetivos de la municipalidad, incluya los objetivos de seguridad de la información, sea accesible y se comparta con toda la organización.	0%
5.3	Roles, responsabilidades y autoridades organizacionales.	No diseñado	De acuerdo con la alta dirección, se debe asignar y transferir la responsabilidad y la autoridad de las tareas relacionadas con la seguridad de la información.	0%

6	*PLANIFICACIÓN*	*No diseñado*	Adoptar, diseñar y documentar el proceso de evaluación y tratamiento de los riesgos de seguridad de la información. Crear un plan para cumplir estos objetivos de seguridad de la información después de establecerlos y documentarlos de acuerdo con los propósitos de la organización.	*0%*
6.1	Cómo manejar las oportunidades y riesgos	*No diseñado*	Acoger, preparar y registrar el proceso de evaluación y gestión de los riesgos de seguridad de la información.	*0%*
6.2	Objetivo de la seguridad de la información y cómo conseguirlos	*No diseñado*	Fijar objetivos de seguridad de la información que estén en consonancia con los objetivos estratégicos de la municipalidad y, a continuación, cree una estrategia para alcanzar dichos objetivos.	*0%*
7	*SOPORTE*	*No diseñado*		*0%*
7.1	**Recursos**	*No diseñado*	Proporcionar un presupuesto para la implementación y mejoramiento continuo del SGSI.	*0%*
7.2	Competencia	*No diseñado*	comprobar las competencias de los miembros del personal en materia de seguridad de la información para garantizar el funcionamiento del SGSI.	*0%*
7.3	Concientización La política de seguridad, la forma en que contribuyen a la eficacia del SGSI y las repercusiones de no adherirse a los criterios del SGSI deben ser conocidas por todos los que trabajan para la	*No diseñado*	Informar al personal de la organización sobre la importancia de la seguridad de la información, la política de seguridad y el papel vital que cada uno de ellos desempeña en el funcionamiento eficaz del SGSI. Además, hágales saber las repercusiones de no cumplir con los requisitos del SGSI.	*0%*

	entidad y deben ser conscientes de ella.			
7.4	**Comunicación** Cuando se trata del SGSI, la organización debe decidir si son necesarias las comunicaciones internas y externas relevantes.	*No diseñado*	Incluir en la documentación los procedimientos de comunicación la comunicación interna. Esto como sugerencia.	*0%*
7.5	Información documentada	*No diseñado*	Para iniciar el diseño y eventual implementación del SGSI en el MDH, existe documentación de origen externo (Resoluciones, etc.) que ha sido descubierta pero que aún no ha sido revisada completamente. Para asegurar la eficacia del SGSI y establecer los procesos de elaboración, actualización y control de la documentación, se aconseja comenzar a crear la documentación que necesita la NTP vigente.	*0%*
8	*OPERACIÓN*	*No diseñado*		*8%*
8.1	Planificación y control operacional	*No diseñado*	Los procesos necesarios para cumplir la normativa de seguridad de la información deben planificarse, controlarse y documentarse para garantizar que se llevan a cabo según lo previsto.	*0%*
8.2	Evaluación de riesgos de seguridad de la información	*Parcialmente diseñado*	Se cuenta con un inventario de activos a bajo nivel.	*25%*
8.3	Tratamiento de riesgos de seguridad de la información.	*No diseñado.*	No se cuenta con plan de tratamiento de riesgos en la municipalidad.	*0%*
9	*EVALUACIÓN DE DESEMPEÑO*	*No diseñado*	Implantar el SGSI y crear un plan para evaluar periódicamente su eficacia con el fin de asegurarse de que el sistema sigue siendo eficiente a lo largo del	*0%*

			tiempo. Documente estas evaluaciones.	
9.1	Monitoreo, medición, análisis y evaluación	*No diseñado*	Crear procesos para el seguimiento, la valoración, la evaluación y el análisis del rendimiento de la seguridad de la información del SGSI. Registrar los resultados del seguimiento, la medición, el análisis y la evaluación del SGSI.	*0%*
9.2	Auditoría interna	*No diseñado*	No existen registros de las conclusiones de la auditoría del órgano de control interno en la que se considere la no conformidad con la seguridad de la información. Se aconseja planificar las auditorías.	*0%*
9.3	Revisión por la gerencia	*No diseñado*	No se encuentra implementado el SGSI en la municipalidad.	*0%*
10	*MEJORAS*	*No diseñado*	Aun no se encuentra implementado el SGSI por lo tanto no existen mejoras. Se recomienda su implementación y su revisión continua para su mejoramiento.	*0%*
10.1	No conformidades y acción correctiva	*No diseñado*	No se encuentra información documentada los resultados de cualquier acción correctiva y las no conformidades.	*0%*
10.2	Mejora Continua	*No diseñado*	Se debe mejorar continuamente el SGSI de acuerdo al contexto de la municipalidad una vez implementada el SGSI	*0%*
PUNTAJE TOTAL DE LA EVALUACION DE REQUISITOS DE LA NTP ISO/IEC 27001:2014				*2%*

ANEXO I: Valoración de los activos.

	CÓDIGO	ACTIVO	UN	DIMENSIONES				
				[D]	[I]	[C]	[A]	[N_R]
Equipos Informáticos (Einf) - Hardware	EIH1	Computadora de escritorio	32	8	9	7		
	EIH2	Laptop	5	8	9	7		
	EIH3	Impresora	36	2	2	0		
	EIH4	Router	3	8	9	3		
	EIH5	Switch	1	8	9	3		
	EIH6	Servidor	1	10	10	9		
Activos Esenciales (Essential)	AED 1	Datos de gestión interna	-	5	5	5		
	AED 2	Análisis de trabajo seguro	-	5	5	5		
	AED 3	Ordenes de trabajo	-	3	3	4	7	
	AED 4	Informes digitales	-	5	6	7	7	
	AED 5	Informes físicos	-	5	5	5		
	AED 6	Expedientes digitales		5	6	7	7	
	AED 7	Expedientes físicos		5	5	5		
	AED 8	Trámites digitales	-	5	6	7	7	
	AED 9	Trámites físicos	-	5	5	5		

	AED 10	Información pública	-	4	3	4		
	AED 11	Información personal	-	4	4	6		
	AED 12	Información clasificada	-	6	6	7		
	AED 13	Registro de actividad	-	3	4	3		
	AED 14	Servicio de correo electrónico	-	4	4	7	5	5
	AED 15	Servicio de página web (Facebook)	-	4	4	7	5	5
	AED 16	Servicio de internet	1	8	7	8		
Aplicaciones Informáticas (Apps)	APS 1	Software ofimático	37	7	6	3	8	
	APS 2	Sistema operativo	37	7	6	7	8	
	APS 3	Antivirus	28	9	8	8	8	
	APS 4	SIAF	1	5	7	5		
	APS 5	RUB PVL	1	5	7	5		
	APS 6	DATAS	1	5	7	5		
	APS 7	SIGOF	1	6	6	5	5	
	APS 8	SEEAP ODO MINSA	1	4	6	3	3	
	APS 9	SISREG	1	4	6	3	3	
	APS 10	SEASE	1	8	8	9	9	

	APS 11	SISTEMA DE DJ	1	4	6	3	3	
	APS 12	Sistema De Control Interno	1	8	8	9	9	
Redes De Comunicación (Ccm)	CRC1	Red Wifi		7	8	8	7	
	CRC2	Red LAN		7	7	7	6	
	CRC3	Internet		7	0	7	7	
Soporte De Información (Spi)	SIS 1	Disco Duro Externo	1	8	9	8		
	SIS 2	Usb's	2	8	9	9		
Equipamiento Auxiliar (Aux)	EAE1	Cableado		3	3	0		
	EAE2	UPS	1	3	3	0		
	EAE3	Sistema De Vigilancia	4	3	4	5		
	EAE4	Estabilizador	21	3	3	0	0	0
	EAE5	Supresor De Pico	9	3	3	0	0	0
	EAE6	Mobiliario		5	4	5	0	0
Instalaciones (Ins)	INI1	Oficinas	16	6	7	7		
	INI2	Sala De Reuniones	2	6	7	7		
Personal (P)	PSP 1	Personal Responsable	-	5	6	5		
	PSP 2	Encargado de informática	-	5	6	5		

ANEXO J: Catálogo de Amenazas sobre los activos informáticos en MAGERIT.

	N°	AMENAZA	DESCRIPCIÓN
DESASTRES NATURALES [N]	**DN1**	Fuego **[N.1]**	Incendios: posibilidad de que el fuego acabe con recursos del sistema
	DN2	Daños por agua **[N.2]**	Inundaciones: posibilidad de que el agua acabe con recursos del sistema
	DN3	Tormentas Eléctricas **[N.3]**	Descarga natural de electricidad que afecte los recursos del sistema
	DN4	Fenómenos Climáticos **[N.4]**	Modificaciones del clima previsto como una amenaza específica
DE ORIGEN INDUSTRIAL [I]	**OI1**	Contaminación Electromagnética **[I1]**	Interferencias de radio, campos magnéticos, radiaciones térmicas
	OI2	Contaminación Mecánica **[I2]**	Vibraciones, polvo, suciedad, etc.
	OI3	Desastres Industriales **[I3]**	Sobrecarga eléctrica, explosiones, contaminación química
	OI4	Avería de origen físico o lógico **[I4]**	Fallos en los equipos, de funcionamiento del hardware o falla en los programas
	OI5	Corte del suministro eléctrico **[I5]**	Pérdida o cese de la alimentación de potencia
	OI6	Condiciones inadecuadas de temperatura o humedad **[I6]**	Fallas en la climatización, excediendo los márgenes de trabajo de los equipos
	OI7	Fallo de servicios de comunicaciones **[I7]**	Pérdida de los medios de telecomunicación, destrucción o detención de los medios o centros de conmutación
	OI8	Interrupción de otros servicios y suministros esenciales **[I8]**	Servicios o recursos de los que depende la operación de los equipos
	OI9	Degradación de los soportes de almacenamiento de la información **[I9]**	Avería o falla del funcionamiento como consecuencia del paso del tiempo
ERRORES Y FALLOS NO INTENCIONADOS [E]	**EF1**	Errores de los usuarios **[F1]**	Error de uso de los servicios o datos
	EF2	Errores del administrador **[F2]**	Error de uso de los responsables de instalación y operación
	EF3	Errores de monitorización (log) **[F3]**	Registros de actividades fallidos, incompletos, faltantes
	EF4	Errores de configuración **[F4]**	Privilegios de acceso, flujos de actividades, registro de actividad erróneos
	EF5	Deficiencias en la organización **[F5]**	Acciones del personal descoordinadas, errores por omisión
	EF6	Difusión de software dañino **[F6]**	Propagación de virus, software, gusanos, troyanos, etc.

	EF7	Errores de re - encaminamiento **[F7]**	Envío de información a través de una ruta, sistema o red incorrecta
	EF8	Errores de secuencia **[F8]**	Alteración accidental del orden de los mensajes transmitidos y almacenados en algún soporte informático
	EF9	Fugas de información **[F9]**	Transferencia o revelación accidental de información almacenada en algún soporte informático
	EF10	Destrucción de información **[F10]**	Pérdida accidental de información almacenada en algún soporte informático
	EF11	Vulnerabilidades de los programas (software) **[F11]**	Defectos en el código o funcionalidad de los programas
	EF12	Errores de mantenimiento o actualización de software **[F12]**	Defectos en los procedimientos o controles de actualización, perjuicio a la mantenibilidad del sistema de información
	EF13	Errores de mantenimiento o actualización de equipos o hardware **[F13]**	Defectos en los procedimientos o controles de actualización, perjuicio a la mantenibilidad del sistema de información
	EF14	Caída del sistema por agotamiento de recursos **[F14]**	Saturación o caída del sistema informático por carencia de recursos
	EF15	Pérdida de equipos **[F15]**	Pérdida de equipos y soportes de información
	EF16	Indisponibilidad del personal **[F16]**	Ausencia accidental del puesto de trabajo
ATAQUES INTENCIONADOS [A]	**AI1**	Manipulación de la configuración **[A1]**	Configuración de procesos y flujos de actividades por personal no responsable del mismo
	AI2	Suplantación de la identidad del usuario **[A2]**	Usurpación de derechos y privilegios de acceso
	AI3	Abuso de privilegios de acceso **[A3]**	Abuso de derecho y nivel de privilegios ajenos a su competencia
	AI4	Uso no previsto **[A4]**	Utilización de los recursos del sistema para fines no previstos
	AI5	Difusión de software dañino **[A5]**	Propagación intencionada de virus, spyware, gusanos, troyanos, etc.
	AI6	Re - encaminamiento o alteración de mensajes **[A6]**	Envío o alteración del orden de los mensajes transmitidos
	AI7	Acceso no autorizado **[A7]**	Acceso y uso ilícito de los recursos del sistema
	AI8	Monitorización de tráfico **[A8]**	Extrae contenido de las comunicaciones: destino, volumen, frecuencia de los intercambios
	AI9	Repudio **[A9]**	Negación de acciones: de origen, de recepción o de entrega
	AI10	Interceptación de información **[A10]**	Escucha pasiva de información que no le corresponde

	AI11	Modificación deliberada de la información **[A11]**	Alteración intencional de la información
	AI12	Destrucción de información **[A12]**	Eliminación intencional de información
	AI13	Divulgación de información **[A13]**	Divulgación, geolocalización y copia ilegal de software
	AI14	Manipulación de programas **[A14]**	Alteración intencionada del funcionamiento de los programas
	AI15	Manipulación de los equipos **[A15]**	Sabotaje del hardware
	AI16	Robo **[A16]**	Sustracción de hardware
	AI17	Ataque destructivo **[A17]**	Destrucción de hardware o de soportes
	AI18	Ocupación enemiga **[A18]**	Locales invadidos y falta de control sobre los equipos
	AI19	Indisponibilidad del personal **[A19]**	Daño a la disponibilidad del personal
	AI20	Extorsión **[A20]**	Consiste en obligar a una persona a realizar un acto involuntario a través de medios tecnológicos
	AI21	Ingeniería social **[A21]**	Abuso de la buena fe de las personas para que realicen actividades que interesan a terceros

ANEXO K: Identificación del nivel de criticidad en los activos.

	CÓDIGO	ACTIVO	UN	DIMENSIONES					NIVEL DE CRITICIDAD
				[D]	[I]	[C]	[A]	[N_R]	
Equipos informáticos (einf) - hardware	EIH1	Computadora de escritorio	32	8	9	7			8
	EIH2	Laptop	5	8	9	7			8
	EIH3	Impresora	36	2	2	0			2
	EIH4	Router	3	8	9	3			6
	EIH5	Switch	1	8	9	3			6
	EIH6	Servidor	1	10	10	9			9
Activos esenciales (essential)	AED 1	Datos de gestión interna	-	5	5	5			5
	AED 2	Análisis de trabajo seguro	-	5	5	5			5
	AED 3	Ordenes de trabajo	-	3	3	4	7		4
	AED 4	Informes digitales	-	5	6	7	7		6
	AED 5	Informes físicos	-	5	5	5			5
	AED 6	Expedientes digitales		5	6	7	7		6
	AED 7	Expedientes físicos		5	5	5			5
	AED 8	Trámites digitales	-	5	6	7	7		6
	AED 9	Trámites físicos	-	5	5	5			5
	AED 10	Información pública	-	4	3	4			3
	AED 11	Información personal	-	4	4	6			4
	AED 12	Información clasificada	-	6	6	7			6
	AED 13	Registro de actividad	-	3	4	3			3
	AED 14	Servicio de correo electrónico	-	4	4	7	5	5	5
	AED 15	Servicio de página web (facebook)	-	4	4	7	5	5	5
	AED 16	Servicio de internet	1	8	7	8			7
Aplicaciones informáticas	APS 1	Software ofimático	37	7	6	3	8		6
	APS 2	Sistema operativo	37	7	6	7	8		7
	APS 3	Antivirus	28	9	8	8	8		8

(apps)	APS 4	SIAF	1	5	7	5			**5**
	APS 5	RUB PVL	1	5	7	5			**5**
	APS 6	DATAS	1	5	7	5			**5**
	APS 7	SIGOF	1	6	6	5	5		**5**
	APS 8	SEEAP ODO MINSA	1	4	6	3	3		**4**
	APS 9	SISREG	1	4	6	3	3		**4**
	APS 10	SEASE	1	8	8	9	9		**8**
	APS 11	Sistema de dj	1	4	6	3	3		**4**
	APS 12	Sistema de control interno	1	8	8	9	9		**8**
Redes de comunicación (ccm)	CRC1	Red wifi		7	8	8	7		**7**
	CRC2	Red LAN		7	7	7	6		**6**
	CRC3	Internet		7	0	7	7		**7**
Soporte de información (spi)	SIS 1	Disco duro externo	1	8	9	8			**8**
	SIS 2	Usb's	2	8	9	9			**8**
Equipamiento auxiliar(aux)	EAE1	Cableado		3	3	0			**3**
	EAE2	Ups	1	3	3	0			**3**
	EAE3	Sistema de vigilancia	4	3	4	5			**4**
	EAE4	Estabilizador	21	3	3	0	0	0	**3**
	EAE5	Supresor de pico	9	3	3	0	0	0	**3**
	EAE6	Mobiliario		5	4	5	0	0	**4**
Instalaciones (ins)	INI1	Oficinas	16	6	7	7			**6**
	INI2	Sala de reuniones	2	6	7	7			**6**
Personal (p)	PSP 1	Personal responsable	-	5	6	5			**5**
	PSP 2	Encargado de informática	-	5	6	5			**5**

ANEXO L: Identificación de amenazas en los activos.

	N°	CODIGO	ACTIVO	PROB	DIMENCIONES				
					[D]	[I]	[C]	[A]	[N_R]
EQUIPOS INFORMÁTICOS (EINF) - HARDWARE	**EIH1**	**[cpu]**	**Computadora de escritorio**	**4**	**90%**	**80%**	**70%**	**0%**	**0%**
		OI1	Contaminación Electromagnética [I1]	4		70%			
		OI2	Contaminación Mecánica [I2]	4	70%	60%			
		OI3	Desastres Industriales [I3]	4	60%		70%		
		OI4	Avería de origen físico o lógico [I4]	4	70%	60%			
		OI5	Corte del suministro eléctrico [I5]	4	90%		70%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	60%				
		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	4			70%		
		AI16	Robo [A16]	3	70%	80%			
	EIH2	**[lap]**	**Laptops**	**4**	**90%**	**90%**	**70%**	**0%**	**0%**
		OI3	Desastres Industriales [I3]	4	70%		70%		
		OI4	Avería de origen físico o lógico [I4]	4	70%	70%			
		OI5	Corte del suministro eléctrico [I5]	4	70%		60%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	70%				

		EF13	Errores de mantenimiento o actualización de equipos o hardware [F13]	4			70%		
		AI16	Robo [A16]	3	90%	90%			
	EIH3	**[imp]**	**Impresora**	**3**	**40%**	**60%**	**40%**	**0%**	**0%**
		OI5	Corte del suministro eléctrico [I5]	3	30%	30%	40%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	40%	60%			
		AI1	Manipulación de la configuración [A1]	4	20%	50%			
	EIH4	**[rou]**	**Router**	**4**	**90%**	**70%**	**70%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	70%	70%	70%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	60%				
		OI7	Fallo de servicios de comunicaciones [I7]	3	70%	60%	60%		
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	5	70%		70%		
		EF4	Errores de configuración [F4]	4	60%				
		AI1	Manipulación de la configuración [A1]	4	90%				
	EIH5	**[swt]**	**Switch**	**4**	**90%**	**70%**	**70%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	70%	70%	70%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	60%				
		OI7	Fallo de servicios de comunicaciones [I7]	3	70%	60%	60%		

		OI9	Degradación de los soportes de almacenamiento de la información [I9]	5	70%		70%		
		EF4	Errores de configuración [F4]	4	60%				
		AI1	Manipulación de la configuración [A1]	4	90%				
	EIH6	**[ser]**	**Servidor**	**4**	**90%**	**70%**	**70%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	70%	70%	70%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	60%				
		OI7	Fallo de servicios de comunicaciones [I7]	3	70%	60%	60%		
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	5	70%		70%		
		EF4	Errores de configuración [F4]	4	60%				
		AI1	Manipulación de la configuración [A1]	4	90%				
ACTIVOS ESENCIALES (ESSENTIAL)	**AED 1**	**[dgi]**	**Datos de gestión interna**	**4**	**50%**	**60%**	**40%**	**0%**	**0%**
		AI11	Modificación deliberada de la información [A11]	3		40%	30%		
		OI8	Interrupción de otros servicios y suministros esenciales [I8]	4	50%	40%			
		EF10	Destrucción de información [F10]	3	40%	60%	30%		
		AI13	Divulgación de información [A13]	4			40%		
	AED 2	**[ats]**	**Análisis de trabajo seguro**	**3**	**50%**	**70%**	**70%**	**0%**	**0%**
		EF9	Fugas de información [F9]	3	30%		60%		
		DN2	Daños por agua [N.2]	2	50%				

		OI9	Degradación de los soportes de almacenamiento de la información [I9]	4	50%	40%			
		EF10	Destrucción de información [F10]	3		70%			
		AI7	Acceso no autorizado [A7]	4			70%		
		AI11	Modificación deliberada de la información [A11]	4		70%			
	AED 3	**[odt]**	**Ordenes de trabajo**	**3**	**60%**	**80%**	**70%**	**0%**	**0%**
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3		40%			
		AI19	Indisponibilidad del personal [A19]	4					
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	60%				
		EF5	Deficiencias en la organización [F5]	3	60%	50%			
		EF10	Destrucción de información [F10]	2	50%	60%	20%		
		AI11	Modificación deliberada de la información [A11]	2		80%	70%		
	AED 4	**[infd]**	**Informes digitales**	**3**	**50%**	**50%**	**50%**	**0%**	**0%**
		EF10	Destrucción de información [F10]	4	30%	50%	50%		
		EF1	Errores de los usuarios [F1]	3	40%	50%			
		EF9	Fugas de información [F9]	2	50%				
	AED 5	**[inff]**	**Informes físicos**	**4**	**40%**	**50%**	**60%**	**0%**	**0%**
		DN2	Daños por agua [N.2]	5			60%		
		EF9	Fugas de información [F9]	4	30%	50%	50%		

	DN1	Fuego [N.1]	3	20%					
	AI16	Robo [A16]	3	40%	50%				
AED 6	**[expd]**	**Expedientes digitales**	**4**	**30%**	**50%**	**60%**	**0%**	**0%**	
	EF10	Destrucción de información [F10]	5			60%			
	EF1	Errores de los usuarios [F1]	4	30%	50%	50%			
	EF9	Fugas de información [F9]	3	20%					
AED 7	**[expf]**	**Expedientes físicos**	**3**	**50%**	**30%**	**40%**	**0%**	**0%**	
	DN2	Daños por agua [N.2]	3	50%					
	EF9	Fugas de información [F9]	4	10%	30%	40%			
	DN1	Fuego [N.1]	2		30%				
	AI16	Robo [A16]	3	50%					
AED 8	**[tramd]**	**Trámites digitales**	**3**	**40%**	**40%**	**50%**	**0%**	**50%**	
	EF10	Destrucción de información [F10]	3	10%	40%				
	EF1	Errores de los usuarios [F1]	3	10%	30%				
	EF9	Fugas de información [F9]	4	40%		50%			
	AI9	Repudio [A9]	3		30%			50%	
	EF7	Errores de re - encaminamiento [F7]	3					20%	
	EF2	Errores del administrador [F2]	4	30%				30%	
AED 9	**[tramf]**	**Trámites físicos**	**4**	**60%**	**50%**	**60%**	**0%**	**0%**	
	DN2	Daños por agua [N.2]	5	60%	50%				

	EF9	Fugas de información [F9]	4	40%		60%		
	DN1	Fuego [N.1]	2		40%	30%		
	AI16	Robo [A16]	3	10%				
AED 10	**[ipub]**	**Información pública**	**4**	**50%**	**50%**	**50%**	**0%**	**0%**
	EF1	Errores de los usuarios [F1]	5		40%			
	EF9	Fugas de información [F9]	4	50%	50%	50%		
	EF5	Deficiencias en la organización [F5]	4	40%		30%		
AED 11	**[iper]**	**Información personal**	**4**	**60%**	**50%**	**50%**	**0%**	**0%**
	EF9	Fugas de información [F9]	4	40%		50%		
	EF10	Destrucción de información [F10]	5	60%	50%	20%		
	AI11	Modificación deliberada de la información [A11]	4					
AED 12	**[iclas]**	**Información clasificada**	**3**	**60%**	**50%**	**50%**	**0%**	**0%**
	AI4	Uso no previsto [A4]	3		40%			
	EF9	Fugas de información [F9]	4	30%		50%		
	AI11	Modificación deliberada de la información [A11]	3	60%	50%			
AED 13	**[ra]**	**Registro de actividad**	**3**	**50%**	**40%**	**50%**	**0%**	**0%**
	EF4	Errores de configuración [F4]	4	20%	30%			
	EF3	Errores de monitorización (log) [F3]	3	30%	10%	50%		
	EF12	Errores de mantenimiento o actualización de software [F12]	3	50%	40%			
AED 14	**[sce]**	**Servicio de correo Electrónico**	**4**	**60%**	**80%**	**40%**	**0%**	**0%**

		EF1	Errores de los usuarios [F1]	4	40%	80%			
		OI4	Avería de origen físico o lógico [I4]	3	40%	20%	40%		
		OI7	Fallo de servicios de comunicaciones [I7]	4	60%	60%			
		OI8	Interrupción de otros servicios y suministros esenciales [I8]	4	50%	50%			
	AED 15	**[spw]**	**Servicio de Página Web (Facebook)**	**4**	**70%**	**60%**	**40%**	**0%**	**0%**
		OI7	Fallo de servicios de comunicaciones [I7]	4	70%		40%		
		EF14	Caída del sistema por agotamiento de recursos [F14]	3	30%	60%			
		EF7	Errores de re - encaminamiento [F7]	4	20%				
	AED 16	**[sint]**	**Servicio de internet**	**4**	**90%**	**80%**	**70%**	**0%**	**0%**
		EF7	Errores de re - encaminamiento [F7]	4	70%				
		OI4	Avería de origen físico o lógico [I4]	3	80%	70%			
		OI5	Corte del suministro eléctrico [I5]	4	70%		60%		
		OI7	Fallo de servicios de comunicaciones [I7]	4	90%		70%		
		EF14	Caída del sistema por agotamiento de recursos [F14]	3	60%	80%			
APLICACIONES INFORMÁICAS (APPS)	**APS 1**	**[sofi]**	**Software Ofimática**	**4**	**60%**	**70%**	**50%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		AI1	Manipulación de la configuración [A1]	4	60%	70%			

		EF12	Errores de mantenimiento o actualización de software [F12]	4	30%	20%	50%		
	APS 2	**[so]**	**Sistema operativo**	**4**	**60%**	**50%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	4	30%				
		AI4	Uso no previsto [A4]	3	30%				
		AI3	Abuso de privilegios de acceso [A3]	4	20%	40%			
		AI7	Acceso no autorizado [A7]	4	60%				
		EF2	Errores del administrador [F2]	3	30%	50%	40%		
	APS 3	**[antv]**	**Antivirus**	**4**	**90%**	**70%**	**70%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	70%				
		EF4	Errores de configuración [F4]	3	60%	70%	70%		
		EF12	Errores de mantenimiento o actualización de software [F12]	4	90%	60%	60%		
		AI1	Manipulación de la configuración [A1]	5	80%		60%		
		AI5	Difusión de software dañino [A5]	4		70%			
	APS 4	**[siaf]**	**SIAF**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				
		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				

	APS 5	**(pvl)**	**RUV PVL**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				
		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				
	APS 6	**[pdt]**	**DATAS**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				
		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				
	APS 7	**[sgd]**	**SIGOF**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				
		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				
	APS 8	**[som]**	**SEEAP ODO MINSA**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		

		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				
		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				
	APS 9	**[sisr]**	**SISREG**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				
		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				
	APS 10	**[seas]**	**SEASE**	**4**	**90%**	**80%**	**90%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	4	70%	70%			
		OI7	Fallo de servicios de comunicaciones [I7]	4	70%	80%			
		EF2	Errores del administrador [F2]	4	60%		60%		
		AI2	Suplantación de la identidad del usuario [A2]	3	70%		70%		
		AI7	Acceso no autorizado [A7]	3	90%		90%		
	APS 11	**[sddj]**	**SISTEMA DE DJ**	**3**	**60%**	**0%**	**40%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	3	30%		40%		
		OI7	Fallo de servicios de comunicaciones [I7]	3	60%		30%		
		EF2	Errores del administrador [F2]	4	20%				

		AI2	Suplantación de la identidad del usuario [A2]	3	40%				
		AI7	Acceso no autorizado [A7]	3	60%				
	APS 12	**[sdci]**	**Sistema de control interno**	**4**	**90%**	**80%**	**90%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	4	70%	70%			
		OI7	Fallo de servicios de comunicaciones [I7]	4	70%	80%			
		EF2	Errores del administrador [F2]	4	60%		60%		
		AI2	Suplantación de la identidad del usuario [A2]	3	70%		70%		
		AI7	Acceso no autorizado [A7]	3	90%		90%		
REDES DE COMUNICACIÓN (CCM)	**CRC1**	**[rwi]**	**Red WIFI**	**4**	**90%**	**70%**	**90%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	4	80%	70%			
		OI5	Corte del suministro eléctrico [I5]	4	90%		90%		
		EF14	Caída del sistema por agotamiento de recursos [F14]	3	90%	60%			
		EF7	Errores de re - encaminamiento [F7]	4	70%				
	CRC2	**[rla]**	**Red LAN**	**4**	**60%**	**50%**	**30%**	**0%**	**0%**
		DN4	Fenómenos Climáticos [N.4]	3	40%	10%			
		OI7	Fallo de servicios de comunicaciones [I7]	4	50%	30%	30%		
		OI4	Avería de origen físico o lógico [I4]	4	50%	50%			
		OI3	Desastres Industriales [I3]	4	60%	50%			
	CRC3	**[int]**	**Internet**	**4**	**50%**	**40%**	**0%**	**0%**	**0%**

		OI4	Avería de origen físico o lógico [I4]	4	50%	50%			
		OI5	Corte del suministro eléctrico [I5]	4	70%		40%		
		EF14	Caída del sistema por agotamiento de recursos [F14]	3	30%	50%			
		EF7	Errores de re - encaminamiento [F7]	4	20%				
SOPORTE DE INFORMACIÓN (SPI)	**SIS 1**	**[dde]**	**Disco duro externo**	**4**	**90%**	**80%**	**90%**	**0%**	**0%**
		AI17	Ataque destructivo [A17]	3	70%	80%	80%		
		AI4	Uso no previsto [A4]	4	80%		70%		
		OI4	Avería de origen físico o lógico [I4]	4	70%				
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	4	90%				
		AI13	Divulgación de información [A13]	4			90%		
		AI16	Robo [A16]	4	90%		90%		
	SIS 2	**[usb]**	**USB'S**	**4**	**90%**	**80%**	**90%**	**0%**	**0%**
		AI4	Uso no previsto [A4]	4	80%				
		OI4	Avería de origen físico o lógico [I4]	2	70%				
		OI9	Degradación de los soportes de almacenamiento de la información [I9]	4	90%				
		AI13	Divulgación de información [A13]	4		80%	70%		
		AI16	Robo [A16]	4	90%		90%		
	EAE1	**[cab]**	**Cableado**	**3**	**60%**	**50%**	**40%**	**0%**	**0%**

EQUIPAMIENTO AUXILIAR (AUX)		OI7	Fallo de servicios de comunicaciones [I7]	4	50%	30%	40%		
		OI3	Desastres Industriales [I3]	3	60%	50%			
		DN4	Fenómenos Climáticos [N.4]	3	40%	20%			
	EAE2	**[usb]**	**UPS**	**4**	**50%**	**30%**	**30%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	4	50%	30%			
		OI5	Corte del suministro eléctrico [I5]	4			30%		
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	40%				
	EAE3	**[siv]**	**Sistema de vigilancia**						
		OI4	Avería de origen físico o lógico [I4]	4	50%	30%			
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	4			30%		
		OI3	Desastres Industriales [I3]	3	40%				
	EIH4	**[est]**	**estabilizador**	**3**	**60%**	**50%**	**30%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	2	60%	50%	30%		
		OI5	Corte del suministro eléctrico [I5]	3	50%	20%			
		OI6	Condiciones inadecuadas de temperatura o humedad [I6]	3	40%				
	EIH5	**[spd]**	**Supresor de pico**	**3**	**60%**	**50%**	**30%**	**0%**	**0%**
		OI4	Avería de origen físico o lógico [I4]	2	60%	50%	30%		
		OI5	Corte del suministro eléctrico [I5]	3	50%	20%			
	EAE6	**[mob]**	**Mobiliario**	**3**	**50%**	**40%**	**50%**	**0%**	**0%**

		OI9	Degradación de los soportes de almacenamiento de la información [I9]	3	50%	40%	50%		
		DN4	Fenómenos Climáticos [N.4]	2	30%	10%			
INSTALACIONES (INS)	**INI1**	**[ofi]**	**Oficina**	**4**	**50%**	**50%**	**60%**	**0%**	**0%**
		AI18	Ocupación enemiga [A18]	4	50%	50%	60%		
		OI2	Contaminación Mecánica [I2]	3	50%				
	INI2	**[sc]**	**Sala de reuniones**	**3**	**10%**	**50%**	**20%**	**0%**	**0%**
		AI17	Ataque destructivo [A17]	3		50%	20%		
		OI2	Contaminación Mecánica [I2]	3	10%	50%			
PERSONAL (P)	**PSP 1**	**[prb]**	**PERSONAL RESPONSABLE**	**4**	**60%**	**50%**	**70%**	**0%**	**0%**
		AI20	Extorsión [A20]	3	50%	30%	20%		
		AI3	Abuso de privilegios de acceso [A3]	4	40%	40%	50%		
		AI2	Suplantación de la identidad del usuario [A2]	4	60%	50%	70%		
		AI21	Ingeniería social [A21]	4	30%	40%	50%		
		AI19	Indisponibilidad del personal [A19]	3	60%	50%			
	PSP 2	**[edi]**	**ENCARGADO DE INFORMÁTICA**	**4**	**60%**	**50%**	**50%**	**0%**	**0%**
		AI3	Abuso de privilegios de acceso [A3]	4	40%	40%	50%		
		AI19	Indisponibilidad del personal [A19]	3	60%	50%			
		AI21	Ingeniería social [A21]	4	30%	40%	50%		
		EF9	Fugas de información [F9]	4			30%		

ANEXO M: Valoración de impacto de los activos.

	N°	CODIGO	ACTIVO	PROB	DIMENCIONES				
					[D]	[I]	[C]	[A]	[N_R]
EQUIPOS INFORMÁTICOS (EINF) - HARDWARE	EIH1	[cpe]	Computadora de escritorio	**4**	7	7	5	0	0
	EIH2	[lap]	Laptop	**4**	7	8	5	0	0
	EIH3	[imp]	Impresora	**3**	1	1	0	0	0
	EIH4	[rou]	Router	**4**	7	6	2	0	0
	EIH5	[swt]	Switch	**4**	7	6	2	0	0
	EIH6	[ser]	Servidor	**4**	9	7	6	0	0
ACTIVOS ESENCIALES (ESSENTIAL)	AED 1	[dgi]	Datos de gestión interna	**4**	3	3	2	0	0
	AED 2	[ats]	Análisis de trabajo seguro	**3**	3	4	4	0	0
	AED 3	[odt]	Ordenes de trabajo	**3**	2	2	3	0	0
	AED 4	[infd]	Informes digitales	**3**	3	3	4	0	0
	AED 5	[inff]	Informes físicos	**4**	2	3	3	0	0
	AED 6	[expd]	Expedientes digitales	**4**	2	3	4	0	0
	AED 7	[expf]	Expedientes físicos	**3**	3	2	2	0	0
	AED 8	[tramd]	Trámites digitales	**3**	2	2	4	0	0
	AED 9	[tramf]	Trámites físicos	**4**	3	3	3	0	0
	AED 10	[ipub]	Información pública	**4**	2	2	2	0	0
	AED 11	[iper]	Información personal	**4**	2	2	3	0	0
	AED 12	[iclas]	Información clasificada	**3**	4	3	4	0	0
	AED 13	[ra]	Registro de actividad	**3**	2	2	2	0	0

	AED 14	[sce]	Servicio de correo Electrónico	**4**	2	3	3	0	0
	AED 15	[spw]	Servicio de Página Web (Facebook)	**4**	3	2	3	0	0
	AED 16	[sint]	Servicio de internet	**4**	7	6	6	0	0
APLICACIONES INFORMÁICAS (APPS)	APS 1	[sofi]	Software Ofimática	**4**	4	4	2	0	0
	APS 2	[so]	Sistema operativo	**4**	4	3	3	0	0
	APS 3	[antv]	Antivirus	**4**	8	6	6	0	0
	APS 4	[siaf]	SIAF	**3**	3	0	2	0	0
	APS 5	[pvl]	RUB PVL	**3**	3	0	2	0	0
	APS 6	[dats]	DATAS	**3**	3	0	2	0	0
	APS 7	[sigo]	SIGOF	**3**	4	0	2	0	0
	APS 8	[seep]	SEEAP ODO MINSA	**3**	2	0	1	0	0
	APS 9	[sire]	SISREG	**3**	2	0	1	0	0
	APS 10	[seas]	SEASE	**4**	7	6	8	0	0
	APS 11	[sidj]	SISTEMA DE DJ	**3**	2	0	1	0	0
	APS 12	[sdci]	SISTEMA DE CONTROL INTERNO	**4**	7	6	8	0	0
REDES DE COMUNICACIÓN (CCM)	CRC1	[rwi]	Red WIFI	**4**	6	6	7	0	0
	CRC2	[rla]	Red LAN	**4**	4	4	2	0	0
	CRC3	[int]	Internet	**4**	4	0	0	0	0
SOPORTE DE INFORMACIÓN (SPI)	SIS 1	[dde]	Disco duro externo	**4**	7	7	7	0	0
	SIS 2	[usb]	USB'S	**4**	7	7	8	0	0
EQUIPAMIENTO AUXILIAR(AUX)	EAE1	[cab]	Cableado	**3**	2	2	0	0	0
	EAE2	[ups]	UPS	**4**	2	1	0	0	0
	EAE3	[siv]	Sistema de vigilancia	**0**	0	0	0	0	0

	EAE5	[est]	Estabilizador	**3**	2	2	0	0	0
	EAE6	[sdp]	Supresor de pico	**3**	2	2	0	0	0
	EAE7	[mob]	Mobiliario	**3**	3	2	3	0	0
INSTALACIONES (INS)	INI1	[ofi]	Oficinas	**4**	3	4	4	0	0
	INI2	[sdr]	Sala de Reuniones	**3**	1	4	1	0	0
PERSONAL (P)	PSP 1	[prb]	PERSONAL RESPONSABLE	**4**	3	3	4	0	0
	PSP 2	[edi]	ENCARGADO DE INFORMÁTICA	**4**	3	3	3	0	0

ANEXO N: Valoración del riesgo de los activos.

	N°	CÓDIGO	ACTIVO	PROB	DIMENCIONES				
					[D]	[I]	[C]	[A]	[N_R]
EQUIPOS INFORMÁTICOS (EINF) - HARDWARE	EIH1	[cpe]	COMPUTADORA DE ESCRITORIO	4	28	28	20	0	0
	EIH2	[lap]	LAPTOP	4	28	32	20	0	0
	EIH3	[imp]	IMPRESORA	3	3	3	0	0	0
	EIH4	[rou]	ROUTER	4	28	24	8	0	0
	EIH5	[swt]	SWITCH	4	28	24	8	0	0
	EIH6	[ser]	SERVIDOR	4	36	28	24	0	0
ACTIVOS ESENCIALES (ESSENTIAL)	AED 1	[dgi]	Datos de gestión interna	4	12	12	8	0	0
	AED 2	[ats]	Análisis de trabajo seguro	3	9	12	12	0	0
	AED 3	[odt]	Ordenes de trabajo	3	6	6	9	0	0
	AED 4	[infd]	Informes digitales	3	9	9	12	0	0
	AED 5	[inff]	Informes físicos	4	8	12	12	0	0
	AED 6	[expd]	Expedientes digitales	4	8	12	16	0	0
	AED 7	[expf]	Expedientes físicos	3	9	6	6	0	0
	AED 8	[tramd]	Trámites digitales	3	6	6	12	0	0
	AED 9	[tramf]	Trámites físicos	4	12	12	12	0	0
	AED 10	[ipub]	Información pública	4	8	8	8	0	0
	AED 11	[iper]	Información personal	4	8	8	12	0	0
	AED 12	[iclas]	Información clasificada	3	12	9	12	0	0

	AED 13	[ra]	Registro de actividad	3	6	6	6	0	0
	AED 14	[sce]	Servicio de correo Electrónico	4	8	12	12	0	0
	AED 15	[spw]	Servicio de Página Web (Facebook)	4	12	8	12	0	0
	AED 16	[sint]	Servicio de internet	4	28	24	24	0	0
APLICACIONES INFORMÁICAS (APPS)	APS 1	[sofi]	Software Ofimática	4	16	16	8	0	0
	APS 2	[so]	Sistema operativo	4	16	12	12	0	0
	APS 3	[antv]	Antivirus	4	32	24	24	0	0
	APS 4	[siaf]	SIAF	3	9	0	6	0	0
	APS 5	[pvl]	RUB PVL	3	9	0	6	0	0
	APS 6	[dats]	DATAS	3	9	0	6	0	0
	APS 7	[sigo]	SIGOF	3	12	0	6	0	0
	APS 8	[seep]	SEEAP ODO MINSA	3	6	0	3	0	0
	APS 9	[sire]	SISREG	3	6	0	3	0	0
	APS 10	[seas]	SEASE	4	28	24	32	0	0
	APS 11	[sidj]	SISTEMA DE DJ	3	6	0	3	0	0
	APS 12	[sdci]	SISTEMA DE CONTROL INTERNO	4	28	24	32	0	0
REDES DE COMUNICACIÓN (CCM)	CRC1	[rwi]	Red WIFI	4	24	24	28	0	0
	CRC2	[rla]	Red LAN	4	16	16	8	0	0
	CRC3	[int]	Internet	4	16	0	0	0	0
SOPORTE DE INFORMACIÓN (SPI)	SIS 1	[dde]	Disco duro externo	4	28	28	28	0	0
	SIS 2	[usb]	USB'S	4	28	28	32	0	0
EQUIPAMIENTO AUXILIAR(AUX)	EAE1	[cab]	Cableado	3	6	6	0	0	0
	EAE2	[ups]	UPS	4	8	4	0	0	0

	EAE3	[siv]	Sistema de vigilancia	**4**	8	4	8	0	0
	EAE5	[est]	Estabilizador	**3**	6	6	0	0	0
	EAE6	[sdp]	Supresor de pico	**3**	6	6	0	0	0
	EAE7	[mob]	Mobiliario	**3**	9	6	9	0	0
INSTALACIONES (INS)	INI1	[ofi]	Oficinas	**4**	12	16	16	0	0
	INI2	[sdr]	Sala de Reuniones	**3**	3	12	3	0	0
PERSONAL (P)	PSP 1	[prb]	PERSONAL RESPONSABLE	**4**	12	12	16	0	0
	PSP 2	[edi]	ENCARGADO DE INFORMÁTICA	**4**	12	12	12	0	0

ANEXO O: *Plan de tratamiento de riesgos*

IDENTIFICACION DE RIESGO		EVALUACION DE RIESGO			TRATAMIENTO DE RIESGO					
		Nivel de riesgo								
Nombre del activo	**amenaza**	**disponibilidad**	**integridad**	**confidencialidad**	**estrategia de respuesta**	**plan de contingencia**	**tipo de control**	**cláusula de la NTP ISO(IEC 27001**	**Control ISO/IEC 27001**	**Responsable**
Computadora de Escritorio	Contaminación Electromagnética [I1]		Intolerable		Transferir	Instalar el cableado de alimentación eléctrica a través de conductos separados.	Correctivo	11. Seguridad Física y del entorno	A.11.2.3 seguridad del cableado	Administrador de la MDH
	Contaminación Mecánica [I2]	Intolerable	Tolerable		Transferir	Llevar un plan de mantenimiento periódico de limpieza a los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH

	Desastres Industriales [I3]	Tolerable		Intolerable	Reducir	Considerar que todas las computadoras de escritorio se usen con un estabilizador para regular la tensión.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Avería de origen físico o lógico [I4]	Intolerable	Tolerable		Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Corte del suministro eléctrico [I5]	Extremo		Intolerable	Transferir	Adquirir y usar un generador eléctrico en la MDH.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Condiciones inadecuadas de temperatura o humedad [I6]	Tolerable			Reducir	Establecer normas de uso y cuidado de los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Errores de mantenimiento o actualización de equipos o hardware [F13]			Intolerable	Transferir	Establecer un plan de mantenimiento del Hardware.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH

	Robo [A16]	Intolerable	Intolerable		Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.1 ubicación y protección de los equipos	Administrador de la MDH
Laptops	Desastres Industriales [I3]	Intolerable		Intolerable	Reducir	Considerar que todas las computadoras de escritorio se usen con un estabilizador para regular la tensión.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Avería de origen físico o lógico [I4]	Intolerable	Intolerable		Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Corte del suministro eléctrico [I5]	Intolerable		Tolerable	Transferir	Adquirir y usar un generador eléctrico en la MDH.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Condiciones inadecuadas de temperatura o humedad [I6]	Intolerable			Reducir	Establecer normas de uso y cuidado de los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH

	Errores de mantenimiento o actualización de equipos o hardware [F13]			Intolerable	Transferir	Elaborar un plan de mantenimiento del Hardware junto al proveedor de los equipos informáticos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Robo [A16]	Extremo	Extremo		Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.1 ubicación y protección de los equipos	Administrador de la MDH
Router	Avería de origen físico o lógico [I4]	Intolerable	Intolerable	Intolerable	Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Condiciones inadecuadas de temperatura o humedad [I6]	Tolerable			Reducir	Establecer normas de uso y cuidado de los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Fallo de servicios de comunicaciones [I7]	Intolerable	Tolerable	Tolerable	Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.1 ubicación y protección de los equipos	Administrador de la MDH

	Degradación de los soportes de almacenamiento de la información [I9]	Intolerable		Intolerable	Reducir	Monitorear el tiempo de vida de los equipos y renovar los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Errores de configuración [F4]	Tolerable			Reducir	Elaborar un manual de configuración del sistema de información.	Preventivo	12. Seguridad de las operaciones	A.12.1.1 procedimientos de operación documentados	Administrador de la MDH
	Manipulación de la configuración [A1]	Extremo			Reducir	Sancionar dependiendo de la gravedad.	Correctivo	7. Seguridad del recurso humano	A.7.2.3 proceso disciplinario	Administrador de la MDH
Switch	Avería de origen físico o lógico [I4]	Intolerable	Intolerable	Intolerable	Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Condiciones inadecuadas de temperatura o humedad [I6]	Tolerable			Reducir	Establecer normas de uso y cuidado de los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH

	Fallo de servicios de comunicaciones [I7]	Intolerable	Tolerable	Tolerable	Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.1 ubicación y protección de los equipos	Administrador de la MDH
	Degradación de los soportes de almacenamiento de la información [I9]	Intolerable		Intolerable	Reducir	Monitorear el tiempo de vida de los equipos y renovar los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Errores de configuración [F4]	Tolerable			Reducir	Elaborar un manual de configuración del sistema de información.	Preventivo	12. Seguridad de las operaciones	A.12.1.1 procedimientos de operación documentados	Administrador de la MDH
	Manipulación de la configuración [A1]	Extremo			Reducir	Sancionar dependiendo de la gravedad.	Correctivo	7. Seguridad del recurso humano	A.7.2.3 proceso disciplinario	Administrador de la MDH
Servidor	Avería de origen físico o lógico [I4]	Intolerable	Intolerable	Intolerable	Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH

	Condiciones inadecuadas de temperatura o humedad [I6]	Tolerable			Reducir	Establecer normas de uso y cuidado de los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Fallo de servicios de comunicaciones [I7]	Intolerable	Tolerable	Tolerable	Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.1 ubicación y protección de los equipos	Administrador de la MDH
	Degradación de los soportes de almacenamiento de la información [I9]	Intolerable		Intolerable	Reducir	Monitorear el tiempo de vida de los equipos y renovar los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos A.11.1.4 protección contra amenazas externas y ambientales	Administrador de la MDH
	Errores de configuración [F4]	Tolerable			Reducir	Elaborar un manual de configuración del sistema de información.	Preventivo	12. Seguridad de las operaciones	A.12.1.1 procedimientos de operación documentados	Administrador de la MDH
	Manipulación de la configuración [A1]	Extremo			Reducir	Sancionar dependiendo de la gravedad.	Correctivo	7. Seguridad del recurso humano	A.7.2.3 proceso disciplinario	Administrador de la MDH

Servicio de Internet	Errores de re - encaminamiento [F7]	Intolerable			Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Avería de origen físico o lógico [I4]	Intolerable	Intolerable		Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Corte del suministro eléctrico [I5]	Intolerable		Tolerable	Transferir	Adquirir y usar un generador eléctrico en la MDH.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Fallo de servicios de comunicaciones [I7]	Extremo		Intolerable	Reducir	Reportar al proveedor del servicio de internet para que solucione a corto tiempo.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Caída del sistema por agotamiento de recursos [F14]	Tolerable	Intolerable		Reducir	Reportar al proveedor del servicio de internet para que solucione a corto tiempo.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
Antivirus	Avería de origen físico o lógico [I4]	Intolerable			Transferir	Realizar un plan de mantenimiento del Software.	Correctivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH

	Errores de configuración [F4]	Tolerable	Intolerable	Intolerable	Transferir	Adquirir licencias originales de software	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Errores de mantenimiento o actualización de software [F12]	Extremo	Tolerable	Tolerable	Transferir	Adquirir licencias originales de software	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Manipulación de la configuración [A1]	Intolerable		Tolerable	Reducir	Establecer normas de uso y cuidado de los equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.2.4 mantenimiento de equipos	Administrador de la MDH
	Difusión de software dañino [A5]		Intolerable		Transferir	Adquirir licencias originales de software	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
SEASE	Avería de origen físico o lógico [I4]	Intolerable	Intolerable		Reducir	Contactar al Sede central del Sistema Electrónico de Contrataciones del estado.	Correctivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1 restricción de acceso a la información	Administrador de la MDH
	Fallo de servicios de comunicaciones [I7]	Intolerable	Intolerable		Reducir	Contactar al Sede central del Sistema Electrónico de Contrataciones del estado.	Correctivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.2 procedimiento de ingreso seguro	Administrador de la MDH

	Errores del administrador [F2]	Tolerable		Tolerable	Reducir	Realizar capacitaciones para el uso del sistema.	Correctivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.4 uso de programas utilitarios privilegiados	Administrador de la MDH
	Suplantación de la identidad del usuario [A2]	Intolerable		Intolerable	Reducir	Realizar un acta de confidencialidad para el responsable del uso del sistema	Preventivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.3 sistema de gestión de contraseñas	Administrador de la MDH
	Acceso no autorizado [A7]	Extremo		Extremo	Reducir	Realizar un acta de confidencialidad para el responsable del uso del sistema	Preventivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.3 sistema de gestión de contraseñas	Administrador de la MDH
Sistema de Control Interno	Avería de origen físico o lógico [I4]	Intolerable	Intolerable		Reducir	Contactar al Sede central del Sistema Electrónico de Contrataciones del estado.	Correctivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1 restricción de acceso a la información	Administrador de la MDH
	Fallo de servicios de comunicaciones [I7]	Intolerable	Intolerable		Reducir	Contactar al Sede central del Sistema Electrónico de Contrataciones del estado.	Correctivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.2 procedimiento de ingreso seguro	Administrador de la MDH

	Errores del administrador [F2]	Tolerable		Tolerable	Reducir	Realizar capacitaciones para el uso del sistema.	Correctivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.4 uso de programas utilitarios privilegiados	Administrador de la MDH
	Suplantación de la identidad del usuario [A2]	Intolerable		Intolerable	Reducir	Realizar un acta de confidencialidad para el responsable del uso del sistema	Preventivo	7. Seguridad del recurso humano	A.7.1.2 términos y condiciones del empleo A.7.2.3 proceso disciplinario	Administrador de la MDH
	Acceso no autorizado [A7]	Extremo		Extremo	Reducir	Realizar un acta de confidencialidad para el responsable del uso del sistema	Preventivo	9.4. Control de acceso a sistemas y aplicaciones	A.9.4.3 sistema de gestión de contraseñas	Administrador de la MDH
Red WIFI	Avería de origen físico o lógico [I4]	Intolerable	Intolerable		Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Corte del suministro eléctrico [I5]	Extremo		Extremo	Transferir	Adquirir y usar un generador eléctrico en la MDH.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH

	Caída del sistema por agotamiento de recursos [F14]	Extremo	Tolerable		Reducir	Reportar al proveedor del servicio de internet para que solucione a corto tiempo.	Preventivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Errores de re - encaminamiento [F7]	Intolerable			Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
Disco Duro Externo	Ataque destructivo [A17]	Intolerable	Intolerable	Intolerable	Reducir	Crear un control específico para regular el uso de estos equipos desmontables y, en caso de ataque destructivo, considerar una sanción teniendo en cuenta la gravedad.	Preventivo	7. Seguridad del recurso humano	A.7.1.2 términos y condiciones del empleo A.7.2.3 proceso disciplinario	Administrador de la MDH

	Uso no previsto [A4]	Intolerable		Intolerable	Reducir	Para evitar el uso indebido, documentar los requisitos de seguridad de la información de los activos cuando se utilicen equipos informáticos.	Correctivo	8. Gestión de activos	A.8.1.3 Reglas para el uso aceptable de activos	Administrador de la MDH
	Avería de origen físico o lógico [I4]	Intolerable			Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Degradación de los soportes de almacenamiento de la información [I9]	Extremo		Extremo	Reducir	Para evitar el deterioro de la información almacenada, es necesario sustituir los dispositivos después de un tiempo determinado.	Preventivo	11. Seguridad Física y del entorno	A.11.1.4 protección contra amenazas externas y ambientales	Administrador de la MDH

	Divulgación de información [A13]		Intolerable	Intolerable	Reducir	Estipular en el contrato la confidencialidad de la información y considerar una sanción tomando en cuenta la gravedad del impacto.	Preventivo	7. Seguridad del recurso humano	A.7.1.2 términos y condiciones del empleo A.7.2.3 proceso disciplinario	Administrador de la MDH
	Robo [A16]	Extremo		Extremo	Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.1.2 controles de acceso físicos	Administrador de la MDH
USB'S	Uso no previsto [A4]	Intolerable			Reducir	Para evitar el uso indebido, documentar los requisitos de seguridad de la información de los activos cuando se utilicen equipos informáticos.	Correctivo	8. Gestión de activos	A.8.1.3 Reglas para el uso aceptable de activos	Administrador de la MDH

	Avería de origen físico o lógico [I4]	Intolerable			Reducir	Contactar al proveedor de los equipos informáticos para un cambio o reparación.	Correctivo	11. Seguridad Física y del entorno	A.11.2.2 servicios de suministro	Administrador de la MDH
	Degradación de los soportes de almacenamiento de la información [I9]	Extremo			Reducir	Para evitar el deterioro de la información almacenada, es necesario sustituir los dispositivos después de un tiempo determinado..	Preventivo	11. Seguridad Física y del entorno	A.11.1.4 protección contra amenazas externas y ambientales	Administrador de la MDH
	Divulgación de información [A13]		Intolerable	Intolerable	Reducir	Estipular en el contrato la confidencialidad de la información y considerar una sanción tomando en cuenta la gravedad del impacto.	Preventivo	7. Seguridad del recurso humano	A.7.1.2 términos y condiciones del empleo A.7.2.3 proceso disciplinario	Administrador de la MDH
	Robo [A16]	Extremo		Extremo	Reducir	Monitorear la identificación a los visitantes y el inventario de equipos.	Preventivo	11. Seguridad Física y del entorno	A.11.1.2 controles de acceso físicos	Administrador de la MDH

ANEXO P: Declaración de aplicabilidad

SECCION	OBJETIVO	CONTROL	ESTADO	JUSTIFICACION
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACION**			
A.5.1	Especificar las políticas de gestión de la seguridad de la información de acuerdo con las necesidades del negocio, los requisitos legales y la normativa.	**5.1.1.** Políticas de seguridad de la información	APLICAR	Exigido por la NTP ISO/IEC 27001:2014
		5.1.2. Revisión de políticas para la seguridad de la información	APLICAR	Exigido por la NTP ISO/IEC 27001:2014
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A.6.1	Organización interna	**6.1.1** Roles y responsabilidades de seguridad de la información	APLICAR	Exigido por la NTP ISO/IEC 27001:2014
		6.1.2 Segregación de funciones	APLICAR	Para evitar los abusos y los efectos de los incidentes de seguridad, las funciones deben estar separadas para la realización de las actividades.
		6.1.3 Contacto con autoridades	APLICAR	La ONGEI, organización encargada de confirmar el nivel de seguridad de la información en las empresas estatales, Se tendrá que estar en comunicación.
		6.1.4 Contacto con grupos especiales de interés	APLICAR	Para estar al tanto de la aparición de nuevos peligros, será importante mantener el contacto con foros especializados, revistas, etc. sobre cuestiones de seguridad.

		6.1.5 Seguridad de información en la gestión de proyectos	APLICAR	Será necesario identificar los riesgos asociados a los proyectos.
A.6.2	**Dispositivos móviles y teletrabajo: G**arantizar la seguridad en el uso de dispositivos móviles en el trabajo.	**6.2.1** Política de dispositivos móviles	APLICAR	El procesamiento y almacenamiento de la información se realiza en los dispositivos móviles.
		6.2.2 Teletrabajo	APLICAR	Por efecto de la pandemia la municipalidad aplica el teletrabajo.
A.7	**SEGURIDAD DEL RECURSO HUMANO**			
A.7.1	**Antes del empleo:** Asegúrese de que los contratistas y empleados conozcan sus obligaciones y están calificados para los puestos a los que optan.	**7.1.1** Investigación de antecedentes	APLICADO	Se buscan referencias y se supervisa la selección de personal.
		7.1.2 Términos y condiciones de empleo	APLICADO	Se especifican en el acuerdo. No obstante, se aconseja comprobar que no se han omitido obligaciones importantes en materia de seguridad de la información
A.7.2	**Durante el empleo:** Garantizar que los contratistas y el personal conozcan y respeten sus obligaciones en materia de seguridad de la información.	**7.2.1** Responsabilidades de la gerencia	APLICAR	Antes de instruir a los miembros del personal para que sigan las normas de seguridad, se deben señalar y explicar las responsabilidades.
		7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	APLICAR	La falta de formación en materia de seguridad es una amenaza común, según el estudio de riesgos.
		7.2.3 Proceso disciplinario	APLICAR	Al comunicar los deberes y las políticas debe incluirse información sobre las repercusiones del incumplimiento.

A.7.3	**Terminación y cambio de empleo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	**7.3.1** Responsabilidades ante la finalización o cambio de empleo	APLICAR	Las obligaciones tras el cese de la relación laboral deben especificarse y tenerse en cuenta en los contratos, especialmente en lo que respecta al secreto de la información.
A.8	**GESTION DE ACTIVOS**			
A.8.1	**Responsabilidad sobre los activos:** Identificar los activos de la organización y especificar las obligaciones de protección adecuadas.	**8.1.1** Inventario de activos	APLICADO	Es esencial seguir el enfoque elegido al realizar el procedimiento de evaluación de riesgos.
		8.1.2 Propiedad de los activos	APLICAR	Es importante determinar quién está a cargo de la seguridad de los activos.
		8.1.3 Uso aceptable de los activos	APLICAR	El uso de los activos se regirá por normas definidas.
		8.1.4 Retorno de activos	APLICAR	El trabajador debe devolver todas sus pertenencias cuando termine la relación laboral.
A.8.2	**Clasificación de la información:** Asegúrese de que el nivel de protección de la información es adecuado para el valor que tiene para la empresa.	**8.2.1** Clasificación de la información	APLICAR	Para aplicar las medidas adecuadas, es necesario clasificar la información dentro de la subgerencia de acuerdo con los requisitos legales, el valor y la criticidad.
		8.2.2 Etiquetado de la información	APLICAR	Los usuarios de la información deben ser capaces de reconocer las precauciones que deben utilizarse.
		8.2.3 Manejo de activos	APLICAR	aplicar los controles de seguridad de acuerdo con la clasificación acordada.
A.8.3	**Manejo de los medios:** Proteger la información almacenada en los medios de	**8.3.1** Gestión de medios removibles	APLICAR	Se requiere dado el creciente uso de soportes USB y dispositivos extraíbles en la municipalidad.

	comunicación de la divulgación, alteración, eliminación o destrucción no deseada.	**8.3.2** Disposición de medios	APLICAR	Es esencial formalizar el proceso y hacer que los soportes sean accesibles de forma segura cuando ya no se necesiten, especialmente para las copias de seguridad.
		8.3.3 Transferencia de medios físicos	APLICAR	Ningún soporte que contenga información importante debe llevarse fuera del lugar de trabajo.
A.9	**CONTROL DE ACCESO**			
A.9.1	**Requisitos de la empresa para el control de acceso: I**mponer restricciones al acceso a la información y a los medios para procesarla.	**9.1.1** Política de control de acceso	APLICAR	Los usuarios desconocen la información pertinente sobre sus privilegios de acceso.
		9.1.2 Acceso a redes y servicios de red	APLICAR	No se restringe el acceso a los servicios de red en función de la necesidad.
A.9.2	**Gestión de acceso de usuario:** Proteger contra el acceso ilegal y garantizar el acceso de los usuarios autorizados: Limitar el acceso de los usuarios autorizados a los sistemas y servicios y el acceso a la información.	**9.2.1** Registro y baja de usuarios	APLICAR	Este control sería necesario debido a la movilidad de los usuarios dentro y fuera de los sistemas. para obtener la documentación oficial sobre el establecimiento o la cancelación de los usuarios que han sido aprobados por el jefe del proceso.
		9.2.2 Aprovisionamiento de acceso a usuario	APLICADO	En función de los requisitos de acceso de los usuarios, los permisos se conceden o se revocan.
		9.2.3 Gestión de derechos de acceso privilegiados	APLICAR	El acceso a los privilegios debe asignarse y utilizarse bajo una estricta supervisión.
		9.2.4 Gestión de información de autentificación secreta de usuarios	APLICAR	La aplicación de este tipo de control se considera adecuada dado el resultado del análisis de riesgos. Dicho de otro modo, proporcionar un procedimiento

				de gestión controlado para la distribución de la información de autenticación privada.
		9.2.5 Revisión de los derechos de acceso de usuarios.	APLICAR	Realizar auditorías de los privilegios de acceso de los usuarios a diversos sistemas de información, manteniendo notas sobre los resultados de las auditorías.
		9.2.6 Remoción o ajuste de derechos de acceso	APLICAR	El responsable directo del usuario lo solicita.
A.9.3	**Responsabilidades de los usuarios: E**xigir a los usuarios que asuman la responsabilidad de proteger sus datos de acceso	**9.3.1** Uso de información de autentificación secreta	APLICAR	Para salvaguardar el acceso a la información, sería necesario contar con procedimientos de seguridad sólidos.
A.9.4	**Control de acceso a sistemas y aplicaciones**: Proteger los sistemas y las aplicaciones contra el acceso ilegal	**9.4.1** Restricción de acceso a la información	APLICAR	Los usuarios sólo tienen acceso a los datos que necesitan para completar sus tareas.
		9.4.2 Procedimientos de ingreso seguro	APLICADO	El acceso a los sistemas y aplicaciones requiere un nombre de usuario y una contraseña.
		9.4.3 Sistema de gestión de contraseñas	APLICAR	Teniendo en cuenta los riesgos en este ámbito, se reforzará el sistema de gestión de contraseñas que ya está en marcha.
		9.4.4 Uso de programas utilitarios privilegiados	APLICAR	Para prevenir eventos de seguridad, tenga cuidado al utilizar herramientas de software que puedan eludir o anular las medidas de seguridad de las aplicaciones y los sistemas.

		9.4.5 Control de acceso de código fuente de los programas	NO APLICAR	El código fuente no es accesible para usted.
A.10	**CRIPTOGRAFIA**			
A.10.1	**Controles criptográficos**: Garantizar la aplicación correcta y eficaz de la criptografía para asegurar los datos.	**10.1.1** Política sobre el uso de controles criptográficos	APLICAR	Crear directrices para el uso de métodos criptográficos que ayuden a salvaguardar los datos de la organización.
		10.1.2 Gestión de claves	APLICAR	No hay llaves secretas en la municipalidad.
A.11	**SEGURIDAD FISICA Y AMBIENTAL**			
A.11.1	**Áreas seguras: P**rohibir el acceso físico de personas no autorizadas, el daño y la interferencia con la información de la organización y la infraestructura de procesamiento de la información.	**11.1.1** Perímetro de seguridad física	APLICAR	Exigido por la NTP ISO/IEC 27001:2014
		11.1.2 Controles de ingreso físico	APLICAR	Crear señales que indiquen las zonas accesibles para los visitantes, establecer restricciones de acceso y restringir el acceso.
		11.1.3 Asegurar oficinas, áreas e instalaciones	APLICAR	Exigido por la NTP ISO/IEC 27001:2014
		11.1.4 Protección contra amenazas externas y ambientales	APLICADO	Para hacer frente a los desafíos medioambientales y ambientales externos, se cuenta con los elementos fundamentales (equipos de extinción de incendios, otros).
		11.1.5 Trabajo en áreas seguras	APLICAR	Aunque el servidor esté alojado en una oficina dentro de la misma organización, este control podría reforzarse vigilando lo que ocurre en el servidor.

		11.1.6 Áreas de despacho y carga	APLICADO	En la recepción se ha habilitado un espacio para la carga y descarga.
A.11.2	**Equipos:** Prevenir la pérdida de activos, el robo, el daño, el compromiso y la interrupción de las operaciones de la organización.	**11.2.1** Emplazamiento y protección de los equipos	APLICADO	El equipo está en lugares que están bajo la autoridad de empleados autorizados.
		11.2.2 Servicios de suministro	APLICAR	No hay un sistema de suministro de energía de reserva.
		11.2.3 Seguridad del cableado	APLICADO	Es casi seguro que hay que mejorar la instalación eléctrica.
		11.2.4 Mantenimiento de equipos	APLICADO	El mantenimiento de los equipos corre a cargo de personal de apoyo técnico que trabaja fuera del municipio. Mantener un registro de todas las averías presuntas y reales, así como de todo el mantenimiento preventivo y correctivo, mejorará el control.
		11.2.5 Remoción de activos	APLICADO	El equipo sensible no sale de la organización.
		11.2.6 Seguridad de equipos y activos fuera de las instalaciones	APLICAR	Controla el uso del equipo prestado y vigila la producción y el rendimiento.
		11.2.7 Disposición y reutilización segura de equipos	APLICADO	Cuando los equipos abandonados se ponen de nuevo en funcionamiento, se reformatean y se reinstalan. Aumente el control examinando los datos sensibles manejados por el equipo y determinando si es necesario otro método que haga imposible la recuperación de esos datos.
		11.2.8 Equipos de usuarios desatendidos	APLICAR	Mejorar el control del equipo en mal estado.
		11.2.9 Política de escritorio limpio y pantalla limpia	APLICAR	Así, se evitarán fugas de información no deseadas.

A.12	SEGURIDAD DE OPERACIONES			
A.12.1	**Procedimientos y responsabilidades operativas:** garantizar el funcionamiento seguro y preciso de las instalaciones de tratamiento de la información.	**12.1.1** Procedimientos operativos documentados	APLICAR	Algunos procedimientos de seguridad, sobre todo los que tienen mayores necesidades técnicas, deberán documentarse (copias de seguridad, mantenimiento de equipos, gestión de soportes, gestión y seguridad del correo, recuperación de sistemas).
		12.1.2 Gestión del cambio	APLICAR	Controlar los cambios realizados.
		12.1.3 Gestión de la capacidad	APLICAR	Por ejemplo, los sistemas más importantes utilizarán una línea dedicada.
		12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones	APLICAR	Para reducir los riesgos de acceso no autorizado o de cambios en los sistemas operativos, los entornos de desarrollo, de prueba y operativos estarán separados.
A.12.2	Protección contra códigos maliciosos	**12.2.1** Controles contra códigos maliciosos	APLICAR	Se puede acceder a un software antivirus obsoleto; es necesario educar y concienciar a los usuarios.
A.12.3	**Respaldo:** Proteger contra la pérdida de datos	**12.3.1** Respaldo de la información	APLICAR	Las copias de seguridad no se realizan. Establezca intervalos de prueba para la recuperación de copias de seguridad, el almacenamiento sin daños y la recuperación de desastres en el sitio primario para reforzar este control.
A.12.4	**Registros y monitoreos**: Registrar eventos y generar evidencias	**12.4.1** Registro de eventos	APLICAR	Es importante utilizar el registro de operadores y de fallos para garantizar que se encuentren los problemas del sistema de información.

		12.4.2 Protección de información de registros	APLICAR	Los datos de los registros deben estar protegidos contra posibles cambios y accesos ilícitos.
		12.4.3 Registro del administrador y del operador	APLICAR	Es necesario revisar y proteger los registros relativos a las operaciones del administrador y del operador del sistema.
		12.4.4 Sincronización del reloj	APLICAR	Para garantizar la integridad del registro de eventos y evitar errores de comunicación.
A.12.5	**Control de software operacional:** garantizar la integridad de los sistemas operacionales.	**12.5.1** Instalación de software en sistemas operacionales	APLICAR	Sin el conocimiento de las oficinas y del personal adecuado, las instalaciones no se llevan a cabo.
A.12.6	**Gestión de vulnerabilidad técnica:** Detener la explotación de los fallos técnicos	**12.6.1** Gestión de vulnerabilidades Técnicas	APLICAR	Las estaciones de trabajo de los usuarios y el servidor no tienen instalada ninguna actualización de seguridad.
		12.6.2 Restricción sobre la instalación de software	APLICAR	Los usuarios sólo deben tener permisos de instalación.
A.12.7	**Consideraciones para la auditoría de sistemas de información:** Reduzca la cantidad de esfuerzos de auditoría que afectarán a sus sistemas operativos.	**12.7.1** Controles de auditoría de sistemas de información	APLICAR	Planificar y llegar a un acuerdo sobre las normas y acciones de auditoría que implican la verificación de los sistemas operativos con el fin de limitar las interrupciones de los procesos relacionados con la empresa.
A.13	**SEGURIDAD DE LAS COMUNICACIONES**			
A.13.1	Gestión de la seguridad de la red	**13.1.1** Controles en la red	APLICAR	No se cuenta con un cortafuegos.

		13.1.2 Seguridad de servicios de red	APLICAR	Asegúrate de que los acuerdos de nivel de servicio se mencionan en el contrato y de que puedes confirmarlos con el proveedor.
		13.1.3 Segregación en redes	APLICAR	Para evitar accesos no deseados, las redes estarán divididas.
A.13.2	**Transferencia de información:** Garantizar la seguridad de la información que se intercambia tanto dentro como fuera de la empresa.	**13.2.1** Políticas y procedimientos de transferencia de la información	APLICAR	El tránsito de la información por las redes se protegerá mediante configuraciones.
		13.2.2 Acuerdo sobre transferencia de información	APLICAR	Deben firmarse contratos de intercambio con los proveedores.
		13.2.3 Mensajes electrónicos	APLICAR	NO hay salvaguardas integradas en los sistemas.
		13.2.4 Acuerdos de confidencialidad o no divulgación	APLICAR	Incluya cláusulas de confidencialidad en los acuerdos con contratistas y empleados.
A.14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**			
A.14.1	**Requisitos de seguridad de los SI:** Asegúrese de que, a lo largo de todo el ciclo de vida de los SI, la seguridad de la información es un componente clave.	**14.1.1** Análisis y especificación de requisitos de seguridad de la información	APLICAR	Deben incluirse requisitos técnicos de seguridad en el sistema para protegerlo de la invasión de programas maliciosos.
		14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas	APLICAR	Para frenar la intrusión de malware, el sistema debe cumplir ciertos requisitos de seguridad tecnológica.

		14.1.3 Protección de transacciones en servicios de aplicación	APLICAR	Basándose en el análisis de las pruebas de penetración más recientes, los sucesos actuales o recientes y las vulnerabilidades conocidas actualmente para detener los ataques en línea, proporcione un informe sobre el grado general de confianza de la dirección.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**: Asegúrese de que el ciclo de vida del desarrollo de los sistemas de información incluye el diseño y la aplicación de la seguridad de la información.	**14.2.1** Política de desarrollo seguro	NO APLICA	No existe desarrollo de SI.
		14.2.2 Procedimiento de control de cambio del sistema	NO APLICA	No existe desarrollo de SI.
		14.2.3 Revisión técnica de aplicaciones después de cambios a la plataforma operativa	NO APLICA	No existe desarrollo de SI.
		14.2.4 Restricciones sobre cambios a los paquetes de software	NO APLICA	No existe desarrollo de SI.
		14.2.5 Principios de ingeniería de sistemas seguros	NO APLICA	No existe desarrollo de SI.
		14.2.6 Ambiente de desarrollo seguro	NO APLICA	No existe desarrollo de SI.
		14.2.7 Desarrollo contratado externamente	NO APLICA	No se contrata desarrollo externo
		14.2.8 Pruebas de seguridad del sistema	NO APLICA	No existe desarrollo de SI.
		14.2.9 Pruebas de aceptación del sistema	NO APLICA	No existe desarrollo de SI.

A.14.3	**Datos de prueba**: Asegúrese de que los datos utilizados para las pruebas están protegidos.	**14.3.1** Protección de datos de prueba	NO APLICAR	No existe desarrollo de SI.
A.15	**RELACION CON LOS SUMINISTRADORES**			
A.15.1	**Seguridad de la información en las relaciones con los proveedores:** Asegúrese de que los activos de la empresa a los que pueden acceder los proveedores están protegidos.	**15.1.1** Política de seguridad de la información para las relaciones con los proveedores	NO APLICAR	Se cree que el gasto de poner este control sería mayor que la ganancia.
		15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores	APLICAR	Los contratos con los proveedores deben contener cláusulas de confidencialidad. Consulte otros temas relacionados con la seguridad.
		15.1.3 Cadena de suministro de tecnología de información y comunicaciones	APLICAR	Los problemas de seguridad de la información relacionados con la cadena de suministro de servicios y bienes de tecnología de la información y las comunicaciones deben abordarse en los acuerdos con los proveedores.
A.15.2	Gestión de entrega de servicios del proveedor	**15.2.1** Monitoreo y revisión de servicios de los proveedores	APLICAR	En caso de incumplimiento del servicio, establecer condiciones.
		15.2.2 Gestión de cambios a los servicios de proveedores	APLICAR	En caso de incumplimiento del servicio, establecer condiciones.
A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			

A.16.1	**Gestión de incidentes de seguridad de la información y mejoras:** Asegúrese de que la gestión de los incidentes de seguridad de la información se realiza de forma coherente y eficaz, y de que los incidentes y fallos de seguridad se comunican.	**16.1.1** Responsabilidades y procedimientos	APLICAR	La participación del personal en la gestión de incidentes es esencial.
		16.1.2 Reporte de eventos de seguridad de la información	APLICAR	Todos los problemas de seguridad deben documentarse para crear un historial de eventos o incidentes que pueda utilizarse posteriormente. Los procesos también deben mantenerse al día. Los procesos deben actualizarse.
		16.1.3 Reporte de debilidades de seguridad de la información	APLICAR	Todos los empleados deben recibir la suficiente formación por parte de la entidad para reconocer e informar de las vulnerabilidades del SGSI.
		16.1.4 Evaluación y decisión sobre eventos de seguridad de la información.	APLICAR	Es fundamental designar a una persona que se encargue de analizar las situaciones y elegir el curso de acción adecuado.
		16.1.5 Respuestas a incidentes de seguridad de la información	APLICAR	Para investigar los incidentes y registrarlos.
		16.1.6 Aprendizaje de los incidentes de seguridad de la información	APLICAR	Para detener los incidentes, mantenga un registro de incidentes y examínelo periódicamente.
		16.1.7 Recolección de evidencias	APLICAR	Llevar un registro de las incidencias y tareas realizadas.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**			

A.17.1	**Continuidad de seguridad de la información:** Los sistemas de gestión de la continuidad de la actividad deben incluir la seguridad de la información.	**17.1.1** planificación de continuidad de seguridad de la información	APLICAR	Es fundamental detectar los puntos débiles de la continuidad de la empresa.
		17.1.2 implementación de continuidad de seguridad de la información	APLICAR	Necesario para garantizar la continuidad del servicio.
		17.1.3 verificación, revisión y evaluación de continuidad de seguridad de la información	APLICAR	Necesarios para garantizar el cumplimiento del plan y la mejora continua.
A.17.2	**Redundancias: G**arantizar la accesibilidad a los recursos y al tratamiento de datos	**17.2.1** Instalaciones de procesamiento de la información	NO APLICAR	Ahora no se considera necesario porque los costes son mayores que los beneficios.
A.18	**CUMPLIMIENTO**			
A.18.1	**Cumplimiento con requisitos legales y contractuales:** Evitar la violación de cualquier obligación legal, legislativa, reglamentaria o contractual relacionada con la seguridad de la información.	**18.1.1** Identificación de requisitos contractuales y de legislación aplicables	APLICAR	Es necesario determinar las leyes que se aplican a la organización.
		18.1.2 Derechos de propiedad intelectual	APLICAR	Crear directrices de seguridad para cumplir la ley de protección de la información personal.

		18.1.3 Protección de registros	APLICAR	Deben utilizarse mecanismos de seguridad, tanto lógicos como físicos, para salvaguardar los registros. La empresa debe establecer políticas y procedimientos que especifiquen el tiempo que conservará los datos.
		18.1.4 Privacidad y protección de datos personales	APLICAR	En cumplimiento de la ley de protección de datos personales, se debe diseñar un método para el manejo adecuado de la información personal que se mantiene en la organización.
		18.1.5 Regulación de controles criptográficos	APLICAR	Una directiva gubernamental conocida como 007-95INEI-SJI establece que los datos sensibles deben ser encriptados para mantener su integridad y secreto (Recomendaciones Técnicas para la Seguridad e Integridad de la Información tratada en la Administración Pública.) En la Administración Pública, los datos procesados).
A.18.2	**Revisiones de seguridad de la información:** Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.	**18.2.1** Revisión independiente de la seguridad de la información	APLICAR	Deben programarse revisiones de la estrategia de gestión e implementación de la seguridad de la información de la organización (objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información).
		18.2.2 Cumplimiento de políticas y normas de seguridad	APLICAR	Las auditorías determinarán si se siguen las políticas, los procedimientos y las normas.
		18.2.3 Revisión del cumplimiento técnico	APLICAR	Establezca una estrategia de revisión de la SI y compruebe si cumple con los requisitos y la normativa de seguridad de la organización.

ANEXO Q: Propuesta de políticas de seguridad

SECCION	DOMINIO	CONTROL	PROPUESTA DE TESISTAS
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACION**		
	Objetivo: Especificar las políticas de gestión de la seguridad de la información de acuerdo con las necesidades corporativas, los requisitos legales y la normativa.		
A.5.1	**5.1.1.** Políticas de seguridad de la información	APLICAR	**I.** El papel de la dirección general de la municipalidad será aprobar la política de seguridad y cualquier cambio futuro, que deberá ser divulgado a todos los miembros del personal interno y a las partes externas pertinentes.
	5.1.2. Revisión de políticas para la seguridad de la información	APLICAR	**I.** El Comité de Gestión de la Seguridad de la Información revisará esta política una vez al año para asegurarse de que está actualizada y garantizar su eficacia.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**		
	Objetivo: Crear una estrategia de gestión para el inicio, la supervisión y el funcionamiento de la seguridad de la información en la organización.		
A.6.1	**6.1.1** Roles y responsabilidades en seguridad de la información	APLICAR	**I.** La responsabilidad de definir y firmar las responsabilidades de seguridad de la información recae en el comité de seguridad de la información.
	6.1.2 Segregación de funciones	APLICAR	**I.** Para reducir el potencial de cambios ilegales o involuntarios o el mal uso de los activos de la organización, deben separarse las funciones y áreas de responsabilidad conflictivas.
	6.1.3 Contacto con autoridades	APLICAR	**I.** Manténgase en contacto con las autoridades competentes cuando sea necesario.
	6.1.4 Contacto con grupos especiales de interés	APLICAR	**I.** Manténgase en contacto con grupos de interés particulares y profesionales de la seguridad de la información.
	6.1.5 Seguridad de información en la gestión de proyectos	APLICAR	**I.** Independientemente del tipo de proyecto, la seguridad de la información debe tenerse en cuenta durante la gestión del mismo.

A.6.2	**6.2.1** Política de dispositivos móviles	APLICAR	**I.** Salvo autorización previa del máximo responsable del área correspondiente a la subárea y el correspondiente registro por parte del responsable de informática, se prohíbe el uso de portátiles, USBs o cualquier otro equipo propiedad del usuario como herramienta de trabajo. Este control pretende evitar que el usuario transfiera datos a su propio portátil, que la empresa considera "limitados". **II.** Es obligación del Usuario utilizar adecuadamente los CD, USB y otros dispositivos de almacenamiento. Queda expresamente prohibido que el Usuario utilice dispositivos externos como USBs u otros dispositivos de almacenamiento que hayan sido previamente utilizados en ordenadores que estén en público o puedan ser utilizados de forma inadvertida, como los que se encuentran en centros educativos, en Internet o incluso en su propio ordenador personal, sin que antes sean debidamente revisados por el antivirus corporativo para comprobar posibles amenazas de virus. **III.** Para asegurar la información propiedad de la entidad que se guarda o conserva en el ordenador portátil del usuario cuando éste lo utiliza con fines personales, se deben seguir las siguientes pautas fundamentales: - Cifrar los datos del portátil para evitar el acceso en caso de robo del dispositivo. - Antes de salir, haga una copia de seguridad de los datos. **IV.** Todos los empleados que utilicen dispositivos inalámbricos de propiedad municipal para el desempeño de sus funciones, como teléfonos móviles, tabletas, etc., están obligados a utilizar una contraseña de acceso y la prohibición automática de dichos dispositivos como medidas de seguridad. Si no lo hacen, se aplicarán las sanciones correspondientes. **V.** Es obligación del usuario realizar periódicamente una copia de seguridad de los datos de los dispositivos móviles o portátiles asignados para evitar su pérdida por robo, extravío, daño del dispositivo o cualquier otro suceso.
	6.2.2 Teletrabajo	APLICAR	**I.** Antes de empezar a teletrabajar, los empleados deben recibir formación sobre ciberseguridad para estar informados de las normas. **II.** A la hora de trabajar de forma remota, debes seleccionar los dispositivos corporativos que te proporciona la organización, ya que cuentan con la configuración que la entidad considera necesaria y tienen el software instalado para permitirte realizar el trabajo de forma segura.
A.7	**SEGURIDAD DEL RECURSO HUMANO**		

A.7.1	**7.1.1** Investigación de antecedentes	APLICADO	**I.** Todos los solicitantes de empleo deben someterse a una comprobación de sus antecedentes en cumplimiento de todas las leyes, normas y principios morales aplicables. **II.** Los requisitos del puesto, la clasificación del material al que se va a acceder y los riesgos previstos deben tenerse en cuenta a la hora de comprobar los antecedentes de los posibles trabajadores.
	7.1.2 Términos y condiciones de empleo	APLICADO	**I.** Se debe proporcionar una copia digital de las políticas cuando se contrate a un nuevo empleado o se utilice el servicio de un tercero para que tenga una referencia de cómo desarrollar su trabajo. **II.** Es importante informar a los miembros del personal de las implicaciones de seguridad de sus funciones.
A.7.2	**7.2.1** Responsabilidades de la gerencia	APLICAR	**I.** El responsable de TI debe asegurarse de que la cuenta de acceso del usuario del ordenador se actualiza para el personal entrante cuando se le informa de un despido o traslado.
	7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	APLICAR	**I.** El trabajo del director de TI es enfatizar constantemente el valor de la seguridad a todos los usuarios del sistema de información. **II**. El programa de concienciación sobre la seguridad debe incluir actualizaciones y charlas continuas. Además, se pueden utilizar diversas técnicas, como carteles, avisos, ppts y vídeos de seguridad de la información, para recordar constantemente a los usuarios su contribución crucial a la seguridad de la información, así como la forma correcta de utilizar los equipos.
	7.2.3 Proceso disciplinario	APLICAR	**I.** Se aplicarán sanciones administrativas y legales en caso de violación de la información restringida, incluida la destitución del cargo y la posterior expulsión de la entidad. - Castigo por violar una de las políticas de seguridad de acuerdo con los términos del contrato. -Otras en función de la gravedad del incidente.
A.7.3	**7.3.1** Responsabilidades ante la finalización o cambio de empleo	APLICAR	**I.** Protección de la información El empleado o contratista debe ser informado de las obligaciones y deberes que persisten después de la terminación o de un cambio de empleo. Es importante definir, notificar e imponer cualquier cambio en el empleo de un empleado o contratista. e impuestas.
A.8	**GESTION DE ACTIVOS**		
	Objetivo: Lograr y mantener la protección apropiada de los activos de la organización		
A.8.1	**8.1.1** Inventario de activos	APLICADO	**I.** La organización debe crear y mantener un inventario de sus activos, tanto materiales como inmateriales. Según las mejores prácticas, la institución debe mantener dos inventarios: uno para sus activos generales y otro para su hardware y software. El gerente de TI y una persona designada por la Oficina de Tecnología de la Información son conjuntamente responsables de mantener el inventario.

	8.1.2 Propiedad de los activos	APLICAR	**I.** Cada activo debe ser categorizado con precisión, asignado a un propietario y con su ubicación actual.
	8.1.3 Uso aceptable de los activos	APLICAR	**I.** Junto con el personal de informática, cada subdivisión de la empresa se encargará de actualizar el inventario de activos. **II.** En el caso de los activos importantes, la entidad debe especificar y reevaluar periódicamente los límites de acceso y la clasificación de los activos. **III.** La corporación debe poner en marcha un programa de formación para el personal de todos los departamentos con el fin de garantizar que conozcan y utilicen adecuadamente los activos identificados.
	8.1.4 Retorno de activos	APLICAR	**I.** Los ordenadores portátiles, los datos, el papeleo, los manuales y cualquier otro bien suministrado al empleado deben ser devueltos al supervisor inmediato con el pago correspondiente.
A.8.2	**8.2.1** Clasificación de la información	APLICAR	**I.** De acuerdo a la relevancia de la información, es importante categorizar la información de la entidad en base a los requerimientos legales y de valor. Las etiquetas asignadas son Restringida, Uso interno y General, de acuerdo con la norma peruana NTP-ISO/IEC 27001:2014. **II.** Sólo el propietario de la información puede modificar la clasificación otorgada a un determinado tipo de información tras justificar legalmente el cambio. **III.** Independientemente del formato, la información que existe en varios soportes (físicos o lógicos) debe clasificarse de la misma manera. **IV.** Todos los trabajadores de la entidad, internos y externos, deben estar familiarizados con las directrices de etiquetado.

	8.2.2 Etiquetado de la información	APLICAR	**I.** Los dispositivos de almacenamiento de medios digitales, como los CD, las unidades USB, los dispositivos de memoria portátiles, etc., deben llevar etiquetas con las clasificaciones adecuadas. Deben establecerse controles para evitar situaciones como la divulgación, la modificación, la eliminación o la destrucción no autorizadas de la información. **II.** Cualquier medio electrónico dentro del municipio puede ser utilizado para almacenar información en formato digital que sea categorizada como "General" (información para consulta, información sobre formación laboral, notas informativas, etc.). Pero hay que tomar precauciones para evitar que se combine información "General" con información de otro grupo (Restringida o de uso interno). **III.** Antes de enviar información "restringida" a un destinatario, el responsable informático debe confirmar que esa persona está autorizada (no repudio). Los remitentes o receptores pueden utilizar la función de no repudio para impedir que la parte contraria impugne una comunicación transmitida. **IV.** Cuando se almacena información "restringida" en formato digital en cualquier soporte, el método de encriptación debe ser aprobado por el responsable informático. Uno de estos métodos consiste en comprimir la información mediante la aplicación WinRAR y proporcionar una clave para su descompresión (CDs, Memory sticks, etc.). **V.** Cualquier comunicación de datos marcados como "Restringidos" o "Uso interno" a o a través de redes ajenas a la Institución requiere el consentimiento previo por escrito de la entidad y la utilización de un canal de transmisión seguro, en este caso el correo institucional. El envío de información con la categoría "General" es suficiente sin la necesaria autorización. **VI**. Todo documento digital debe mostrar la categorización adecuada, indicando si es "Restringido", "Uso interno" o "General", en la parte superior (cabecera) e inferior (pie de página) de cada página.
	8.2.3 Manejo de activos	APLICAR	**I.** Los empleados que están a cargo de los bienes del municipio deben utilizarlos adecuadamente y gestionar o proporcionar el mantenimiento necesario para su conservación.
A.8.3	**8.3.1** Gestión de medios removibles	APLICAR	**I.** Excepto en los ordenadores en los que se prohíbe el acceso físico o si se implementa un software de seguridad y se gestiona suficientemente el acceso a la máquina y su contenido, los discos duros no deberían almacenar datos sensibles.
	8.3.2 Disposición de medios	APLICAR	**I.** Cuando los recursos ya no son necesarios, deben ser eliminados adecuadamente de acuerdo con los protocolos establecidos.
	8.3.3 Transferencia de medios físicos	APLICAR	**I.** Los soportes de información deben estar protegidos del acceso ilegal, el abuso y la corrupción durante el transporte. uso o manipulación durante el transporte
A.9	**CONTROL DE ACCESO**		
	Objetivo: Garantizar que la información reciba un nivel de protección adecuado en función de su importancia para la organización.		

A.9.1	**9.1.1** Política de control de acceso	APLICAR	**I.** A través de una cuenta de usuario local, el sistema operativo, cada usuario debe autenticarse para acceder a su máquina de estación de trabajo. Este requisito de identidad se estrena con Windows 10. **II.** Cada usuario de un sistema debe tener su propia cuenta de usuario de PC. **III.** Cuando un empleado es despedido o transferido, debe implementarse un proceso para asegurarse de que su cuenta de usuario sea cerrada. **IV**. La inactividad en los ordenadores portátiles personales debería provocar el bloqueo después de quince (15) minutos. Antes de continuar su actividad, el usuario deberá autenticarse. **V.** Todas las plataformas, estaciones de trabajo, ordenadores personales, etc., deben disponer de características y funcionalidades de seguridad del terminal que deben ser utilizadas correctamente por el usuario, quien además debe cerrar la sesión o bloquear el puesto de trabajo cuando lo deje desatendido. **VI.** Cada usuario es responsable del uso y la conservación de su contraseña con respecto al "inicio de sesión" en su puesto de trabajo, por lo que es crucial que todos los empleados la mantengan segura. **VII.** Las contraseñas sólo deben ser reveladas a otros usuarios a petición de su supervisor inmediato y después de recibir el permiso del encargado de TI. La próxima vez que se registre, deberá cambiar su contraseña si ha sido revelada. **VIII.** El usuario autorizado es responsable de todas las acciones realizadas por cualquier persona a la que se le haya comunicado la contraseña o la identificación de usuario. **IX.** Cuando se almacenan o envían a través de las redes, las contraseñas deben estar siempre encriptadas.
	9.1.2 Acceso a redes y servicios de red	APLICAR	**I.** Todas y cada una de las conexiones a una red o dispositivo externo requieren la aprobación del responsable de TI. **II.** El esquema de direccionamiento interno de la red no debe ser accesible a los ordenadores u otras redes del exterior. Esto impide que los "hackers" u otras personas adquieran simplemente datos sobre la arquitectura de la red del municipio y los ordenadores internos.
A.9.2	**9.2.1** Registro y baja de usuarios	APLICAR	**I.** Sin la autorización requerida y de acuerdo con los lineamientos del formulario aplicable para este fin, denominado "FORMULARIO PARA LA PRESENTACIÓN, REMOCIÓN Y CAMBIO DE PERSONAL EN LOS SISTEMAS INFORMÁTICOS", ningún usuario podrá ser removido de la municipalidad.

	9.2.2 Aprovisionamiento de acceso a usuario	APLICADO	**I.** El jefe inmediato debe notificar al Departamento de TI mediante el formulario LOGIN FORM dos días antes de que un usuario abandone la empresa de forma permanente o cambie de puesto para que se puedan ajustar, eliminar los niveles de acceso y seguridad del usuario o realizar una copia de seguridad de los archivos. Con dos días de antelación, para dar tiempo a que se realicen copias de seguridad de los archivos, se modifiquen o se eliminen sus niveles de acceso y seguridad.
	9.2.3 Gestión de derechos de acceso privilegiados	APLICAR	**I.** Sólo se debe dar acceso a la información necesaria para que los usuarios ejecuten sus responsabilidades.
	9.2.4 Gestión de información de autentificación secreta de usuarios	APLICAR	**I.** El director de cada área de usuarios es el encargado de enviar al responsable de informática la "Solicitud de usuarios y/o perfiles de acceso a los sistemas informáticos" para asignar las cuentas de usuario a los puestos de trabajo. A continuación, el responsable de informática creará los usuarios y contraseñas necesarios y los enviará al departamento de recursos humanos, que los entregará al usuario final con la confidencialidad necesaria.
	9.2.5 Revisión de los derechos de acceso de usuarios.	APLICAR	**I.** De vez en cuando, los empleados deben comprobar si tienen los privilegios adecuados para el trabajo. .
	9.2.6 Remoción o ajuste de derechos de acceso	APLICAR	**I.** Todos los privilegios de acceso a la información y a las instalaciones de procesamiento de la información de los trabajadores y de los usuarios de terceros deben ser cancelados al finalizar su empleo, contrato o acuerdo, o modificados para reflejar el cambio.
A.9.3	**9.3.1** Uso de información de autentificación secreta	APLICAR	**I.** De acuerdo con el manual de funciones establecido para cada puesto de trabajo dentro de la entidad, todos los equipos informáticos que posea la entidad sólo se utilizarán para las tareas asociadas al puesto del usuario. **II.** El empleado que recibió un ID de usuario es responsable de todas las acciones realizadas con ese ID. Los usuarios no deben divulgar la información de su ID de usuario a terceros ni permitir que otros empleados la utilicen para ningún fin.
A.9.4	**9.4.1** Restricción de acceso a la información	APLICAR	**I.** El responsable de TI debe asegurarse de que los privilegios de acceso de cada usuario se ajustan a lo necesario para la correcta ejecución de sus tareas dentro de la organización.
	9.4.2 Procedimientos de ingreso seguro	APLICADO	**I.** Se debe comprobar que la conexión sea segura por parte del personal. **II.** El acceso a sitios web de riesgo no es recomendable para los empleados. **III.** Debe extremar las precauciones cuando descargue programas o archivos gratuitos de Internet.
	9.4.3 Sistema de gestión de contraseñas	APLICAR	**I.** El director de cada área de usuarios es el encargado de enviar al responsable de informática la "Solicitud de usuarios y/o perfiles de acceso a los sistemas informáticos" para asignar las cuentas de usuario a los puestos de trabajo. A continuación, el responsable de informática creará los usuarios y contraseñas correspondientes y los enviará al departamento de

			recursos humanos, que los entregará al usuario final con la confidencialidad necesaria.
	9.4.4 Uso de programas utilitarios privilegiados	APLICAR	**I.** Los programas informáticos que se coloquen en los ordenadores deben estar autorizados, ser legales y estar inventariados regularmente. En los ordenadores sólo se instalarán programas informáticos autorizados o adquiridos por la institución. **II.** Los programas de juegos gratuitos o de propiedad privada no pueden ser instalados o utilizados de ninguna manera.
A.10	**CRIPTOGRAFIA**		
	Objetivo: Garantizar la aplicación adecuada y eficiente de la criptografía para salvaguardar la confidencialidad, autenticidad e integridad de los datos.		
A.10.1	**10.1.1** Política sobre el uso de controles criptográficos	APLICAR	**I.** Cada contraseña debe tener al menos ocho (8) caracteres y no puede tener espacios vacíos. **II.** Las contraseñas deben ser difíciles de descifrar. Evite utilizar combinaciones de caracteres populares como "12345678" o "ABCDEFG", así como frases de diccionario e identidades de usuario. **III.** Sólo cuando se combina con otros personajes que no tienen relación entre sí, se debe utilizar información personal como los nombres de los miembros de la familia, los números de identificación, los números de teléfono o los cumpleaños. **IV.** Se requiere al menos un carácter no alfanumérico en las contraseñas. En las contraseñas se debe incluir como mínimo un carácter alfabético en mayúscula y otro en minúscula. letra alfabética en mayúscula y otra en minúscula.
	10.1.2 Gestión de claves	APLICAR	**I.** Todas las contraseñas deben caducar en un plazo que no supere los 150 días. **II.** Al menos una vez al mes, los usuarios no deberían poder restablecer sus contraseñas. **III.** En el punto de gestión de contraseñas, se debe documentar una excepción a la política que detalle la viabilidad de cambiar la aplicación para soportar las características establecidas para las contraseñas, en los casos en que los sistemas utilizados no soporten los controles de las características establecidas para la estructura, validez, reutilización e intentos fallidos de inicio de sesión.
A.11	**SEGURIDAD FISICA Y AMBIENTAL**		
	Objetivo: Proteger la información de la organización y las instalaciones de procesamiento de información de intrusiones físicas, daños e interferencias.		
A.11.1	**11.1.1** Perímetro de seguridad física	APLICAR	**I.** Aplicar medidas de seguridad para proteger las instalaciones de propiedad municipal, que contienen bienes valiosos. **II.** Sólo debe permitirse el acceso a las instalaciones al personal autorizado y/o con permiso de la alta dirección.

	11.1.2 Controles de ingreso físico	APLICAR	**I.** La integridad de los edificios y de los ordenadores de cada puesto de trabajo de la entidad debe garantizarse mediante la aplicación de medidas de seguridad física. **II.** El nivel de clasificación de los activos y el valor de la información procesada y conservada en las instalaciones deben tenerse en cuenta a la hora de diseñar las medidas de protección. **III.** Cualquier edificio u oficina sólo debe permitir el acceso a los trabajadores autorizados o a los ciudadanos que hayan sido previamente identificados. **IV**. Todas las consultas del público que necesiten ser admitidas en la entidad deben ser identificadas con exactitud utilizando los datos del DNI de la persona, y se debe conservar un registro escrito junto con la fecha y la hora. Esta información también debe conservarse en un registro escrito y guardarse en un archivo Excel para su futuro control. **V.** Aunque no se utiliza actualmente, el sistema de control biométrico de la entidad debería ponerse en marcha y utilizarse para salvaguardar las instalaciones. **VI.** Sólo las personas a las que se les ha permitido previamente acceder a los ordenadores de las oficinas que contienen datos sensibles o tienen acceso al equipo router que ofrece conexión a Internet.
	11.1.3 Asegurar oficinas, áreas e instalaciones	APLICAR	**I.** El personal responsable de cada oficina debe asegurar las puertas al momento de retirarse y entregar las llaves al personal de seguridad. **II.** Las llaves de cada oficina no debe salir de la municipalidad. **III.** El personal de limpieza solo debe realizar su trabajo si está presente el responsable de cada ofician o el personal de seguridad.
	11.1.4 Protección contra amenazas externas y ambientales	APLICADO	**I.** Debe existir un plan de contingencia de desastres naturales. **II.** Elaborar capacitaciones al personal en cómo actuar al momento de que existan amenazas externas y ambientales.
	11.1.5 Trabajo en áreas seguras	APLICAR	**I.** Es necesario diseñar y aplicar los procedimientos para trabajar en zonas seguras.
	11.1.6 Áreas de despacho y carga	APLICADO	**I.** Todas las consultas del público que necesiten ser admitidas en la entidad deben ser identificadas con exactitud utilizando los datos de la tarjeta de identificación de la persona, y se debe conservar un registro escrito junto con la fecha y la hora. Esta información también debe conservarse en un registro escrito y guardarse en un archivo Excel para su futuro control.
A.11.2	**11.2.1** Emplazamiento y protección de los equipos	APLICADO	**I.** Hay que vigilar la transferencia de información desde estos equipos, y los soportes de almacenamiento, incluidos los discos duros de los ordenadores, que contengan información marcada como "Restringida", deben colocarse en una zona concreta autorizada por el responsable de informática.

	11.2.2 Servicios de suministro	APLICAR	I. En el caso de estar conectado a un ordenador, normalmente se le añaden componentes adicionales (teclados, ratones, grabadoras, discos duros, luces, etc.) que acabarán requiriendo energía para su funcionamiento, por lo que es fundamental que la fuente de alimentación tenga una potencia idónea que le permita trabajar de forma más cómoda. Por ello, si la potencia es insuficiente, es probable que se produzca un fallo en alguno de los dispositivos, impidiendo su funcionamiento porque no le llega la energía necesaria.
	11.2.3 Seguridad del cableado	APLICADO	**I.** Los cables deben mantenerse limpios, en buen estado y enlazados correctamente. Nunca hay que dejar que se doblen, y no debe haber ningún tipo de tensión. **II.** Las instalaciones eléctricas en los edificios deben cumplir con las normas o reglas, según la Norma Técnica Peruana NTP 370.301:2002. **III.** Hay que examinar el cableado de la red para asegurarse de que cumple los requisitos y es del calibre adecuado, a menudo CAT5 o CAT6. Se recomienda canalizar el cableado de la red o incorporarlo a la construcción del municipio para evitar cualquier seccionamiento.
	11.2.4 Mantenimiento de equipos	APLICADO	**I.** Los programas informáticos que se coloquen en los ordenadores deben estar autorizados, ser legales y estar inventariados regularmente. En los ordenadores sólo se instalarán programas informáticos autorizados o adquiridos por la institución. **II**. Los programas de juegos gratuitos o de propiedad privada no pueden ser instalados o utilizados de ninguna manera.
	11.2.5 Remoción de activos	APLICAR	**I.** El responsable informático del municipio es el encargado de verificar y ejecutar las transferencias o asignaciones de equipos, así como la demanda.
	11.2.6 Seguridad de equipos y activos fuera de las instalaciones	APLICAR	**I.** Sin el consentimiento del personal responsable y de la alta dirección, ningún equipo debe salir de la municipalidad.
	11.2.7 Disposición y reutilización segura de equipos	APLICADO	**I.** Cualquier alteración o transferencia debe ser solicitada previamente por la Subárea designada por el usuario. Es obligación del usuario utilizar adecuadamente el equipo informático y los programas cargados en él. El usuario debe confirmar que los miembros del personal informático instalaron o eliminaron programas, así como cambiaron o transfirieron cualquier equipo informático que se les entregó.
	11.2.8 Equipos de usuarios desatendidos	APLICAR	**I.** Los empleados de la municipalidad son responsables de garantizar que los equipos desatendidos estén debidamente protegidos.

	11.2.9 Política de escritorio limpio y pantalla limpia	APLICAR	**I.** El responsable del departamento de informática se encarga del mantenimiento preventivo y correctivo de los equipos. II. Los empleados están obligados a bloquear sus sesiones de ordenador siempre que abandonen su puesto de trabajo. **III.** El equipo de seguridad de la información debe definir un cierre de sesión por inactividad para todos los ordenadores y dispositivos móviles. Cuando se disponga de un salvapantallas protegido por contraseña, se aconseja configurar los ordenadores con uno cuando estén inactivos durante más de 15 minutos. **IV.** El usuario tiene la obligación de proteger el hardware siguiendo las siguientes directrices básicas: - Evite comer o beber cerca, sobre o cerca del Hardware. - Evite amontonar objetos pesados encima del Hardware. - Mantenga todos los dispositivos electromagnéticos, como imanes, teléfonos, radios, etc., lejos del hardware. - Evite colocar el hardware en zonas en las que pueda ser volcado accidentalmente, expuesto a caídas o destruido parcial o totalmente. - Evite retirar el hardware. Si es necesario, el responsable informático se encargará de esta labor. - Es obligación de los usuarios mantener en todo momento el orden en su espacio de trabajo y en los equipos asignados.
A.12	**SEGURIDAD DE OPERACIONES**		
	Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.		
A.12.1	**12.1.1** Procedimientos operativos documentados	APLICAR	**I.** El director de cada área de usuarios es el encargado de enviar al responsable de informática la "Solicitud de usuarios y/o perfiles de acceso a los sistemas informáticos" para asignar las cuentas de usuario a los puestos de trabajo. A continuación, el responsable de informática creará los usuarios y contraseñas necesarios y los enviará al departamento de recursos humanos, que los entregará al usuario final con la confidencialidad necesaria.
A.12.3	**12.3.1** Respaldo de la información	APLICAR	**I.** Las copias de seguridad de la institución deben ser creadas por el responsable informático, ya sea en soporte físico o en la nube, y el personal debe ser instruido para ello. **II.** Es importante especificar adecuadamente los procesos de realización de copias de seguridad y de recuperación de las mismas. **III.** Para aumentar la capacidad de restaurar los datos en caso de un incidente imprevisto, se deben realizar pruebas cada dos meses para confirmar el buen funcionamiento de los archivos almacenados, así como el funcionamiento de las memorias USB. **IV.** Los usuarios deben crear copias de seguridad de la información restringida y almacenarla al mismo tiempo en un pendrive designado sólo para ese tipo de información, moviendo los archivos a la carpeta personal que el responsable de TI haya creado por ese motivo.

A.12.5	**12.5.1** Instalación de software en sistemas operacionales	APLICAR	**I.** Los empleados de la institución deben utilizar únicamente los programas incluidos en su plataforma estándar y cuyas licencias hayan sido adquiridas por la institución. **II.** No se podrá descargar e instalar software adicional al requerido para el crecimiento de las actividades del usuario de la red dentro de la institución, y el usuario de la red no podrá utilizarlo para acceder a sitios de redes sociales o páginas web que no sean necesarias para el crecimiento de sus actividades. **III.** Para ello, se aconseja realizar las siguientes acciones. Todos los usuarios que no sean administradores de equipos tendrán impedida la instalación de apps de cualquier origen en los equipos de la entidad. - Utilizando el atajo de teclado Win+R, lanzamos una ventana de ejecución de Windows. - Entramos o pulsamos OK después de escribir gpedit.msc. - A continuación, visitamos Configuración del equipo. - Entramos en Plantillas administrativas. - Después, en Componentes de Windows - A continuación, decidimos utilizar el Instalador de Windows. - Elegimos Prohibir instalaciones de usuario en el panel derecho. Seleccionamos la casilla Habilitado. Salimos del editor.
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
	Objetivo: Evitar el acceso no autorizado a las redes.		
A.13.1	**13.1.1** Controles en la red	APLICAR	**I.** Un cortafuegos debe encargarse de todas las conexiones realizadas entre la red interna del municipio -que incluye tanto la red física como la inalámbrica- e Internet para evitar accesos no deseados.
	13.1.2 Seguridad de servicios de red	APLICAR	**II.** Todas las conexiones de red internas y externas, ya sean realizadas a través de cableado o de un punto de acceso, deben estar protegidas por contraseña para poder ser utilizadas. También deben cumplir con los estándares de la Institución para los servicios de red y el control de acceso. El responsable de TI debe evaluar si los servicios son óptimos o crear normas para el nivel de suficiencia que requiere la entidad.
A.14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
	Objetivo: A lo largo de cada etapa del ciclo de vida de un sistema de información, asegúrese de que la seguridad de la información es un componente fundamental. Esto también abarca las especificaciones de los sistemas informáticos que prestan servicios a través de redes abiertas.		
A.14.1	**14.1.1** Análisis y especificación de requisitos de seguridad de la información	APLICAR	**I.** El personal especializado en sistemas de la universidad analizará cualquier software de aplicación de terceros antes de contratarlo para ver si cumple con los criterios institucionales y de seguridad.
	14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas	APLICAR	**I.** Se confirmará que el desarrollo de software de aplicación de los grupos o proyectos de investigación institucionales se encuentra bajo el paraguas del desarrollo de software, multimedia o herramientas de instrucción para los que la universidad tiene acuerdos de licencia.

	14.1.3 Protección de transacciones en servicios de aplicación	APLICAR	**I.** Implementará conexiones seguras para los usuarios para el software de aplicación que necesita credenciales de acceso.
A.15	**RELACION CON LOS PROVEEDORES**		
	Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores		
	15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores	APLICAR	**I.** medidas de seguridad obligatorias. Debemos determinar los controles de seguridad que consideramos necesarios para garantizar la contratación de un servicio externo seguro. de obligado cumplimiento.
	15.1.3 Cadena de suministro de tecnología de información y comunicaciones	APLICAR	**I. M**edidas de seguridad obligatorias. Debemos determinar los controles de seguridad que consideramos necesarios para garantizar la contratación de un servicio externo seguro. de obligado cumplimiento. Estos controles deben tener en cuenta los siguientes factores - Los componentes y servicios informáticos a los que la organización permite acceder - cómo manejar cualquier situación que implique el acceso de los proveedores a nuestros sistemas.
A.15.2	**15.2.1** Monitoreo y revisión de servicios de los proveedores	APLICAR	**I.** Control y auditoría de los servicios contratados. Debemos crear un sistema para controlar, evaluar y auditar el servicio prestado por sus proveedores en materia de ciberseguridad si queremos prestar de forma constante el servicio contratado con el máximo nivel de calidad posible. Debemos decidir cómo manejar cualquier problema que pueda ocurrir con los bienes o servicios de nuestros proveedores. Estos procedimientos se utilizarán en toda la cadena de suministro.
A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		
	Objetivo:		
A.16.1	**16.1.1** Responsabilidades y procedimientos	APLICAR	**II.** Los empleados están obligados a alertar al responsable de informática si descubren o sospechan que se ha producido un incidente de seguridad. **II.** El responsable de TI debe llevar un registro de todos los informes de incidentes de seguridad.
	16.1.2 Reporte de eventos de seguridad de la información	APLICAR	**I.** Si un empleado descubre una vulnerabilidad (por ejemplo, que el software antivirus está desactualizado, que el software de la oficina no está correctamente activado, etc.), debe alertar al responsable de informática de ello.

	16.1.3 Reporte de debilidades de seguridad de la información	APLICAR	**I.** El gestor informático se encargará de eliminar el virus o evento advertido si un usuario sospecha de la presencia de un virus en un sistema y lo notifica al gestor. **II.** Todos los fallos y averías en el tratamiento de la información -en este caso, el sitio web de la entidad- o en los sistemas de comunicación deben ser documentados por las personas encargadas de la gestión de los sistemas de información, que deben alertar al administrador de la red. La estructura para documentar un fallo es la siguiente: En el caso del municipio, la dirección debe pensar en contratar a un profesional de la red, que desempeñe el papel de gestor de la red: Nombre y cargo de la persona que informa del error, hora y fecha de ocurrencia del fallo, Descripción del error o problema. **III.** Antes de volver a conectar el equipo a la red de datos, el responsable informático debe asegurarse de que el virus ha sido totalmente eliminado del sistema.
	16.1.4 Evaluación y decisión sobre eventos de seguridad de la información.	APLICAR	**I.** Los registros de fallos deben guardarse en archivos de Excel para que puedan ser controlados posteriormente para auditorías en el futuro. **II.** Los registros de fallos deben examinarse una vez a la semana. **III.** Los registros de los problemas no resueltos deben mantenerse abiertos hasta que se identifique una solución; este plazo no debe superar los dos días laborables. Si el problema sigue sin resolverse, debe informarse al departamento de TI del municipio. Estos registros también deben conservarse para una futura verificación independiente.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**		
	Objetivo:		
A.17.1	**17.1.1** planificación de continuidad de seguridad de la información	APLICAR	I. El comité de aplicación debe decidir lo que es necesario para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones de emergencia o catástrofe, por ejemplo. Ante circunstancias difíciles, como una crisis o una tragedia, el comité de aplicación debe decidir lo que es necesario para la seguridad de la información y la continuidad de la gestión de la seguridad de la información.
	17.1.2 implementación de continuidad de seguridad de la información	APLICAR	**I.** El comité de implementación es responsable de establecer, implementar y mantener los procesos, procedimientos y controles necesarios para mantener el grado requerido de seguridad de la información en caso de crisis.
	17.1.3 verificación, revisión y evaluación de continuidad de seguridad de la información	APLICAR	**I.** La continuidad del plan de seguridad debe ser verificada en intervalos de tiempos cortos por el comité de implementación.
A.18	**CUMPLIMIENTO**		
	Objetivo: Prevenir las violaciones de las obligaciones legales, estatutarias y reglamentarias relacionadas con la seguridad de la información.		

A.18.1	**18.1.1** Identificación de requisitos contractuales y de legislación aplicables	APLICAR	**I.** Para sustentar la metodología de estas políticas de seguridad se utilizó el siguiente fundamento legal: - Resolución Nº 458-2008-CG de la Contraloría General de la República, denominada "Guía para la implementación del sistema de control interno de las entidades del Estado." - Resolución Ministerial Nº 004-2016-PCM que aprueba la NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. 2da. Edición como norma requerida en el Perú.
	18.1.4 Privacidad y protección de datos personales	APLICAR	**I.** Los controles de acceso ayudan a limitar la probabilidad de acceso ilegal. La información manejada por los sistemas de información y las redes conexas debe protegerse eficazmente contra la alteración, divulgación o destrucción no autorizadas.
A.18.2	**18.2.1** Revisión independiente de la seguridad de la información	APLICAR	**I.** La NTP ISO/IEC 27001:2014 recomienda que las entidades realicen auditorías cada año para afinar los controles de seguridad y tener en cuenta otros factores. La entidad debe mejorar continuamente la eficacia del plan de seguridad a través de los resultados de las auditorías de seguridad, así como de las acciones correctivas y preventivas del municipio, además de disponer de los recursos necesarios para ello.

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" DE HUÁNUCO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE EXCLUSIVIDAD DEL TEMA

De acuerdo al Reglamento General de Grados y Títulos Modificado de la Universidad Nacional Hermilio Valdizán de Huánuco aprobado con Resolución del Consejo Universitario N° 0734-2022-UNHEVAL, de fecha 07 de marzo de 2022, considerando el Art. 24. Art 35 y en atención a lo solicitado y el informe de conformidad y Originalidad del tema de investigación de parte del señor Asesor, se hace Constar que:

La investigación titulada:

"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"

Tesista:

BACH. VILLADEZA ROMERO, KAREN LUCILA.
BACH. CONDOR SIMON, REYNALDO DAVID.

Presenta ORIGINALIDAD respecto al tema de investigación.

Huánuco, 24 de octubre de 2022

Nérida del Carmen Pastrana Díaz
Directora de Investigación - FIIS

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" DE HUÁNUCO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE APTO

De acuerdo al Reglamento General de Grados y Títulos Modificado de la Universidad Nacional Hermilio Valdizán de Huánuco aprobado con Resolución del Consejo Universitario N° 1893-2021-UNHEVAL, de fecha 17 de agosto de 2021 y en atención a la Tercera Disposición Complementaria, donde estipula que los trabajos de investigación y tesis de pregrado deberán tener una similitud máxima del 30%.

Después de aplicado el Software Turnitin, se evidencia una similitud del 23% encontrándose bajo los parámetros reglamentados.

Tesis para optar el Título Profesional de Ingeniero de Sistemas:

"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"

Tesistas

Bach. Ingeniería de Sistemas **VILLADEZA ROMERO, KAREN LUCILA**
Bach. Ingeniería de Sistemas **CÓNDOR SIMÓN, REYNALDO DAVID**

Huánuco, 01 de diciembre de 2022

Nérida del Carmen Pastrana Díaz
Directora de Investigación - FIIS

Año del Fortalecimiento de la Soberanía Nacional"

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" HUÁNUCO – PERÚ
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS - PROFI

En Huánuco, a los 29 días del mes de diciembre de 2022, siendo las 19:30 horas de acuerdo al Reglamento del Programa de Fortalecimiento en Investigación PROFI de la Universidad Nacional Hermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 48° al 52°, se procedió a la evaluación de la sustentación de la tesis virtual, titulado: **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;** presentado por el Bachiller en Ingeniería de Sistemas**: REYNALDO DAVID CONDOR SIMON.**
Este evento se realizó de manera virtual vía Cisco Webex, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Mg. VELSY RIVERA VIDAL
SECRETARIO: Mg. ALEXANDER PASQUEL CAJAS
VOCAL: Mg. WALTER BALDEÓN CANCHAYA.

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51° y 52° del Reglamento del Programa de Fortalecimiento en Investigación PROFI, obteniéndose el siguiente resultado. **Nota: Quince** (15) equivalente a la calificación de **BUENO** Quedando el bachiller en Ingeniería de Sistemas: **REYNALDO DAVID CONDOR SIMON: APROBADO**

Con lo que se dio por concluido el acto y en fe de la cual firman los miembros del jurado Calificador.

.....
PRESIDENTE

.....
SECRETARIO

.....
VOCAL

UNHEVAL UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN | VICERRECTORADO DE INVESTIGACIÓN | DIRECCIÓN DE INVESTIGACIÓN | RI UNHEVAL | DI UNHEVAL

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	INGENIERIA INDUSTRIAL Y DE SISTEMAS
Escuela Profesional	INGENIERIA DE SISTEMAS
Carrera Profesional	INGENIERIA 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:	VILLADEZA ROMERO KAREN LUCILA							
Tipo de Documento:	DNI	X	Pasaporte		C.E.		Nro. de Celular:	935891235
Nro. de Documento:	71316094						Correo Electrónico:	LUCILAVILLADEZA0@GMAIL.COM

Apellidos y Nombres:	CONDOR SIMON REYNALDO DAVID							
Tipo de Documento:	DNI	X	Pasaporte		C.E.		Nro. de Celular:	944117577
Nro. de Documento:	46971920						Correo Electrónico:	REYNALDO.CONDORS@GMAIL.COM

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:	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:	RIVERA VIDAL VELSY
Secretario:	PASQUEL CAJAS ALEXANDER
Vocal:	BALDEč N CANCHAYA WALTER
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)*
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
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)*						2022	
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)*	NORMA TÉCNICA PERUANA	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	MAGERIT

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, Título 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:	VILLADEZA ROMERO KAREN LUCILA	**Huella Digital**
DNI:	71316094	
Firma:		
Apellidos y Nombres:	CONDOR SIMON REYNALDO DAVID	**Huella Digital**
DNI:	46971920	
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Fecha:	23/02/2023	

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.