UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"LA METODOLOGÍA MAGERIT V3 Y SU INCIDENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA, 2019"

TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

TESISTAS:

Bach. Pedro PAJUELO GODOY

Bach. Sesi Beatriz VELÁSQUEZ GUDIÑO

ASESOR:

Dra. INÉS EUSEBIA JESÚS TOLENTINO

HUÁNUCO – PERÚ

2019

DEDICATORIA

A nuestros padres y hermanos por su gran apoyo y confianza depositada en nosotros a fin de seguir adelante, superándonos en el desarrollo profesional y personal.

AGRADECIMIENTO

- A la Universidad Nacional Hermilio Valdizan, por permitirnos y convertirnos en profesionales en lo que tanto nos apasiona.
- A cada maestro por ser parte de este proceso de formación académico, quienes a través de sus conocimientos y experiencias nos brindaron herramientas necesarias para culminar con éxito nuestros estudios.
- A nuestros padres que han estado con nosotros en todo momento brindándonos su apoyo incondicional, económico y moral.

RESUMEN

El objetivo general de la investigación fue determinar la incidencia de la Aplicación de la Metodología Magerit V3 en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019. La técnica utilizada para la recolección de datos fue la observación y la entrevista, el instrumento el cuestionario. La hipótesis general en esta investigación fue la Aplicación de la Metodología Magerit V3 incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019; se elaboró la distribución de frecuencias para cada variable y su respectiva dimensión, se utilizó la prueba de Test de Wilcoxon para la contrastación de la hipótesis general y específica. El Nivel de investigación explicativo, tipo aplicada, el diseño cuasi-experimental, la muestra 103 activos informáticos de la Municipalidad. En los resultados de la estadística inferencial se demostró que la aplicación de la Metodología Magerit V3 incide significativamente en la seguridad de información, obteniendo el valor de significancia (valor crítico observado) es: 0,000 < 0,05, por lo que se acepta la hipótesis alterna y se rechaza la hipótesis nula.

Palabras clave

Análisis de riesgo, seguridad de la información, información, metodologías, activos, amenazas, vulnerabilidad, impacto, políticas de seguridad, salvaguardas, riesgos.

SUMMARY

The general objective of the investigation was to determine the incidence of the Application of the Magerit V3 Methodology in the information security of the District Municipality of Pillco Marca, 2019. The technique used for data collection was observation and interview, the instrument questionnaire. The general hypothesis in this research was the Application of the Magerit V3 Methodology has a significant impact on the information security of the District Municipality of Pillco Marca, 2019; The frequency distribution for each variable and its respective dimension was elaborated, the Wilcoxon Test test was used to verify the general and specific hypothesis. The level of explanatory research, applied type, quasi-experimental design, shows 103 IT assets of the Municipality. In the results of the inferential statistics it was shown that the application of the Magerit V3 Methodology has a significant impact on information security, obtaining the significance value (observed critical value) is: 0.000 <0.05, so the hypothesis is accepted alternates and the null hypothesis is rejected.

Keywords

Risk analysis, information security, information, methodologies, assets, threats, vulnerability, impact, security policies, safeguards, risks.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

La presente investigación se refiere al tema de “Aplicación de la Metodología Magerit V3 en la Seguridad de la Información en la Municipalidad distrital de Pillco Marca”, que se puede definir como el uso de la Metodología para analizar y gestionar los riesgos, implementar salvaguardas y proponer políticas de seguridad, para que la capacidad de las redes o sistemas de información puedan resistir; con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y no repudio; de los datos almacenados o transmitidos, y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

La característica principal de esta Metodología es que nos permite determinar el grado de riesgo en que se encuentran los sistemas de información (físicos y lógicos), para de esta manera implementar salvaguardas y políticas que nos permitan reducir o eliminar los riesgos a los que se expone.

Para analizar esta problemática es necesario mencionar sus causas las cuales son: fallos en la seguridad de la información de carácter malicioso, intencional o criminal, errores técnicos del propio sistema, fallos en la seguridad de la información debido al error humano. Afectando directamente a la productividad y desempeño de las funciones de la Municipalidad.

Así mismo cabe mencionar que la Municipalidad no cuenta con políticas de seguridad y mecanismos de salvaguarda que puedan gestionar los riesgos a los que se encuentran expuestos sus activos de mayor valor, como Municipio tiene el objetivo de brindar servicios de calidad, con transparencia y tecnología en beneficio del ciudadano, logrando el desarrollo integral y sostenible de la ciudad, a través de una gestión participativa e innovadora, desarrollando actividades orientadas a la mejora de la calidad de servicio, parte de ello, involucra la evaluación de la seguridad de la información, protección y desempeño efectivo de los activos para evitar la duplicación de actividades, también una adecuada y oportuna toma de decisiones y el uso eficaz y eficiente de la información a través de la gestión de riesgo.

Para afrontar los riesgos que se consideren inaceptables se llevó a cabo un plan de seguridad que corrija la situación actual. Un plan de seguridad se materializa en una colección de programas de seguridad. La serie de programas se planifica en el tiempo por medio del denominado Plan de Seguridad que ordena y organiza las actuaciones encaminadas a llevar el estado de riesgo a un punto aceptable y aceptado por la Institución.

La finalidad de la presente investigación es: analizar y gestionar los riesgos, identificar y seleccionar mecanismos de salvaguardas a implementar y la elaboración de políticas de seguridad.

El trabajo se limita por la demora en el proceso de obtención de datos, debido a la burocracia de la institución.

I. PLANTEAMIENTO DE PROBLEMA

1.1 Antecedentes y fundamentación de problema.

No se encontró estudios relacionados con el tema.

Durante las visitas preliminares constatamos que, la realidad de la Municipalidad Distrital de Pillco Marca es preocupante debido a que se presentan casos de extravío y/o pérdida de recursos, algunas veces la información transmitida no es la misma que recibe el destinatario, o llega a la persona equivocada; causando incumplimiento de sus funciones y obligaciones al no entregar sus trabajos a tiempo, mal clima laboral e incomodidad de las personas que laboran en el municipio; por ende es importante que toda organización pública tenga políticas de seguridad de los sistemas de información.

En tal contexto, La Municipalidad Distrital de Pillco Marca, tiene vulnerabilidades que se hacen presente quebrantando la seguridad de la información atacando su confidencialidad, integridad y disponibilidad de la información, si no se realiza una gestión de

riesgos para salvaguardar los recursos que hace uso y manejo de información del municipio, considerando como activo más importante la información; lo más probable es que se les presente una situación en la que la entrega de un documento sea de suma importancia y resulte que este está dañado, ocasionándoles problemas graves, desde despidos hasta sanciones administrativas, además de un clima laboral caótico.

La aplicación del análisis y gestión de riesgos mediante MAGERIT, nos permitirá evaluar qué tan seguros son nuestros sistemas, cuantificando y comparando los requerimientos de seguridad de la información, determinar los activos y sus características de mayor valor, considerando los criterios del ACID (Autenticación, Confidencialidad, Integridad, Disponibilidad y No Repudio), identificar salvaguardas existentes, amenazas, su origen y el tipo de vulnerabilidad que pueden afectar la estimación y valoración de impactos, concluyendo en la evaluación de riesgos a los que se encuentran expuestos los activos del municipio. Lo cual nos permitirá una adecuada implementación de salvaguardas para conocer, provenir, impedir, reducir o controlar los riesgos identificados. Las actuaciones encaminadas a llevar el estado de riesgo a un punto aceptable y aceptado por la Dirección.

1.2 Formulación del problema.

1.2.1 Problema general.

¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019?

1.2.2 Problemas específicos

1. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019?
2. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019?
3. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019?
4. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019?
5. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en no repudio de información de la Municipalidad Distrital de Pillco Marca, 2019?

1.3 Objetivos: general y específicos.

Después de haber formulado nuestro problema, se plantean los siguientes objetivos de la investigación:

1.3.1 Objetivo General

Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019.

1.3.2 Objetivo Específicos

1. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019.
2. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019.
3. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019.
4. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

5. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en no repudio de información de la Municipalidad Distrital de Pillco Marca, 2019.

1.4 Hipótesis: general y específicos.

1.4.1 Hipótesis General

La Aplicación de la Metodología Magerit V3, incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019.

1.4.2 Hipótesis Específicas

1. La Aplicación de la Metodología Magerit V3, incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019.
2. La Aplicación de la Metodología Magerit V3, incide significativamente en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019.
3. La Aplicación de la Metodología Magerit V3, incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

4. La Aplicación de la Metodología Magerit V3, incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019.
5. La Aplicación de la Metodología Magerit V3, incide significativamente en No repudio de información de la Municipalidad Distrital de Pillco Marca, 2019.

1.5 Variables, dimensiones e indicadores

A continuación, se describen la variable independiente como dependiente y sus dimensiones e indicadores respectivamente.

1.5.1 Variable Independiente:

Metodología Magerit V3

- **Dimensión 1:** Riesgos

  Indicador: Estado de riesgo.

- **Dimensión 2:** Salvaguardas

  Indicador: Mecanismos de salvaguarda implantados actualmente.

- **Dimensión 3:** Políticas

  Indicador: Políticas de Integridad, disponibilidad y confidencialidad de la información.

1.5.2 Variable Dependiente:

Seguridad de Información

- **Dimensión 1:** Confidencialidad

  Indicador: Riesgo en la Confidencialidad de los activos informáticos.

- **Dimensión 2:** Integridad

  Indicador: Riesgo en la Integridad de los activos informáticos.

- **Dimensión 3:** Disponibilidad

  Indicador: Riesgo en la Disponibilidad de los activos informáticos.

- **Dimensión 4:** Autenticidad

  Indicador: Riesgo en la Autenticidad de los activos informáticos.

- **Dimensión 5:** No Repudio

  Indicador: Riesgo en No Repudio de los activos informáticos.

1.6 Definición operacional de: Variables, dimensiones e indicadores

Tabla 1

Operacionalización de Variables

VARIABLES		DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	RANGO/FORMULA	TIPO DE VARIABLE
V. Independiente (x)	Metodología Magerit v3	MAGERIT es una metodología, que estudia los riesgos soportados por los Sistemas de Información para recomendar aquellas medidas más encaminadas a controlar su impacto. Sus objetivos básicos, concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de que éstos sean controlados antes de que se materialicen; ofrecer un método sistemático para el análisis de dichos riesgos; planificar medidas oportunas para mantener los riesgos bajo control; y ayudar a la Organización para que ésta se encuentre preparada para procesos de evaluación, auditoría, certificación y acreditación.	Riesgos	Estado de riesgo	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo	Ordinal
			Salvaguardas	Mecanismos de salvaguarda implantados actualmente	1= Si se evidencia 0 = No se evidencia	Ordinal
			Políticas	Verificación de políticas de integridad, confidencialidad, disponibilidad, autenticidad y no repudio de la información	1= Si se evidencia 0 = No se evidencia	Ordinal
V. Dependiente (x)	Seguridad de la Información	La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.	Confidencialidad	Riesgo en la confidencialidad de los Activos Informáticos	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo	Ordinal
			Integridad	Riesgo en la integridad de los Activos Informáticos	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo	Ordinal
			Disponibilidad	Riesgo en la disponibilidad de los Activos Informáticos	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo	Ordinal
			Autenticidad	Riesgo en la autenticidad de los Activos Informáticos	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo	Ordinal
			No repudio	Riesgo en No repudio de los Activos Informáticos	0 – 1 = Controlable 2 – 5 = Aceptable 6 – 16 = Tolerable 17 – 30 = Intolerable 31 – 50 = Extremo	Ordinal

Fuente: Elaboración Propia

1.7 Justificación e importancia.

Los recursos de tecnologías de información como cualquier activo en las organizaciones, se encuentran expuestos a riesgos, cuando estos se materializan, no solo degrada el recurso, sino que impactan en menor o mayor grado el cumplimiento de los objetivos.

Dado que la Municipalidad Distrital de Pillco Marca tiene como objetivo brindar servicios de calidad con transparencia y tecnología en beneficio del ciudadano, logrando el desarrollo integral y sostenible de la ciudad, a través de una gestión participativa e innovadora. Sin embargo hemos constatado que el municipio no cuenta con políticas de seguridad y mecanismos de salvaguarda que puedan gestionar los riesgos a los que se encuentran expuestos sus activos de mayor valor, el cual involucra la evaluación de la seguridad de la información, protección y desempeño efectivo de los activos para evitar la duplicación de actividades, de esta manera evitar problemas graves, desde despidos hasta sanciones administrativas, además de un clima laboral inaceptable, con el antecedente indicado, el presente estudio tiene como finalidad aplicar la Metodología Magerit V3 y su incidencia en la seguridad de la información.

El resultado del presente estudio nos permitirá establecer las medidas de seguridad apropiadas para controlar o eliminar riesgos identificados, asegurando la continuidad operacional de la

organización, una adecuada y oportuna toma de decisiones y el uso eficaz y eficiente de la información. Además, permite un óptimo aprovechamiento de recursos y reducción de pérdidas.

1.8 Limitaciones.

1.8.1 Limitación Temporal

Consideramos insuficiente el período de tres meses, para elaborar un correcto análisis y gestión de riesgos utilizando la metodología Magerit V3 en la Municipalidad Distrital de Pillco Marca.

II. MARCO TEÓRICO

2.1 ANTECEDENTES

6. A nivel Nacional

(Talavera Álvarez , 2015) en la tesis denominada “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”, tiene como objetivo Diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013., porque en la actualidad, los problemas de la seguridad de la información se manifiestan en torno a la alineación de las Tecnologías de Información y Comunicación con los procesos de la organización, convirtiéndose en un aspecto muy crítico cuyo tratamiento es de vital consideración, es por ello que en el desarrollo del estudio, los tesista concluye que la no elaboración de documentos en los cuales se describen los procedimientos, políticas de seguridad a utilizar y controles que permitan garantizar la autenticidad, confidencialidad y disponibilidad de los datos de los usuarios, puede en un futuro

ser un peligro latente, ya que la El Instituto Nacional Materno Perinatal – INMP está creciendo de forma considerada.

7. A nivel Internacional

- (Lucero G. & Valverde P., 2012)Lucero en la tesis denominada "Análisis y gestión de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT", platea como objetivo el análisis de la situación actual y especificación de necesidades funcionales de seguridad para el diseño de los mecanismos de salvaguarda, centrado en el departamento Informático de la Cooperativa de Ahorro y Crédito Jardín Azuayo, oficina de Coordinación y Cuenca. La investigación concluye que la prevención, detección y mitigación de los riesgos es imprescindible, razón por la que se deberá aplicar una metodología con su respectiva herramienta, usando perfiles de seguridad y salvaguardas adecuadas como lo recomienda la herramienta PILAR basic. Actualmente, en nuestro medio no se pone real énfasis en temas referentes al análisis y gestión de riesgos de los sistemas de información, lo que ocasiona que no se tenga un conocimiento adecuado de dichos temas y no se cuente con el personal especializado para realizar dicho análisis.

- (Perafán Ruiz & Caicedo Cuchimba, 2014) en la tesis denominada, “Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca”, se planteó como objetivo realizar un análisis de riesgos que permita generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en la Institución Universitaria Colegio Mayor del Cauca; concluyendo que el análisis de riesgo aplicado, permite conocer de manera global el estado actual de la seguridad informática dentro de la Institución Universitaria Colegio Mayor del Cauca y los controles y políticas de seguridad de la información resultado de este análisis de riesgos, pueden ser tomados como soporte para la implementación del SGSI.
- (Gallardo Piedra & Jácome Cordones , 2011)En la tesis denominada “Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I. para la Empresa Eléctrica Quito S.A.” se planteó como objetivo la identificación de los principales riesgos informáticos y en base a ellos elaborar un plan de contingencia T.I. para la Empresa Eléctrica Quito. Por ese motivo, el trabajo comienza analizando las principales metodologías que existen, para realizar en primer lugar, la

identificación de los riesgos informáticos que puedan existir en la empresa. Posteriormente se realizó el análisis de las metodologías o guías existentes para elaborar el respectivo plan de contingencia, en donde se realizó una descripción y comparación de las mismas, para de esta manera, seleccionar la más idónea para realizar el trabajo.

Una vez seleccionadas las metodologías se procedió a realizar el respectivo análisis de riesgos informáticos, principalmente dentro del departamento de TIC de la EEQ basándonos en la metodología escogida, que en este caso fue OCTAVE la que involucra desde el comienzo a los principales niveles organizacionales de la empresa como son los altos directivos, directivos de ares operativos y personal en general. Garantizado de este modo una participación activa y por ende un análisis de riesgo más objetivo y en base a las necesidades actuales de la empresa. Tomando este precedente se consiguió recopilar el conocimiento y criterio de los participantes en lo referente a los activos que consideran más importantes dentro de las empresas, principales áreas de interés, requerimiento de seguridad, prácticas de estrategias de protección actual y vulnerabilidades que existen dentro de la misma, logrando de esta manera una

selección acertada de los activos críticos, que para las empresas son fundamentales para su normal funcionamiento.

2.2 LEYES FUNDAMENTALES, PRINCIPIOS, DEFINICIONES Y CONCEPTOS FUNDAMENTALES

2.2.1 Buen gobierno:

"La gestión de los riesgos es una piedra angular en las guías de buen gobierno" (ISO 38500), público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican: Recopilación de los beneficios, costos, riesgos, oportunidades, y otros factores que deben tenerse en cuenta en las decisiones que se tomen. En pocas palabras, la gestión de los riesgos es nuclear al gobierno de las organizaciones. En particular, los riesgos que tienen su origen en el uso de tecnologías de la información deben trasladarse a los órganos de gobierno y contextualizarse en la misión de la organización.

2.2.2 Confianza

La confianza es la esperanza firme que se tiene de que algo responderá a lo previsto. La confianza es un valor crítico en cualquier organización que preste servicios. Las administraciones públicas son especialmente sensibles a esta valoración.

2.2.3 Gestión

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

En el periodo transcurrido desde la publicación de la primera versión de Magerit (1997) hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

2.2.4 Metodología MAGERIT

(Consejo Superior de Administración Electrónica, 2012) De España, ha elaborado y promueve MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) como respuesta a la percepción de que la administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio.

La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de

seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generan confianza cuando se utilicen tales medios. Una organización no alcanzará sus objetivos, metas y misión si no tiene a su alcance los elementos informáticos básicos e indispensables que le ayuden y soporten sus decisiones.

MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de n análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (UNE 71504:2008)

FASES DE MAGERIT VERSIÓN 3

- ✓ **Identificación de activos informáticos**: Se identifica los activos informáticos existentes en la organización.
- ✓ **Catálogos de amenazas:** En este punto las amenazas ya vienen denotadas y estas amenazas están agrupados según el origen industrial, errores y fallos no intencionados y ataques intencionados.
- ✓ **Caracterización:** En la caracterización denotamos las amenazas que se pueden ser afectados a cada activo informático; así mismo obtenemos las probabilidades que pueden dañar estas amenazas a estos activos informáticos. Las dimensiones son valoradas por cada amenaza que contiene dichos activos.
- ✓ **Impacto:** Pasa saber el impacto por cada dimensión y por cada activo informático se realiza una operación que es

obtenida de los valores de dimensiones que esto fue realizado en la identificación de activos con los valores de dimensiones que se obtuvo en la tabla de caracterización.

- ✓ **Mapa de riesgos:** Relación de las amenazas a que están expuesto los activos.
- ✓ **Salvaguardas:** En esta tarea las salvaguardas están agrupados tipos de protección

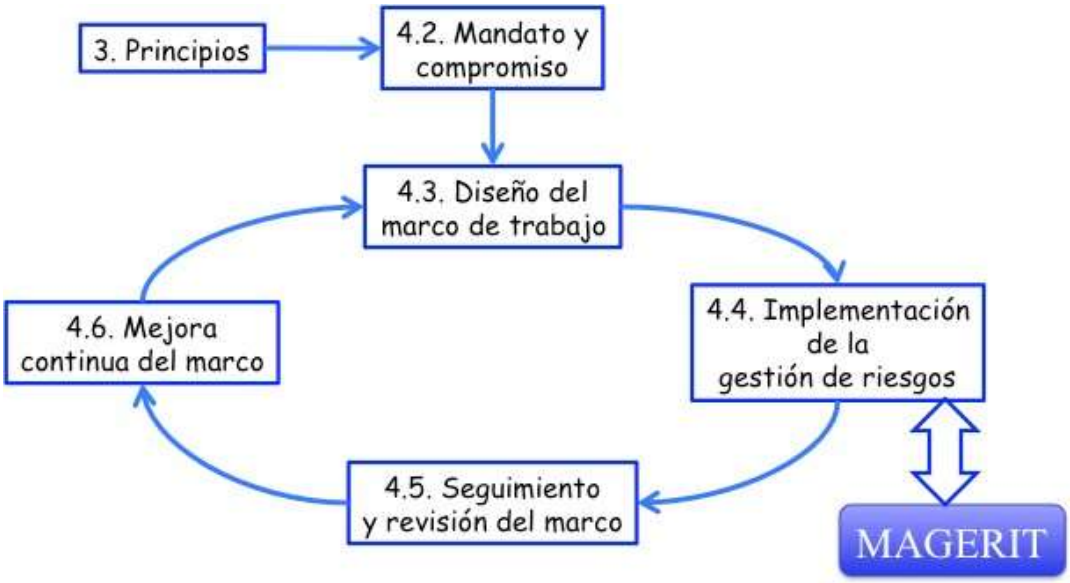


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

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.

Magerit persigue los siguientes objetivos: Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

Modelo de valor: Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.

Mapa de riesgos: Relación de las amenazas a que están expuestos los activos.

Declaración de aplicabilidad: Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Evaluación de salvaguardas: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

Cumplimiento de normativa: Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

Plan de seguridad: Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

a) Análisis y gestión de riesgos

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que compro-metan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad: disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- Integridad: mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.
- Confidencialidad: que la información llegue solamente a las personas autorizadas. Contra la confidencialidad secreto

pueden darse fugas y filtraciones de información, así como accesos no autoriza- dos. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la con- fianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

- Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.
- Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente

que se disfruten sin más. Lo habitual que haya que poner medios y es- fuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

- Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema:
- Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

  Sabiendo lo que podría pasar, hay que tomar decisiones:
- **Tratamiento de los riesgos:** Proceso destinado a modificar el riesgo. Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio. Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo:

"Efecto de la incertidumbre sobre la consecución de los objetivos". [ISO Guía 73], como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

b) El análisis y el tratamiento de los riesgos en su contexto

Las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con

los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

La implantación de las medidas de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La

fase de tratamiento estructura las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis.

Los sistemas de gestión de la seguridad de la información (SGSI) [ISO 27001] formalizan cuatro etapas cíclicas:

Ilustración 2. Ciclo PDCA

El análisis de riesgos es parte de las actividades de planificación, donde se toman decisiones de tratamiento. Estas decisiones se materializan en la etapa de implantación, donde conviene des- plegar elementos que permitan la monitorización de las medidas desplegadas para poder evaluar la efectividad de las mismas y actuar en consecuencia, dentro de un círculo de excelencia o mejora continua.

c) Concienciación y formación

El mejor plan de seguridad se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria a las medidas, o tienen la percepción de pasarse el día "luchando contra las [absurdas] medidas de seguridad". Es por ello que se requiere la creación de una "cultura de seguridad" que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia.

Son tres los pilares fundamentales para la creación de esta cultura:

- Una política de seguridad corporativa que se entienda (escrita para los que no son expertos en la materia), que se difunda y que se mantenga al día
- Una normativa se seguridad que, entrando en áreas específicas de actividad, aclare la postura de la Organización; es decir, defina lo que es uso correcto y lo que es incumplimiento
- Una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo

A fin de que estas actividades cuajen en la organización, es imprescindible que la seguridad sea:

- Mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos,
- Sea “natural”: que no dé pie a errores gratuitos, que facilite el cumplimiento de las buenas prácticas propuestas y
- Practicada por la Dirección: que dé ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias.

d) Modo de empleo

Siempre se explican informalmente las actividades a realizar, y en ciertos casos se formalizan como tareas que permiten una planificación y seguimiento:

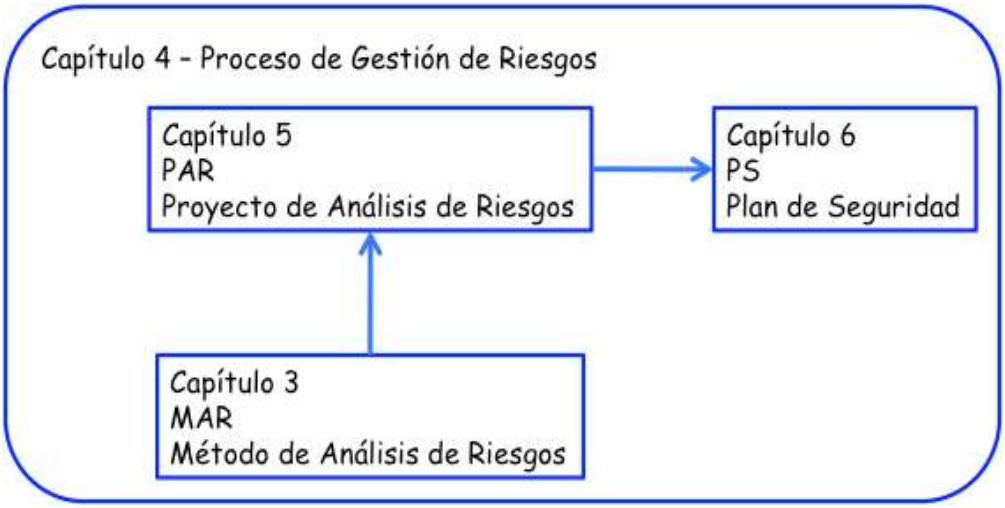


Ilustración 3. Actividades formalizadas

En sistemas pequeños, estas actividades pueden llevarse a cabo sin muchos formalismos; pero cuando el sistema adquiere envergadura e involucra a diferentes personas y equipos de

trabajo durante varias semanas, meses o años, la planificación formal ayuda a mantener el proceso bajo control.

En el planteamiento de estas guías se ha seguido un criterio "de máximos", reflejando todo tipo de situaciones. En la práctica, el usuario puede encontrarse ante situaciones donde el alcance es más restringido. Ante estas situaciones, conviene ser práctico y no pretender aplicar todas las tareas descritas en Magerit desde el primer momento. Suele ser prudente realizar una aproximación iterativa, aplicando el método primero con trazo grueso y luego ir revisando el modelo para entrar en detalles. El proceso de gestión de riesgos debe identificar y tratar urgentemente los riesgos críticos, pudiendo ir tratando progresivamente riesgos de menor criticidad. Como se dice popular- mente "lo perfecto es enemigo de lo bueno". Lo prudente es armonizar el esfuerzo al valor de la información y los servicios que se sustentan.

Entiéndase pues Magerit como una guía que se puede y se debe adaptar al caso y sus circunstancias.

e) Visión de conjunto

Hay dos grandes tareas a realizar:

I. Análisis de riesgos

Que permite determinar qué tiene la Organización y estimar lo que podría pasar.

II. Tratamiento de los riesgos

Que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado

Gestión de Riesgos.

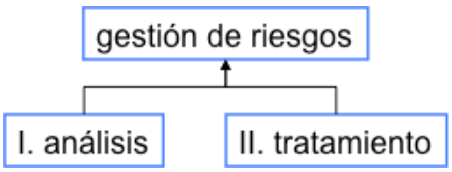


Ilustración 4. Gestión de riesgos

El análisis de riesgos considera los siguientes elementos:

1. Activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
2. Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
3. Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no

causen [tanto] daño.

Con estos elementos se puede estimar:

1. El impacto: lo que podría pasar
2. El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

Formalmente, la gestión de los riesgos está estructurada de forma metódica en las normas ISO. Se propone el siguiente esquema:

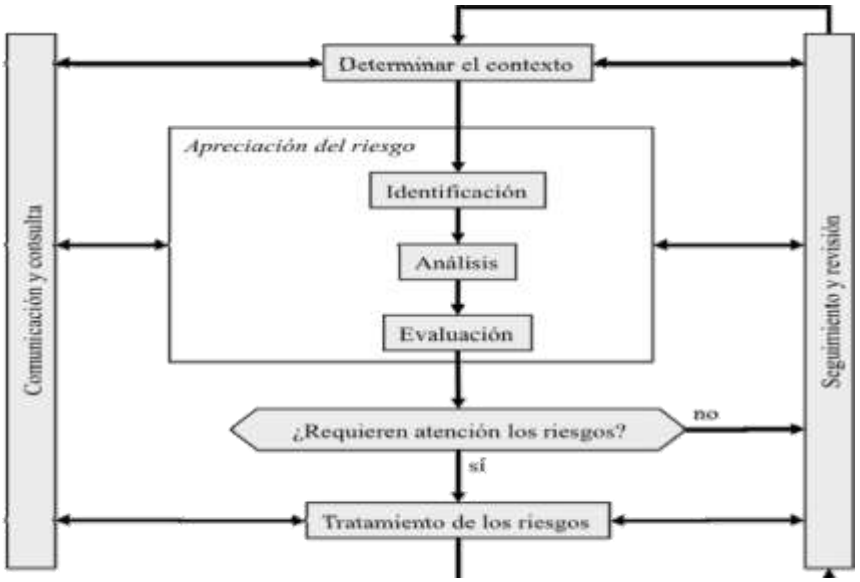


Ilustración 5. Proceso de gestión de riesgos (fuente: ISO 31000)

La **determinación del contexto** lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados. Véase la norma [ISO 31000] para un mayor desarrollo de los factores que determinan el contexto.

La **identificación de los riesgos** busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado.

El **análisis de los riesgos** busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

La **evaluación de los riesgos** va un paso más allá del análisis técnico y traduce las consecuencias a términos de

negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

El **tratamiento de los riesgos** recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones como veremos más adelante.

Comunicación y consulta. Es importante no olvidar nunca que los sistemas de información de- ben ser soporte de la productividad de la Organización. Es absurdo un sistema muy seguro pero que impide que la Organización alcance sus objetivos. Siempre hay que buscar un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores:

Los usuarios cuyas necesidades deben ser tenidas en cuenta y a los que hay que informar para que colaboren activamente en la operación del sistema dentro de los parámetros de seguridad determinados por la Dirección

- Los proveedores externos, a los que hay proporcionar instrucciones claras para poder exigir- les tanto el

cumplimiento de los niveles de servicio requeridos, como la gestión de los incidentes de seguridad que pudieran acaecer

- Los órganos de gobierno para establecer canales de comunicación que consoliden la con- fianza de que el sistema de información responderá sin sorpresas para atender a la misión de la Organización y que los incidentes serán atajados de acuerdo el plan previsto

Seguimiento y revisión. Es importante no olvidar nunca que el análisis de riesgos es una actividad de despacho y que es imprescindible ver qué ocurre en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

f) Análisis de riesgo:

(MAGERIT, 2012) “Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como ‘activos’); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre”.

Razones para realizar el análisis de riesgos

Actualmente, existen motivos para aplicar el análisis de riesgos en todo tipo de organizaciones, ya que es una técnica que, entre otras cosas permite:

- Identificar los activos y controles de seguridad.
- Gestionar las alertas de los riesgos próximos.
- Identificar la necesidad de acciones correctivas.
- Proporcionar una guía de cara a los gastos de recursos.
- Relacionar el programa de control con la misión de la organización.
- Proporcionar criterios para diseñar y evaluar planes de contingencia y continuidad de negocios.
- Mejorar la concienciación global sobre la seguridad a todos los niveles.

Tipos de análisis de riesgos

Existen dos enfoques básicos para realizar un completo análisis de riesgos, uno cuantitativo y otro cualitativo.

Enfoque cualitativo:

El enfoque cualitativo de análisis de riesgos es de uso muy común en la actualidad, especialmente entre las nuevas empresas consultoras de seguridad, en aquéllas más especializadas en seguridad lógica, cortafuegos, test de intrusión y similares. Es mucho

más sencillo e intuitivo que el cuantitativo, ya que no entran en juego probabilidades exactas sino, simplemente, una estimación de pérdidas potenciales.

El método o enfoque cualitativo es más apropiado para instalaciones menores y es el más utilizado en la actualidad. Se pueden medir ciertos parámetros:

- Riesgo de amenazas, empleando escalas como: elevado, medio, bajo.
- Gravedad del ataque, en base a escalas como 1, 2, 3.
- Daño, utilizando escalas como: vital, crítico, importante, conveniente, informativo.

Para este análisis, no se requieren datos de probabilidad y sólo se utiliza la pérdida potencial estimada. En lugar de utilizar números exactos, utiliza métricas más difusas para los valores de los activos, la frecuencia de las amenazas y la efectividad del control. Utiliza un conjunto de elementos interrelacionados, como son:

- Amenazas
- Vulnerabilidades
- Controles.

Existen cuatro tipos de controles:

Controles disuasorios. Reducen la probabilidad de un ataque deliberado.

Controles preventivos. Protegen las vulnerabilidades y hacen que un ataque no tenga éxito o bien, reducen su impacto.

Controles correctores. Reducen el efecto de un ataque.

Controles de investigación. Descubren los ataques y ponen en funcionamiento controles preventivos, también llamados proactivos o correctivos, así como reactivos.

Con estos cuatro elementos, podemos obtener un indicador cualitativo del nivel de riesgo, asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

Enfoque cuantitativo

El enfoque cuantitativo es, con diferencia, el menos utilizado, ya que, en muchos casos, implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales, que son la probabilidad de que se produzca un suceso y una estimación del coste o de las pérdidas, en caso de que así sea. El producto de ambos términos es lo que se denomina coste anual estimado.

Tabla 2.
Ventajas e inconvenientes de los tipos de análisis de riesgos

	Ventajas	Inconvenientes
Cualitativo	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Influyen factores intangibles. No se necesita cuantificar la frecuencia de las amenazas. El proceso para alcanzar resultados creíbles y un consenso consume menos tiempo. Permite una visibilidad y entendimiento del ranking de riesgos.	Depende fuertemente de la habilidad y calidad del personal involucrado. Pueden excluir riesgos significantes desconocidos. Insuficiente diferenciación entre los riesgos importantes. Dificultad de justificar la inversión en la implantación del control, debido a la no existencia de una base de análisis costes/ beneficios. Los resultados son dependientes de la calidad del equipo de gestión de riesgos.
Cuantitativo	Es objetivo, independiente del proceso. Base sólida para un análisis de costes y beneficios de las salvaguardas. Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. Proporciona una cifra justificante para cada contramedida.	No es fiable para eventos raros o impactos impensables. En la mayoría de los casos, es difícil de enumerar todos los tipos de eventos y obtener datos con significado sobre la probabilidad e impacto. Es difícil de estimar el valor de un activo intangible, en concreto, la disponibilidad de la información para la que se diseñó el sistema. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodología estándar. Consume mucho tiempo y es costoso a la hora de hacerlo bien. Dependencia de un profesional.

Fuente: Elaboración Propia

g) Gestión de riesgos:

(MAGERIT, 2012) "La gestión de riesgos, se basa en todos los resultados obtenidos durante el análisis que hemos hecho anteriormente, se seleccionan medidas de seguridad adecuadas para poder conocer, prevenir, impedir, recudir o controlar todos los

riesgos que se han identificado, pudiendo de este modo reducir al mínimo la potencialidad del riesgo".

La Gestión de Riesgos implica dos grandes tareas a realizar:

• Análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.

• Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por la gravedad de los mismos y por las obligaciones a las que esté sometida la Organización por ley, reglamento sectorial o por contrato Pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

• Imagen pública de cara a la Sociedad (aspectos reputaciones)

• Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a

los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.

• Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.

• Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia.

• Relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.

• Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad

• Acceso a sellos o calificaciones reconocidas de seguridad.

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si:

1. Es crítico y requiere atención urgente

2. Es grave y requiere atención

3. Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento 4. Es asumible, en el sentido de que no se van a tomar acciones para atajarlo.

Las opciones 1,2 y 3 requieren tratamiento técnico del riesgo.

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación cuando el impacto y el riesgo residual es asumible o cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

Ilustración 6. Evolución de Riesgos.

2.2.5 Seguridad de la Información

"Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables". (UNE 71504:2008)

Según (Ministerio de Hacienda y Administraciones Públicas 2012), la seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la

disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

La seguridad de la información, según (ISO 27001, 2013), consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información.

Conceptos relacionados a Seguridad de Información

 Seguridad de Información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, norepudio y confiabilidad.

 Evento de Seguridad de la Información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de una política de seguridad de la información o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que

tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

 Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. La información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema. Implica también la prevención de ataque de denegación de servicio.

 Confidencialidad: La propiedad de que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Es el acceso a la información únicamente por personas que cuentan con la debida autorización.

 Integridad: Propiedad de salvaguardar por la exactitud y completitud de los activos. Busca mantener la información libre de modificaciones no autorizadas, de tal manera que se conserve tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad: Disponibilidad, Autenticación, Confidencialidad e Integridad.

En cuanto al tratamiento, la Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

- Reducir el riesgo residual (aceptar un menor riesgo)
- Ampliar el riesgo residual (aceptar un mayor riesgo)

Ilustración 7. Seguridad y riesgos en las TIC (IV), proceso de administración del riesgo, Security Art Work

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

- Cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- Posibles beneficios derivados de una actividad que en sí entraña riesgos.
- Condicionantes técnicos, económicos, culturales, políticos, etc.
- Equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales.

Para tomar la decisión del tratamiento, hay múltiples formas de reducir el riesgo:

- Eliminar el riesgo eliminando sus causas: información tratada, servicios prestados, arquitectura del sistema.
- Reducir o limitar el impacto.
- Reducir la probabilidad de que la amenaza ocurra
- En el caso de amenazas derivadas de defectos de los productos (vulnerabilidades técnicas).
- Implantar nuevas salvaguardas o mejorar la calidad de las presentes.
- Externalizar partes del sistema.
- Contratar seguros de cobertura.

- A veces la decisión consiste en aceptar un incremento del riesgo: Aceptando trabajar con nueva información o prestar nuevos servicios.
- Alterando la arquitectura del sistema.
- Reduciendo las salvaguardas presentes.
- Reduciendo la calidad de las salvaguardas presentes (es decir, dedicando menos recursos)

En última instancia siempre hay que acabar aceptando un cierto riesgo residual, en cuyo caso es posible que se decide reservar fondos para hacer frente a alguna contingencia.

“Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir”. (UNE 71504, 2008)

“Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información”. (Magerit, 1997)

Cualquier sistema o producto destinado a almacenar, procesar o transmitir información. (CESID, 1997)

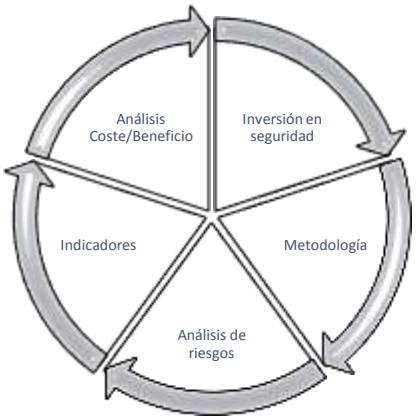


Ilustración 8. Modelo de gestión de seguridad

a) Salvaguarda

Mecanismos, estrategias o procedimientos que nos permiten asegurar y mantener efectiva la viabilidad del funcionamiento del recurso. Según (Rodríguez, 2009), salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas, felonías y de forma amplia todos los disturbios sociales que pongan en peligro el progreso e incluso la vida del negocio. Es, generalmente hablando, todas las medidas para conferir la requerida paz y tranquilidad al personal.

Conociendo y evaluando los riesgos a los que se encuentran expuestos nuestros activos de mayor valor podemos adquirir información para medir y controlar, pero ello no es suficiente como menciona (Jara H. y Pacheco, F. 2012) en este punto es importante detenernos y aclarar que las evaluaciones de seguridad en sí solo

muestran una instantánea, una fotografía de la postura de seguridad de la organización en un momento determinado. Únicamente representan un verdadero valor agregado cuando son llevadas adelante en forma sistemática y continua en el tiempo, y cuando las recomendaciones de salvaguardas que surgen de ellas son implementadas. Por ello, a medida que la criticidad del activo de información aumenta, también lo hace la velocidad con la que se debe remediar.

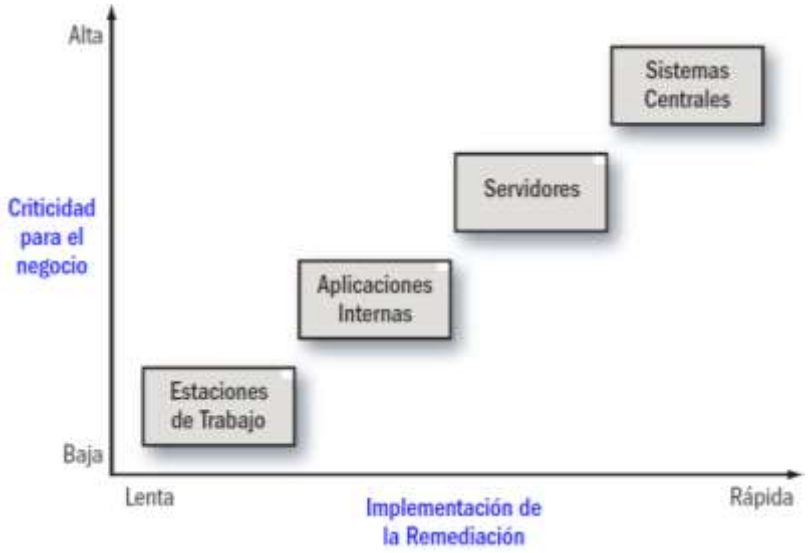


Ilustración 09 Priorización de activo

Fuente: Ethical Hacking 2.0: Implementación de un sistema para la gestión de la seguridad.

También es importante evaluar para el despliegue de salvaguardas complementarias o propuestas, aquellas existentes o deficientes que la organización posee, como menciona (Gómez,

2013), muchas organizaciones no han definido e implantado de forma eficaz unas adecuadasprocedimientos de seguridad, de acuerdo con sus necesidades de seguridad de la información, por ello es fundamental evaluar factores como:

- ✓ Políticas de contraseñas poco robustas.
- ✓ Deficiente control de los intentos de acceso al sistema.
- ✓ Escaso rigor en el control de acceso a los recursos.
- ✓ Procedimientos inadecuados para la gestión de soportes informáticos o el control de equipos portátiles.
- ✓ Escaso control de las copias generadas en papel con información sensible.
- ✓ Falta de control de los tratamientos realizados por terceros.
- ✓ Deficiente o inexistente limitación del acceso físico a los equipos más sensibles.
- ✓ Instalación de programas poco fiables.

La función esencial de los salvaguardas consiste en proteger y resguardar los criterios de seguridad de los activos de mayor valor, son medidas, procedimientos o mecanismos que permiten asegurar el desenvolvimiento efectivo de los mismos hasta el cumplimiento de su vida útil, como menciona (Merino, C. y Cañizares, R., 2011) Las salvaguardas son medidas de seguridad o controles que ha establecido la organización para mitigar sus

riesgos, pueden reducir la probabilidad de éxito de una amenaza reduciendo por lo tanto su frecuencia y/o reducir el impacto en caso de materialización de dicha amenaza, por ello para valorar las salvaguardas se deben tener en cuenta los siguientes factores:

- ✓ Diseño de la salvaguarda.
- ✓ Tipo de salvaguarda.
- ✓ Fiabilidad de la salvaguarda.
- ✓ Facilidad de implantación o despliegue de la salvaguarda.
- ✓ Dependencias de las salvaguardas.
- ✓ Revisión de la salvaguarda.

Gran parte de la implementación de salvaguardas implica un rediseño de los procesos que tienen cierta implicancia con el mismo, mucho más aquellos que ofrecen más rentabilidad a la organización, por ello es de vital importancia que un despliegue de salvaguardas vaya acompañado de planes y normativas que permitan adaptar a la organización a los cambios generados por las salvaguardas.

Es importante tener en cuenta, como menciona (Merino, C. y Cañizares, R., 2011) no todas las salvaguardas ayudan a proteger de la misma forma el activo, y por tanto se les deberá dar un peso a cada salvaguarda para el grupo de aquellas que afectan a un activo o grupo de activos.

Selección de salvaguardas

Según (Ministerio de Hacienda y Administraciones Públicas 2012), para la selección de salvaguardas, ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante
2. La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo)
3. La cobertura del riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- No aplica – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- No se justifica – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

Como resultado de estas consideraciones dispondremos de una "declaración de aplicabilidad" o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

Efecto de las salvaguardas

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- Reduciendo la probabilidad de las amenazas

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

- Limitando el daño causado

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema

cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

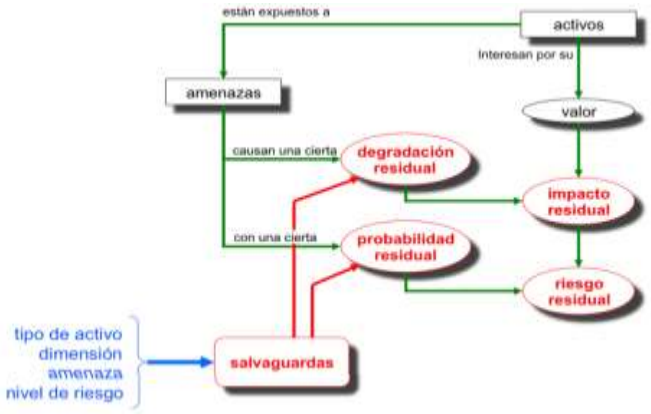


Ilustración 9. Elementos de análisis de riesgo residual - Ministerio de Hacienda y Administraciones Públicas.

b) Política de seguridad

Según (Ministerio de Hacienda y Administraciones Públicas, 2012) “manifiesta que es una o más reglas de seguridad, procedimientos, prácticas o directrices impuestas por una organización sobre sus operaciones”.

La evaluación de seguridad es continua y evolutiva como referencian Jara y Pacheco (2012), las evaluaciones de seguridad en sí solo muestran una instantánea, una fotografía de la postura de seguridad de la organización en un momento determinado. Únicamente representan un verdadero valor agregado cuando son llevadas adelante en forma sistemática y continua en el tiempo, y

cuando las recomendaciones que surgen de ellas son implementadas.

Principios Fundamentales

Romero (2002), hace referencia a los principios fundamentales de la seguridad informática que deben ser considerados en el establecimiento e implementación de políticas de seguridad de la información en una organización:

- Principio de menor privilegio: afirma que cualquier objeto debe tener tan solo los privilegios de uso necesarios para desarrollar su tarea y ninguno más.
- Seguridad no equivale a oscuridad: Un sistema no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corrijamos estableciendo las medidas de seguridad adecuadas.
- Principio del eslabón más débil: No basta con establecer unos mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.
- Defensa en profundidad: es necesario establecer varios mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

- Punto de control centralizado: Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él.
- Seguridad en caso de fallo: En caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro.
- Participación universal: La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro.
- Principio de simplicidad: Mantener las cosas simples, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro.

La evaluación de los principios de seguridad de nivel informático se efectúa con mayor énfasis y aplicación en sistemas operativos, bases de datos, redes, etc. debido al aumento exponencial de usuarios involucrados (potenciales atacantes) en las redes informáticas, aumento de la complejidad del sistema, límites desconocidos y por los múltiples puntos de ataque a través de la red.

Ilustración 10. Business Protección

ONGEI (Oficina Nacional de Gobierno Electrónico e informática)

Agrupa los trámites que brindan las instituciones del Estado al ciudadano. Entre la normatividad peruana se encuentra:

- Nuevo código Penal 163. Supresión o extravío indebido de correspondencia.
- Nuevo código Penal 164. Publicación indebida de correspondencia
- Nuevo código Penal 165. Violación del secreto profesional
- Nuevo código Penal 185. Hurto Simple
- Nuevo código Penal 186. Hurto Agravado
- Nuevo código Penal 198. Administración fraudulenta

- Nuevo código Penal 207-A.Espionaje Informático
- Nuevo código Penal 207-B.Sabotaje Informático
- Nuevo código Penal 207-C. Modalidad Agravada
- Nuevo código Penal 217. Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor
- Nuevo código Penal 218. Formas agravadas
- Nuevo código Penal 219. Plagio
- Nuevo código Penal 220-E. Etiquetas, carátulas o empaques
- Nuevo código Penal 220-F. Manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador
- Nuevo código Penal 427. Falsificación de documentos
- Nuevo código Penal 428. Falsedad ideológica
- Nuevo código Penal 429. Omisión de consignar declaraciones en documentos.
- Código civil 140. Acto jurídico
- Código civil 141. Manifestación de la voluntad
- Código civil 141-A. Manifestación de la voluntad a través de medios electrónicos.
- Código Procesal Civil 2034. Documentos electrónicos
- Constitución Política del Perú 2 inc. 5 Derecho de acceso a la información

- Constitución Política del Perú 2 inc. 6. Derecho a la privacidad
- Constitución Política del Perú 200 inc. 3 Habeas Data
- Constitución Política del Perú 58. Economía social del Mercado
- Constitución Política del Perú 59. Rol Económico del Estado
- Constitución Política del Perú 61. Libre competencia
- Declaración Universal de los Derechos Humanos (19). Libertad de Expresión
- Código de Ética del Ingeniero Art 4. Relación con la Sociedad
- Código de Ética del Ingeniero Art 5. Relación con la Sociedad
- Código de Ética del Ingeniero Art6. Relación con la Sociedad
- Código de Ética del Ingeniero Art7. Relación con la Sociedad
- Código de Ética del Ingeniero. Art20. De la Competencia y Perfeccionamiento de Profesionales
- Código de ética del Ingeniero Art44. De las Relaciones con el personal
- Código de ética del Ingeniero Art54 inc. De las Relaciones con los colegas
- Código de ética del Ingeniero Art54 inc. De las Relaciones con los colegas
- Ley de firmas digitales 8. Confidencialidad de la información
- Ley de delitos informáticos N° 27309 - Delitos informáticos

- Ley de protección de datos personales N° 29733 - Protección de datos personales.
- Decreto legislativo Nº 681. Dictan normas que regular el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto de la elaborada en forma convencional como la producida por procedimientos informáticos en computadoras.
- Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) - Ley N° 28493 (8) Derecho a compensación pecuniaria.

Cultura de seguridad

Para que la implementación de las políticas de seguridad se desarrolle de manera efectiva requiere el involucramiento del personal que labora en la organización, por lo tanto, la labor de las direcciones de la organización debe ser el fomentar una cultura y un clima de seguridad, donde todos los involucrados puedan ser conscientes de la importancia de la seguridad de los activos de mayor valor de la organización, como menciona, Fernández, Montes y Vázquez (2005) que es algo más que un simple “sistema de papeles” de políticas y procedimientos. Reúne un conjunto de prácticas implantadas en las empresas tendentes a la eliminación o reducción de los riesgos derivados del trabajo, las cuales se han

venido considerando como factores integrantes de la cultura de seguridad de la empresa.

Por lo mencionado anteriormente se puede afirmar que gran parte de la viabilidad de la eficacia y eficiencia de las políticas de seguridad, depende de la cultura de seguridad y de las normativas que desarrolla en la organización para su adopción, como menciona (Rodríguez, 2009) hoy, la seguridad desde la legislación está en manos de los políticos, quienes son los encargados de decidir, sobre su importancia, los delitos que pueden incurrir y su respectivo castigo.

Según (Merino, C. y Cañizares, R. 2011) los fines principales de las políticas de seguridad son:

- ✓ Proteger mediante controles o medidas.
- ✓ Paliar los efectos de los incidentes de seguridad.
- ✓ Establecer un sistema de clasificación de la información.
- ✓ Definir las responsabilidades en materia de seguridad.
- ✓ Elaborar un conjunto de reglas, estándares y procedimientos.
- ✓ Especificar los efectos que conlleva el incumplimiento de la política de seguridad.
- ✓ Evaluar los riesgos.
- ✓ Verificar el funcionamiento de las medidas / controles de seguridad.
- ✓ Formar a los usuarios en la gestión de la seguridad.

- ✓ Controlar el tráfico de información y de datos.
- ✓ Observar y cumplir la legislación.
- ✓ Proteger el capital intelectual de la organización.
- ✓ Reducir las posibilidades de indisponibilidad.
- ✓ Defender los activos.
- ✓ Controlar el funcionamiento de las medidas de seguridad.

Considerando ello, al establecer dichas políticas, el incumplimiento de las mismas por parte del personal podrá dar lugar a responsabilidad disciplinaria, y al ejercicio de los procedimientos legales por la empresa.

2.3 DEFINICIONES DE TÉRMINOS BÁSICOS.

- **Activo: "**Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos". (UNE 71504, 2008)
- **Amenaza: "**Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización". (UNE 71504, 2008)

- **Análisis de impacto**: “Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización” (UNE 71504, 2008).
- **Análisis de riesgos:** “Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Análisis del riesgo Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo”. (UNE-ISO Guía 73, 2010)
- **Autenticidad**: “Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos”. (UNE 71504, 2008)
- **Confidencialidad:** “Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados”. (UNE 71504, 2008)
- **Degradación de valor de un activo:** “Pérdida de valor de un activo como consecuencia de la materialización de una amenaza”.
- **Disponibilidad:** “Característica que previene contra la denegación no autorizada de acceso a activos del dominio”. (MAGERIT, 2012)
- **Frecuencia: “**Tasa de ocurrencia de una amenaza. Número de sucesos o de efectos en una unidad de tiempo” (ISO Guide 73, 2009)
- **Gestión de riesgos**: “Selección e implantación de las medidas o ‘salvaguardas’ de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de

riesgos se basa en los resultados obtenidos en el análisis de los riesgos". (MAGERIT, 2012)

- **Impacto**: "Consecuencia que sobre un activo tiene la materialización de una amenaza". (MAGERIT, 2012)
- **Integridad: "**Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio". (MAGERIT, 2012)
- **Plan de seguridad**: Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.
- **Probabilidad**: "Posibilidad de que un hecho se produzca". (UNE-ISO Guía 73, 2010)
- **Políticas de seguridad**: "Es una o más reglas de seguridad, procedimientos, prácticas o directrices impuestas por una organización sobre sus operaciones". (MAGERIT, 2012)
- **Riesgo**: "Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización". (MAGERIT, 2012)
- **Salvaguarda:** "Procedimiento o mecanismo tecnológico que reduce el riesgo. Control: Medida que modifica un riesgo". (UNE-ISO Guía 73, 2010)

- **Seguridad de la información**: “Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables”. (UNE 71504, 2008)
- **Vulnerabilidad:** “Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia”. (UNE-ISO Guía 73, 2010).

III. MARCO METODOLÓGICO

3.1 Nivel y tipo de investigación.

- **Nivel**: Es explicativo, porque determina si la Metodología Magerit V3 incide significativamente en la seguridad de la información.
- **Tipo**: Es aplicada, porque se va predecir el comportamiento de la Metodología Magerit V3 en la seguridad de Información de la Municipalidad de Pillco Marca – 2019 (Hernández S., Fernández C., & Baptista L., 2014).

3.2 Diseño de la investigación.

Es Cuasi-experimental, la evaluación se aplica en dos momentos: PRE y POST test, con un solo grupo **(SENA, 2014).** De esta manera se realizará un análisis antes y después de la Aplicación de la Metodología Magerit V3.

Donde:

GE = Activos informáticos

O1= Pre - Observación, medición

O2= Post - Observación, medición

X = Estimulo

Esquema de la Investigación

En el diseño de pre prueba – post prueba:

GE: O1 --- X ----O2

Tabla 3.
Diseño de investigación

Pre - Observación, medición	Estimulo	Post - Observación, medición
O1	X	O2
Activos informáticos estado inicial	Metodología Magerit V3	Activos informáticos estado final

Fuente: elaboración propia

3.3 Determinación de universo/Población.

La población está conformada por los activos informáticos que se encuentra dentro de la Municipalidad Distrital de Pillco Marca.

N= 103

3.4 Selección de muestra.

Para hallar la muestra se utilizó el método de muestreo no probabilístico de tipo intencional o de conveniencia, se caracteriza por un esfuerzo deliberado de obtener muestras "representativas".

n = 103

3.5 Técnicas e instrumentos de recolección de dato.

Tabla 4.
Técnicas e Instrumentos

TÉCNICAS	INSTRUMENTOS
La observación: Esta técnica se usa con el fin de estudiar a las personas en sus actividades de grupo y como miembros de la organización. Permite al analista determinar que se está haciendo, como se está haciendo, quien lo hace, cuando se lleva a cabo, cuanto tiempo toma, dónde se hace y por qué se hace.	-Fichas de observación -Cámara fotográfica.
La Entrevista: Su propósito es obtener información general, medir opiniones, actitudes, percepciones sobre una situación o problema de investigación. Se realizó la entrevista semiestructurada.	- Cuestionario

Fuente: elaboración propia

3.6 Procesamiento y presentación de datos.

Para el procesamiento de los datos se utilizará el SPSS, Minitab y Excel para analizar los resultados de los ítems cuantificables.

- **Elaboración de plantillas en Excel 2016-activos:** Se elaboró una plantilla en Excel de acuerdo a los parámetros de la Metodología MARGERIT V3, con la finalidad de poder ingresar, procesar y analizar los datos relacionados a los activos.
- **Procesamiento y presentación del resultado de la investigación.** Se utilizará SPSS para analizar y realizas las pruebas de hipótesis.

IV. APLICACIÓN DE LA METODOLOGÍA MAGERIT V3

4.1 ANÁLISIS DE RIESGOS

Se realiza a través de un conjunto de actividades y son los siguientes:

4.1.1 CARACTERIZACIÓN DE LOS ACTIVOS:

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado “modelo de valor”.

Tarea MAR.11: Identificación de los activos

Tarea MAR.13: Valoración de los activos

	N°	CAPA	CÓDIGO	ACTIVO	UN	COSTO UNITARIO	COSTO TOTAL	DIMENSIONES				
								[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS	[dge]	Datos de gestión interna	-	-	-	9	8	6	7	7
	AED2		[mul]	Multimedia (información de audio, video)	-	-	-	4		3	5	
	AED3	INFORMACIÓN [info]	[doc]	Documentos	-	-	-	8	7	7	10	8
	AED4		[inf]	Informes	-	-	-	9		6	8	7
	AED5		[exp]	Expedientes	-	-	-	9	9	7		6
	AED6		[tram]	Trámites	-	-	-	9	9	7	8	7
	AED7		[ipu]	Información pública	-	-	-	9	8	7	8	
	AED8		[ipe]	Información personal	-	-	-	9	8	7	9	8
	AED9		[icl]	Información clasificada	-	-	-	9	8	7	8	7
	AED10	SERVICIO [service]	[sei]	Servicio de Internet	-	-	-	9	8	7	6	7
	AED11		[sep]	Servicio de impresión	-	-	-	8		7	5	
	AED12		[idm]	Gestión de identidades	-	-	-	9	9	9	9	7
	AED13		[dir]	Servicios de directorio	-	-	-	9	8		8	8
	AED14		[email]	Correo electrónico	-	-	-	9	6	9	9	8
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [SW]	[siaf]	SIAF	-	-	-	9	9	7	9	7
	APS2		[aut]	Autocad	30	S/.165.00	S/.4,950.00	5		5	6	5
	APS3		[afp]	Adobe flash player	104	S/.25.00	S/.2,600.00	2	3		4	
	APS4		[siga]	SIGA	-	-	-	9	9	7	9	6
	APS5		[off]	Microsoft Office Professional Plus 2010	104	S/.144.00	S/.14,976.00	6	2	3	7	6
	APS6		[msp]	Ms project	104	S/.144.00	S/.14,976.00	2	4		3	
	APS7		[av]	Antivirus ESET NOD32	104	S/.25.00	S/.2,600.00	9	9	8	9	6
	APS8		[os]	Sistema operativo Windows	104	S/.280.00	S/.29,120.00	8	8	2	7	5

	APS9		[bck]	Sistema de backup	-	-	-	8	9	3	7	6
	APS10		[gm]	GESMUN	-	-	-	9	7	5	6	6
	APS11		[web]	Pagina Web (munipillcomarca.com.pe)	1	S/.1,500.00	S/.1,500.00	8	6			6
	APS12		[std]	Sistema de tramite documentario(escritorio)	1	S/.2,500.00	S/.2,500.00	9		8	7	5
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [HW]	[ipm]	Impresora multifuncional	11	S/.250.00	S/.2,750.00	9	9		3	
	EIH2		[sva]	Servidor de archivos	1	S/.8,000.00	S/.8,000.00	9	9	9	7	4
	EIH3		[svc]	Servidor de impresión	3	S/.150.00	S/.450.00	6	3		4	
	EIH4		[cpu]	Microprocesador(también llamado CPU)	104	S/.207.00	S/.21,528.00	10	8	8	8	4
	EIH5		[m]	Motherboard o placa madre	104	S/.260.00	S/.27,040.00	10	9	9	9	4
	EIH6		[mr]	Memoria RAM	104	S/.180.00	S/.18,720.00	10	9	9	9	4
	EIH7		[dd]	Disco Duro	104	S/.270.00	S/.28,080.00	8	9	9	9	4
	EIH8		[lo]	Lectores ópticos	104	S/.150.00	S/.15,600.00	8	9	9	9	4
	EIH9		[trg]	Tarjeta Red, Gráfica y Sonido	104	S/.50.00	S/.5,200.00	8	9	9	9	4
	EIH10		[ms]	Mouse	104	S/.50.00	S/.5,200.00	10	9	9	9	5
	EIH11		[tc]	Teclado	104	S/.30.00	S/.3,120.00	10	9	9	9	4
	EIH12		[mon]	Monitor	104	S/.550.00	S/.57,200.00	10	9	9	9	5
	EIH13		[mrom]	Memoria ROM	104	S/.150.00	S/.15,600.00	10	9	9	9	5
	EIH14		[dis]	Disipador(culer)	104	S/.15.00	S/.1,560.00	10	9	9	9	5
	EIH15		[fdp]	Fuente de Poder	104	S/.194.00	S/.20,176.00	10	9	9	9	5
	EIH16		[cIS]	Cable IDE/SATA	104	S/.15.00	S/.1,560.00	10	9	9	9	5
	EIH17		[ucd]	Unidad de CD/DVD	104	S/.180.00	S/.18,720.00	7	7	6	5	5
	EIH18		[paw]	Punto de acceso wireless	5	S/.250.00	S/.1,250.00	8	5	3	3	4
	EIH19		[rpt]	Radio portátil	35	S/.240.00	S/.8,400.00	6	7	9	3	3
	EIH20		[mvf]	Teléfono móvil	30	S/.500.00	S/.15,000.00	4	6	5	6	2
	EIH21		[tbl]	Tablet	6	S/.2,000.00	S/.12,000.00	3	3		5	
	EIH22		[tvs]	Televisor	3	S/.1,500.00	S/.4,500.00	9	9	2	2	
	EIH23		[caf]	Cámaras fijas	14	S/.350.00	S/.4,900.00	7	7	4	4	3
	EIH24		[cam]	Cámaras móviles	6	S/.750.00	S/.4,500.00	7	8	8	5	4
	EIH25		[cap]	Cámara portátil	3	S/.650.00	S/.1,950.00	4	3	4	2	1

	EIH26		[nvr]	Grabador de video	3	S/.900.00	S/.2,700.00	7		4	3	5
	EIH27		[frw]	Cortafuego	1	S/.350.00	S/.350.00	7	5	2	4	5
	EIH28		[svc]	Servidor SIAF	1	S/.25,000.00	S/.25,000.00	8	7	5		3
	EIH29		[pc]	Laptop	15	S/.2,500.00	S/.2,485.00	10	9	8	8	5
	EIH30		[scan]	Escaner	15	S/.450.00	S/.6,750.00	7	8	5	5	4
	EIH31		[st]	Switch	35	S/.350.00	S/.12,250.00	10	8	9	5	5
	EIH32		[md]	Modem	25	S/.250.00	S/.6,250.00	10		9	3	5
	EIH33		[rout]	Router	15	S/.450.00	S/.6,750.00	10	9	7	7	5
	EIH34		[ups]	UPS	50	S/.550.00	S/.27,500.00	10	9	7		3
	EIH35		[pt]	Pozo a tierra	1	S/.980.00	S/.980.00	8	9	7		3
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [COM]	[lan]	Red local	-	-	-	9	7	9	3	3
	CRC2		[ite]	Internet	1	S/.1,000.00	S/.1,000.00	8	9	4	3	4
	CRC3		[ptp]	Punto a punto	-	-	-	9	8		2	
	CRC4		[vpn]	Red privada virtual	-	-	-	8	7	8	1	4
	CRC5		[rte]	Red telefónica	1	S/.100.00	S/.100.00	7		9	2	3
	CRC6		[ads]	ADSL	-	-	-	9		7		5
	CRC7		[crd]	Comunicaciones radio	-	-	-	9	6	7	3	3
	CRC8		[wif]	Red inalámbrica	-	-	-	9	5		3	2
	CRC9		[mob]	Telefonía móvil	-	-	-	4	4	3	2	4
	CRC10		[rmv]	Red microondas	-	-	-	6	2		3	3
SOPORTES DE INFORMACIÓN [spi]	SIS1	SOPORTE [media]	[dsk]	Almacenamiento en la nube	-	-	-	7	4	7		7
	SIS2		[cdv]	CD / DVD	-	-	-	2	3	3	4	
	SIS3		[pml]	Proyector multimedia	3	S/.1,700.00	S/.5,100.00	3	4			4
	SIS4		[usb]	Dispositivo USB	25	S/.35.00	S/.875.00	9	9	2	3	
	SIS5		[tjm]	Tarjeta de memoria	5	S/.80.00	S/.400.00	2		3	2	4
	SIS6		[hdv]	Hard drive	10	S/.250.00	S/.2,500.00	3	4	3	3	4
EQUIPAMIENTO AUXILIAR	EAE1	EQUIPAMIENTO [aux]	[ups]	Sistema de alimentación ininterrumpida	5	-	-	9	6		2	3
	EAE2		[fal]	Fuentes de alimentación	-	-	-	7	4	9	9	2
	EAE3		[cbl]	Cableado	-	-	-	8	5		2	5

	EAE4		[mbl]	Mobiliario	-	-	-	7		4		3
	EAE5		[eqc]	Equipos de climatización	3	S/.935.00	S/.2,805.00	6	7		1	3
	EAE6		[cbl]	Cable eléctrico	-	-	-	6	5	2		
	EAE7		[fbr]	Fibra óptica	-	-	-	7	4		3	4
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[off]	Oficinas	-	-	-	6	5	3	3	
	INI2		[tlr]	Auditorio	-	-	-	7	4			3
	INI3		[grt]	Centro Informatico	-	-	-	9	4	9	4	
	INI4		[vhc]	Estacionamiento	-	-	-	6	4	2		4
	INI5		[dep]	Centro de vigilancia	-	-	-	6	5	7		4
PERSONAL [per]	PSP1	PERSONAL [P]	[alc]	Alcaldía	1	-	-	9	7	5	3	3
	PSP2		[gg]	Gerencia general	1	-	-	9	7	5	3	3
	PSP3		[gsg]	Gerencia de secretaria general	4	-	-	9	7	5	3	3
	PSP4		[ga]	Gerencia de administración	10	-	-	9	7	5	3	3
	PSP5		[gat]	Gerencia de administración tributaria.	8	-	-	9	7	5	3	3
	PSP6		[gdse]	Gerencia de desarrollo social y económico	12	-	-	9	7	5	3	3
	PSP7		[gma]	Gerencia de medio ambiente	4	-	-	9	7	5	3	3
	PSP8		[gid]	Gerencia de infraestructura y desarrollo territorial	10	-	-	9	7	5	3	3
	PSP9		[gid]	Gerencia de planeamiento y presupuesto	3	-	-	9	7	5	3	3
	PSP10		[gaj]	Gerencia de asesoría jurídica	2	-	-	9	7	5	3	3
	PSP11		[aei]	Area de estadistica e informatica	2	-	-	9	7	5	3	3
	PSP12		[pdp]	Personal de apoyo	7	-	-	9	7		2	3
	PSP13		[usx]	Usuarios Externos	-	-	-	9	7		2	3
	PSP14		[pvd]	Proveedores	-	-	-	9	7		2	3

4.1.2 CARACTERIZACIÓN DE LAS AMENAZAS

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

Tarea MAR.21: Identificación de las amenazas

Tarea MAR.22: Valoración de las amenazas

	N°	CÓDIGO	ACTIVO	PROBAB	DIMENSIONES				
					[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	[dge]	Datos de gestión interna	4	70%	80%	70%	60%	10%
		OI8	Interrupción de otros servicios y suministros esenciales[I8]	4	70%	40%			
		EF10	Destrucción de información[F10]	3	40%	80%	30%		
		AI11	Modificación deliberada de la información[A11]	5		50%	30%	60%	
		AI13	Divulgación de información[A13]	4			70%	20%	10%
	AED2	[mul]	Multimedia (información de audio, video)	4	80%	80%	70%	50%	20%
		OI9	Degradación de los soportes de almacenamiento de la información[I9]	4	50%	70%			
		EF7	Errores de re - encaminamiento[F7]	3		80%	70%		20%
		AI4	Uso no previsto[A4]	4	80%			50%	

AED3	**[doc]**	**Documentos**	**5**	**60%**	**70%**	**70%**	**30%**	**40%**
	AI12	Destrucción de información[A12]	**4**	30%	70%	40%		
	AI13	Divulgación de información[A13]	**5**			70%	30%	40%
	OI9	Degradación de los soportes de almacenamiento de la información[I9]	**5**	60%	50%			
	OI6	Condiciones inadecuadas de temperatura o humedad[I6]	**5**	10%				
AED4	**[inf]**	**Informes**	**4**	**70%**	**70%**	**50%**	**50%**	**40%**
	EF9	Fugas de información[F9]	**4**	10%		50%	50%	40%
	DN2	Daños por agua[N.2]	**4**	70%	70%			
	DN1	Fuego[N.1]	**3**	20%	40%			
AED5	**[exp]**	**Expedientes**	**4**	**70%**	**70%**	**70%**	**40%**	**30%**
	DN2	Daños por agua[N.2]	**3**	70%	70%			
	OI9	Degradación de los soportes de almacenamiento de la información[I9]	**4**	30%		70%	40%	
	EF1	Errores de los usuarios[F1]	**4**	10%	40%		20%	30%
AED6	**[tram]**	**Trámites**	**5**	**70%**	**70%**	**70%**	**40%**	**30%**
	EF9	Fugas de información[F9]	**5**	30%		70%	10%	
	EF10	Destrucción de información[F10]	**5**	70%	70%		40%	30%
	AI4	Uso no previsto[A4]	**4**	10%				
AED7	**[ipu]**	**Información pública**	**5**	**70%**	**70%**	**60%**	**30%**	**40%**
	EF1	Errores de los usuarios[F1]	**5**		30%		30%	40%
	EF5	Deficiencias en la organización[F5]	**4**	40%		20%		
	EF9	Fugas de información[F9]	**5**	70%	70%	60%	20%	

	AED8	[ipe]	Información personal	5	70%	70%	70%	40%	60%
		EF10	Destrucción de información[F10]	5	70%	70%	10%		
		EF9	Fugas de información[F9]	5	40%		70%	30%	60%
		AI3	Abuso de privilegios de acceso[A3]	5		50%		40%	20%
	AED9	[icl]	Información clasificada	4	70%	70%	80%	40%	40%
		AI4	Uso no previsto[A4]	3		70%			20%
		EF9	Fugas de información[F9]	4	30%		80%	20%	40%
		AI11	Modificación deliberada de la información[A11]	4	70%	50%		40%	10%
	AED10	[sei]	Servicio de Internet	4	80%	70%	70%	30%	40%
		OI4	Avería de origen físico o lógico[I4]	4	50%	50%			20%
		OI5	Corte del suministro eléctrico[I5]	4	80%		40%		
		EF14	Caída del sistema por agotamiento de recursos[F14]	3	30%	70%			
		EF7	Errores de re - encaminamiento[F7]	4	20%			30%	40%
		OI7	Fallo de servicios de comunicaciones[I7]	4	50%		70%		
	AED11	[sep]	Servicio de impresión	4	70%	70%	50%	30%	50%
		EF4	Errores de configuración[F4]	4		30%		10%	
		EF1	Errores de los usuarios[F1]	3		70%	50%	30%	50%
		OI4	Avería de origen físico o lógico[I4]	4	70%				
	AED12	[idm]	Gestión de identidades	3	70%	60%	50%	30%	30%
		EF3	Errores de monitorización (log)[F3]	2		20%	50%		30%
		EF8	Errores de secuencia[F8]	4	70%				
		AI1	Manipulación de la configuración[A1]	4		60%	20%	30%	
	AED13	[dir]	Servicios de directorio	3	70%	60%	50%	30%	40%

		EF2	Errores del administrador[F2]	4		60%		30%	
		EF4	Errores de configuración[F4]	3		20%	50%	20%	40%
		EF8	Errores de secuencia[F8]	2	70%			10%	
	AED14	[email]	Correo electrónico	4	80%	70%	40%	30%	30%
		OI4	Avería de origen físico o lógico[I4]	3	30%	70%			
		OI7	Fallo de servicios de comunicaciones[I7]	4	80%	50%			
		EF1	Errores de los usuarios[F1]	5	30%	20%	40%	30%	30%
		OI8	Interrupción de otros servicios y suministros esenciales[I8]	4	50%	50%			
APLICACIONES INFORMÁTICAS [apps]	APS1	[siaf]	SIAF	4	80%	70%	70%	50%	40%
		EF2	Errores del administrador[F2]	5		70%	70%	50%	40%
		EF8	Errores de secuencia[F8]	3		40%		20%	
		EF11	Vulnerabilidades de los programas (software)[F11]	4	80%				
	APS2	[aut]	Autocad	4	80%	70%	70%	70%	40%
		EF12	Errores de mantenimiento o actualización de software[F12]	5	50%		70%		
		EF4	Errores de configuración[F4]	4	80%	70%		70%	40%
		EF8	Errores de secuencia[F8]	2		50%		10%	
	APS3	[afp]	Adobe flash player	3	80%	50%	50%	60%	30%
		AI1	Manipulación de la configuración[A1]	2	80%		50%		
		EF12	Errores de mantenimiento o actualización de software[F12]	3	40%	50%		60%	30%
	APS4	[siga]	SIGA	3	80%	30%	60%	50%	30%
		EF11	Vulnerabilidades de los programas (software)[F11]	4	40%	30%			
		EF9	Fugas de información[F9]	3	80%		60%	50%	30%
		EF14	Caída del sistema por agotamiento de recursos[F14]	3	40%				

APS5	[off]	Microsoft Office Professional Plus 2010	3	60%	60%	50%	70%	50%
	AI1	Manipulación de la configuración[A1]	3	60%	60%		70%	50%
	EF12	Errores de mantenimiento o actualización de software[F12]	3	30%	20%	50%	10%	
APS6	[msp]	Ms project	3	70%	50%	60%	30%	40%
	EF11	Vulnerabilidades de los programas (software)[F11]	2	40%	50%		30%	
	EF12	Errores de mantenimiento o actualización de software[F12]	3	70%		60%		40%
APS7	[av]	Antivirus ESET NOD32	4	90%	60%	50%	40%	50%
	EF4	Errores de configuración[F4]	2	20%	20%	30%	40%	50%
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	4	90%	60%	50%	20%	
	AI1	Manipulación de la configuración[A1]	5	30%		20%		40%
	EF6	Difusión de software dañino[F6]	4		30%			
APS8	[os]	Sistema operativo Windows	3	80%	60%	40%	50%	50%
	AI3	Abuso de privilegios de acceso[A3]	4	20%	40%		30%	
	AI4	Uso no previsto[A4]	3	30%				
	AI7	Acceso no autorizado[A7]	2	80%			50%	50%
	EF2	Errores del administrador[F2]	4	30%	60%	40%		
APS9	[bck]	Sistema de backup	3	80%	70%	40%	40%	50%
	AI1	Manipulación de la configuración[A1]	2	30%			40%	
	EF4	Errores de configuración[F4]	3	80%	70%	40%	20%	50%
APS10	[gm]	GESMUN	3	70%	60%	70%	50%	30%
	AI1	Manipulación de la configuración[A1]	2	30%			40%	
	EF11	Vulnerabilidades de los programas (software)[F11]	4	40%	60%			

		EF9	Caída del sistema por agotamiento de recursos[F14]	3	70%		70%	50%	30%
		EF14	Destrucción de información[F10]	3	40%				
	APS11	[web]	Pagina Web (munipillcomarca.com.pe)	3	80%	70%	60%	30%	50%
		AI1	Manipulación de la configuración[A1]	4	50%	60%	20%	30%	
		AI14	Manipulación de programas[A14]	2		70%			50%
		EF14	Caída del sistema por agotamiento de recursos[F14]	3	60%				
		EF11	Vulnerabilidades de los programas (software)[F11]	4	80%	60%	60%	30%	
		EF8	Errores de secuencia[F8]	4		60%		20%	
	APS12	[std]	Sistema de tramite documentario(escritorio)	3	70%	20%	60%	60%	50%
		AI2	Suplantación de la identidad del usuario[A2]	2		20%	50%	60%	10%
		AI13	Divulgación de información[A13]	4	70%		60%		
		AI9	Repudio[A9]	3		10%		40%	50%
EQUIPOS INFORMÁTICOS [einf]	EIH1	[ipm]	Impresora multifuncional	5	80%	60%	40%	50%	50%
		OI4	Avería de origen físico o lógico[I4]	5	80%	30%	40%	20%	50%
		EF1	Errores de los usuarios[F1]	4	40%	60%		50%	30%
	EIH2	[sva]	Servidor de archivos	4	80%	80%	70%	60%	40%
		DN4	Fenómenos Climáticos[N.4]	4	30%				
		OI5	Corte del suministro eléctrico[I5]	4	80%	40%			40%
		OI7	Fallo de servicios de comunicaciones[I7]	4	60%		20%	40%	30%
		EF12	Errores de mantenimiento o actualización de software[F12]	4	40%	80%	70%	60%	40%
		OI2	Contaminación Mecánica[I2]	4	30%				
	EIH3	[svc]	Servidor de impresión	4	70%	70%	60%	70%	50%
		DN4	Fenómenos Climáticos[N.4]	4	50%				

	OI5	Corte del suministro eléctrico[I5]	4	50%	70%			
	OI7	Fallo de servicios de comunicaciones[I7]	3	70%	60%		50%	30%
	EF12	Errores de mantenimiento o actualización de software[F12]	4	40%	50%	60%	70%	50%
	OI2	Contaminación Mecánica[I2]	4	20%				
EIH4	**[cpu]**	**Microprocesador(también llamado CPU)**	**4**	**80%**	**70%**	**70%**	**20%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			20%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	4	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH5	**[m]**	**Motherboard o placa madre**	**4**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	4	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%

	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH6	[mr]	Memoria RAM	4	80%	70%	70%	10%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	3	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH7	[dd]	Disco Duro	4	80%	70%	70%	10%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	3	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH8	[lo]	Lectores ópticos	3	80%	70%	70%	10%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				

	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH9	**[trg]**	**Tarjeta Red, Gráfica y Sonido**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH10	**[ms]**	**Mouse**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			

	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH11	**[tc]**	**Teclado**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH12	**[mon]**	**Monitor**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%

	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH13	[mrom]	Memoria ROM	3	80%	70%	70%	10%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH14	[dis]	Disipador(culer)	3	80%	70%	70%	10%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH15	[fdp]	Fuente de Poder	3	80%	70%	70%	10%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				

	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH16	**[clS]**	**Cable IDE/SATA**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH17	**[ucd]**	**Unidad de CD/DVD**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			

		AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
		AI15	Manipulación de los equipos[A15]	4	60%		60%		
		AI16	Robo[A16]	3	60%		70%		10%
		OI5	Corte del suministro eléctrico[I5]	4	60%				
	EIH18	**[paw]**	**Punto de acceso wireless**	**4**	**60%**	**50%**	**50%**	**30%**	**40%**
		OI4	Avería de origen físico o lógico[I4]	3	40%	40%	50%	10%	20%
		OI7	Fallo de servicios de comunicaciones[I7]	4	60%	50%	20%	30%	40%
	EIH19	**[rpt]**	**Radio portátil**	**4**	**70%**	**50%**	**40%**	**40%**	**50%**
		OI4	Avería de origen físico o lógico[I4]	4	70%		20%	40%	
		EF4	Errores de configuración[F4]	3	20%	50%	40%		50%
	EIH20	**[mvf]**	**Teléfono móvil**	**4**	**60%**	**50%**	**50%**	**20%**	**50%**
		OI8	Interrupción de otros servicios y suministros esenciales[I8]	3		10%			
		EF4	Errores de configuración[F4]	4	60%	50%	50%	20%	50%
	EIH21	**[tbl]**	**Tablet**	**3**	**60%**	**60%**	**30%**	**50%**	**50%**
		EF1	Errores de los usuarios[F1]	4	60%	20%	30%		50%
		AI1	Manipulación de la configuración[A1]	2	20%	60%	20%	50%	
	EIH22	**[tvs]**	**Televisor**	**4**	**60%**	**60%**	**30%**	**60%**	**40%**
		AI1	Manipulación de la configuración[A1]	3	60%		30%	60%	40%
		AI4	Uso no previsto[A4]	4		60%			
	EIH23	**[caf]**	**Cámaras fijas**	**4**	**70%**	**60%**	**40%**	**50%**	**50%**
		DN2	Daños por agua[N.2]	3	10%	40%			
		OI2	Contaminación Mecánica[I2]	3	50%				
		OI4	Avería de origen físico o lógico[I4]	4	70%	60%	40%	50%	50%

	DN3	Tormentas Eléctricas[N.3]	4	10%	10%			
EIH24	[cam]	Cámaras móviles	4	60%	70%	60%	60%	40%
	OI4	Avería de origen físico o lógico[I4]	3	50%	60%	60%	60%	40%
	OI5	Corte del suministro eléctrico[I5]	3	60%			10%	
	DN4	Fenómenos Climáticos[N.4]	5	30%	70%			
	OI3	Desastres Industriales[I3]	4	20%				
EIH25	[cap]	Cámara portátil	4	50%	50%	60%	40%	30%
	OI4	Avería de origen físico o lógico[I4]	3	50%	50%	60%	40%	30%
	AI4	Uso no previsto[A4]	4	20%				20%
EIH26	[nvr]	Grabador de video	4	40%	50%	60%	50%	50%
	AI11	Modificación deliberada de la información[A11]	4	10%	50%	60%		
	EF4	Errores de configuración[F4]	4	40%	50%		50%	
	EF2	Errores del administrador[F2]	3	20%	40%		10%	50%
EIH27	[frw]	Cortafuego	3	80%	70%	30%	30%	40%
	EF2	Errores del administrador[F2]	2	30%		20%	30%	20%
	EF12	Errores de mantenimiento o actualización de software[F12]	4	80%	70%	30%		40%
EIH28	[svc]	Servidor SIAF	4	80%	80%	80%	70%	50%
	OI4	Avería de origen físico o lógico[I4]	4	50%	70%			
	OI7	Fallo de servicios de comunicaciones[I7]	3	70%				
	EF4	Errores de configuración[F4]	4		70%	50%	50%	30%
EIH29	[pc]	Laptop	4	80%	80%	70%	70%	10%
	DN4	Fenómenos Climáticos[N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			70%	

	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	4	60%	80%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
	OI5	Corte del suministro eléctrico[I5]	4	60%				
EIH30	**[scan]**	**Escaner**	**3**	**80%**	**70%**	**70%**	**10%**	**10%**
	DN4	Fenómenos Climáticos [N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			10%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		
	AI16	Robo[A16]	3	60%		70%		10%
EIH31	**[st]**	**Switch**	**4**	**80%**	**80%**	**70%**	**50%**	**10%**
	DN4	Fenómenos Climáticos [N.4]	4	50%				
	OI2	Contaminación Mecánica[I2]	3	50%			50%	
	OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
	EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
	AI1	Manipulación de la configuración[A1]	3	60%	80%	60%		
	AI15	Manipulación de los equipos[A15]	4	60%		60%		

		AI16	Robo[A16]	3	60%		70%		10%
		OI5	Corte del suministro eléctrico[I5]	4	60%				
	EIH32	[md]	Modem	4	80%	70%	80%	30%	10%
		DN4	Fenómenos Climáticos[N.4]	4	50%				
		OI2	Contaminación Mecánica[I2]	3	50%			30%	
		OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
		EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
		AI1	Manipulación de la configuración[A1]	3	60%	70%	60%		
		AI15	Manipulación de los equipos[A15]	4	60%		60%		
		AI16	Robo[A16]	3	60%		80%		10%
		OI5	Corte del suministro eléctrico[I5]	4	60%				
	EIH33	[rout]	Router	4	80%	70%	80%	30%	10%
		DN4	Fenómenos Climáticos[N.4]	4	50%				
		OI2	Contaminación Mecánica[I2]	3	50%			30%	
		OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
		EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
		AI1	Manipulación de la configuración[A1]	3	60%	70%	60%		
		AI15	Manipulación de los equipos[A15]	4	60%		60%		
		AI16	Robo[A16]	3	60%		80%		10%
		OI5	Corte del suministro eléctrico[I5]	4	60%				
	EIH34	[ups]	UPS	4	80%	70%	80%	50%	50%

		DN4	Fenómenos Climáticos[N.4]	4	50%				
		OI2	Contaminación Mecánica[I2]	3	50%			50%	
		OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
		EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
		AI1	Manipulación de la configuración[A1]	2	60%	70%	60%		
		AI15	Manipulación de los equipos[A15]	4	60%		60%		
		AI16	Robo[A16]	3	60%		80%		50%
		OI5	Corte del suministro eléctrico[I5]	4	60%				
	EIH35	[pt]	Pozo a tierra	4	80%	70%	80%	50%	50%
		DN4	Fenómenos Climáticos[N.4]	4	50%				
		OI2	Contaminación Mecánica[I2]	3	50%			10%	
		OI4	Avería de origen físico o lógico[I4]	4	70%	50%			
		EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	3	80%	20%			
		AI1	Manipulación de la configuración[A1]	3	60%	70%	60%		
		AI15	Manipulación de los equipos[A15]	4	60%		60%		
		AI16	Robo[A16]	3	60%		80%		10%
		OI5	Corte del suministro eléctrico[I5]	4	60%				
COMUNICACIONES	CRC1	[lan]	Red local	4	80%	70%	50%	40%	30%
		OI7	Fallo de servicios de comunicaciones[I7]	3	80%			20%	
		OI8	Interrupción de otros servicios y suministros esenciales[I8]	4	60%	70%	50%	40%	30%
		EF14	Caída del sistema por agotamiento de recursos[F14]	4	20%				20%

	CRC2	**[ite]**	**Internet**	**4**	**80%**	**70%**	**40%**	**30%**	**40%**
		OI5	Corte del suministro eléctrico[I5]	**5**	60%				
		OI4	Avería de origen físico o lógico[I4]	**3**	40%	70%	40%	30%	40%
		OI3	Desastres Industriales[I3]	**3**	80%				
	CRC3	**[ptp]**	**Punto a punto**	**3**	**70%**	**70%**	**60%**	**40%**	**40%**
		DN2	Daños por agua[N.2]	**3**	50%	10%			
		OI7	Fallo de servicios de comunicaciones[I7]	**3**	70%	60%	30%	40%	
		OI4	Avería de origen físico o lógico[I4]	**4**	40%	70%	60%	30%	40%
	CRC4	**[vpn]**	**Red privada virtual**	**4**	**60%**	**60%**	**40%**	**40%**	**30%**
		OI1	Contaminación Electromagnética[I1]	**4**	30%				
		OI8	Interrupción de otros servicios y suministros esenciales[I8]	**3**	60%	60%			30%
		OI7	Fallo de servicios de comunicaciones[I7]	**4**	40%	40%	40%	40%	10%
	CRC5	**[rte]**	**Red telefónica**	**4**	**60%**	**60%**	**70%**	**30%**	**30%**
		OI4	Avería de origen físico o lógico[I4]	**4**		60%	70%	30%	30%
		OI7	Fallo de servicios de comunicaciones[I7]	**3**	60%				10%
	CRC6	**[ads]**	**ADSL**	**3**	**50%**	**60%**	**50%**	**40%**	**30%**
		OI1	Contaminación Electromagnética[I1]	**3**	40%	10%			
		OI7	Fallo de servicios de comunicaciones[I7]	**3**	50%	60%	50%	40%	30%
	CRC7	**[crd]**	**Comunicaciones radio**	**4**	**60%**	**70%**	**40%**	**30%**	**40%**
		OI1	Contaminación Electromagnética[I1]	**3**	60%	40%			
		DN4	Fenómenos Climáticos[N.4]	**4**	60%				
		EF4	Errores de configuración[F4]	**4**	40%	70%	30%	20%	40%
		OI4	Avería de origen físico o lógico[I4]	**3**	20%	30%	40%	30%	

	CRC8	**[wif]**	**Red inalámbrica**	**3**	**80%**	**70%**	**50%**	**50%**	**50%**
		EF4	Errores de configuración[F4]	3		50%		10%	50%
		EF13	Errores de mantenimiento o actualización de equipos o hardware[F13]	4	60%	40%	50%	50%	10%
		OI1	Contaminación Electromagnética[I1]	3	40%	70%			
	CRC9	**[mob]**	**Telefonía móvil**	**4**	**60%**	**70%**	**40%**	**30%**	**40%**
		EF7	Errores de re - encaminamiento[F7]	3	30%	40%	40%	30%	40%
		OI1	Contaminación Electromagnética[I1]	4	60%	70%			
	CRC10	**[rmv]**	**Red microondas**	**4**	**70%**	**50%**	**40%**	**40%**	**10%**
		OI6	Condiciones inadecuadas de temperatura o humedad[I6]	4	40%	30%	30%		
		OI1	Contaminación Electromagnética[I1]	3	70%	50%	40%	40%	10%
SOPORTES DE INFORMACIÓN [spi]	**SIS1**	**[dsk]**	**Almacenamiento en la nube**	**3**	**50%**	**50%**	**40%**	**20%**	**30%**
		AI13	Ataque destructivo[A17]	2	50%	50%	40%	20%	30%
		AI4	Uso no previsto[A4]	3				10%	
	SIS2	**[cdv]**	**CD / DVD**	**3**	**20%**	**50%**	**30%**	**30%**	**20%**
		AI4	Uso no previsto[A4]	3	20%	50%	30%	30%	20%
	SIS3	**[pml]**	**Proyector multimedia**	**3**	**70%**	**60%**	**70%**	**40%**	**30%**
		OI4	Avería de origen físico o lógico[I4]	2	30%	60%	70%	40%	30%
		OI5	Corte del suministro eléctrico[I5]	4	70%			10%	
	SIS4	**[usb]**	**Dispositivo USB**	**4**	**70%**	**40%**	**50%**	**60%**	**40%**
		EF1	Errores de los usuarios[F1]	3	40%	40%	50%	60%	40%
		AI4	Uso no previsto[A4]	4	70%				10%
	SIS5	**[tjm]**	**Tarjeta de memoria**	**3**	**60%**	**50%**	**60%**	**40%**	**30%**

		EF10	Destrucción de información[F10]	3	60%	50%	60%	40%	
		AI4	Uso no previsto[A4]	3	30%				30%
	SIS6	[hdv]	Hard drive	3	60%	60%	60%	60%	40%
		EF1	Errores de los usuarios[F1]	2	50%	10%		60%	40%
		OI4	Avería de origen físico o lógico[I4]	3	60%	60%	60%	50%	20%
EQUIPAMIENTO AUXILIAR [eax]	EAE1	[ups]	Sistema de alimentación ininterrumpida	4	70%	70%	40%	40%	30%
		OI4	Avería de origen físico o lógico[I4]	3	70%	70%	40%	20%	30%
		OI7	Fallo de servicios de comunicaciones[I7]	4	60%	20%		40%	30%
	EAE2	[fal]	Fuentes de alimentación	3	60%	60%	40%	30%	40%
		OI4	Avería de origen físico o lógico[I4]	2	60%	50%	40%	30%	40%
		OI5	Corte del suministro eléctrico[I5]	3	50%	60%			
	EAE3	[cbl]	Cableado	4	90%	80%	30%	30%	20%
		DN4	Fenómenos Climáticos[N.4]	3	40%	10%			
		OI7	Fallo de servicios de comunicaciones[I7]	5	50%	50%	30%	30%	20%
		OI3	Desastres Industriales[I3]	4	90%	80%			
	EAE4	[mbl]	Mobiliario	3	50%	60%	50%	30%	30%
		DN4	Fenómenos Climáticos[N.4]	2	30%	60%			
		OI9	Degradación de los soportes de almacenamiento de la información[I9]	3	50%	40%	50%	30%	30%
	EAE5	[eqc]	Equipos de climatización	4	50%	60%	50%	20%	30%
		OI4	Avería de origen físico o lógico[I4]	3	50%	60%	50%	20%	30%
		OI5	Corte del suministro eléctrico[I5]	4	40%				
	EAE6	[cbl]	Cable eléctrico	4	80%	80%	50%	40%	20%

		OI4	Avería de origen físico o lógico[I4]	4	50%	80%	50%	40%	20%
		OI1	Contaminación Electromagnética[I1]	4		40%			10%
		OI5	Corte del suministro eléctrico[I5]	4	80%				
	EAE7	[fbr]	Fibra óptica	4	80%	70%	50%	20%	40%
		OI6	Condiciones inadecuadas de temperatura o humedad[I6]	3	40%	70%			
		OI7	Fallo de servicios de comunicaciones[I7]	4	80%			20%	20%
		AI13	Ataque destructivo[A17]	4	50%	50%	50%	10%	40%
INSTALACIONES [ins]	INI1	[off]	Oficinas	4	80%	70%	60%	30%	30%
		AI14	Ocupación enemiga[A18]	4	60%	70%	60%	30%	30%
		OI2	Contaminación Mecánica[I2]	3	80%				
	INI2	[tlr]	Auditorio	4	60%	50%	50%	30%	50%
		AI3	Abuso de privilegios de acceso[A3]	3	60%		50%	30%	50%
		AI4	Uso no previsto[A4]	4		50%	30%		
	INI3	[grt]	Centro Informatico	4	90%	80%	80%	30%	60%
		AI7	Acceso no autorizado[A7]	4	90%	80%	50%	30%	60%
		AI11	Modificación deliberada de la información[A11]	4		50%		30%	
		AI4	Uso no previsto[A4]	3			80%		10%
	INI4	[vhc]	Estacionamiento	3	50%	60%	40%	30%	30%
		AI15	Manipulación de los equipos[A15]	2	50%			10%	
		AI7	Acceso no autorizado[A7]	4		60%	40%	30%	30%
	INI5	[dep]	Centro de vigilancia	4	50%	60%	10%	10%	10%
		DN4	Fenómenos Climáticos[N.4]	3	40%	60%			
		OI6	Condiciones inadecuadas de temperatura o humedad[I6]	4	50%	50%	10%	10%	

		OI2	Contaminación Mecánica[I2]	4		50%			10%
PERSONAL [per]	PSP1	[alc]	Alcaldía	3	80%	70%	70%	70%	50%
		AI15	Indisponibilidad del personal[A19]	3	30%	30%			
		AI3	Abuso de privilegios de acceso[A3]	4	40%	50%	30%	40%	50%
		AI2	Suplantación de la identidad del usuario[A2]	3	80%	70%	70%	70%	
	PSP2	[gg]	Gerencia general	4	80%	70%	70%	70%	50%
		AI3	Abuso de privilegios de acceso[A3]	4	40%	50%	30%	40%	50%
		AI2	Suplantación de la identidad del usuario[A2]	3	80%	70%	70%	70%	
	PSP3	[gsg]	Gerencia de secretaria general	4	80%	50%	40%	40%	40%
		AI3	Abuso de privilegios de acceso[A3]	4	80%			10%	20%
		AI2	Suplantación de la identidad del usuario[A2]	3		50%	40%	40%	40%
	PSP4	[ga]	Gerencia de administración	3	80%	70%	70%	50%	40%
		AI3	Abuso de privilegios de acceso[A3]	4	80%		70%	50%	40%
		AI2	Suplantación de la identidad del usuario[A2]	2		70%			30%
	PSP5	[gat]	Gerencia de administración tributaria.	4	80%	60%	50%	40%	70%
		AI3	Abuso de privilegios de acceso[A3]	4	70%		50%	40%	70%
		AI2	Suplantación de la identidad del usuario[A2]	3	80%	60%			
	PSP6	[gdse]	Gerencia de desarrollo social y económico	4	80%	70%	50%	60%	40%
		AI3	Abuso de privilegios de acceso[A3]	4	50%				40%
		AI2	Suplantación de la identidad del usuario[A2]	4	80%	70%	50%	60%	
	PSP7	[gma]	Gerencia de medio ambiente	3	80%	70%	30%	50%	70%
		AI3	Abuso de privilegios de acceso[A3]	2	80%	70%			
		AI2	Suplantación de la identidad del usuario[A2]	3		40%	30%	50%	70%

PSP8	[gid]	Gerencia de infraestructura y desarrollo territorial	4	80%	70%	50%	70%	50%
	AI3	Abuso de privilegios de acceso[A3]	3	40%	30%		70%	50%
	AI2	Suplantación de la identidad del usuario[A2]	4	80%	70%	50%	60%	
PSP9	[gid]	Gerencia de planeamiento y presupuesto	3	80%	70%	30%	70%	70%
	AI3	Abuso de privilegios de acceso[A3]	2	80%	70%			
	AI2	Suplantación de la identidad del usuario[A2]	3		20%	30%	70%	70%
PSP10	[gaj]	Gerencia de asesoría jurídica	3	80%	70%	30%	60%	60%
	AI3	Abuso de privilegios de acceso[A3]	3		30%			
	AI2	Suplantación de la identidad del usuario[A2]	3	80%	70%	30%	60%	60%
PSP11	[aei]	Area de estadistica e informatica	3	70%	70%	70%	60%	50%
	AI3	Abuso de privilegios de acceso[A3]	2	70%				
	AI2	Suplantación de la identidad del usuario[A2]	4		70%	70%	60%	50%
PSP12	[pdp]	Personal de apoyo	3	80%	70%	60%	70%	60%
	AI3	Abuso de privilegios de acceso[A3]	2	80%	50%			
	AI2	Suplantación de la identidad del usuario[A2]	4		70%	60%	70%	60%
PSP13	[usx]	Usuarios Externos	4	80%	70%	70%	40%	30%
	AI3	Abuso de privilegios de acceso[A3]	3	80%	70%	70%	40%	30%
	AI2	Suplantación de la identidad del usuario[A2]	4		30%			
PSP14	[pvd]	Proveedores	3	80%	70%	40%	50%	50%
	AI3	Abuso de privilegios de acceso[A3]	3		70%	40%		50%
	AI2	Suplantación de la identidad del usuario[A2]	3	80%			50%	

4.1.3 CARACTERIZACIÓN DE LAS SALVAGUARDAS

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

MAR.31: Identificación de las salvaguardas pertinentes

Tarea MAR.32: Valoración de las salvaguardas

			ORGANIZANDO LA SEGURIDAD DE LA INFORMACIÓN							
	N°	SALVAGUARDAS	Gestión de activos	Seguridad en RRHH	Seguridad física y ambiental	Gestión de comunicaciones y operaciones	Control de acceso	Adquisición, desarrollo y mantenimiento de SI	Gestión de incidentes de los SI	Gestión de la continuidad del negocio
PROTECCIONES GENERALES U HORIZONTALES	PGH1	Identificación y autenticación					X			
	PGH2	Control de acceso lógico					X			
	PGH3	Segregación de tareas								X
	PGH4	Gestión de incidencias							X	
	PGH5	Herramientas de seguridad			X					
	PGH6	Herramientas contra código dañino						X		
	PGH7	Herramient de detección / prevención de intrusión						X		
	PGH8	Herramienta de chequeo de configuración						X		
	PGH9	Herramienta de análisis de vulnerabilidades				X				
	PGH10	Herramienta de monitorización de tráfico	X					X		X

	PGH11	DLP: Herramienta de monitorización de contenidos	X			X		X		
	PGH12	Gestión de vulnerabilidades				X			X	X
	PGH13	Registro y auditoría	X			X				X
PROTECCIÓN DE LOS DATOS /	PDI1	Copias de seguridad (backup)					X		X	
	PDI2	Aseguramiento de la integridad		X	X				X	X
	PDI3	Cifrado de la información					X	X		
	PDI4	Protección de la información					X	X		
PROTECCIÓN DE LAS CLAVES	PCC1	Gestión de claves criptográficas				X				
	PCC2	Gestión de claves de comunicaciones					X			
	PCC3	Gestión de certificados								X
PROTECCIÓN DE LOS SERVICIOS	PPS1	Aseguramiento de la disponibilidad	X			X			X	X
	PPS2	Aceptación y puesta en operación				X				X
	PPS3	Perfiles de seguridad	X	X	X				X	
	PPS5	Protección de servicios y aplicaciones web				X		X		
	PPS6	Protección del correo electrónico					X	X		
	PPS7	Protección del directorio				X	X	X		
	PPS8	Protección de nombres de dominio (DNS)					X	X		
PROTECCIÓN DE LAS APLICACIONE	PPA1	Copias de seguridad (backup)					X			
	PPA2	Actualizaciones ymantenimiento	X			X		X		X
	PPA3	Protección de las aplicaciones informáticas				X	X	X		X
PROTECCIÓN DE LOS EQUIPOS (HARDWARE)	PPH1	Aseguramiento de la disponibilidad					X	X	X	
	PPH2	Cambios (Actualizaciones y mantenimiento)				X		X		X
	PPH3	Informática móvil			X			X		X
	PPH4	Reproducción de documentos				X	X			

	PPH5	Protección de los equipos informáticos				X		X		X
PROTECCION DE LSO EQUIPOS DE COMUNICACIÓN	PPC1	Autenticación de canal				X	X		X	
	PPC2	Protección de la integridad de los datos intercambiados			X	X		X		
	PPC3	Perfiles de seguridad		X		X				X
	PPC4	Telefonía móvil					X	X		
	PPC5	Seguridad Wireless		X	X		X		X	
	PPC6	Protección de las comunicaciones				X			X	
PROTECCIÓN EN LOS	PPI1	Puntos de interconexión: conexiones entre zonas de confianza				X				X
	PPI2	Protección de los equipos informáticos		X	X	X				
PROTECCIÓN DE LOS SOPORTES DE	PSI1	Aseguramiento de la disponibilidad				X				X
	PSI2	Limpieza de contenidos			X		X		X	
	PSI3	Destrucción de soportes	X				X		X	
	PSI4	Protección de los soportes de información			X		X		X	
PROTECCIÓN DE LOS ELEMENTOS	PEA1	Protección del cableado							X	X
	PEA2	Climatización				X			X	
	PEA3	Suministro eléctrico			X	X				
	PEA4	Aseguramiento de la disponibilidad	X				X		X	
PROTECCIÓN DE LAS INSTALACIONES	PPI1	Diseño								
	PPI2	Defensa de profundidad								
	PPI3	Control de acceso físico					X	X		
	PPI4	Aseguramiento de la disponibilidad								
	PPI5	Protección de las instalaciones	X		X					
SALVAGUARDAS RELATIVAS	SRP1	Gestión del personal		X	X	X		X		
	SRP2	Formación y concienciación				X		X		X
	SRP3	Aseguramiento de la disponibilidad				X		X		

SALVAGUARDAS DE TIPO ORGANIZATIV	STO1	Organización				X				
	STO2	Gestión de riesgos				X				X
	STO3	Planificación de la seguridad				X				
	STO4	Inspecciones de seguridad		X	X					
CONTINUIDAD DE OPERACIO	CDO1	Continuidad del negocio				X				X
	CDO2	Análisis de impacto								X
	CDO3	Plan de recuperación de desastres				X				X
EXTERNALIZACIÓN	EXT1	Niveles de servicio				X				X
	EXT2	Compromiso de confidencialidad					X			
	EXT3	Identificación y calificación del personal encargado		X	X					
	EXT4	Procedimiento de escalado y resolución de incidencias				X		X		X
	EXT5	Asunción de responsabilidades y penalizaciones por incumplimiento		X	X					
	EXT6	Acuerdos para intercambio de información y software				X		X		
ADQUISICIÓN Y DESARROLLO	AYD2	Aplicaciones						X		
	AYD3	Equipos	X							X
	AYD4	Comunicaciones				X				
	AYD5	Soportes de información	X					X		
	AYD6	Productos certificados o acreditados	X			X		X		X

4.1.4 ESTIMACIÓN DEL ESTADO DE RIESGO

Tarea MAR.41: Estimación del impacto

	N°	CAPA	CÓDIGO	ACTIVO	PROB	DIMENSIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS	[dge]	Datos de gestión interna	4	6	6	4	4	1
	AED2		[mul]	Multimedia (información de audio, video)	4	6	0	4	3	0
	AED3	INFORMACIÓN [info]	[doc]	Documentos	5	5	5	5	3	3
	AED4		[inf]	Informes	4	6	0	3	4	3
	AED5		[exp]	Expedientes	4	6	6	5	0	2
	AED6		[tram]	Trámites	5	6	6	5	3	2
	AED7		[ipu]	Información pública	5	6	6	4	2	0
	AED8		[ipe]	Información personal	5	6	6	5	4	5
	AED9		[icl]	Información clasificada	4	6	6	6	3	3
	AED10	SERVICIO [service]	[sei]	Servicio de Internet	4	7	6	5	2	3
	AED11		[sep]	Servicio de impresión	4	6	0	4	2	0
	AED12		[idm]	Gestión de identidades	3	6	5	5	3	2
	AED13		[dir]	Servicios de directorio	3	6	5	0	2	3
	AED14		[email]	Correo electrónico	4	7	4	4	3	2
EQUIPOS INFORMÁTICOS [einf]	APS1	SOFTWARE [SW]	[siaf]	SIAF	4	7	6	5	5	3
	APS2		[aut]	Autocad	4	4	0	4	4	2
	APS3		[afp]	Adobe flash player	3	2	2	0	2	0
	APS4		[siga]	SIGA	3	7	3	4	5	2
	APS5		[off]	Microsoft Office Professional Plus 2010	3	4	1	2	5	3
	APS6		[msp]	Ms project	3	1	2	0	1	0
	APS7		[av]	Antivirus ESET NOD32	4	8	5	4	4	3
	APS8		[os]	Sistema operativo Windows	3	6	5	1	4	3
	APS9		[bck]	Sistema de backup	3	6	6	1	3	3
	APS10		[gm]	GESMUN	3	6	4	4	3	2
	APS11		[web]	Pagina Web (munipillcomarca.com.pe)	3	6	4	0	0	3
	APS12		[std]	Sistema de tramite documentario(escritorio)	3	6	0	5	4	3
EQUIPOS INFORMÁTICOS	EIH1	HARDWARE [HW]	[ipm]	Impresora multifuncional	5	7	5	0	2	0
	EIH2		[sva]	Servidor de archivos	4	7	7	6	4	2
	EIH3		[svc]	Servidor de impresión	4	4	2	0	3	0

	EIH4		[cpu]	Microprocesador(también llamado CPU)	4	8	6	6	2	0
	EIH5		[m]	Motherboard o placa madre	4	8	6	6	1	0
	EIH6		[mr]	Memoria RAM	4	8	6	6	1	0
	EIH7		[dd]	Disco Duro	4	6	6	6	1	0
	EIH8		[lo]	Lectores ópticos	3	6	6	6	1	0
	EIH9		[trg]	Tarjeta Red, Gráfica y Sonido	3	6	6	6	1	0
	EIH10		[ms]	Mouse	3	8	6	6	1	1
	EIH11		[tc]	Teclado	3	8	6	6	1	0
	EIH12		[mon]	Monitor	3	8	6	6	1	1
	EIH13		[mrom]	Memoria ROM	3	8	6	6	1	1
	EIH14		[dis]	Disipador(culer)	3	8	6	6	1	1
	EIH15		[fdp]	Fuente de Poder	3	8	6	6	1	1
	EIH16		[clS]	Cable IDE/SATA	3	8	6	6	1	1
	EIH17		[ucd]	Unidad de CD/DVD	3	6	5	4	1	1
	EIH18		[paw]	Punto de acceso wireless	4	5	3	2	1	2
	EIH19		[rpt]	Radio portátil	4	4	4	4	1	2
	EIH20		[mvf]	Teléfono móvil	4	2	3	3	1	1
	EIH21		[tbl]	Tablet	3	2	2	0	3	0
	EIH22		[tvs]	Televisor	4	5	5	1	1	0
	EIH23		[caf]	Cámaras fijas	4	5	4	2	2	2
	EIH24		[cam]	Cámaras móviles	4	4	6	5	3	2
	EIH25		[cap]	Cámara portátil	4	2	2	2	1	0
	EIH26		[nvr]	Grabador de video	4	3	0	2	2	3
	EIH27		[frw]	Cortafuego	3	6	4	1	1	2
	EIH28		[svc]	Servidor SIAF	4	6	6	4	0	2
	EIH29		[pc]	Laptop	4	8	7	6	6	1
	EIH30		[scan]	Escaner	3	6	6	4	1	0
	EIH31		[st]	Switch	4	8	6	6	5	1
	EIH32		[md]	Modem	4	8	0	7	2	1
	EIH33		[rout]	Router	4	8	6	6	3	1
	EIH34		[ups]	UPS	4	8	6	6	0	4
	EIH35		[pt]	Pozo a tierra	4	6	6	6	0	4
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓ	[lan]	Red local	4	7	5	5	1	1
	CRC2		[ite]	Internet	4	6	6	2	1	2
	CRC3		[ptp]	Punto a punto	3	6	6	0	1	0
	CRC4		[vpn]	Red privada virtual	4	5	4	3	0	1

	CRC5		[rte]	Red telefónica	4	4	0	6	1	1
	CRC6		[ads]	ADSL	3	5	0	4	0	2
	CRC7		[crd]	Comunicaciones radio	4	5	4	3	1	1
	CRC8		[wif]	Red inalámbrica	3	7	4	0	2	1
	CRC9		[mob]	Telefonía móvil	4	2	3	1	1	2
	CRC10		[rmv]	Red microondas	4	4	1	0	1	0
SOPORTES DE INFORMACIÓN [spi]	SIS1	SOPORTE [media]	[dsk]	Almacenamiento en la nube	3	4	2	3	0	2
	SIS2		[cdv]	CD / DVD	3	0	2	1	1	0
	SIS3		[pml]	Proyector multimedia	3	2	2	0	0	1
	SIS4		[usb]	Dispositivo USB	4	6	4	1	2	0
	SIS5		[tjm]	Tarjeta de memoria	3	1	0	2	1	1
	SIS6		[hdv]	Hard drive	3	2	2	2	2	2
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[ups]	Sistema de alimentación ininterrumpida	4	6	4	0	1	1
	EAE2		[fal]	Fuentes de alimentación	3	4	2	4	3	1
	EAE3		[cbl]	Cableado de red	4	8	6	0	1	1
	EAE4		[mbl]	Mobiliario	3	4	0	2	0	1
	EAE5		[eqc]	Equipos de climatización	4	3	4	0	0	1
	EAE6		[cbl]	Cable eléctrico	4	6	6	1	0	0
	EAE7		[fbr]	Fibra óptica	4	6	3	0	1	2
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[off]	Oficinas	4	5	4	2	1	0
	INI2		[tlr]	Auditorio	4	4	2	0	0	2
	INI3		[grt]	Centro Informatico	4	8	3	7	1	0
	INI4		[vhc]	Estacionamiento	3	3	2	1	0	1
	INI5		[dep]	Centro de vigilancia	4	3	3	1	0	0
PERSONAL [per]	PSP1	PERSONAL [P]	[alc]	Alcaldía	3	7	5	4	2	2
	PSP2		[gg]	Gerencia general	4	7	5	4	2	2
	PSP3		[gsg]	Gerencia de secretaria general	4	7	4	2	1	1
	PSP4		[ga]	Gerencia de administración	3	7	5	4	2	1
	PSP5		[gat]	Gerencia de administración tributaria.	4	7	4	3	1	2
	PSP6		[gdse]	Gerencia de desarrollo social y económico	4	7	5	3	2	1
	PSP7		[gma]	Gerencia de medio ambiente	3	7	5	2	2	2
	PSP8		[gid]	Gerencia de infraestructura y desarrollo territorial	4	7	5	3	2	2
	PSP9		[gid]	Gerencia de planeamiento y presupuesto	3	7	5	2	2	2
	PSP10		[gaj]	Gerencia de asesoría jurídica	3	7	5	2	2	2

	PSP11		[aei]	Area de estadistica e informatica	3	6	5	4	2	2
	PSP12		[pdp]	Personal de apoyo	3	7	5	0	1	2
	PSP13		[usx]	Usuarios Externos	4	7	5	0	1	1
	PSP14		[pvd]	Proveedores	3	7	5	0	1	2

Tarea MAR.42: Estimación del riesgo

	N°	CAPA	CÓDIGO	ACTIVO	PROB	DIMENSIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS	[dge]	Datos de gestión interna	4	24	24	16	16	4
	AED2		[mul]	Multimedia (información de audio, video)	4	24	0	16	12	0
	AED3	INFORMACIÓN [info]	[doc]	Documentos	5	25	25	25	15	15
	AED4		[inf]	Informes	4	24	0	12	16	12
	AED5		[exp]	Expedientes	4	24	24	20	0	8
	AED6		[tram]	Trámites	5	30	30	25	15	10
	AED7		[ipu]	Información pública	5	30	30	20	10	0
	AED8		[ipe]	Información personal	5	30	30	25	20	25
	AED9		[icl]	Información clasificada	4	24	24	24	12	12
	AED10	SERVICIO [service]	[sei]	Servicio de Internet	4	28	24	20	8	12
	AED11		[sep]	Servicio de impresión	4	24	0	16	8	0
	AED12		[idm]	Gestión de identidades	3	18	15	15	9	6
	AED13		[dir]	Servicios de directorio	3	18	15	0	6	9
	AED14		[email]	Correo electrónico	4	28	16	16	12	8
EQUIPOS INFORMÁTICOS [einf]	APS1	SOFTWARE [SW]	[siaf]	SIAF	4	28	24	20	20	12
	APS2		[aut]	Autocad	4	16	0	16	16	8
	APS3		[afp]	Adobe flash player	3	6	6	0	6	0
	APS4		[siga]	SIGA	3	21	9	12	15	6
	APS5		[off]	Microsoft Office Professional Plus 2010	3	12	3	6	15	9
	APS6		[msp]	Ms project	3	3	6	0	3	0
	APS7		[av]	Antivirus ESET NOD32	4	32	20	16	16	12
	APS8		[os]	Sistema operativo Windows	3	18	15	3	12	9
	APS9		[bck]	Sistema de backup	3	18	18	3	9	9
	APS10		[gm]	GESMUN	3	18	12	12	9	6
	APS11		[web]	Pagina Web (munipillcomarca.com.pe)	3	18	12	0	0	9
	APS12		[std]	Sistema de tramite documentario(escritorio)	3	18	0	15	12	9
EQUIP	EIH1	HARD	[ipm]	Impresora multifuncional	5	35	25	0	10	0

	EIH2		[sva]	Servidor de archivos	4	28	28	24	16	8
	EIH3		[svc]	Servidor de impresión	4	16	8	0	12	0
	EIH4		[cpu]	Microprocesador(también llamado CPU)	4	32	24	24	8	0
	EIH5		[m]	Motherboard o placa madre	4	32	24	24	4	0
	EIH6		[mr]	Memoria RAM	4	32	24	24	4	0
	EIH7		[dd]	Disco Duro	4	24	24	24	4	0
	EIH8		[lo]	Lectores ópticos	3	18	18	18	3	0
	EIH9		[trg]	Tarjeta Red, Gráfica y Sonido	3	18	18	18	3	0
	EIH10		[ms]	Mouse	3	24	18	18	3	3
	EIH11		[tc]	Teclado	3	24	18	18	3	0
	EIH12		[mon]	Monitor	3	24	18	18	3	3
	EIH13		[mrom]	Memoria ROM	3	24	18	18	3	3
	EIH14		[dis]	Disipador(culer)	3	24	18	18	3	3
	EIH15		[fdp]	Fuente de Poder	3	24	18	18	3	3
	EIH16		[cIS]	Cable IDE/SATA	3	24	18	18	3	3
	EIH17		[ucd]	Unidad de CD/DVD	3	18	15	12	3	3
	EIH18		[paw]	Punto de acceso wireless	4	20	12	8	4	8
	EIH19		[rpt]	Radio portátil	4	16	16	16	4	8
	EIH20		[mvf]	Teléfono móvil	4	8	12	12	4	4
	EIH21		[tbl]	Tablet	3	6	6	0	9	0
	EIH22		[tvs]	Televisor	4	20	20	4	4	0
	EIH23		[caf]	Cámaras fijas	4	20	16	8	8	8
	EIH24		[cam]	Cámaras móviles	4	16	24	20	12	8
	EIH25		[cap]	Cámara portátil	4	8	8	8	4	0
	EIH26		[nvr]	Grabador de video	4	12	0	8	8	12
	EIH27		[frw]	Cortafuego	3	18	12	3	3	6
	EIH28		[svc]	Servidor SIAF	4	24	24	16	0	8
	EIH29		[pc]	Laptop	4	32	28	24	24	4
	EIH30		[scan]	Escaner	3	18	18	12	3	0
	EIH31		[st]	Switch	4	32	24	24	20	4
	EIH32		[md]	Modem	4	32	0	28	8	4
	EIH33		[rout]	Router	4	32	24	24	12	4
	EIH34		[ups]	UPS	4	32	24	24	0	16
	EIH35		[pt]	Pozo a tierra	4	24	24	24	0	16
COMUNICACI	CRC1	REDES DE	[lan]	Red local	4	28	20	20	4	4
	CRC2		[ite]	Internet	4	24	24	8	4	8

	CRC3		[ptp]	Punto a punto	3	18	18	0	3	0
	CRC4		[vpn]	Red privada virtual	4	20	16	12	0	4
	CRC5		[rte]	Red telefónica	4	16	0	24	4	4
	CRC6		[ads]	ADSL	3	15	0	12	0	6
	CRC7		[crd]	Comunicaciones radio	4	20	16	12	4	4
	CRC8		[wif]	Red inalámbrica	3	21	12	0	6	3
	CRC9		[mob]	Telefonía móvil	4	8	12	4	4	8
	CRC10		[rmv]	Red microondas	4	16	4	0	4	0
SOPORTES DE INFORMACIÓN	SIS1	SOPORTE [media]	[dsk]	Almacenamiento en la nube	3	12	6	9	0	6
	SIS2		[cdv]	CD / DVD	3	0	6	3	3	0
	SIS3		[pml]	Proyector multimedia	3	6	6	0	0	3
	SIS4		[usb]	Dispositivo USB	4	24	16	4	8	0
	SIS5		[tjm]	Tarjeta de memoria	3	3	0	6	3	3
	SIS6		[hdv]	Hard drive	3	6	6	6	6	6
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[ups]	Sistema de alimentación ininterrumpida	4	24	16	0	4	4
	EAE2		[fal]	Fuentes de alimentación	3	12	6	12	9	3
	EAE3		[cbl]	Cableado de red	4	32	24	0	4	4
	EAE4		[mbl]	Mobiliario	3	12	0	6	0	3
	EAE5		[eqc]	Equipos de climatización	4	12	16	0	0	4
	EAE6		[cbl]	Cable eléctrico	4	24	24	4	0	0
	EAE7		[fbr]	Fibra óptica	4	24	12	0	4	8
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[off]	Oficinas	4	20	16	8	4	0
	INI2		[tlr]	Auditorio	4	16	8	0	0	8
	INI3		[grt]	Centro Informatico	4	32	12	28	4	0
	INI4		[vhc]	Estacionamiento	3	9	6	3	0	3
	INI5		[dep]	Centro de vigilancia	4	12	12	4	0	0
PERSONAL [per]	PSP1	PERSONAL [P]	[alc]	Alcaldía	3	21	15	12	6	6
	PSP2		[gg]	Gerencia general	4	28	20	16	8	8
	PSP3		[gsg]	Gerencia de secretaria general	4	28	16	8	4	4
	PSP4		[ga]	Gerencia de administración	3	21	15	12	6	3
	PSP5		[gat]	Gerencia de administración tributaria.	4	28	16	12	4	8
	PSP6		[gdse]	Gerencia de desarrollo social y económico	4	28	20	12	8	4
	PSP7		[gma]	Gerencia de medio ambiente	3	21	15	6	6	6
	PSP8		[gid]	Gerencia de infraestructura y desarrollo territorial	4	28	20	12	8	8
	PSP9		[gid]	Gerencia de planeamiento y presupuesto	3	21	15	6	6	6

	PSP10		[gaj]	Gerencia de asesoría jurídica	3	21	15	6	6	6
	PSP11		[aei]	Area de estadistica e informatica	3	18	15	12	6	6
	PSP12		[pdp]	Personal de apoyo	3	21	15	0	3	6
	PSP13		[usx]	Usuarios Externos	4	28	20	0	4	4
	PSP14		[pvd]	Proveedores	3	21	15	0	3	6

4.2 GESTIÓN DE RIESGOS

4.2.1 **PLAN DE SEGURIDAD**

PLAN DE SEGURIDAD - MUNICIPALIDAD DE PILLCO MARCA

Contenido

1. PROGRAMAS DE SEGURIDAD

N°	PROGRAMAS
1	POLÍTICAS GENERALES DE SEGURIDAD DE INFORMACIÓN
2	SEGURIDAD DEL PERSONAL
3	SEGURIDAD FÍSICA DE LAS INSTALACIONES DE PROCESAMIENTO DE DATOS
4	ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES
5	CONTROL DE ACCESO DE DATOS
6	SEGURIDAD DE COMPUTADORAS Y/O DISPOSITIVOS
7	AUDITORIA DE SISTEMAS

2. CRONOGRAMA DE EJECUCIÓN DEL PLAN DE SEGURIDAD

N°	ACTIVIDADES	SEMANAS															
		ENERO				FEBRER				MARZO				ABRIL			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
POLÍTICAS GENERALES DE SEGURIDAD DE INFORMACIÓN																	
1	Inventario de activos							X									
2	Clasificación del acceso de la información.								X								
3	Aplicación de controles para información clasificada									X	X						
SEGURIDAD DEL PERSONAL																	
4	Seguridad en la definición de puestos de trabajo y recursos										X	X	X	X	X	X	X
5	Capacitación de usuarios										X	X	X	X	X	X	X
6	Procedimientos de respuesta ante incidentes de seguridad										X	X	X	X	X	X	X
SEGURIDAD FÍSICA DE LAS INSTALACIONES DE PROCESAMIENTO DE DATOS																	
7	Control de acceso a las instalaciones u oficinas										X	X	X	X	X	X	X
8	Acuerdo con regulaciones y leyes										X	X	X	X	X	X	X
ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES																	
9	Protección contra virus										X	X	X	X	X	X	X
10	Copias de respaldo										X	X	X	X	X	X	X
11	Control de acceso de datos										X	X	X	X	X	X	X
12	Identificación de usuarios										X	X	X	X	X	X	X
13	Seguridad de contraseñas										X	X	X	X	X	X	X
14	Controles de acceso de programas										X	X	X	X	X	X	X
15	Administración de acceso de usuarios										X	X	X	X	X	X	X
16	Responsabilidades del usuario										X	X	X	X	X	X	X
17	Control de acceso a redes										X	X	X	X	X	X	X
18	Control de acceso al sistema operativo										X	X	X	X	X	X	X
19	Control de acceso de aplicación										X	X	X	X	X	X	X
SEGURIDAD DE COMPUTADORAS Y/O DISPOSITIVOS																	
20	Seguridad del hardware										X	X	X	X	X	X	X
21	Dispositivos móviles (laptop										X	X	X	X	X	X	X
22	Equipamientos auxiliares										X	X	X	X	X	X	X
AUDITORÍA DE SISTEMAS																	
23	Protección de herramientas de auditoria										X	X	X	X	X	X	X
24	Controles de auditoria de sistemas										X	X	X	X	X	X	X

3. NORMAS LEGALES DE USO

- ✓ Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.
- ✓ Ley de Protección de Datos Personales del Perú (Ley N° 29733)
- ✓ Ley N° 27269: Ley de Firmas y Certificados Digitales.

4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El documento de políticas de seguridad ha sido elaborado tomando como base la siguiente documentación:

- ✓ Los lineamientos de MAGERIT V3
- ✓ Estándar de seguridad de la información NTP – ISO/IEC 17799:2007

4.1 DEFINICIÓN

Una Política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

La información se clasifica según la siguiente descripción:

- ✓ **Restringida:** Información con mayor grado de sensibilidad; el acceso a esta información debe de ser autorizado caso por caso.
- ✓ **Confidencial:** Información sensible que solo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

- ✓ **Uso Interno:** Datos generados para facilitar las operaciones diarias; deben de ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.
- ✓ **General:** Información que es generada específicamente para su divulgación a la población general de usuarios.

4.2 PROPÓSITO

El propósito de las políticas de seguridad de la información es proteger la información y los activos de la Municipalidad Distrital de Pillco Marca. Estas políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

4.3 CUMPLIMIENTO OBLIGATORIO

El cumplimiento de las políticas y estándares de seguridad de la información son obligatorios y deben ser considerados como una condición en los contratos del personal.

La Municipalidad Distrital de Pillco Marca. Puede obviar algunas de las políticas de seguridad definidas en este documento, cuando se ha demostrado claramente que el cumplimiento de dichas políticas tendría un impacto adverso e inaceptable para el cumplimiento de las funciones del personal. Toda excepción a las políticas debe ser documentada y aprobada por el área de Administración de Sistemas, detallando el motivo que justifica el no-cumplimiento de la política.

4.4 POLÍTICAS GENERALES DE SEGURIDAD DE INFORMACIÓN

4.4.1 INVENTARIO DE ACTIVOS

a) Se debe elaborar y mantener un inventario de los activos (tangibles e intangibles) asociados a cada sistema de información.

b) Cada activo debe ser claramente identificado, clasificado y asignado a un propietario, además de ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una pérdida o daño).

c) Cada activo del área de Sistemas posee un código único que lo identifica.

4.4.2 CLASIFICACIÓN DEL ACCESO DE LA INFORMACIÓN

a) Toda la información debe de ser clasificada como Restringida, Confidencial, Uso Interno o General.

b) La clasificación de información debe de ser documentada por el Propietario.

c) La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

d) La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red, etc.) debe de tener la misma clasificación sin importar el formato.

4.4.3 APLICACIÓN DE CONTROLES PARA INFORMACIÓN CLASIFICADA

Las medidas de seguridad aplicables a los activos de información clasificados, incluyen, pero no se limitan a las siguientes:

4.4.3.1 INFORMACIÓN DE LA INSTITUCIÓN ALMACENADA EN FORMATO DIGITAL

a) Todo contenedor de información en medio digital (CD´s, USB, Memorias portables, etc.) debe presentar una etiqueta con la clasificación correspondiente.

b) La información en formato digital clasificada como de acceso “General”, puede ser almacenada en cualquier medio electrónico en la Cooperativa (información para consultas, fichas de publicidad, promociones, descuentos, etc.). Sin embargo, se deben tomar las medidas necesarias para no mezclar información “General” con información correspondiente a otra clasificación (Restringida, Confidencial o de uso interno).

c) La información digital debe almacenarse según un orden establecido por la entidad; el cual es la siguiente:

   - Carpetas con nombres claros y legibles.
   - Ordenadas en orden alfabético.
   - Restringidas y con un límite de tiempo de acceso activo.
   - Carpetas digitales que establezcan claramente la antigüedad de cada documento.

d) Todo personal del área de Sistemas, antes de transmitir información clasificada como “Restringida” o “Confidencial”, debe asegurarse que el destinatario de la información esté autorizado (No repudio). El no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

e) Todo usuario que requiere acceso a información clasificada como “Restringida” o “Confidencial”,

debe ser autorizado por el propietario de la misma en el período establecido por la entidad o tener una clave de acceso. Las autorizaciones de acceso al sistema, deben ser documentadas.

f) Información en formato digital, clasificada como “Restringida”, debe ser encriptado con un método aprobado por los encargados de la administración de seguridad de la información, cuando es almacenada en cualquier medio (CDs, Memorias portables, etc.).

g) Toda transmisión de Información clasificada como “Restringida”, “Confidencial” o de “Uso Interno” realizada hacia o a través de redes externas a la Institución debe contar con el debido respaldo u autorización de la entidad, además debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de inscripción aprobadas.

h) Todo documento en formato digital, debe presentar la clasificación correspondiente en la parte superior (cabecera) e inferior (pie de página) de cada página del documento.

i) Los medios de almacenamiento, incluyendo discos duros de computadoras, que albergan información clasificada como “Restringida”, deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información.

4.4.3.2 INFORMACIÓN DE LA INSTITUCIÓN ALMACENADA EN FORMATO NO DIGITAL

a) Todo documento o contenedor de información debe ser etiquetado como “Restringida”, “Confidencial”, de “Uso interno” o de Acceso “General”, dependiendo de la clasificación asignada.

b) Todo documento que presente información clasificada como “Confidencial” o “Restringida”, debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente.

c) Todo documento clasificado como “Confidencial” o “Restringido” debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

d) El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con

adecuados controles de acceso y protección cuando se encuentre sin vigilancia.

e) El acceso debe ser permitido solo al personal formalmente autorizado.

f) Personal de limpieza debe ingresar al ambiente acompañado por personal autorizado.

g) Solo el personal formalmente autorizado debe tener acceso a información clasificada como “Restringida” o “Confidencial”.

h) Los usuarios que utilizan documentos con información “Confidencial” o “Restringida” deben asegurarse de:

- Almacenarlos en lugares adecuados.
- Evitar que usuarios no autorizados accedan a dichos documentos.
- Destruir los documentos si luego de su utilización dejan de ser necesarios.

4.5 SEGURIDAD DEL PERSONAL

a) Los estándares relacionados al personal deben ser aplicados para asegurarse que los empleados sean seleccionados adecuadamente antes de ser contratados y que el acceso sea denegado oportunamente cuando un empleado es despedido o transferido.

b) Deben desarrollarse estándares adicionales para asegurar que el personal sea consciente de todas sus responsabilidades y acciones apropiadas en el reporte de incidentes.
c) Se tendrá una variación continua de las claves de acceso al personal para mantener la seguridad de los sistemas de información.
d) Cuando se contrata, transfiere y despide al personal deben de ser tomadas medidas de precaución.
e) Deben de establecerse controles para comunicar los cambios del personal y los requerimientos de recursos de cómputo a los responsables de la Administración del área de Sistemas. Es crucial que estos cambios sean atendidos a tiempo.

4.5.1 SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y RECURSOS

a) El área de Administración debe de notificar al área de Sistemas, la renuncia o despido de los empleados, así como el inicio y fin de los periodos de vacaciones de los mismos.
b) Cuando se notifique un despido o transferencia, el Administrador del área de Sistemas debe de asegurarse que el identificador de usuario sea revocado o desactivado.
c) Cualquier ítem entregado al empleado como computadoras portátiles, llaves, tarjetas de identificación, software, datos,

documentación, manuales, etc. deben de ser entregados a jefe inmediato con cargo.

4.5.2 CAPACITACIÓN DE USUARIOS

a) Es responsabilidad de la Administración de Área de Sistemas promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información.

b) El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches, llaveros, mensajes de log-in, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

c) Cuando se contrate a un empleado nuevo y/o el servicio de algún tercero, se debe de entregar la política de seguridad, así como las normas y procedimientos para el uso de software y sistemas de información de la entidad.

d) El personal debe de ser comunicado de las implicancias de seguridad en relación a las responsabilidades de su trabajo

e) Una copia firmada de la política de seguridad de información debe de ser guardada en el archivo del empleado

4.5.3 PROCEDIMIENTOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD

a) Si un empleado detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al personal de Área de Sistemas.

b) Si se sospecha la presencia de un virus en un sistema, el usuario debe desconectar el equipo de la red de datos, notificar al Administrador del Área de Sistemas quien se encargará de la eliminación del virus antes de restablecer la conexión a la red de datos.

c) Es responsabilidad del usuario (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos.

d) Si un empleado detecta una vulnerabilidad en la seguridad de la información debe notificarlo al personal encargado de la administración de la seguridad, asimismo, está prohibido para el empleado realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

e) El Administrador del Área de Sistemas debe documentar todos los reportes de incidentes de seguridad.

f) Cualquier error o falla en los sistemas debe ser notificado al Administrador del Área de Sistemas, quién determinará si el error es indicativo de una vulnerabilidad en la seguridad.

g) Las acciones disciplinarias tomadas contra los empleados por la ocurrencia de una violación de seguridad, deben ser consistentes con la magnitud de falta, ellas deben ser coordinadas con el área de Recursos Humanos.

4.5.3.1 REGISTRO DE FALLAS

a) El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones y notificar al Administrador de Red. Estos registros deben incluir lo siguiente:
   - Nombre y cargo de quien reporta la falla
   - Hora y fecha de ocurrencia de la falla
   - Descripción del error o problema
   - Firma del responsable de la detección de la falla.

b) Los registros de fallas deben ser revisados semanalmente.

c) Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una

solución al problema. Además, estos registros deben ser almacenados para una posterior verificación independiente.

4.5.3.2 INTERCAMBIOS DE INFORMACIÓN Y CORREO ELECTRÓNICO

a) Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros y están sujetos a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser utilizados para lo siguiente:
   - Enviar cadenas de mensajes
   - Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de la Administración de Área de Sistemas
   - Enviar propaganda de candidatos políticos
   - Actividades ilegales, no éticas o impropias
   - Actividades no relacionadas con la institución
   - Diseminar direcciones de correo electrónico a listas públicas
b) No deben realizarse el reenvío automático de correos a direcciones que no pertenecen a la institución.

Puesto que no existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red de la Municipalidad de Pillco Marca.

c) El intercambio de información puede darse dentro de la misma municipalidad o entre distintas municipalidades o entidades, pero sea como sea deben existir controles de seguridad que ofrezcan seguridad y protección a la información que se está intercambiando. Cuando esto ocurra es necesario establecer una política que acoja a todos los medios de intercambio que la organización emplee. Los aspectos que esta política debería incluir son:

   - Procedimientos de un correcto uso de los medios.
   - Controles para evitar la modificación, la interceptación, el copiado o la destrucción de la información.
   - Controles de protección contra el código malicioso.
   - Técnicas de ingeniería social.
   - Uso de cifrado en datos que se consideren necesarios.

d) Debe establecerse un proceso formal para aprobar la publicación de información de la institución.

e) El desarrollo de páginas Web programables o inteligentes debe considerarse como desarrollo de software y debe estar sujeto a los mismos controles.

f) La información contenida en sistemas públicos no debe contener información restringida, confidencial o de uso interno. De igual manera, los equipos que brindan servicios Web, correo electrónico, u otros servicios públicos no deben almacenar información restringida, confidencial o de uso interno.

g) Debe establecerse controles sobre equipos de oficina como teléfonos, faxes e impresoras que procesan información sensible de la institución.

h) Información restringida o confidencial solo debe imprimirse en equipos específicamente designados para esta tarea.

4.5.3.3 SEGURIDAD PARA MEDIDAS EN TRÁNSITO

a) La información a ser transferida en media digital o impresa debe ser etiquetada con la clasificación de información respectiva y detallando claramente el remitente y recipiente del mismo.

b) La información enviada por servicios postales debe ser protegida de accesos no autorizados mediante la utilización de:

- Paquetes sellados o lacrados
- Entrega en persona
- Firmado y sellado de un cargo

4.6 SEGURIDAD FÍSICA DE LAS INSTALACIONES DE PROCESAMIENTO DE DATOS

a) Se deben implementar medidas de seguridad física para asegurar la integridad de las instalaciones y centros de cómputo.

b) Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las instalaciones.

4.6.1 CONTROL DE ACCESO A LAS INSTALACIONES U OFICINAS

a) El acceso a cualquier instalación u oficinas debe estar restringido únicamente al personal autorizado.

b) Todas las visitas deben ser identificadas y se debe mantener un registro escrito de las mismas, estas visitas deben ser en compañía de un empleado durante la permanencia en las instalaciones u oficinas.

c) Todo el personal en las instalaciones u oficinas deben de portar un carné, placa o ficha de identificación.

d) Medidas apropiadas como guardias o puertas con alarmas, deben de ser utilizadas para proteger las instalaciones durante las horas no laborables.

e) El retiro de cualquier equipo o medio electrónico de las instalaciones de cómputo debe de ser aprobado por escrito por personal autorizado

f) Todos los sitios donde se encuentren sistemas de procesamiento informático o de almacenamiento, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.

g) En aquellas oficinas en donde existen empleados con acceso al lugar o los equipos de comunicación hacia las redes de datos o telefonía del municipio, el jefe del área deberá tomar las medidas pertinentes para el resguardo y cuidados especiales del equipo.

4.6.2 ACUERDO CON REGULACIONES Y LEYES

a) Se entenderá como riesgo laboral la posibilidad de que un trabajador sufra un determinado daño derivado del trabajo. Para calificar un riesgo desde el punto de vista de su

gravedad, se valorarán conjuntamente la probabilidad de que se produzca el daño y la severidad del mismo.

b) Por otro lado, se definirá como condición de trabajo, cualquier característica de la realización de tareas que abarcan tres aspectos diferenciados, tales como las condiciones medioambientales en torno al trabajo, las condiciones físicas en las que se realiza el trabajo y las condiciones organizativas que rigen en la entidad.

4.7 ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

a) Los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las comunicaciones y las operaciones.

b) Todas las comunicaciones e intercambios de información, tanto dentro de las instalaciones y sistemas de la institución como externas a ella, deben ser aseguradas, de acuerdo al valor de la información protegida.

4.7.1 PROTECCIÓN CONTRA VIRUS

a) La oficina de Administración del Área de Sistemas debe realizar esfuerzos para determinar el origen de la infección por virus informático, para evitar la reinfección de los equipos de la institución.

b) La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios.

c) Se tomarán medidas disciplinarias en caso se encuentren dichos programas en computadoras personales de usuarios.

d) Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet deben ser revisados por un antivirus antes de ejecutarlos.

e) Asimismo, está prohibido el uso de USB´s y discos compactos provenientes de otra fuente que no sea de la misma institución, a excepción de los provenientes de los órganos reguladores de control interno.

f) El programa antivirus debe encontrarse licenciado y habilitado en todas las computadoras de la institución y debe ser actualizado periódicamente.

g) En caso de detectar fallas en el funcionamiento de dichos programas éstas deben ser comunicadas al área de Administración del Área de Sistemas.

h) El programa antivirus debe ser configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de la institución.

i) Debe contarse con un procedimiento para la actualización periódica de los programas antivirus y el monitoreo de los virus detectados.

j) Es obligación del personal de la institución, emplear sólo los programas cuyas licencias han sido obtenidas por la institución y forman parte de su plataforma estándar.

k) Todo el personal de la institución debe utilizar los protectores de pantalla y/o papel tapiz autorizados por la Institución; el estándar es:

- Papel Tapiz: MUNICIPALIDAD DISTRITAL DE PILLCO MARCA
- Protector de Pantalla: MUNICIPALIDAD DISTRITAL DE PILLCO MARCA

4.7.2 COPIAS DE RESPALDO

a) El administrador del área de Sistemas responsables de asegurar que se generen copias de respaldo del software de los servidores de la institución o en la nube si se consideraran necesario.

b) Debe formalmente definirse procedimientos para la creación y recuperación de copias de respaldo.

c) Trimestralmente deben efectuarse pruebas para asegurar la capacidad de restaurar información en caso sea necesario. Estas pruebas deben efectuarse en equipos que no comprometan la integridad de los datos.

d) Los usuarios deben generar copias de respaldo de información crítica transfiriendo o duplicando archivos a la carpeta personal establecida para dicho fin por la Administración de Área del Sistemas, la cual se encuentra ubicada en uno de los servidores de la institución.

4.8 CONTROL DE ACCESO DE DATOS

a) La información manejada por los sistemas de información y las redes asociadas debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción.

b) El uso inteligente de controles de acceso previene errores o negligencias del personal, así como reduce la posibilidad del acceso no autorizado.

c) Contar con un reporte “mensual” sobre los accesos efectuados a los sistemas de información, teniendo en cuenta que éstos reportes deben detallarse la fecha, hora, usuario, pc y otras características que se consideren necesarias por la entidad.

d) Deben reportarse las incidencias de accesos o intentos de acceso no autorizados al sistema.

4.8.1 IDENTIFICACIÓN DE USUARIOS

a) Cada usuario de un sistema automatizado debe de ser identificado de manera única, y el acceso del usuario, así como su actividad en los sistemas debe de ser controlado, monitoreado y revisado.

b) Cada usuario de un sistema debe tener un código de identificación que no sea compartido con otro usuario.

c) Para lograr el acceso a los sistemas automatizados, se requiere que el usuario provea una clave que solo sea conocida por él.

d) Debe establecerse un procedimiento para asegurar que el código de identificación de un usuario sea retirado de todos los sistemas cuando un empleado es despedido o transferido.

e) Los terminales y computadoras personales deben bloquearse luego de quince (15) minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad.

f) El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, computadoras

personales, etc., y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

g) Todos los consultores, contratistas, proveedores y personal temporal deben tener los derechos de acceso cuidadosamente controlados. El acceso solo debe ser válido hasta el final del trimestre o incluso antes, dependiendo de la terminación del contrato.

h) Todos los sistemas deben proveer pistas de auditoria del ingreso a los sistemas y violaciones de los mismos.

i) A partir de estos datos, los auditores de los sistemas deben elaborar reportes periódicos los cuales deben ser revisados por el Administrador de Área de Sistemas. Estos reportes también deben incluir la identidad del usuario, y la fecha y hora del evento. Si es apropiado, las violaciones deben ser reportadas al jefe inmediato del individuo.

j) Violaciones repetitivas o significantes o atentados de accesos deben ser reportados al jefe inmediato de la persona y al área de Administración Del Área de Sistemas.

4.8.2 SEGURIDAD DE CONTRASEÑAS

4.8.2.1 ESTRUCTURA

a) Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no deben contener espacios en blanco.

b) Las contraseñas deben ser difíciles de adivinar. Palabras de diccionario, identificadores de usuario y secuencias comunes de caracteres, como por ejemplo “12345678” o “ABCDEFG”, no deben ser empleadas.

c) Detalles personales como los nombres de familiares, número de documento de identidad, número de teléfono o fechas de cumpleaños no deben ser usados salvo acompañados con otros caracteres adicionales que no tengan relación directa.

d) Las contraseñas deben incluir al menos un carácter no alfanumérico. Las contraseñas deben contener al menos un carácter alfabético en mayúscula y uno en minúscula.

4.8.2.2 VIGENCIA

a) Todas las contraseñas deben expirar dentro de un periodo que no exceda los treinta (30) días.

4.8.2.3 REUTILIZACIÓN DE CONTRASEÑAS

a) No debe permitirse la reutilización de ninguna de las 3 últimas contraseñas. Esto asegura que los usuarios no utilicen las mismas contraseñas en intervalos regulares.

b) Los usuarios no deben poder cambiar sus contraseñas más de una vez al día.

c) A los usuarios con privilegios administrativos, no se les debe permitir la reutilización de las últimas 10 contraseñas.

4.8.2.4 INTENTOS FALLIDOS DE INGRESO

a) Todos los sistemas deben estar configurados para deshabilitar los identificadores de los usuarios en caso de ocurrir (3) intentos fallidos de autenticación.

b) En los casos que los sistemas utilizados no soporten controles para las características establecidas para la estructura, vigencia, reutilización e intentos fallidos de ingreso, se debe documentar la excepción a la política, detallando la viabilidad de modificar la aplicación para soportar las características establecidas para las contraseñas.

4.8.2.5 SEGURIDAD DE CONTRASEÑAS

a) Es importante que todos los empleados protejan sus contraseñas, debiéndose seguir las siguientes regulaciones:

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados.
- Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de su jefe inmediato, con autorización del Administrador de Área de Sistemas y auditoría interna. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.
- El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.
- Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas.

- Las contraseñas deben estar siempre encriptados cuando se encuentren almacenadas o cuando sean transmitidas a través de redes.
- El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.

4.8.3 CONTROLES DE ACCESO DE PROGRAMAS

a) Los controles de acceso de programas deben asegurar que los usuarios no puedan acceder a la información sin autorización.

b) Los programas deben poder generar una pista de auditoria de todos los accesos y violaciones.

c) Las violaciones de los controles de acceso deben ser registradas y revisadas por el propietario o por el personal del área de auditoría interna de los datos.

d) Las violaciones de seguridad deben ser reportadas al jefe inmediato del empleado y al área responsable de la administración de la seguridad de la información.

e) Se debe tener cuidado particular en todos los ambientes para asegurar que ninguna persona tenga control absoluto. No deben tener acceso ilimitado a los identificadores de usuario. Dichos identificadores de usuario, son solo

necesarios durante una emergencia y deben ser cuidadosamente controlados por la Administración del Área de Sistemas, quien debe realizar un monitoreo periódico de su utilización.

4.8.4 ADMINISTRACIÓN DE ACCESO DE USUARIOS

a) La asignación de usuarios especiales o privilegiados (como cuentas administrativas y supervisores) debe ser revisada cada 3 meses.

b) Es recomendable realizar revisiones trimestralmente debido al continuo cambio de los ambientes de trabajo y la importancia de los datos.

c) Es responsabilidad del administrador de área de Sistemas ver que los privilegios de acceso estén alineados con las necesidades de la institución.

d) En las situaciones donde los usuarios con accesos a información altamente sensible sean despedidos, el área de Recursos Humanos debe coordinar directamente con el Administrador de Área de Sistemas para eliminar el acceso de ese usuario.

e) Se debe buscar el desarrollo de soluciones técnicas para evitar el uso de accesos privilegiados innecesarios.

f) Luego del despido o renuncia de algún empleado, es responsabilidad del jefe inmediato del empleado revisar cualquier archivo físico o digital elaborado o modificado por el usuario, debe también asignar la propiedad de dicha información a la persona relevante, así como determinar la destrucción de los archivos innecesarios.

g) Cuentas de usuario que no son utilizadas por noventa (90) días deben ser automáticamente deshabilitadas. Las cuentas que no han sido utilizadas por un periodo largo demuestran que el acceso de información de ese sistema no es necesario.

h) Todos los usuarios de los sistemas de información deben de tener un identificador de usuario único que sea válido durante el período laboral del usuario.

i) Los identificadores de usuarios no deben de ser utilizados por otros individuos incluso luego de que el usuario original haya renunciado o haya sido despedido.

j) Los sistemas no deben permitir que los usuarios puedan tener sesiones múltiples para un mismo sistema, salvo bajo autorización específica del propietario de la información.

4.8.5 RESPONSABILIDADES DEL USUARIO

a) Todo equipo de cómputo de propiedad de la institución, serán usados solo para actividades relacionadas a la institución.

b) Los sistemas de la institución no pueden ser usados para desarrollar software para negocios personales o externos a la institución.

c) Toda la actividad realizada utilizando un identificador de usuario determinado, es de responsabilidad del empleado a quién le fue asignado. Por consiguiente, los usuarios no deben compartir la información de su identificador con otros o permitir que otros empleados utilicen su identificador de usuario para realizar cualquier acción.

d) En caso de una incidencia las penalidades, sanciones administrativas, y legales son:

- Destitución del cargo y consiguiente despido de la entidad.
- Penalidad de acuerdo a lo estipulado en el contrato, por transgresión de una de las políticas de seguridad.
- Denuncia Oficial de acuerdo a como lo considere el Fiscal Coordinador.
- Otros de acuerdo a la gravedad de la incidencia.

4.8.6 CONTROL DE ACCESO A REDES

4.8.6.1 CONEXIONES CON REDES EXTERNAS

a) Todas las conexiones realizadas entre la red interna de la institución e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados.

b) El área de Administración del Área de Sistemas debe aprobar todas las conexiones con redes o dispositivos externos.

c) El acceso desde Internet hacia la red interna de la institución no debe ser permitido sin un dispositivo de fuerte autenticación o certificado basado en utilización de contraseñas dinámicas.

d) El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que “hackers” u otras personas pueden obtener fácilmente información sobre la estructura de red de la Municipalidad y computadoras internas.

e) Solo tienen acceso a la red particular de la entidad aquellas personas del área de Sistemas, las cuales son autorizadas y supervisadas por el

jefe de esta área en mención. El acceso de este personal puede ser por: SmartPhone´s, Tablet´s, Laptop (particular), etc.

4.8.6.2 POLÍTICA DEL USO DE SERVICIO DE REDES

a) Todas las conexiones de red internas y externas deben cumplir con las políticas de la Institución sobre servicios de red y control de acceso. Es responsabilidad del área de sistemas de información y seguridad de información determinar lo siguiente:
   - Elementos de la red que pueden ser accedidos
   - El procedimiento de autorización para la obtención de acceso
   - Controles para la protección de la red.

b) Todos los servicios habilitados en los sistemas deben contar con una justificación coherente con las necesidades del negocio. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio. Algunos servicios

estrictamente prohibidos incluyen TFTP e IRC/Chat.

4.8.7 CONTROL DE ACCESO AL SISTEMA OPERATIVO

4.8.7.1 ESTÁNDARES GENERALES

a) Los usuarios que posean privilegios de usuario, deben utilizar el mismo identificador con el que se autentican normalmente en los sistemas.

b) Todos los usuarios deben poseer un único identificador. El uso de identificadores de usuario compartidos debe estar sujeto a autorización.

c) Cada cuenta de usuario debe poseer una contraseña asociada, la cual solo debe ser conocida por el dueño del identificador de usuario. Seguridad adicional puede ser añadida al proceso, como identificadores biométricos o generadores de contraseñas dinámicas.

4.8.7.2 LIMITACIONES DE HORARIO

Las aplicaciones críticas deben estar sujetas a periodos de acceso restringidos, el acceso a los

sistemas en un horario distinto debe ser deshabilitado o suspendido.

4.8.7.3 ADMINISTRACIÓN DE CONTRASEÑAS

a) Los administradores de seguridad deben realizar pruebas mensuales sobre la calidad de las contraseñas que son empleadas por los usuarios, esta actividad puede involucrar el uso de herramientas para obtención de contraseñas.

b) Todas las bases de datos o aplicaciones que almacenen contraseñas deben ser aseguradas, de tal manera, que solo los administradores de los sistemas tengan acceso a ellas.

4.8.7.4 INACTIVIDAD DEL SISTEMA

a) Las sesiones en los sistemas que no se encuentren activas por más de 30 minutos deben ser concluidas de manera automática.

b) Las computadoras personales, laptops y servidores, deben ser configurados con un protector de pantalla con contraseña, cuando sea aplicable. El periodo de inactividad para la

activación del protector de pantalla debe ser de 5 minutos.

c) Los sistemas deben forzar la re-autenticación de los usuarios luego de 2 horas de inactividad.

4.8.8 CONTROL DE ACCESO DE APLICACIÓN

4.8.8.1 RESTRICCIONES DE ACCESO A INFORMACIÓN

a) Para la generación de cuentas de usuario en los sistemas, así como para la asignación de perfiles, el jefe máximo del área usuaria es el responsable de presentar la 'Solicitud de Usuarios y/o Perfiles de Acceso a los Sistemas de Cómputo', al Administración de Área del Sistemas, quien generará los Usuarios y Contraseñas correspondientes, para luego remitirlas al área de Recursos Humanos, para que éste a su vez los entregue al Usuario Final, con la confidencialidad requerida.

b) Se debe otorgar a los usuarios acceso solamente a la información mínima necesaria para la realización de sus labores.

4.8.8.2 RESPONSABILIDADES GENERALES

Los administradores de los sistemas deben realizar monitoreo periódico de los sistemas como parte de su rutina diaria de trabajo, este monitoreo no debe estar limitado solamente a la utilización y performance del sistema sino debe incluir el monitoreo del acceso de los usuarios a los sistemas.

4.8.8.3 REGISTRO DE EVENTOS DEL SISTEMA

a) La actividad de los usuarios vinculada al acceso a información clasificada como “confidencial” o “restringida” debe ser registrada para su posterior inspección. El propietario de la información debe revisar dicho registro mensualmente.

b) Todos los eventos de seguridad relevantes de una computadora que alberga información confidencial, deben ser registrados en un log de eventos de seguridad. Esto incluye errores en autenticación, modificaciones de datos, utilización de cuentas privilegiadas, cambios en la configuración de acceso a archivos,

modificación a los programas o sistema operativo instalados, cambios en los privilegios o permisos de los usuarios o el uso de cualquier función privilegiada del sistema.

c) Los “logs” (bitácoras) de seguridad deben ser almacenados por un periodo mínimo de 3 meses. Acceso a dichos logs debe ser permitido solo a personal autorizado. En la medida de lo posible, los logs deben ser almacenados en medios de “solo lectura”.

4.9 SEGURIDAD DE COMPUTADORAS Y/O DISPOSITIVOS

a) Se debe mantener un inventario actualizado de todo el software y hardware existente en la institución, la responsabilidad del mantenimiento del inventario es de la Administración del Área de Sistemas.

b) Todo traslado o asignación de equipos, es de responsabilidad del administrador de área de Sistemas, la verificación y realización del requerimiento.

c) Es de responsabilidad del usuario, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas en él instalados; cualquier cambio y/o traslado deberá ser solicitado con anticipación por su respectiva Área. Asimismo, el usuario debe

verificar que cualquier cambio y/o traslado del Equipo de Cómputo que le fue asignado, se realice por personal de Administración del Área de Sistemas, así como también la instalación o retiro de software.

d) Cualquier microcomputador, computadora personal o portátil / notebook perteneciente a la institución debe ser únicamente utilizada para propósitos de cumplimiento de funciones.
e) Los discos duros no deben contener datos sensibles salvo en las computadoras cuyo acceso físico sea restringido o que tengan instalados un programa de seguridad y que los accesos a la computadora y a sus archivos sean controlados adecuadamente.
f) Todos los programas instalados en las computadoras deben ser legales, aprobados y periódicamente inventariados.
g) Solo los programas adquiridos o aprobados por la institución, serán instalados en las computadoras.
h) El uso de programas de juegos, de distribución gratuita (freeware o shareware) o de propiedad personal está totalmente prohibido.

4.9.1 SEGURIDAD DEL HARDWARE

a) El responsable del área de sistemas debe realizar el mantenimiento preventivo y correctivo de los equipos informáticos.

b) Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:

- No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.
- No colocar objetos pesados encima del Hardware.
- Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc.
- No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente.
- No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por la administración de sistemas.
- Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
- Conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos.

4.9.2 DISPOSITIVOS MÓVILES (LAPTOP).

a) Se prohibe tener como herramientas de trabajo, computadores portátiles (laptops), CPU’s, USB´s o cualquier otro equipo de propiedad del usuario, salvo autorización

previa emitida por el jefe de mayor jerarquía del área que corresponda y el correspondiente registro en el área de sistemas y en el área de Bienes

b) Es responsabilidad del Usuario utilizar los disquetes, discos compactos, USB´s, etcétera, de manera adecuada. Queda terminantemente prohibido al Usuario usar en los equipos del Municipio disquetes, CD's, USB u otros dispositivos de almacenamiento que previamente hayan sido utilizados en computadores de uso público o dudoso, como, por ejemplo: centros educativos, café Internet, o incluso, su computador personal sin la debida revisión por parte del antivirus corporativo

c) Es responsabilidad del Usuario que usa una Laptop del Municipio o personal proteger la información propiedad de la Municipalidad guardada o archivada en el mismo, para lo cual deberá cumplir las siguientes reglas básicas:

- No dejar la Laptop desatendida en lugares públicos para evitar que el equipo o la información sea sustraída.
- Cifrar el contenido de la Laptop para evitar el acceso a los datos en caso de que el equipo sea objeto de robo.
- Usar contraseñas robustas, en lo posible con encriptación para evitar el acceso no autorizado a datos importantes.

- Respaldar la información antes de viajar.
- No desensamblar la Laptop. Sólo un representante técnico autorizado por el fabricante podrá dar servicio y reparar la computadora.

d) Toda laptop perteneciente a la Municipalidad debe tener instalado el software oficial de antivirus y de ser posible el cifrado del disco para evitar el acceso a los datos en caso de que sea objeto de pérdida o robo.

e) Es obligatorio para todo el personal que usa dispositivos inalámbricos, propiedad de la Municipalidad, para el desarrollo de sus funciones, como: teléfonos celulares, Ipad, Ipod, etc. que utilice como mecanismo de seguridad el bloqueo automático de los mismos y el uso de contraseña de acceso, caso contrario se aplicarán las sanciones correspondientes.

f) Es responsabilidad del usuario, realizar un respaldo periódico de la información contenida en los dispositivos móviles o portátiles asignados, para evitar la pérdida de dicha información por robo, extravío, daño del aparato o cualquier otra circunstancia.

g) Es responsabilidad del Usuario que usa una Laptop de la Municipalidad, proteger la información guardada o archivada

en la misma, para lo cual deberá cumplir las siguientes normas:

- Utilizar un candado físico para anclar la Laptop cuando vaya a ausentarse temporalmente.
- Eliminar datos innecesarios que puedan estar almacenados en la Laptop.
- Guardar todos los detalles del computador, incluyendo fabricante, modelo y número serial para poder llenar formularios en caso de ser necesitados.
- Asegurarse de apagar la Laptop, no dejarla en modo hibernación ni suspenso (stand-by) antes de empacarla.
- No empacar la Laptop dentro de un portafolio o valija que se encuentre densamente cargada con otros objetos. La compresión podría ocasionar un daño interno a ésta.
- No rayar, flexionar, golpear, o presionar la superficie de la pantalla de cristal líquido (LCD) de la Laptop.
- No colocar ningún objeto entre la pantalla y el teclado. No levantar la computadora deteniéndola por la pantalla únicamente. Cuando se levante la Laptop abierta, detenerla a por la mitad inferior.

- No voltear la Laptop sobre si misma mientras el adaptador de corriente está conectado. Esto podría romper su conector.
- No fijar la Laptop dentro de un vehículo o en cualquier otro lugar que esté sujeto a vibraciones continuas.

4.9.3 EQUIPAMIENTOS AUXILIARES

a) El cableado eléctrico requiere el cumplimiento de las normas o reglamentos eléctricos que apliquen NFPA 70:20081, National Electrical Code (Código Nacional Eléctrico), IEC 60364-1:20052, Low-voltage electrical installation.

b) En el cableado eléctrico, para los cortes deben emplear Sistemas de Alimentación Ininterrumpida (SAI), que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener varios minutos los aparatos conectados a ellos, permitiendo que los sistemas se apaguen de forma ordenada (generalmente disponen de algún mecanismo para comunicarse con los servidores y avisarlos de que ha caído la línea o de que se ha restaurado después de una caída).

c) En las unidades SAI se debe tener en cuenta que varían en tamaño desde unidades diseñadas para proteger una única

CPU de computadora (sin monitor de vídeo), a grandes unidades que alimentan centros de datos enteros o edificio.

d) Es muy importante que la fuente de alimentación cuente con una potencia ideal que le permita trabajar de una manera más holgada, ya que en el caso de estar conectada a una computadora, a esta se le suelen añadir otros elementos (teclados, ratones, grabadoras, disco duro, luces, etc.) que terminarán demandándole la energía para poder funcionar; por lo tanto si la potencia es insuficiente, es probable que se origine un fallo en algunos de los dispositivos, impidiéndole funcionar al no llegarle la potencia requerida, originando que la computadora no funcione.

e) Para el cableado de red se debe utilizar las y/cumplir las Normas de Cableado Estructurado como ANSI/TIA/EIA/IEEE

f) Se debe comprobar que el cableado de red cumple las normativas necesarias y que tiene la calidad necesaria, normalmente CAT5 o CAT7. Para evitar el posible seccionamiento del cableado de red lo mejor es entubarlo o integrarlo en la estructura del edificio. Para los cables de fibra óptica deberemos estudiar la posibilidad del seccionamiento del cable, las características ópticas de este

(para esto necesitamos instrumental al efecto, puede ser necesario contratar a un especialista) y vigilar que este tipo de cables que suelen ser frágiles no estén acodados o doblados excesivamente.

g) Los mobiliarios que almacenan o contiene el Hardware debe encontrarse en óptimas condiciones.

h) Se debe instalar y realizar el mantenimiento periódico de del sistema pozo a tierra.

4.10 CONSIDERACIONES DE AUDITORIA DE SISTEMAS

4.10.1 PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORIA

Todas las herramientas, incluyendo programas, aplicaciones, documentación y papeles de trabajo, requeridos para la auditoria de sistemas deben protegerse de amenazas posibles como se indica en esta política de seguridad.

4.10.2 CONTROLES DE AUDITORIA DE SISTEMAS

Todas las actividades de auditoria deben ser revisadas para el planeamiento y la ejecución correcta de la auditoria. Esto incluye, pero no se limita a lo siguiente:

- Minimizar cualquier interrupción de las operaciones de la institución.

- Límite del alcance de la evaluación de un ambiente controlado, asegurando que nos brinde accesos impropios para la realización de las tareas de auditoria.
- Identificación de los recursos y habilidades necesarias para cualquier tarea técnica.
- Registro de todas las actividades y desarrollo de la documentación de las tareas realizadas, procedimientos de auditoria, hallazgos y recomendaciones.

5. ESTADO DE RIESGO (POST-TEST)

	N°	CAPA	CÓDIGO	ACTIVO	PROB	DIMENSIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1		[dge]	Datos de gestión interna	3	9	9	9	3	0
	AED2		[mul]	Multimedia (información de audio, video)	3	6	0	3	6	0
	AED3	INFORMACIÓN [info]	[doc]	Documentos	3	6	6	6	3	3
	AED4		[inf]	Informes	3	9	0	3	6	3
	AED5		[exp]	Expedientes	3	9	9	9	0	3
	AED6		[tram]	Trámites	3	6	9	6	6	6
	AED7		[ipu]	Información pública	3	9	9	6	6	0
	AED8		[ipe]	Información personal	3	9	9	6	6	6
	AED9		[icl]	Información clasificada	3	9	12	9	9	9
	AED10		[sei]	Servicio de Internet	3	9	9	6	3	3
	AED11	SERVICIO [service]	[sep]	Servicio de impresión	3	9	0	9	3	0
	AED12		[idm]	Gestión de identidades	2	2	4	4	2	4
	AED13		[dir]	Servicios de directorio	3	6	12	0	3	6
	AED14		[email]	Correo electrónico	3	12	9	3	3	3
EQUIPOS INFORMÁTIC	APS1	SOFTWARE [SW]	[siaf]	SIAF	3	3	6	9	6	6
	APS2		[aut]	Autocad	3	6	0	6	9	6
	APS3		[afp]	Adobe flash player	3	3	3	0	6	0
	APS4		[siga]	SIGA	3	9	6	12	9	3

	APS5		[off]	Microsoft Office Professional Plus 2010	3	9	3	6	3	3
	APS6		[msp]	Ms project	3	3	6	0	3	0
	APS7		[av]	Antivirus ESET NOD32	3	15	9	9	9	6
	APS8		[os]	Sistema operativo Windows	3	6	6	3	9	6
	APS9		[bck]	Sistema de backup	3	6	3	3	6	3
	APS10		[gm]	GESMUN	3	9	9	9	6	3
	APS11		[web]	Pagina Web (munipillcomarca.com.pe)	3	9	12	0	0	3
	APS12		[std]	Sistema de tramite documentario(escritorio)	3	3	0	6	0	0
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [HW]	[ipm]	Impresora multifuncional	2	4	2	0	2	0
	EIH2		[sva]	Servidor de archivos	2	4	4	6	6	2
	EIH3		[svc]	Servidor de impresión	2	4	2	0	4	0
	EIH4		[cpu]	Microprocesador(también llamado CPU)	2	4	4	2	2	0
	EIH5		[m]	Motherboard o placa madre	2	4	4	2	2	0
	EIH6		[mr]	Memoria RAM	2	4	4	2	2	0
	EIH7		[dd]	Disco Duro	2	4	4	2	2	0
	EIH8		[lo]	Lectores ópticos	2	4	4	2	2	2
	EIH9		[trg]	Tarjeta Red, Gráfica y Sonido	2	4	4	2	0	0
	EIH10		[ms]	Mouse	2	4	4	2	0	0
	EIH11		[tc]	Teclado	2	4	4	2	0	0
	EIH12		[mon]	Monitor	2	4	4	2	0	0
	EIH13		[mrom]	Memoria ROM	2	4	4	2	0	0
	EIH14		[dis]	Disipador(culer)	2	4	4	2	0	0
	EIH15		[fdp]	Fuente de Poder	2	4	4	2	0	0
	EIH16		[cIS]	Cable IDE/SATA	2	4	4	2	0	0
	EIH17		[ucd]	Unidad de CD/DVD	2	4	4	2	0	0
	EIH18		[paw]	Punto de acceso wireless	2	4	4	0	2	2
	EIH19		[rpt]	Radio portátil	2	4	6	4	2	2
	EIH20		[mvf]	Teléfono móvil	2	4	4	4	2	2
	EIH21		[tbl]	Tablet	2	2	2	0	6	0
	EIH22		[tvs]	Televisor	2	4	2	2	2	0

	EIH23		[caf]	Cámaras fijas	2	4	4	2	2	2
	EIH24		[cam]	Cámaras móviles	2	4	8	4	6	2
	EIH25		[cap]	Cámara portátil	2	4	2	4	2	0
	EIH26		[nvr]	Grabador de video	2	4	0	4	2	4
	EIH27		[frw]	Cortafuego	2	4	4	0	2	2
	EIH28		[svc]	Servidor …	2	4	6	4	0	2
	EIH29		[pc]	Laptop	2	6	8	4	2	0
	EIH30		[scan]	Escaner	2	4	6	6	2	0
	EIH31		[st]	Switch	2	4	4	4	0	0
	EIH32		[md]	Modem	2	4	0	4	0	2
	EIH33		[rout]	Router	2	4	4	2	0	2
	EIH34		[ups]	UPS	2	4	4	6	0	0
	EIH35		[pt]	Pozo a tierra	2	4	4	6	0	0
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [COM]	[lan]	Red local	4	16	8	8	4	4
	CRC2		[ite]	Internet	2	4	2	2	2	2
	CRC3		[ptp]	Punto a punto	2	4	2	0	2	0
	CRC4		[vpn]	Red privada virtual	2	4	2	4	0	2
	CRC5		[rte]	Red telefónica	2	4	0	4	0	2
	CRC6		[ads]	ADSL	2	4	0	2	0	2
	CRC7		[crd]	Comunicaciones radio	2	4	6	4	2	2
	CRC8		[wif]	Red inalámbrica	3	9	9	0	6	3
	CRC9		[mob]	Telefonía móvil	2	4	4	2	0	0
	CRC10		[rmv]	Red microondas	2	4	2	0	2	0
SOPORTES DE INFORMACIÓN	SIS1	SOPORTE [media]	[dsk]	Almacnamiento en la nuve	1	2	1	1	0	1
	SIS2		[cdv]	CD / DVD	1	0	2	1	1	0
	SIS3		[pml]	Proyector multimedia	1	1	2	0	0	0
	SIS4		[usb]	Dispositivo USB	2	2	2	2	2	0
	SIS5		[tjm]	Tarjeta de memoria	2	2	0	2	0	0
	SIS6		[hdv]	Hard drive	2	2	4	2	2	2
EQUIPAMIENTO AUXILIAR	EAE1	EQUIPAMIENTO [aux]	[ups]	Sistema de alimentación ininterrumpida	2	6	6	0	0	2
	EAE2		[fal]	Fuentes de alimentación	2	6	4	2	2	2
	EAE3		[cbl]	Cableado de Red	4	20	20	0	0	4
	EAE4		[mbl]	Mobiliario	2	6	0	4	0	2
	EAE5		[eqc]	Equipos de climatización	2	4	6	0	0	2

	EAE6		[cbl]	Cable eléctrico	3	9	9	3	0	0
	EAE7		[fbr]	Fibra óptica	3	12	6	0	3	3
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[off]	Oficinas	2	4	4	2	2	0
	INI2		[tlr]	Auditorio	2	4	2	0	0	2
	INI3		[grt]	Centro Informatico	2	4	2	4	2	0
	INI4		[vhc]	Estacionamiento	2	4	4	2	0	2
	INI5		[dep]	Centro de vigilancia	2	4	4	2	0	0
PERSONAL [per]	PSP1	PERSONAL [P]	[alc]	Alcaldía	1	2	1	3	2	1
	PSP2		[gg]	Gerencia general	2	4	2	4	4	2
	PSP3		[gsg]	Gerencia de secretaria general	2	4	2	2	2	2
	PSP4		[ga]	Gerencia de administración	3	6	3	9	3	3
	PSP5		[gat]	Gerencia de administración tributaria.	2	6	4	4	2	2
	PSP6		[gdse]	Gerencia de desarrollo social y económico	2	4	4	4	2	2
	PSP7		[gma]	Gerencia de medio ambiente	2	4	2	2	2	4
	PSP8		[gid]	Gerencia de infraestructura y desarrollo territorial	2	4	2	4	4	2
	PSP9		[gid]	Gerencia de planeamiento y presupuesto	2	4	2	4	4	4
	PSP10		[gaj]	Gerencia de asesoría jurídica	2	4	2	2	2	2
	PSP11		[aei]	Area de estadistica e informatica	2	4	4	4	4	4
	PSP12		[pdp]	Personal de apoyo	2	4	2	0	2	4
	PSP13		[usx]	Usuarios Externos	2	4	2	0	2	2
	PSP14		[pvd]	Proveedores	2	6	2	0	2	2

6. CLASIFICACIÓN DE POLÍTICAS

CLASIFICACIÓN DE POLÍTICAS

		[D]	[I]	[C]	[A]	[N_R]	POLITICAS				
DATOS	Datos de gestión interna	24	24	16	16	4	4.4.2	4.4.3	4.7	4.8	4.10
	Multimedia (información de audio, video)	24	0	16	12	0	4.4.2	4.4.3	4.7	4.8	4.10

INFORMACIÓN [info]	Documentos	25	25	25	15	15	4.4.2	4.4.3	4.7	4.8	4.10
	Informes	24	0	12	16	12	4.4.2	4.4.3	4.7	4.8	4.10
	Expedientes	24	24	20	0	8	4.4.2	4.4.3	4.7	4.8	4.10
	Trámites	30	30	25	15	10	4.4.2	4.4.3	4.7	4.8	4.10
	Información pública	30	30	20	10	0	4.4.2	4.4.3	4.7	4.8	4.10
	Información personal	30	30	25	20	25	4.4.2	4.4.3	4.7	4.8	4.10
	Información clasificada	24	24	24	12	12	4.4.2	4.4.3	4.7	4.8	4.10
SERVICIO [service]	Servicio de Internet	28	24	20	8	12	4.7	4.8	4.10		
	Servicio de impresión	24	0	16	8	0	4.7	4.8	4.10		
	Gestión de identidades	18	15	15	9	6	4.7	4.8	4.10		
	Servicios de directorio	18	15	0	6	9	4.7	4.8	4.10		
	Correo electrónico	28	16	16	12	8	4.7	4.8	4.10		
SOFTWARE [SW]	SIAF	28	24	20	20	12	4.7	4.8	4.10		
	Autocad	16	0	16	16	8	4.7	4.8	4.10		
	Adobe flash player	6	6	0	6	0	4.7	4.8	4.10		
	SIGA	21	9	12	15	6	4.7	4.8	4.10		
	Microsoft Office Professional Plus 2010	12	3	6	15	9	4.7	4.8	4.10		
	Ms project	3	6	0	3	0	4.7	4.8	4.10		
	Antivirus ESET NOD32	32	20	16	16	12	4.7	4.8	4.10		
	Sistema operativo Windows	18	15	3	12	9	4.7	4.8	4.10		
	Sistema de backup	18	18	3	9	9	4.7	4.8	4.10		
	GESMUN	18	12	12	9	6	4.7	4.8	4.10		
	Pagina Web (munipillcomarca.com.pe)	18	12	0	0	9	4.7	4.8	4.10		
	Sistema de tramite documentario(escritorio)	18	0	15	12	9	4.7	4.8	4.10		
HARDWARE [HW	Impresora multifuncional	35	25	0	10	0	4.9	4.8	4.10		
	Servidor de archivos	28	28	24	16	8	4.9	4.8	4.10		
	Servidor de impresión	16	8	0	12	0	4.9	4.8	4.10		
	Microprocesador(también llamado CPU)	32	24	24	8	0	4.9	4.8	4.10		
	Motherboard o placa madre	32	24	24	4	0	4.9	4.8	4.10		
	Memoria RAM	32	24	24	4	0	4.9	4.8	4.10		
	Disco Duro	24	24	24	4	0	4.9	4.8	4.10		
	Lectores ópticos	18	18	18	3	0	4.9	4.8	4.10		
	Tarjeta Red, Gráfica y Sonido	18	18	18	3	0	4.9	4.8	4.10		
	Mouse	24	18	18	3	3	4.9	4.8	4.10		

	Teclado	24	18	18	3	0	4.9	4.8	4.10
	Monitor	24	18	18	3	3	4.9	4.8	4.10
	Memoria ROM	24	18	18	3	3	4.9	4.8	4.10
	Disipador(culer)	24	18	18	3	3	4.9	4.8	4.10
	Fuente de Poder	24	18	18	3	3	4.9	4.8	4.10
	Cable IDE/SATA	24	18	18	3	3	4.9	4.8	4.10
	Unidad de CD/DVD	18	15	12	3	3	4.9	4.8	4.10
	Punto de acceso wireless	20	12	8	4	8	4.9	4.8	4.10
	Radio portátil	16	16	16	4	8	4.9	4.8	4.10
	Teléfono móvil	8	12	12	4	4	4.9	4.8	4.10
	Tablet	6	6	0	9	0	4.9	4.8	4.10
	Televisor	20	20	4	4	0	4.9	4.8	4.10
	Cámaras fijas	20	16	8	8	8	4.9	4.8	4.10
	Cámaras móviles	16	24	20	12	8	4.9	4.8	4.10
	Cámara portátil	8	8	8	4	0	4.9	4.8	4.10
	Grabador de video	12	0	8	8	12	4.9	4.8	4.10
	Cortafuego	18	12	3	3	6	4.9	4.8	4.10
	Servidor SIAF	24	24	16	0	8	4.9	4.8	4.10
	Laptop	32	28	24	24	4	4.9	4.8	4.10
	Escaner	18	18	12	3	0	4.9	4.8	4.10
	Switch	32	24	24	20	4	4.9	4.8	4.10
	Modem	32	0	28	8	4	4.9	4.8	4.10
	Router	32	24	24	12	4	4.9	4.8	4.10
	UPS	32	24	24	0	16	4.9	4.8	4.10
	Pozo a tierra	24	24	24	0	16	4.9	4.8	4.10
REDES DE COMUNICACIÓN [COM]	Red local	28	20	20	4	4	4.8	4.10	
	Internet	24	24	8	4	8	4.8	4.10	
	Punto a punto	18	18	0	3	0	4.8	4.10	
	Red privada virtual	20	16	12	0	4	4.8	4.10	
	Red telefónica	16	0	24	4	4	4.8	4.10	
	ADSL	15	0	12	0	6	4.8	4.10	
	Comunicaciones radio	20	16	12	4	4	4.8	4.10	
	Red inalámbrica	21	12	0	6	3	4.8	4.10	
	Telefonía móvil	8	12	4	4	8	4.8	4.10	
	Red microondas	16	4	0	4	0	4.8	4.10	
SOPORTE [media	Almacenamiento en la nube	12	6	9	0	6	4.8	4.10	
	CD / DVD	0	6	3	3	0	4.8	4.10	

	Proyector multimedia	6	6	0	0	3	4.8	4.10
	Dispositivo USB	24	16	4	8	0	4.8	4.10
	Tarjeta de memoria	3	0	6	3	3	4.8	4.10
	Hard drive	6	6	6	6	6	4.8	4.10
EQUIPAMIENTO [aux]	Sistema de alimentación ininterrumpida	24	16	0	4	4	4.9.3	4.10
	Fuentes de alimentación	12	6	12	9	3	4.9.3	4.10
	Cableado de red	32	24	0	4	4	4.9.3	4.10
	Mobiliario	12	0	6	0	3	4.9.3	4.10
	Equipos de climatización	12	16	0	0	4	4.9.3	4.10
	Cable eléctrico	24	24	4	0	0	4.9.3	4.10
	Fibra óptica	24	12	0	4	8	4.9.3	4.10
INSTALACIONES [L]	Oficinas	20	16	8	4	0	4.6	4.10
	Auditorio	16	8	0	0	8	4.6	4.10
	Centro Informatico	32	12	28	4	0	4.6	4.10
	Estacionamiento	9	6	3	0	3	4.6	4.10
	Centro de vigilancia	12	12	4	0	0	4.6	4.10
PERSONAL [P]	Alcaldía	21	15	12	6	6	4.5	4.10
	Gerencia general	28	20	16	8	8	4.5	4.10
	Gerencia de secretaria general	28	16	8	4	4	4.5	4.10
	Gerencia de administración	21	15	12	6	3	4.5	4.10
	Gerencia de administración tributaria.	28	16	12	4	8	4.5	4.10
	Gerencia de desarrollo social y económico	28	20	12	8	4	4.5	4.10
	Gerencia de medio ambiente	21	15	6	6	6	4.5	4.10
	Gerencia de infraestructura y desarrollo territorial	28	20	12	8	8	4.5	4.10
	Gerencia de planeamiento y presupuesto	21	15	6	6	6	4.5	4.10
	Gerencia de asesoría jurídica	21	15	6	6	6	4.5	4.10
	Area de estadistica e informatica	18	15	12	6	6	4.5	4.10
	Personal de apoyo	21	15	0	3	6	4.5	4.10
	Usuarios Externos	28	20	0	4	4	4.5	4.10
	Proveedores	21	15	0	3	6	4.5	4.10

V. RESULTADOS

5.1 Procesamiento de Datos:

ANÁLISIS DESCRIPTIVO DE LA VARIABLE INDEPENDIENTE:

METODOLOGÍA MAGERIT V3

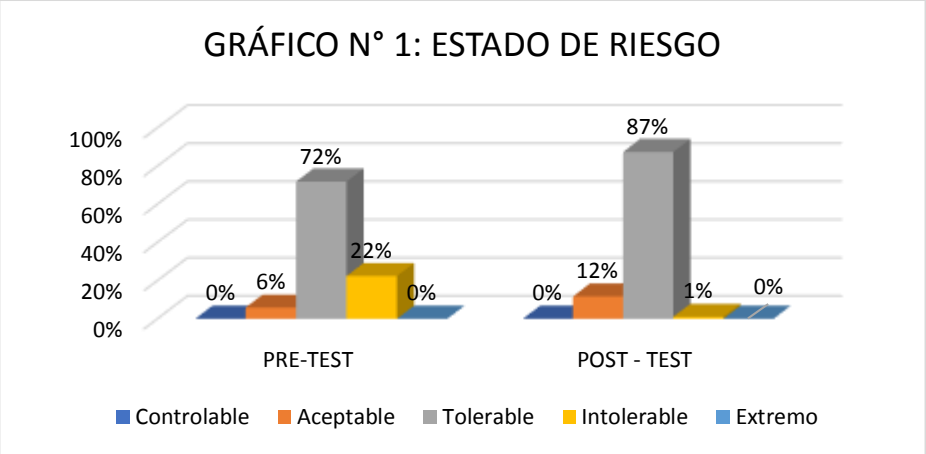
1. DIMENSIÓN: Riesgos

Indicador: Estado de riesgo

CUADRO N° 1: ESTADO DE RIESGO

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
Controlable	0	0%	0	0%
Aceptable	6	6%	12	12%
Tolerable	74	72%	90	87%
Intolerable	23	22%	1	1%
Extremo	0	0%	0	0%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 1, se observa que en los resultados obtenidos en la prueba pre-test, el 72% que representa a 74 activos informáticos se encuentra en un estado de riesgo “tolerable”, el 22% que representan a 23 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo “intolerable” disminuyó a 1%, y “tolerable” aumentó a 87% y “aceptable” a 12%.

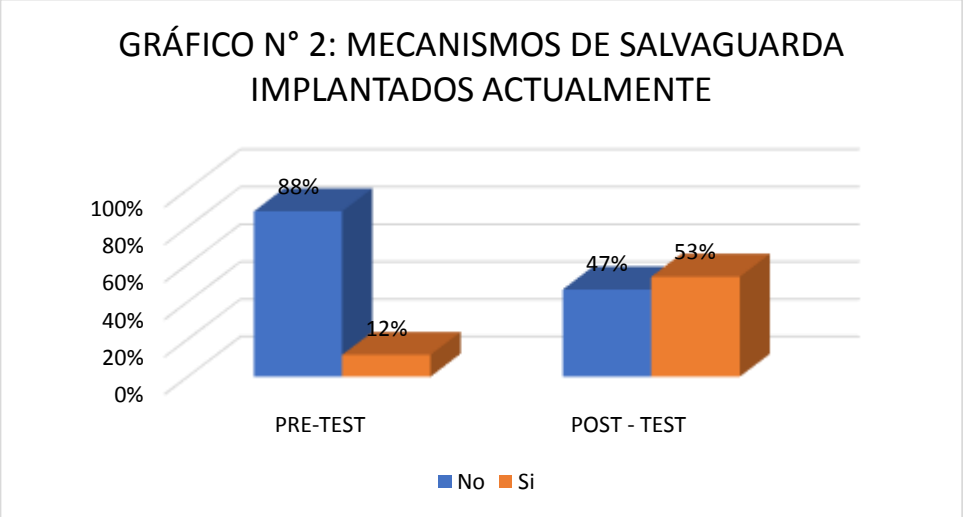
2. DIMENSIÓN: Salvaguardas

Indicador: Mecanismos de salvaguarda implantados actualmente

CUADRO N° 2: MECANISMOS DE SALVAGUARDA IMPLANTADOS ACTUALMENTE

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
No	91	88%	48	47%
Si	12	12%	55	53%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 2, se observa que en los resultados obtenidos en la prueba pre-test, el 88% que representa a 91 activos informáticos, “No” cuentan con mecanismos de salvaguarda implantados actualmente. Mientras que en la prueba post-test se puede visualizar que aumentó la cantidad de activos en 41% que “Si” cuentan con algún mecanismo de salvaguarda.

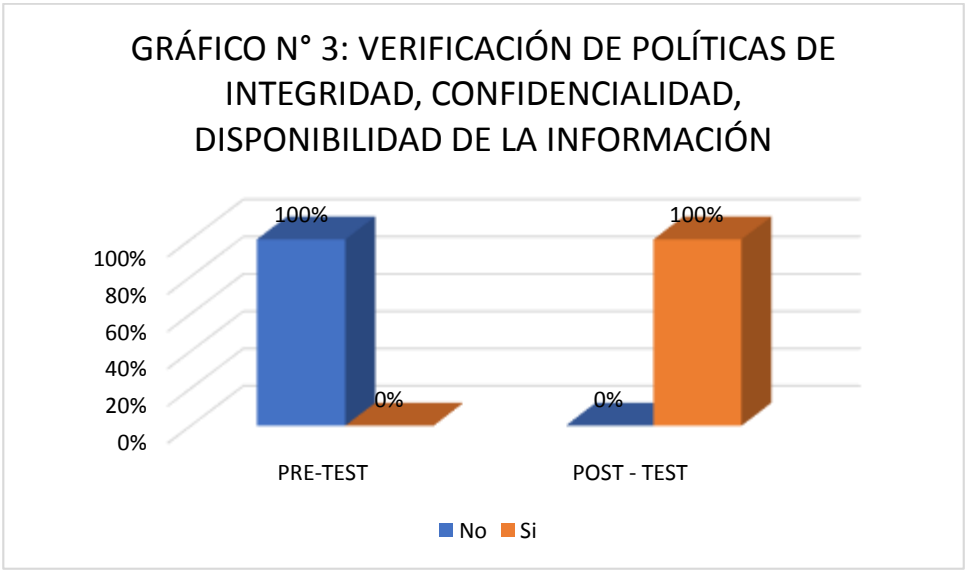
3. DIMENSIÓN: Políticas

Indicador: Verificación de políticas de integridad, confidencialidad, disponibilidad de la información

CUADRO N° 3: VERIFICACIÓN DE POLÍTICAS DE INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD DE LA INFORMACIÓN

RANGO	PRE-TEST		POST - TEST	
	fi	%	fi	%
No	103	100%	0	0%
Si	0	0%	103	100%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 3, se observa que en los resultados obtenidos en la prueba pre-test, el 100% que representa a 103 activos informáticos, "No" cuentan con políticas de seguridad. Mientras que en la prueba post-test se puede visualizar que aumentó la cantidad de activos en 100%, que "Si" cuentan con políticas de seguridad.

ANÁLISIS DESCRIPTIVO DE LA VARIABLE DEPENDIENTE:

SEGURIDAD DE INFORMACIÓN V3

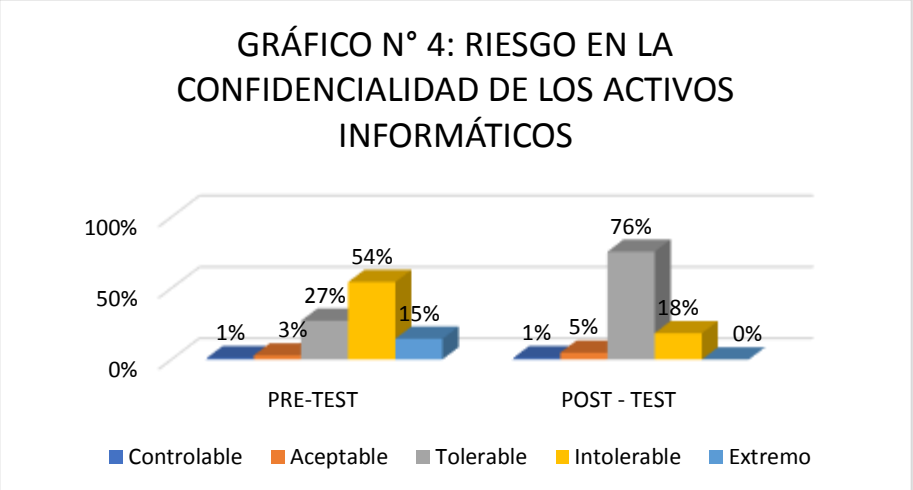
4. DIMENSIÓN: Confidencialidad

Indicador: Riesgo en la confidencialidad de los Activos Informáticos

CUADRO N° 4: RIESGO EN LA CONFIDENCIALIDAD DE LOS ACTIVOS INFORMÁTICOS

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
Controlable	1	1%	1	1%
Aceptable	3	3%	5	5%
Tolerable	28	27%	78	76%
Intolerable	56	54%	19	18%
Extremo	15	15%	0	0%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 4, se observa que en los resultados obtenidos en la prueba pre-test, el 54% que representa a 56 activos informáticos se encuentra en un estado de riesgo en la confidencialidad “intolerable”, el 15% que representan a 15 activos informáticos “Extremo”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la confidencialidad “intolerable” disminuyó a 18%, y “extremo” a 0%.

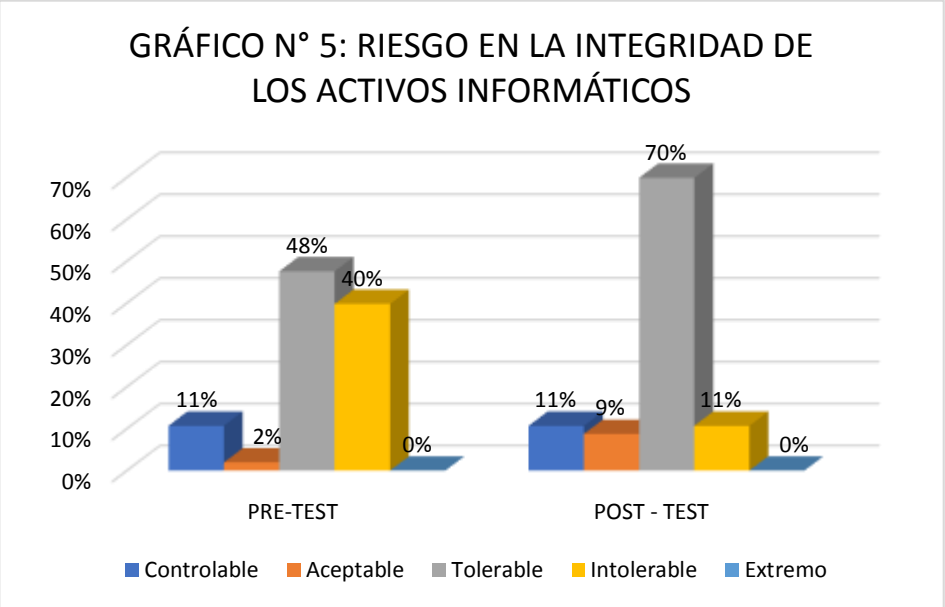
5. DIMENSIÓN: Integridad

Indicador: Riesgo en la integridad de los Activos Informáticos

CUADRO N° 5: RIESGO EN LA INTEGRIDAD DE LOS ACTIVOS INFORMÁTICOS

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
Controlable	11	11%	11	11%
Aceptable	2	2%	9	9%
Tolerable	49	48%	72	70%
Intolerable	41	40%	11	11%
Extremo	0	0%	0	0%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 5, se observa que en los resultados obtenidos en la prueba pre-test, el 48% que representa a 49 activos informáticos se encuentra en un estado de riesgo en la integridad “tolerable”, el 40% que representan a 41 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la integridad “intolerable” disminuyó a 11%, y “tolerable” aumentó a 70%.

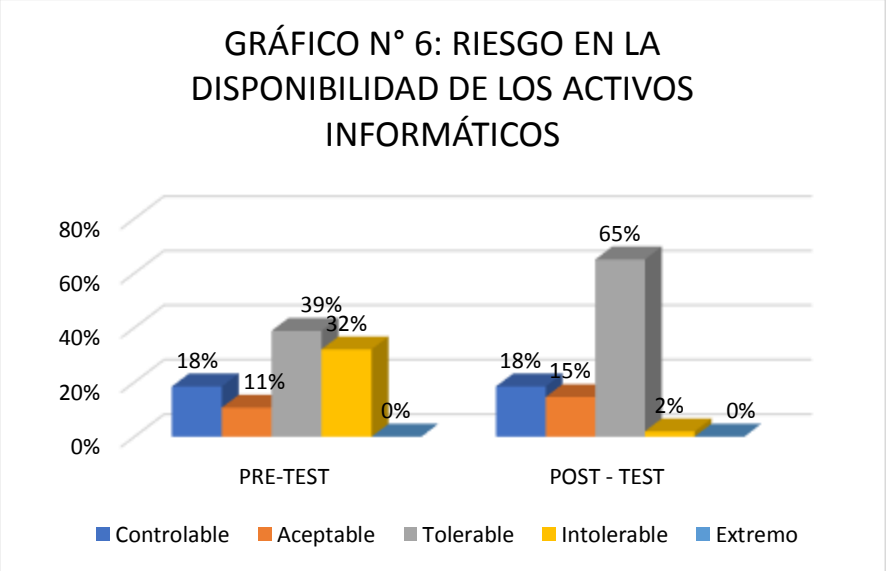
6. DIMENSIÓN: Disponibilidad

Indicador: Riesgo en la disponibilidad de los Activos Informáticos

CUADRO N° 6: RIESGO EN LA DISPONIBILIDAD DE LOS ACTIVOS INFORMÁTICOS

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
Controlable	19	18%	19	18%
Aceptable	11	11%	15	15%
Tolerable	40	39%	67	65%
Intolerable	33	32%	2	2%
Extremo	0	0%	0	0%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 6, se observa que en los resultados obtenidos en la prueba pre-test, el 39% que representa a 40 activos informáticos se encuentra en un estado de riesgo en la disponibilidad “tolerable”, el 32% que representan a 33 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la disponibilidad “intolerable” disminuyó a 2%, y “tolerable” aumentó a 65%.

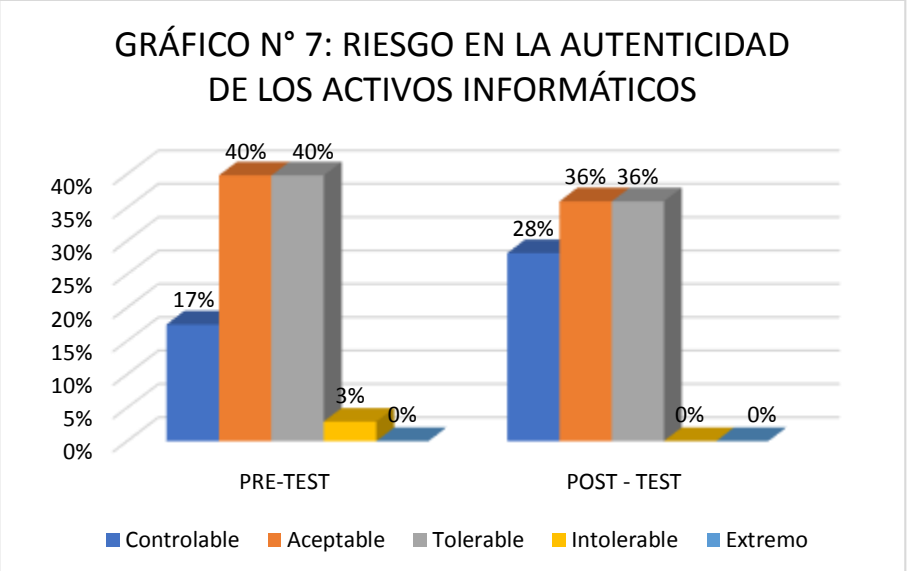
7. DIMENSIÓN: Autenticidad

Indicador: Riesgo en la autenticidad de los Activos Informáticos

CUADRO N° 7: RIESGO EN LA AUTENTICIDAD DE LOS ACTIVOS INFORMÁTICOS

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
Controlable	18	17%	29	28%
Aceptable	41	40%	37	36%
Tolerable	41	40%	37	36%
Intolerable	3	3%	0	0%
Extremo	0	0%	0	0%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 7, se observa que en los resultados obtenidos en la prueba pre-test, el 40% que representa a 41 activos informáticos se encuentra en un estado de riesgo en la autenticidad “tolerable”, el 3% que representan a 3 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la autenticidad “intolerable” disminuyó a 0%, y “tolerable” a 36%, ya que “aceptable” aumentó a 10%.

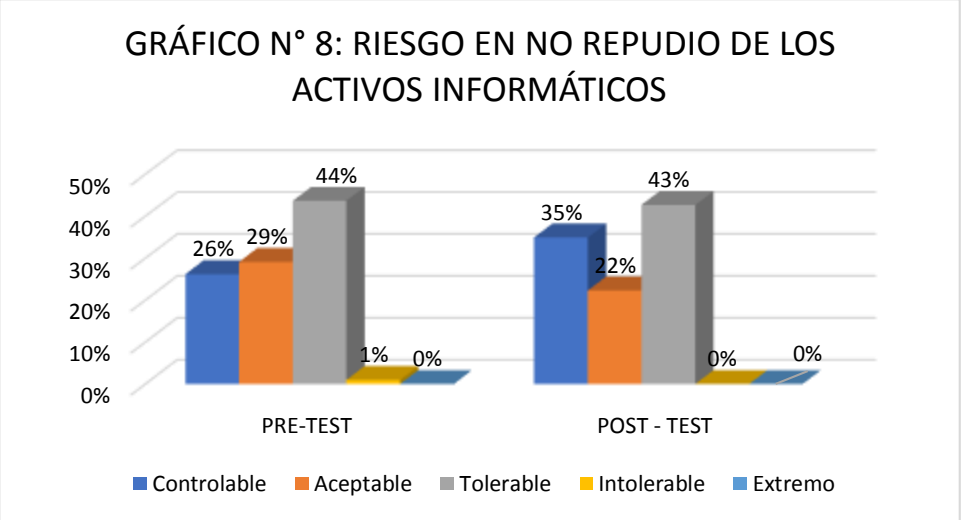
8. DIMENSIÓN: No Repudio

Indicador: Riesgo en No repudio de los Activos Informáticos

CUADRO N° 8: RIESGO EN NO REPUDIO DE LOS ACTIVOS INFORMÁTICOS

RANGO	PRE-TEST		POST - TEST	
	Fi	%	Fi	%
Controlable	27	26%	36	35%
Aceptable	30	29%	23	22%
Tolerable	45	44%	44	43%
Intolerable	1	1%	0	0%
Extremo	0	0%	0	0%
TOTAL	103	100%	103	100%

Fuente: Elaboración propia



Fuente: Elaboración propia

INTERPRETACIÓN:

Del gráfico N° 8, se observa que en los resultados obtenidos en la prueba pre-test, el 44% que representa a 45 activos informáticos se encuentra en un estado de riesgo en No repudio “tolerable”, el 1% que representan a 1 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo “intolerable” disminuyó a 0%, asimismo “tolerable” a 43%, ya que “aceptable” aumentó a 10%.

5.2 Contrastación de Hipótesis

Las pruebas de la Hipótesis General y Específicas, se realizará mediante el **TEST DE WILCOXON (Pruebas No Paramétricas)**, ya que se realiza para muestras relacionadas (pre y post) y las variables son cualitativas ordinales. Se realizará de la siguiente manera:

- Se calcula la **NORMALIDAD: Kolmogorov Smirnov**, para muestras pequeñas (> 30 datos).

  Criterios para determinar la Normalidad:

  P-valor => α ; Ha: Los datos provienen de una distribución Normal.

  P-valor < α ; Ho: Los datos **NO** provienen de una distribución Normal.

  - Como se trata de **PRUEBAS NO PARAMÉTRICAS, P- Valor < α.**

- Se calcula P-Valor de la PRUEBA DE WILCOXON

PRUEBA DE HIPÓTESIS GENERAL

H_a : La Aplicación de la Metodología Magerit V3, incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019.

H_0 : La Aplicación de la Metodología Magerit V3, no incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019.

a) NORMALIDAD:

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PREtestMAGERIT	103	100,0%	0	0,0%	103	100,0%
POStestMAGERIT	103	100,0%	0	0,0%	103	100,0%

Descriptivos

			Estadístico	Error estándar
PREtestMAGERIT	Media		3,18	,053
	95% de intervalo de confianza para la media	Límite inferior	3,08	
		Límite superior	3,29	
	Media recortada al 5%		3,19	
	Mediana		3,00	
	Varianza		,289	
	Desviación estándar		,538	
	Mínimo		2	
	Máximo		5	
	Rango		3	
	Rango intercuartil		0	
	Asimetría		,516	,238
	Curtosis		1,005	,472
POStestMAGERIT	Media		2,89	,034
	95% de intervalo de confianza para la media	Límite inferior	2,83	
		Límite superior	2,96	
	Media recortada al 5%		2,93	
	Mediana		3,00	
	Varianza		,116	
	Desviación estándar		,340	
	Mínimo		2	

	Máximo	4	
	Rango	2	
	Rango intercuartil	0	
	Asimetría	-1,795	,238
	Curtosis	3,989	,472

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**	Estadístico	gl	Sig.
PREtestMAGERIT	,401	103	,000	,704	103	,000
POStestMAGERIT	,507	103	,000	,431	103	,000

a. Corrección de significación de Lilliefors

P-valor (PRE-TEST MAGERIT V3) = 0,000 < α=0.05

P-valor (POST-TEST MAGERIT V3) = 0,000 < α=0.05

CONCLUSIÓN: Los datos no provienen de una distribución normal.

b) TEST DE WILCOXON

Rangos

		N	Rango promedio	Suma de rangos
POStestMAGERIT - PREtestMAGERIT	Rangos negativos	29[a]	15,52	450,00
	Rangos positivos	1[b]	15,00	15,00
	Empates	73[c]		
	Total	103		

a. POStestMAGERIT < PREtestMAGERIT
b. POStestMAGERIT > PREtestMAGERIT
c. POStestMAGERIT = PREtestMAGERIT

Estadísticos de prueba[a]

	POStestMAGERIT - PREtestMAGERIT
Z	-5,048[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

INTERPRETACIÓN: El valor de significancia (Valor crítico observado) es: 0,000 < 0,05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna, quiere decir que la Aplicación de la Metodología Magerit V3, incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

PRUEBA DE HIPÓTESIS ESPECÍFICA N° 1

H_a : La aplicación de la Metodología Magerit V3, incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

H_0 : La aplicación de la Metodología Magerit V3, no incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

a) NORMALIDAD:

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PREtestCONFID	103	100,0%	0	0,0%	103	100,0%
POStestCONFID	103	100,0%	0	0,0%	103	100,0%

Descriptivos

			Estadístico	Error estándar
PREtest CONFID	Media		3,79	,075
	95% de intervalo de confianza para la media	Límite inferior	3,64	
		Límite superior	3,94	
	Media recortada al 5%		3,82	
	Mediana		4,00	
	Varianza		,581	
	Desviación estándar		,762	
	Mínimo		1	
	Máximo		5	
	Rango		4	
	Rango intercuartil		1	
	Asimetría		-,564	,238
	Curtosis		1,038	,472
POStest CONFID	Media		3,12	,050
	95% de intervalo de confianza para la media	Límite inferior	3,02	
		Límite superior	3,22	
	Media recortada al 5%		3,14	
	Mediana		3,00	
	Varianza		,261	
	Desviación estándar		,511	
	Mínimo		1	

Máximo	4	
Rango	3	
Rango intercuartil	0	
Asimetría	-,260	,238
Curtosis	2,937	,472

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREtestCONFID	,300	103	,000	,833	103	,000
POStestCONFID	,406	103	,000	,649	103	,000

a. Corrección de significación de Lilliefors

P-valor (PRE-TEST CONFIDENCIALIDAD) = 0,000 < α=0.05

P-valor (POST-TEST CONFIDENCIALIDAD) = 0,000 < α=0.05

CONCLUSIÓN: Los datos no provienen de una distribución normal.

b) TEST DE WILCOXON

Rangos

		N	Rango promedio	Suma de rangos
POStestCONFID - PREtestCONFID	Rangos negativos	59[a]	30,00	1770,00
	Rangos positivos	0[b]	,00	,00
	Empates	44[c]		
	Total	103		

a. POStestCONFID < PREtestCONFID
b. POStestCONFID > PREtestCONFID
c. POStestCONFID = PREtestCONFID

Estadísticos de prueba[a]

	POStestCONFID - PREtestCONFID
Z	-7,206[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

INTERPRETACIÓN: El valor de significancia (Valor critico observado) es: 0,000 < 0,05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna, quiere decir que la aplicación de la Metodología Magerit V3, incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

PRUEBA DE HIPÓTESIS ESPECÍFICA N° 2

H_a: La aplicación de la Metodología Magerit V3, incide significativamente en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019.

H_0: La aplicación de la Metodología Magerit V3, no incide significativamente en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019.

a) NORMALIDAD:

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PREtestINTEGRI	103	100,0%	0	0,0%	103	100,0%
POStestINTEGRI	103	100,0%	0	0,0%	103	100,0%

Descriptivos

			Estadístico	Error estándar
PREtestINTEGRI	Media		3,17	,090
	95% de intervalo de confianza para la media	Límite inferior	2,99	
		Límite superior	3,34	
	Media recortada al 5%		3,24	
	Mediana		3,00	
	Varianza		,825	
	Desviación estándar		,909	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		-1,215	,238
	Curtosis		,959	,472
POStestINTEGRI	Media		2,81	,076
	95% de intervalo de confianza para la media	Límite inferior	2,66	
		Límite superior	2,96	
	Media recortada al 5%		2,84	
	Mediana		3,00	
	Varianza		,589	
	Desviación estándar		,768	
	Mínimo		1	

Máximo	4	
Rango	3	
Rango intercuartil	0	
Asimetría	-1,110	,238
Curtosis	1,198	,472

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREtestINTEGRI	,302	103	,000	,739	103	,000
POStestINTEGRI	,406	103	,000	,709	103	,000

a. Corrección de significación de Lilliefors

P-valor (PRE-TEST INTEGRIDAD) = 0,000 < α=0.05

P-valor (POST-TEST INTEGRIDAD) = 0,000 < α=0.05

CONCLUSIÓN: Los datos no provienen de una distribución normal.

b) TEST DE WILCOXON

Rangos

		N	Rango promedio	Suma de rangos
POStestINTEGRI - PREtestINTEGRI	Rangos negativos	34[a]	17,50	595,00
	Rangos positivos	0[b]	,00	,00
	Empates	69[c]		
	Total	103		

a. POStestINTEGRI < PREtestINTEGRI
b. POStestINTEGRI > PREtestINTEGRI
c. POStestINTEGRI = PREtestINTEGRI

Estadísticos de prueba[a]

	POStestINTEGRI - PREtestINTEGRI
Z	-5,621[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

INTERPRETACIÓN: El valor de significancia (Valor critico observado) es: 0,000 < 0,05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna, quiere decir que la aplicación de la Metodología Magerit V3, incide significativamente en la integridad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

PRUEBA DE HIPÓTESIS ESPECÍFICA N° 3

H_a : La aplicación de la Metodología Magerit V3, incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

H_0 : La aplicación de la Metodología Magerit V3, no incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

a) NORMALIDAD:

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PREtestDISPONI	103	100,0%	0	0,0%	103	100,0%
POSTestDISPONI	103	100,0%	0	0,0%	103	100,0%

Descriptivos

			Estadístico	Error estándar
PREtestDISPONI	Media		2,83	,105
	95% de intervalo de confianza para la media	Límite inferior	2,63	
		Límite superior	3,04	
	Media recortada al 5%		2,87	
	Mediana		3,00	
	Varianza		1,139	
	Desviación estándar		1,067	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		2	
	Asimetría		-,600	,238
	Curtosis		-,849	,472
POSTestDISPONI	Media		2,50	,080
	95% de intervalo de confianza para la media	Límite inferior	2,35	
		Límite superior	2,66	
	Media recortada al 5%		2,54	
	Mediana		3,00	
	Varianza		,664	
	Desviación estándar		,815	

Mínimo	1	
Máximo	4	
Rango	3	
Rango intercuartil	1	
Asimetría	-,958	,238
Curtosis	-,440	,472

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREtestDISPONI	,270	103	,000	,821	103	,000
POSTestDISPONI	,398	103	,000	,695	103	,000

a. Corrección de significación de Lilliefors

P-valor (PRE-TEST DISPONIBILIDAD) = 0,000 **<** α=0.05

P-valor (POST-TEST DISPONIBILIDAD) = 0,000 **<** α=0.05

CONCLUSIÓN: Los datos no provienen de una distribución normal.

b) TEST DE WILCOXON

Rangos

		N	Rango promedio	Suma de rangos
POSTestDISPONI - PREtestDISPONI	Rangos negativos	33[a]	17,00	561,00
	Rangos positivos	0[b]	,00	,00
	Empates	70[c]		
	Total	103		

a. POSTestDISPONI < PREtestDISPONI
b. POSTestDISPONI > PREtestDISPONI
c. POSTestDISPONI = PREtestDISPONI

Estadísticos de prueba[a]

	POSTestDISPONI - PREtestDISPONI
Z	-5,667[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

INTERPRETACIÓN: El valor de significancia (Valor critico observado) es: 0,000 < 0,05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna, quiere decir que la aplicación de la Metodología Magerit V3, incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

PRUEBA DE HIPÓTESIS ESPECÍFICA N° 4

H_a: La aplicación de la Metodología Magerit V3, incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

H_0: La aplicación de la Metodología Magerit V3, no incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019.

a) NORMALIDAD:

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PREtestAUTENTI	103	100,0%	0	0,0%	103	100,0%
POStestAUTENTI	103	100,0%	0	0,0%	103	100,0%

Descriptivos

			Estadístico	Error estándar
PREtest AUTENTI	Media		2,30	,079
	95% de intervalo de confianza para la media	Límite inferior	2,14	
		Límite superior	2,46	
	Media recortada al 5%		2,29	
	Mediana		2,00	
	Varianza		,644	
	Desviación estándar		,802	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		-,137	,238
	Curtosis		-,707	,472
POStest AUTENTI	Media		2,08	,079
	95% de intervalo de confianza para la media	Límite inferior	1,92	
		Límite superior	2,23	
	Media recortada al 5%		2,09	
	Mediana		2,00	
	Varianza		,641	
	Desviación estándar		,801	

	Mínimo	1	
	Máximo	3	
	Rango	2	
	Rango intercuartil	2	
	Asimetría	-,142	,238
	Curtosis	-1,423	,472

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREtestAUTENTI	,245	103	,000	,849	103	,000
POStestAUTENTI	,235	103	,000	,797	103	,000

a. Corrección de significación de Lilliefors

P-valor (PRE-TEST AUTENTICIDAD) = 0,000 **<** α=0.05

P-valor (POST-TEST AUTENTICIDAD) = 0,000 **<** α=0.05

CONCLUSIÓN: Los datos no provienen de una distribución normal.

b) TEST DE WILCOXON

Rangos

		N	Rango promedio	Suma de rangos
POStestAUTENTI - PREtestAUTENTI	Rangos negativos	21[a]	11,00	231,00
	Rangos positivos	0[b]	,00	,00
	Empates	82[c]		
	Total	103		

a. POStestAUTENTI < PREtestAUTENTI
b. POStestAUTENTI > PREtestAUTENTI
c. POStestAUTENTI = PREtestAUTENTI

Estadísticos de prueba[a]

	POStestAUTENTI - PREtestAUTENTI
Z	-4,413[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

INTERPRETACIÓN: El valor de significancia (Valor critico observado) es: 0,000 < 0,05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna, quiere decir que la aplicación de la Metodología Magerit V3 incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

PRUEBA DE HIPÓTESIS ESPECÍFICA N° 5

H_a: La aplicación de la Metodología Magerit V3, incide significativamente en No repudio de información de la Municipalidad Distrital de Pillco Marca, 2019.

H_0: La aplicación de la Metodología Magerit V3, no incide significativamente en No repudio de información de la Municipalidad Distrital de Pillco Marca, 2019.

a) NORMALIDAD:

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PREtestNOREPU	103	100,0%	0	0,0%	103	100,0%
POStestNOREPU	103	100,0%	0	0,0%	103	100,0%

Descriptivos

			Estadístico	Error estándar
PREtest NOREPU	Media		2,19	,083
	95% de intervalo de confianza para la media	Límite inferior	2,03	
		Límite superior	2,36	
	Media recortada al 5%		2,20	
	Mediana		2,00	
	Varianza		,707	
	Desviación estándar		,841	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		2	
	Asimetría		-,282	,238
	Curtosis		-1,331	,472
POStest NOREPU	Media		2,08	,087
	95% de intervalo de confianza para la media	Límite inferior	1,91	
		Límite superior	2,25	
	Media recortada al 5%		2,09	
	Mediana		2,00	
	Varianza		,778	
	Desviación estándar		,882	

Mínimo	1	
Máximo	3	
Rango	2	
Rango intercuartil	2	
Asimetría	-,154	,238
Curtosis	-1,710	,472

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREtestNOREPU	,278	103	,000	,798	103	,000
POStestNOREPU	,279	103	,000	,754	103	,000

a. Corrección de significación de Lilliefors

P-valor (PRE-TEST NO REPUDIO) = 0,000 < α=0.05

P-valor (POST-TEST NO REPUDIO) = 0,000 < α=0.05

CONCLUSIÓN: Los datos no provienen de una distribución normal.

b) TEST DE WILCOXON

Rangos

		N	Rango promedio	Suma de rangos
POStestNOREPU - PREtestNOREPU	Rangos negativos	13[a]	7,50	97,50
	Rangos positivos	1[b]	7,50	7,50
	Empates	89[c]		
	Total	103		

a. POStestNOREPU < PREtestNOREPU
b. POStestNOREPU > PREtestNOREPU
c. POStestNOREPU = PREtestNOREPU

Estadísticos de prueba[a]

	POStestNOREPU - PREtestNOREPU
Z	-3,207[b]
Sig. asintótica (bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

INTERPRETACIÓN: El valor de significancia (Valor critico observado) es: 0,000 < 0,05 rechazamos la hipótesis nula y aceptamos la hipótesis alterna, quiere decir que la aplicación de la Metodología Magerit V3, incide significativamente en No repudio de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

VI. DISCUSIÓN O CONTRASTACIÓN DE RESULTADOS

6.1 Contrastación de Resultados

En este capítulo, presentamos la confrontación de los resultados obtenidos: con la demostración del nivel de incidencia de la Metodología Magerit V3 en la Seguridad de Información, en términos de causa – efecto en los grupos de análisis ya determinados.

En los resultados de la presente investigación se determinó que existe influencia de la variable independiente (Metodología Magerit V3) y variable dependiente(Seguridad de Información), es decir que la Metodología Magerit V3, incide significativamente en la Seguridad de Información de la Municipalidad Distrital de Pillco Marca, tal como se observa en la prueba de la hipótesis general, donde: el valor de significancia es: 0.000 < 0.05, con la cual se aceptó la hipótesis general alterna y se rechazó la hipótesis nula, a un nivel de 95% de confiabilidad. Concuerdan con nuestros resultados las investigaciones de (Lucero G. & Valverde P., 2012), encontró que existe una influencia fuerte y significativa

entre la Metodología Magerit V3 y la Seguridad de Información en la Cooperativa de Ahorro y Crédito Jardín Azuayo.

Referente a la hipótesis específica N° 01. H_1:"La aplicación de la metodología Magerit V3, incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019";H_0: La aplicación de la metodología Magerit V3, no incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019", en los resultados del Cuadro N° 04 y Gráfico N° 04, se observa los resultados de la prueba del pre test, donde el 54%, que representa a 56 activos informáticos, se encuentran en estado de riesgo, en la confidencialidad "intolerable", el 15% que representan a 15 activos informáticos "Extremo"; después de la aplicación de la Metodología Magerit, en los resultados de la prueba de post test, se observa que el estado de riesgo en la confidencialidad intolerable disminuyó a 18%, y el extremo a 0%. Asimismo, en los resultados de la prueba de hipótesis especifica N° 01, se obtiene el valor de significancia: 0,00<0,05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, lo que significa que la metodología Magerit V3 incide significativamente en la confidencialidad de la información de la Municipalidad Distrital de Pillco Marca.

Con respecto a la hipótesis específica N° 02. H_1:"La aplicación de la metodología Magerit V3, incide significativamente en la integridad de

información de la Municipalidad Distrital de Pillco Marca, 2019";H_0: "La aplicación de la metodología Magerit V3, no incide significativamente en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019", En los resultados del Cuadro N° 05 y Gráfico N° 05, se observa que en los resultados en la prueba pre-test, el 48% que representa a 49 activos informáticos se encuentra en un estado de riesgo en la integridad "tolerable", y el 40% que representan a 41 activos informáticos "Intolerable". Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la integridad "intolerable" disminuyó a 11%, y "tolerable" aumentó a 70%. Así como también se visualiza en la comprobación de la hipótesis específica N° 02, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto significa que la metodología Magerit V3 incide en la integridad de información de la Municipalidad Distrital de Pillco Marca.

Concerniente a la hipótesis específica N° 03. H_1:"La aplicación de la metodología Magerit V3, incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019";H_0: "La aplicación de la metodología Magerit V3, no incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019", en el Cuadro N° 06 y Gráfico N° 06, se observa que en los resultados obtenidos en la prueba pre-test, el 39% que representa a 40

activos informáticos se encuentra en un estado de riesgo en la disponibilidad “tolerable”, el 32% que representan a 33 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la disponibilidad “intolerable” disminuyó a 2%, y “tolerable” aumentó a 65%. Asimismo, se observa en la comprobación de la hipótesis específica N° 03, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto significa que la metodología Magerit V3 incide en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca.

Referente a la hipótesis específica N° 04. H_1: “La aplicación de la metodología Magerit V3, incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019”;H_0: “La aplicación de la metodología Magerit V3, no incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019”, en el Cuadro N° 07 y Gráfico N° 07, se visualiza en los resultados obtenidos en la prueba pre-test, el 40% que representa a 41 activos informáticos se encuentra en un estado de riesgo en la autenticidad “tolerable”, el 3% que representan a 3 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo en la autenticidad “intolerable” disminuyó a 0%, y “tolerable” a 36%, ya que “aceptable” aumentó a 10%. También se observa en la

comprobación de la hipótesis específica N° 04, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, el cual significa que la metodología Magerit V3 incide en la autenticidad de información de la Municipalidad Distrital de Pillco Marca.

Con respecto a la hipótesis específica N° 05 H_1: “La aplicación de la metodología Magerit V3, incide significativamente en no rupudio de información de la Municipalidad Distrital de Pillco Marca, 2019”;H_0: “La aplicación de la metodología Magerit V3, no incide significativamente en no repudio de información de la Municipalidad Distrital de Pillco Marca, 2019”, en el Cuadro N° 08 y Gráfico N° 08, se observa que en los resultados obtenidos en la prueba pre-test, el 44% que representa a 45 activos informáticos se encuentra en un estado de riesgo en No repudio “tolerable”, el 1% que representan a 1 activos informáticos “Intolerable”. Mientras que en la prueba post-test se puede visualizar que el estado de riesgo “intolerable” disminuyó a 0%, asimismo “tolerable” a 43%, ya que “aceptable” aumentó a 10%. Asimismo, se observa en la comprobación de la hipótesis específica N° 05, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto significa que la metodología Magerit V3 incide en la no repudia de información de la Municipalidad Distrital de Pillco Marca.

CONCLUSIONES

Después de haber analizado y desarrollado la investigación, determinamos lo siguiente:

- Con respecto al objetivo general :“Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la seguridad de información de la Municipalidad Distrital de Pillco Marca 2019”, se ha determinado la incidencia de la Metodología Magerit V3 en la seguridad de información de la municipalidad, esto se demuestra en la comprobación de la hipótesis general, según el test de Wilcoxon, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, lo que significa que la metodología Magerit V3 incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.
- Referente al objetivo específico N° 01, se ha determinado la incidencia de la aplicación de la Metodología Magerit V3, en la confidencialidad de la Municipalidad Distrital de Pillco Marca 2019, tal como se observa en la comprobación de la hipótesis específica N° 01, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, lo que significa que la metodología Magerit V3 incide significativamente en la confidencialidad de información de la

Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

- En cuanto al objetivo específico N° 02, se ha determinado la incidencia de la aplicación de la Metodología Magerit V3, en la integridad de información de la Municipalidad Distrital de Pillco Marca 2019, tal como se observa en la comprobación de la hipótesis específica N° 02, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto quiere decir que la metodología Magerit V3 incide en la integridad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.
- Concerniente al objetivo específico N° 03, se ha determinado la incidencia de la aplicación de la Metodología Magerit V3, en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca 2019, tal como se observa en la comprobación de la hipótesis específica N° 03, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto significa que la metodología Magerit V3 incide en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.
- Con referente al objetivo específico N° 04, se ha determinado la incidencia de la aplicación de la Metodología Magerit V3, en la autenticidad de información de la Municipalidad Distrital de Pillco Marca

2019, tal como se observa en la comprobación de la hipótesis específica N° 04, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto significa que la metodología Magerit V3 incide en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

- Con respecto al objetivo específico N° 05, se ha determinado la incidencia de la aplicación de la Metodología Magerit V3, en no repudio de información de la Municipalidad Distrital de Pillco Marca 2019, tal como se observa en la comprobación de la hipótesis específica N° 05, donde el valor de significancia es: 0.00<0.05, con el cual se rechaza la hipótesis nula y se acepta la hipótesis alterna, esto significa que la metodología Magerit V3 incide en la no repudia de información de la Municipalidad Distrital de Pillco Marca, a un nivel de 95% de confiabilidad.

RECOMENDACIONES

A partir de los resultados obtenidos, se recomienda lo siguiente:

- A los profesionales y/o estudiantes, aplicar la metodología Magerit V3 en el análisis y gestión de riesgos de una organización ya que incide significativamente en la seguridad de la información.
- A los trabajadores de la Municipalidad Distrital de Pillco Marca, poner en práctica las políticas de seguridad, para mantener la confidencialidad de información de los activos informáticos con los que cuenta.
- A todas las oficinas de la Municipalidd Distrital de Pillco Marca, utilizar las políticas de seguridad en lo que respecta a integridad, para prevenir modificaciones no autorizadas de la información, y de esta manera se mantenga inalterada, ante accidentes o intentos maliciosos.
- A los gerentes de las diversas oficinas administrativas de la Municipalidad, monitorear que la información debe permanecer accesible a los usuarios autorizados, de esta manera prevenir interrupciones no autorizadas de los recursos informáticos y que estos se mantengan disponibles siempre.
- A los encargados del área de Informática de la municipalidad Distrital de Pillco Marca, hacer uso de cuentas de usario y contraseñas de acceso, para estar seguro que al recibir un mensaje o información de algún usuario, sea ese usuario el que lo ha enviado, y no una tercera persona; de esta manera permitirá identificar al generador de la información y reducir riesgos de suplantación de identidad.

- A los trabajadores de la Municipalidad Distrital de Pillco Marca, encargados de enviar y recibir información de diversas formas (digital o físico), tomar en cuenta y hacer uso de las políticas de seguridad proporcionadas, para garantizar la participación de las partes (emisor y receptor) en una comunicación, esto permitirá tener pruebas del envío y recepción de información por parte de la Municipalidad hacia otras entidades o usuarios finales.

BIBLIOGRAFÍA

Perafán Ruiz, J., & Caicedo Cuchimba, M. (2014). Análisis de Riesgos de la Seguridad de la Información para la Institución. *Tesis*.

Porras, L. (2000). Diseño Estadístico de Experimentos, Análisis de la Varianza y Temas Relacionados: Tratamiento Informático mediante SPSS. *Proyecto Sur de Ediciones*.

Talavera Álvarez , V. (2015). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD ESTATAL DE SAUD DE ACUERDO A LA ISO/IEC 27001:2013. *Tesis*.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). IIntroducción a Octave Allegro: Mejora del Proceso de Evaluación de Riesgos de Seguridad de la Información. *El Instituto de Ingeniería de Software*.

Consejo Superior de Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Colección: administración electrónica*.

Gallardo Piedra, M., & Jácome Cordones , P. (2011). Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I. para la Empresa Eléctrica Quito S.A. *Tesis* .

ISO 27001. (2013). Sistema de Gestión de la Seguridad de la Seguridad.

ISO Guide 73. (2009). Risk management — Vocabulary.

Kinkos' S impresores SAC. (2015). *Guía Básica del Registrador Civil.* Lima.

kuehl, R. (2001). Diseño de experimentos .

Lucero G. , A., & Valverde P., J. (2012). “Análisis y gestión de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT. *Tesis*.

MAGERIT. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

UNE 71504. (2008). “Metodología de análisis y gestión de riesgos para los sistemas de informa-ción”.

UNE-ISO Guía 73. (2010). “Gestión del riesgo. Vocabulario”.

ANEXOS

FORMATO DE ENTREVISTA

NOMBRE DEL ENTREVISTADOR: _____

FECHA: ____/_____/_____

PREGUNTAS:	RESPUESTAS:
¿Se han identificado amenazas que pueden llegar afectar la seguridad de información en la Municipalidad?	
¿Con qué frecuencia los impactos generan riesgos en la seguridad de información?	
¿Las políticas de seguridad planteadas, descruben y planifican el tratamiento oportuno, para mantener los riesgos bajo control?	
¿La Municipalidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de su infraestructura, redes, sistemas de información, aplicaciones y/o uso de los servicios?	
¿La Municipalidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?	
¿La Municipalidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?	
¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?	
¿La Municipalidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la Municipalidad?	
¿Con qué frecuencia La Municipalidad recibe ataques informáticos, que impidieron la prestación de algunos de los servicios que la Municipalidad ofrece a los ciudadanos y empresas?	
¿La Municipalidad ha definido lineamientos, normas y/o estándares para el desarrollo o adquisición de software, sistemas y aplicaciones?	

MATRIZ DE CONSISTENCIA

TÍTULO: "LA METODOLOGÍA MAGERIT V3 Y SU INCIDENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA MUNICIPALIDAD DE PILLCO MARCA, 2019"

FORMULACIÓN DE PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	METODOLOGÍA
General: ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3 en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019? **Específicos:** 1. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019? 2. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019? 3. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019? 4. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019? 5. ¿Cuál es la incidencia de la aplicación de la Metodología Magerit V3, en no repudio de información de la Municipalidad Distrital de Pillco Marca, 2019?	**General:** Determinar la incidencia de la Aplicación de la Metodología Magerit V3, en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019. **Específicos:** 1. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019. 2. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019. 3. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019. 4. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019. 5. Determinar la incidencia de la aplicación de la Metodología Magerit V3, en no repudio de información de la Municipalidad Distrital de Pillco Marca, 2019.	**General:** La Aplicación de la Metodología Magerit V3 incide significativamente en la seguridad de información de la Municipalidad Distrital de Pillco Marca, 2019. **Específicos:** 1. La Aplicación de la Metodología Magerit V3, incide significativamente en la confidencialidad de información de la Municipalidad Distrital de Pillco Marca, 2019. 2. La Aplicación de la Metodología Magerit V3, incide significativamente en la integridad de información de la Municipalidad Distrital de Pillco Marca, 2019. 3. La Aplicación de la Metodología Magerit V3, incide significativamente en la disponibilidad de información de la Municipalidad Distrital de Pillco Marca, 2019. 4. La Aplicación de la Metodología Magerit V3, incide significativamente en la autenticidad de información de la Municipalidad Distrital de Pillco Marca, 2019. 5. La Aplicación de la Metodología Magerit V3, incide significativamente en No repudio de información de la Municipalidad Distrital de Pillco Marca, 2019.	VARIABLE INDEPENDIENTE: Metodología MAGERIT V3	Riesgos Salvaguardas Políticas	• **Nivel**: Descriptivo – Explicativo. • **Tipo**: Aplicada. • **Diseño:** Cuasiexperimental. • **Población:** Los activos informáticos de la Municipalidad Distrital de Pillco Marca N=103 • **Muestra:** Muestreo intencional o de conveniencia. n = 103
			VARIABLE DEPENDIENTE: Seguridad de Información	Confidencialidad Integridad Disponibilidad Autenticidad No repudio	

GALERÍA DE FOTOS DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA


SUB GERENCIA DE
DESARROLLO ECONOMICO

VALIDACIÓN DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

1.1 NOMBRE DEL INSTRUMENTO DE EVALUACIÓN: La Metodología Magerit V3

1.2 TÍTULO DE LA INVESTIGACIÓN: "La Metodología MAGERIT V3 y su incidencia en la seguridad de información de la municipalidad de Pillco Marca, 2019"

1.3 TESISTAS:

- Bach. Pedro Pajuelo Godoy
- Bach. Sesi Beatriz Velasquez Gudiño

1.4 EXPERTO: Dra. Inés Jesús Tolentino

1.5 ASESOR: Dra. Inés Jesús Tolentino

II. ASPECTOS DE VALIDACIÓN:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS	Muy malo	Malo	Regular	Bueno	Muy Bueno
		1	2	3	4	5
1. CLARIDAD	Esta formulado con lenguaje apropiado.					X
2. OBJETIVIDAD	Esta expresado en conductas observables.				X	
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					X
4. ORGANIZACIÓN	Existe una organización lógica.					X
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias					X
7. CONSISTENCIA	Basado en aspectos teóricos-científicos				X	
8. COHERENCIA	De índices, indicadores y las dimensiones.				X	
9. METODOLOGÍA	La estrategia responde al propósito del diagnostico					X
10.OPORTUNIDAD	El instrumento ha sido aplicado en el momento oportuno o más adecuado.				X	
SUMATORIA PARCIAL					16	30
SUMATORIA TOTAL		46				

III. RESULTADOS DE LA VALIDACIÓN:

3.1 VALORACIÓN TOTAL CUANTITATIVA: 46

3.2 OPINIÓN: Favorable X Debe mejorar___ No favorable __

3.3 OBSERVACIONES:

Firma

VALIDACIÓN DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES:

1.1 NOMBRE DEL INSTRUMENTO DE EVALUACIÓN: La Metodología Magerit V3

1.2 TÍTULO DE LA INVESTIGACIÓN: "La Metodología MAGERIT V3 y su incidencia en la seguridad de información de la municipalidad de Pillco Marca, 2019"

1.3 TESISTAS:

- Bach. Pedro Pajuelo Godoy
- Bach. Sesi Beatriz Velasquez Gudiño

1.4 EXPERTO: Velsy Heidy Rivera Vidal

1.5 ASESOR: Dra. Inés Jesús Tolentino

II. ASPECTOS DE VALIDACIÓN:

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS	Muy malo	Malo	Regular	Bueno	Muy Bueno
		1	2	3	4	5
1. CLARIDAD	Esta formulado con lenguaje apropiado.				X	
2. OBJETIVIDAD	Esta expresado en conductas observables.					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					X
4. ORGANIZACIÓN	Existe una organización lógica.				X	
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad.				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias				X	
7. CONSISTENCIA	Basado en aspectos teóricos-científicos				X	
8. COHERENCIA	De índices, indicadores y las dimensiones.				X	
9. METODOLOGÍA	La estrategia responde al propósito del diagnostico					X
10.OPORTUNIDAD	El instrumento ha sido aplicado en el momento oportuno o más adecuado.				X	
SUMATORIA PARCIAL					28	15
SUMATORIA TOTAL					43	

III. RESULTADOS DE LA VALIDACIÓN:

3.1 VALORACIÓN TOTAL CUANTITATIVA: 43

3.2 OPINIÓN: Favorable X Debe mejorar___ No favorable __

3.3 OBSERVACIONES:

Firma

CONSTANCIA

EL QUE SUSCRIBE EL ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA:

HACE CONSTAR:

Que, los Bachilleres **Pedro Pajuelo Godoy**; y **Sesi Velásquez Gudiño**; egresados de la Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería Industrial de la Universidad Hermilio Valdizan-Huánuco; realizaron la aplicación de su trabajo de investigación denominado: "La Metodología Magerit V3 y su Incidencia en la Seguridad de Información de la Municipalidad Distrital de Pillco Marca 2019"; y como resultado de dicho trabajo hicieron la entrega de: ***Un Plan de Seguridad de Información para la Municipalidad Distrital de Pillco Marca, Provincia de Huánuco, Región Huánuco***.

Se expide la presente, a solicitud de los interesados para los fines que estimen conveniente.

Cayhuayna, abril del 2019

MUNICIPALIDAD DISTRITAL DE PILLCO MARCA
Prof. Lidgardo Vara Estrada
ALCALDE

CONSTANCIA

EL QUE SUSCRIBE EL ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA:

HACE CONSTAR:

Que, los Bachilleres **Pedro Pajuelo Godoy**; y **Sesi Velásquez Gudiño**; egresados de la Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería Industrial de la Universidad Hermilio Valdizan-Huánuco; realizaron la aplicación de su trabajo de investigación denominado: "La Metodología Magerit V3 y su Incidencia en la Seguridad de Información de la Municipalidad Distrital de Pillco Marca 2019"; durante el desarrollo del trabajo de investigación realizaron: ***La Charla Informativa sobre el Plan y Políticas de Seguridad de Información para la Municipalidad Distrital de Pillco Marca, Provincia de Huánuco, Región Huánuco.***

Se expide la presente, a solicitud de los interesados para los fines que estimen conveniente.

Cayhuayna, abril del 2019

MUNICIPALIDAD DISTRITAL DE PILLCO MARCA
Prof. Lidgardo Yara Estrada

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 - PROCATP

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" - HUÁNUCO - Lic. Teresa Lui Chin y González FEDATARIA

En Huánuco, a los 09 Días del mes de DICIEMBRE de 2019, siendo las 07:00 p.m. hrs de acuerdo al Reglamento del Programa de Capacitación y Titulación Profesional - PROCATP de la Universidad Nacional Hermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 51°, 52° y 53°, aprobado con Resolución N° 973-2014-UNHEVAL-CU de fecha 02.ABR.2014; se procedió a la evaluación de la sustentación de la tesis: **"LA METODOLOGÍA MAGERIT V3 Y SU INCIDENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA, 2019".**, presentado por el Bachiller en Ingeniería de Sistemas: **Sesi Beatriz VELÁSQUEZ GUDIÑO.** Este evento se realizó en el Salón de Sustentaciones de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Dr. Pedro G. Villavicencio Guardia

SECRETARIO: Ing. Elmer Chuquiyauri Saldivar

VOCAL: Dr. Víctor Cabrera Abanto.

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51°, 52° y 53° del Reglamento del Programa de Capacitación y Titulación Profesional-PROCATP, obteniéndose el siguiente resultado: **Nota:** 15 equivalente a la calificación de Bueno Quedando (el) (la) Bachiller en Ingeniería de Sistemas: **Sesi Beatriz VELÁSQUEZ GUDIÑO** 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

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN"
HUÁNUCO
ES COPIA FIEL DEL ORIGINAL
Huánuco 11-12-2019

Lic. Teresa Lui Chin y González
FEDATARIA
Registro N° 5080

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 - PROCATP

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" - HUÁNUCO - Lic. Teresa Lui Chin y Gonzáles FEDATARIA

En Huánuco, a los 07 Días del mes de DICIEMBRE de 2019, siendo las 07:00 p.m. hrs de acuerdo al Reglamento del Programa de Capacitación y Titulación Profesional - PROCATP de la Universidad Nacional Hermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 51°, 52° y 53°, aprobado con Resolución N° 973-2014-UNHEVAL-CU de fecha 02.ABR.2014; se procedió a la evaluación de la sustentación de la tesis: **"LA METODOLOGÍA MAGERIT V3 Y SU INCIDENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA, 2019".**, presentado por el Bachiller en Ingeniería de Sistemas: **Pedro PAJUELO GODOY** Este evento se realizó en el Salón de Sustentaciones de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Dr. Pedro G. Villavicencio Guardia

SECRETARIO: Ing. Elmer Chuquiyauri Saldivar

VOCAL: Dr. Víctor Cabrera Abanto.

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51°, 52° y 53° del Reglamento del Programa de Capacitación y Titulación Profesional-PROCATP, obteniéndose el siguiente resultado: **Nota:** ..15..... equivalente a la calificación de.....Bueno..... Quedando (el) (la) Bachiller en Ingeniería de Sistemas: **Pedro PAJUELO GODOY.** .....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

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN"
HUÁNUCO
ES COPIA FIEL DEL ORIGINAL
Huánuco 13 - 12 - 2019

Lic. Teresa Lui Chin y González
FEDATARIA
Registro N° 5142

AUTORIZACIÓN PARA PUBLICACIÓN DE TESIS ELECTRÓNICAS DE PREGRADO

IDENTIFICACIÓN PERSONAL (especificar los datos de los autores de la tesis).

Apellidos y Nombres: VELASQUEZ GUDIÑO, SESI BEATRIZ

DNI: 47396789 Correo Electrónico: SESI_VE_GU@HOTMAIL.COM

Teléfono: Casa _____ Celular: 989434248 Oficina: _____

Apellidos y Nombres: PAJUELO GODOY, PEDRO

DNI: 46380924 Correo Electrónico: PAJUE_LO23@HOTMAIL.COM

Teléfono: Casa _____ Celular: 980443189 Oficina: _____

Apellidos y Nombres: _____

DNI: _____ Correo Electrónico: _____

Teléfono: Casa _____ Celular: _____ Oficina: _____

IDENTIFICACIÓN DE LA TESIS

Pregrado
Facultad de: INGENIERÍA INDUSTRIAL Y DE SISTEMAS
E.P.: INGENIERÍA DE SISTEMAS

Título Profesional obtenido:

INGENIERO DE SISTEMAS

Título de la tesis:

"LA METODOLOGÍA MAGERIT V3 Y SU INCIDENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE PILLCO MARCA, 2019"

Tipo de acceso que autoriza (n) el (los) autor (es):

Marcar "X"	Categoría de Acceso	Descripción de Acceso
X	PÚBLICO	Es púbico y accesible al documento a texto completo por cualquier tipo de usuario que consulta el repositorio
	RESTRINGIDO	Solo permite el acceso al registro del metadato con información básica más no al texto completo

Al elegir la opción "Público", a través de la presente autorizo o autorizamos de manera gratuita al Repositorio Institucional – UNHEVAL, a publicar la versión electrónica de esta tesis en el Portal Web repositorio.unheval.edu.pe, por un 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.

En caso haya (n) marcado la opción "Restringido", por favor detallar las razones por las que se eligió este tipo de acceso.

Asimismo, pedimos indicar el periodo de tiempo en que la tesis tendría el tipo de acceso restringido:

( ) 1 año

( ) 2 años

( ) 3 años

( ) 4 años

Luego del período señalado por usted (es), automáticamente la tesis pasará a ser de acceso público.

Fecha de firma:

Firma del Autor y/o autores: