UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2022

AUTOR:

Bach. Hoces Román, Santiago Juan

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

ASESOR:

Mg. Corilla Baquerizo Eduardo Cancio

ID ORCID: 0000-0003-3472-2696

DNI N° 20037930

LIMA- PERÚ

2024

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

Facultad de Ciencias e Ingeniería

INFORME DE SIMILITUD Nº 047-2023-FCI-UPCI-T-ECB

A	:	**Mg. Ruben Edgar Hermoza Ochante** Decano (e) de la Facultad de Ciencias e Ingeniería
DE	:	**Mg. Eduardo Cancio Corilla Baquerizo**
ASUNTO	:	Informe de Evaluación de Similitud de Tesis
FECHA	:	Jesús María, 28 de agosto del 2023

Tengo el agrado de dirigirme a Ud. a fin de informar lo siguiente:

1. Mediante el uso del programa informático TURNITIN (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 15 palabras) se ha analizado la tesis titulada: **"Diseño de un Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2022"**, presentada por el Br:

   Bach. Hoces Román, Santiago Juan

2. El resultado de la evaluación indica que la tesis en mención tiene un INDICE DE SIMILITUD DE 27% (cumpliendo con el art. 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019)
3. Al término del análisis, se concluye que PUEDE(N) CONTINUAR su trámite.

Sin otro particular quedo de usted.

Atentamente

Mg. Eduardo Cancio Corilla Baquerizo
Docente UPCI

PD:
Se adjunta:
- Recibo digital Turnitin
- Resultado de similitud

DEDICATORIA

La presente tesis está dedicada a Dios, por permitirme tener vida, salud y poder realizar mis metas, A mi madre, padre y novia por el apoyo incondicional, quienes supieron tener paciencia, asistirme en todo lo que estaba a su alcance y darme fuerzas cuando flaqueaba para que este propósito me resulte posible.

AGRADECIMIENTO

A mis profesores y asesor de tesis por compartir sus conocimientos y experiencias en el desarrollo del presente trabajo.

PRESENTACION

Señores miembros del jurado, “en cumplimiento del Reglamento de Grado de Bachiller y Título Profesional de la Universidad Peruana de Ciencias e Informática, aprobado por Resolución N° 373-2019-UPCI-R; y en estricto cumplimiento del requisito establecido por el Artículo N° 45, ley N° 30220; donde se indica que la obtención de grados y títulos es realizada de acuerdo a las exigencias académicas que cada universidad establezca”, presento ante ustedes mi tesis titulada “Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2021”, la cual será puesto a vuestra consideración, evaluación y juicio profesional; para su aprobación y esta me conlleve a ostentar el Título profesional de Ingeniero de Sistemas e Informática.

Bach. Hoces Román, Santiago Juan

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este trabajo de investigación tuvo como principal objetivo Proponer un “sistema de gestión de seguridad de la información para disminuir riesgos de perdida de información en CENARES”.

La metodología utilizada y el tipo de investigación fue básica, el diseño fue no experimental, de nivel descriptivo correlacional; con una población de 30 usuarios del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud.

Se aplicó una encuesta, y un cuestionario de preguntas que permitió la recopilación de datos para un sistema de gestión de seguridad de la información, que disminuirá los riesgos de perdida de información en CENARES existiendo una correlación directamente proporcional.

Para el análisis y procesamiento de datos se utilizó software de Microsoft Excel y SPSS, (Statistical Package for Social Sciences). Para el análisis de confiabilidad se aplicó el alfa de Cronbach cuyo resultado fue 0.851, siendo este resultado superior al mínimo aceptable de 0.7.

Se pudo observar una correlación de 0.729 y el $P=0.000 < 0.05$, se rechaza H0, por lo tanto, “Si existe relación entre el sistema de gestión de seguridad de la información, entonces disminuye el riesgo de pérdida de información en CENARES”.

Palabras clave: Activos, Disminuir, Información, Sistema de Gestión de Seguridad de la Información, Riesgos.

ABSTRACT

This research work had as main objective Propose an “information security management system to reduce risks of information loss in CENARES".

The methodology used and the type of research was basic, the design was non-experimental, descriptive correlational level; with a population of 30 users of the National Center for the Supply of Strategic Resources in Health.

A survey was applied, and a questionnaire of questions that allowed the data collection to design an information security management system, which will reduce the risks of information loss in CENARES and there is a directly proportional correlation.

For data analysis and processing, Microsoft Excel and SPSS software (Statistical Package for Social Sciences) was used. For the reliability analysis, Cronbach's alpha was applied, the result of which was 0.851, this result being higher than the minimum acceptable of 0.7.

It was possible to observe a correlation of 0.729 and P=0.000 < 0.05, H0 is rejected, therefore, "If there is a relationship between the information security management system, then the risk of loss of information in CENARES decreases."

Keywords: Assets, Reduce, Information, Information Security Management System, Risks.

I. INTRODUCCIÓN

En los últimos tiempos, el avance tecnológico de las tecnologías de información y comunicaciones se ha convertido en uno de los activos más importantes dentro de las organizaciones, encontrándose en diferentes formatos: papel, almacenados electrónicamente, películas, hablada en conversaciones o transmitida usando las tecnologías de información y comunicaciones, entre otros. (Ampuero Chang, 2011).

En el Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud, considera primordial la protección de los activos de información, y todos los procesos de negocio y uno de los más importantes el proceso de backup, en caso de pérdida de información para recuperarla, seguridad en los equipos, entre otros.

En los procesos de negocio de la entidad que intervienen en la gestión de la seguridad de la información; Es importante evaluar los activos de información asociados al proceso de abastecimiento del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud; seleccionar los controles que permitan gestionar y tratar los riesgos identificados con base en la Norma ISO/IEC 27002; Asimismo, preparar la documentación requerida por la Norma ISO/IEC 27001 adoptada para el diseño del SGSI en CENARES.

Al desarrollar el SGSI, se reducirán económicamente los costos en términos de gestión de la seguridad de la información. En la parte tecnológica ayudará a permitir

una buena gestión de los recursos informáticos. Socialmente dentro de la institución, les permitió familiarizarse con los conceptos de seguridad en relación con las actividades diarias de los trabajadores.

El diseño del SGSI comienza con la definición de los procesos de negocio, identificando los activos de información y valorándolos; luego vemos cómo avanzamos hacia una identificación de los riesgos más destacados para luego desarrollar una metodología de evaluación de riesgos y un plan de evaluación basado en una serie de actividades para hacer cumplir el SGSI. Seguido de ello, se tomarán las políticas que adoptará la institución y los controles para la mitigación de los riesgos que no puedan ser aceptados por causar perjuicio a la continuidad del negocio.

1.1. Realidad problemática

En la actualidad, los continuos avances en las tecnologías de la información constituyen una herramienta para mejorar de manera eficiente los servicios de salud apoyados en sistemas informáticos en los que se almacena, procesa y transmite la información a través de redes de comunicación, para que esté cada vez más disponible. un mayor número de personas accediendo a la información, dejando presente el riesgo de fuga de información, ya sea por parte del personal que tiene acceso a la información o por personas externas que acceden a ella a través de intrusiones.

El Centro Nacional para el Abastecimiento de Recursos Estratégicos en Salud, en adelante CENARES, es un organismo desconcentrado del Ministerio de Salud que tiene a su cargo la gestión del abastecimiento de recursos estratégicos en salud,

también ejecuta los procesos de compras corporativas y tiene como objetivo apoyar de manera eficiente a la salud.

Tiene la dirección general y cuatro centros principales que la ejecutan: el Centro de Programación, Adquisiciones, Almacenamiento y Distribución, y la Gerencia Administrativa, que se encarga de dirigir, supervisar y evaluar el desarrollo del Personal, Contabilidad, Tesorería, Informática y patrimonio.

Actualmente la entidad cuenta con una certificación ISO 9001 la cual ha tenido un impacto positivo en la imagen organizacional pero que se ha visto afectada en los últimos años por la falta de un sistema de gestión de seguridad de la información que le permita garantizar la confidencialidad, su integridad y que la información esté disponible.

El propósito es asegurar que los riesgos y amenazas a la seguridad de la información sean conocidos, para luego asumirlos, gestionarlos y minimizarlos de manera bien estructurada y documentada.

En el CENARES, uno de los problemas en materia de seguridad de la información es que no se planeó un control adecuado en cuanto a la vigencia de los sistemas de seguridad de la información, como lo es la licencia de firmware del servidor, que actualmente mantiene un nivel básico de seguridad por 4 meses. , es decir, sin licencia, lo que provocó la pérdida de información que fue parcialmente recuperada. La adquisición de la licencia está en proceso, la cual tardará un par de meses más en actualizarse, mientras la información esté disponible, expuestos a vulnerabilidades a través de la intrusión.

Otro problema en la institución es que los equipos de cómputo no pueden ser administrados desde la sede porque la red no está segmentada, los equipos de cómputo están configurados a la red con IPs dinámicas lo que dificulta aún más el

control, no se encuentra el antivirus actualizado en todas las computadoras, lo que contribuye a que el sistema de seguridad esté expuesto a vulnerabilidades y amenazas externas que ponen en alto riesgo las funciones de la organización, las cuales pueden ser interrumpidas parcial o totalmente.

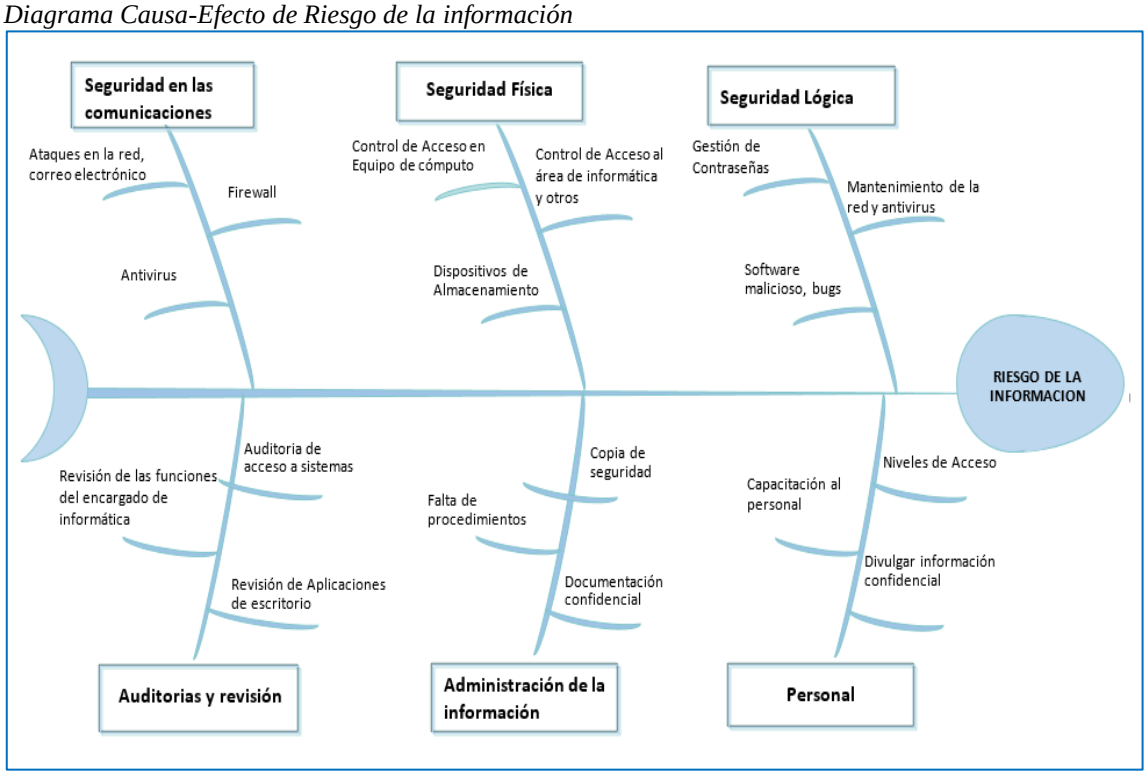
Otro problema en materia de seguridad de la información es que diariamente se generan reportes, se registran datos, se digitalizan documentos confidenciales y rutinarios, y diversos tipos de material de gran importancia para la institución, los cuales se almacenan tanto en medios físicos como electrónicos. , encontrándose así en la mayoría de los casos registrados en sistemas de información y aplicaciones tecnológicas y este se encuentra a disposición del personal autorizado que lo requiera al momento de tomar decisiones, emitir informes estadísticos, entre otros.

Los riesgos de seguridad de la información pueden ocurrir en cualquier parte de los procesos de desarrollo de las funciones, ya que pueden ser vulnerables por fallas que puedan existir en los sistemas de cómputo, hardware, red de comunicación de datos, tanto por parte del personal que tiene acceso como por parte de terceros a través de algún mecanismo de intrusión.

Los riesgos a los que se encuentra expuesto CENARES van desde pérdida de información en equipos de cómputo hasta amenazas en la red, esto se debe a que no cuenta con un sistema que gestione la seguridad de la información y solo se han implementado controles aislados, asumidos por el conocimiento del personal, experiencias adquiridas y aplicados según el criterio del personal de TI.

A continuación, presento el diagrama de Ishikawa, (ver figura 01) también conocido como diagrama de causa-efecto, el cual nos muestra los problemas existentes en relación a la seguridad de la información en el CENARES.

Figura 1.
Diagrama Causa-Efecto de Riesgo de la información



Fuente: Cenares Elaboración: propia

La información puede verse afectada por diversas causas, entre ellas:

- Falta de procedimiento y aplicación de controles según norma.
- Insuficiencia de manual de funciones de informática.
- Deficiencia de políticas en seguridad de información.
- Capacitación del personal relacionada a seguridad informática.
- Concientizar al personal en seguridad de las informaciones.

Por lo que en consecuencia se puede ver afectado por falta de seguridad en las informaciones:

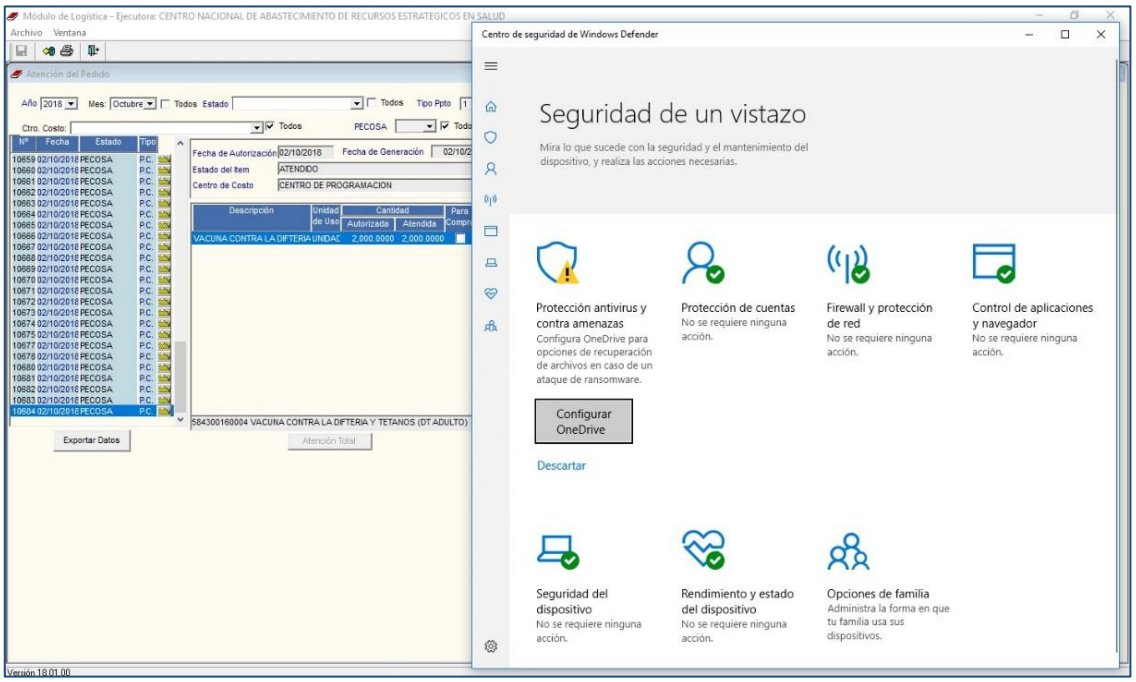
- La disponibilidad de las informaciones
- Alteración de informaciones
- Perdida de informaciones
- La integridad y confidencialidad de las informaciones

El problema en cuanto al proceso del riesgo de la información es que la institución no cuenta con políticas, procedimientos bien estructurados cuyo propósito es proteger la información implementando controles de seguridad que reduzcan el riesgo y las vulnerabilidades en los sistemas contribuyendo a mantener la confidencialidad, su integridad y disponibilidad de la información en la institución.

Uno de los problemas se presenta en las redes de comunicación, puesto que en CENARES existen tanto aplicaciones web como de escritorio, sitio web, intranet, los cuales facilitan la interacción con los usuarios pero que a su vez quedan expuesta a diversos mecanismos de intrusión como denegación de servicios, bloqueos de página web, hackers, que comprometen la integridad de la información.

Como medida de protección se utiliza el firewall, antivirus, Antispyware de red que es administrado por el personal de informática, donde se evidencia actualmente que la licencia a caducado por lo que se cuenta con un nivel de seguridad básico en el data center, en las estaciones de trabajo no son actualizados constantemente y no se realizan con frecuencia las copias de seguridad, por lo que se ve expuesto a pérdida o fuga de información.

Figura 02.
Equipo informático sin antivirus

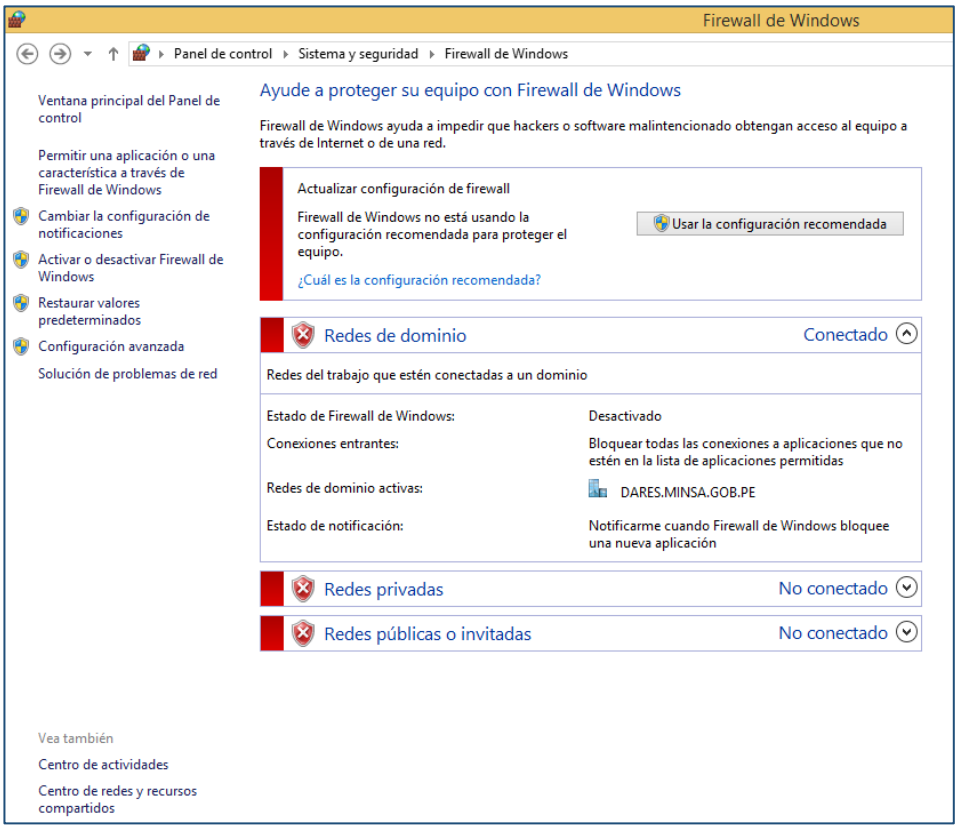


Fuente: Cenares -

Tal como se evidencia en la siguiente imagen (ver figura 02), el cual nos muestra que el equipo informático actualmente tiene información valiosa para la institución, una de ellas registrado en el sistema institucional SIGA (Sistema Integrado de Gestión Administrativa) pero que no cuenta con un antivirus instalado, el cual está expuesto a vulnerabilidades atreves de la red y sobre todo a perdida de información el cual afectaría gravemente a la institución ocasionando que la continuidad de las operaciones necesarias de la entidad se vean afectadas.

En otro equipo de cómputo se evidencia que no está activo el firewall de Windows, Como se muestra en la siguiente figura, el cual ayuda a impedir que hacker o software mal intencionados tengan acceso al equipo a través de la red o internet y esta a su vez se expanda por toda la red ocasionando perdida de información y continuidad de las operaciones en la institución. (Ver figura 03)

Figura 03.
Equipo informático sin activación de firewall

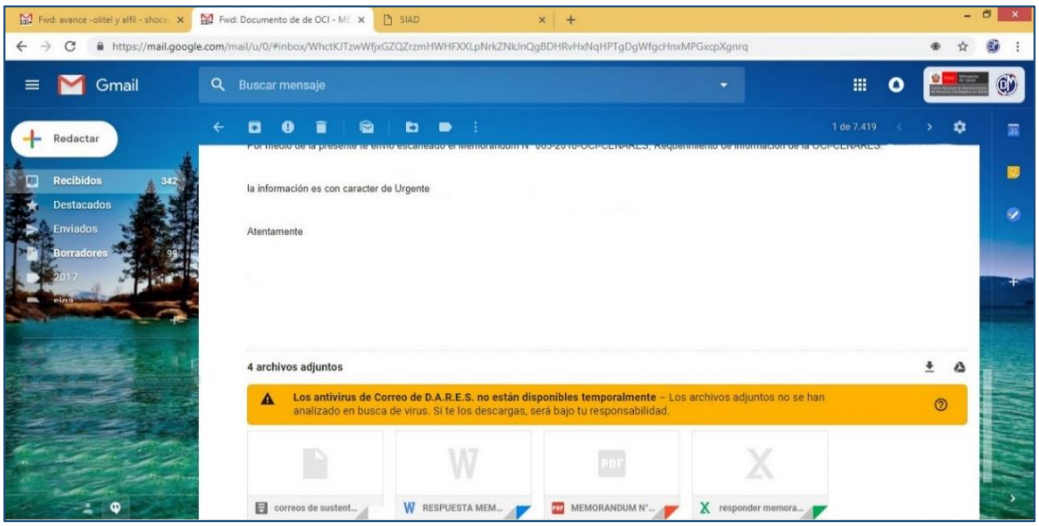


Fuente: Cenares

Esto sucede en razón a que actualmente no se cuenta con una buena administración del riesgo en la información por falta de políticas, procedimientos y normas, en donde todas las partes involucradas se comprometan a cumplir y hacer cumplir lo dispuesto en cada uno de ellos.

Otro caso se encuentra en la cuenta de correo institucional, el cual muestra en la siguiente imagen que el antivirus no se encuentra disponibles estando expuesto a software malicioso (Malware) el cual se puede filtrar o dañar el sistema y a la vez se propague por toda la red comprometiendo otros equipos de cómputo. (Ver figura 04)

Figura 04.
Cuenta de correo institucional sin antivirus



Fuente: Cenares -

Otro problema identificado en la institución es que los procesos de control de riesgo de la información no se encuentran estandarizados, es decir no existen políticas, normas, procedimientos alineados a ningún estándar internacional como la norma ISO 27001, ni la norma técnica peruana NTP-ISO/IEC 27001-2014 el cual se dispuso de uso obligatorio en toda institución pública y se encuentra alineada a la ISO 27001 el cual brinda un patrón a seguir en el establecimiento y conservación de un SGSI.

Actualmente solo se viene implementando controles aislados, asumidos por los conocimientos del personal a través de las experiencias adquiridas, y aplicadas según criterio del personal informático el cual brinda una solución, pero de corto plazo, no contando así con un plan de mejora continua en donde se determina que actividades, funciones y desempeño se pueden mejorar.

El personal de informática y otras áreas realiza sus actividades diarias acorde a las funciones que le han sido establecidas pero no revisa que parte de los procesos o actividades tienen deficiencias o posibles problemas, como obstáculos que generen

retrasos los cuales se puede mejorar, por lo que no se involucra e identifica con la institución.

Tal es el caso que cuando se presenta un incidente en un equipo informático se comunica por medio telefónico o por correo al responsable de informática el cual deriva al técnico para dar solución, pero por la sobrecarga laboral pasa en mayoría de los casos más de 24 horas en dar solución al problema.

Esto puede incidir un riesgo critico puesto que el equipo de cómputo puede verse comprometido a principales amenazas como Malware (infección de virus, código malicioso, troyanos, spyware, adware), spam, y toda aplicación que pueda ocasionar perdida de información, interrupciones en los sistemas de información o la obtención de información privada e importante para la institución.

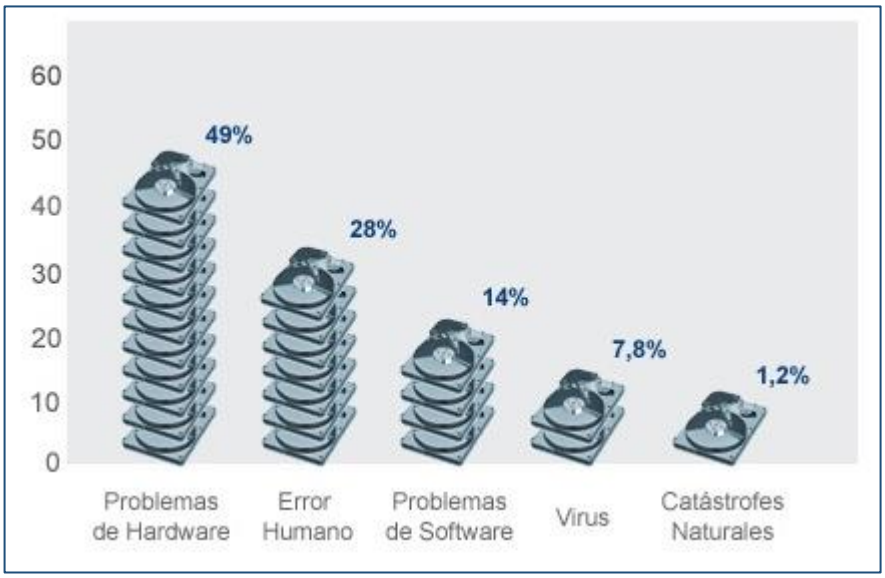
Las causas principales de pérdidas de información que suceden son:

- Riesgo operacional, fallo en el software, en la red, corte de fluido eléctrico.
- Malware y ciberataque, virus, amenazas en la red.
- Errores del personal, borrar información, robo.
- Desastres naturales, incendios e inundaciones.

Tal como muestro en la figura siguiente: (ver figura 05)

Los problemas relacionados al tema de seguridad de la información que engloba a la seguridad informática son otros medios de información como impresos en papel, medio magnético e incluso al personal, esto a razón que en la institución existe un área de recepción en el ingreso el cual controla el acceso de los usuarios, pero una vez adentro los usuarios no autorizados acceden a áreas restringidas teniendo acceso a sustraer información importante para la institución, por lo que no existe así un mecanismo de control de acceso en las oficinas.

Figura 05.
Causas de pérdida de información



Fuente: recovery labs

Esta información es confidencial para la institución y queda expuesta a intrusión, tanto los documentos en físico como expedientes, orden de servicio, orden de compra, etc. así también como acceso a la computadora como se puede ver en la siguiente figura, no se encuentra bloqueado y se puede acceder fácilmente obteniendo información privilegiada para la institución. (Ver figura 06)

La información es el activo más preciado de la organización el cual se encuentra expuesto a ser vulnerado por diversas razones tanto internas como externas, por ello se debe tener una adecuada seguridad de la información en la institución de la mano con la mejora continua resolviendo el problema de forma eficaz y no conformarse con la primera solución sin seguir el origen que ocasiono el problema.

Otro problema identificado en la institución sucede en el tratamiento del riesgo, ya que actualmente no existe ningún plan de seguridad en la información para tratarlos, identificando los incidentes que podrían ocurrir evaluando los riesgos y encontrar formas apropiadas de evitarlas.

Actualmente el personal de la institución no está enfocado en los riesgos que puedan suceder y el impacto que puede ocasionar en la entidad, si sucede fuga de

información, sustracción de datos, vulnerabilidad en la red e internet, no realizar copia de seguridad de la información, etc.

Figura 06.
Equipo y documentos expuestos a intrusión

Fuente: Cenares

Los riesgos a los que están propenso las informaciones en la institución son:

- Falta de capacitaciones y concientización al funcionario en temas de seguridad de la información.
- Falta de gestión de incidentes de seguridad, ello en razón a la necesidad de mejora en respuesta ante un incidente.
- Control en la red, por falta de control de acceso del personal e invitados a la intranet.
- Fuga de información, tanto por personal de la institución como usuarios externos.

- Deficiente control de acceso a las aplicaciones, en razón a que las contraseñas son muy débiles o genéricas.

Tal es el caso como el siniestro que sucedió en octubre del 2016 donde por factores externos se incendió la sede del almacén de CENARES donde se encontraba gran parte documentada de información confidencial que no se encontraba digitalizada, donde también funcionaba el área administrativa que contaba con gran cantidad de información confidencial y en su momento no se realizó las copias de seguridad necesarias y en consecuencia se perdió gran parte de la misma.

La información también se encuentra en riesgo sino se tiene una adecuada gestión de tratamiento de riesgo. Actualmente no se ha capacitado al personal en gestión del riesgo lo cual permitiría tener controles ajustados a las necesidades de la institución.

1.2. Planteamiento del problema

Delimitación del problema

Espacial

El SGSI se diseñó para aplicarlo con el personal que tenga acceso o haga uso de los activos de información del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud.

Temporal

El desarrollo de la tesis se llevó a cabo durante el periodo comprendido del mes de agosto 2022 – diciembre 2022.

1.2.1. Problema general

¿De qué manera el sistema de gestión de seguridad de la información disminuirá riesgos de perdida de información en CENARES?

1.2.2. Problemas específicos

a) ¿En qué medida el sistema de gestión de seguridad de la información disminuirá riesgos de confidencialidad de la información?
b) ¿En qué medida el sistema de gestión de seguridad de la información disminuirá riesgos de integridad de la información?
c) ¿En qué medida el sistema de gestión de seguridad de la información disminuirá riesgos de disponibilidad de la información?

1.3. Hipótesis de la investigación

1.3.1. Hipótesis general

Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye el riesgo de pérdida de información en CENARES.

1.3.2. Hipótesis específicas

a) Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de confidencialidad de la información.
b) Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de integridad de la información.
c) Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de disponibilidad de la información.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Determinar la relación entre el sistema de gestión de seguridad de la información y la disminución de riesgos de perdida de información en CENARES.

1.4.2. Objetivos específicos

a) Determinar la relación entre el sistema de seguridad de la información y la disminución de riesgos de confidencialidad de la información.

b) Determinar la relación entre el sistema de seguridad de la información y la disminución de riesgos de integridad de la información.

c) Determinar la relación entre el sistema de seguridad de la información y disminución de los riesgos de disponibilidad de la información.

1.5. Variables, dimensiones e indicadores

1.5.1. Variables Independientes

- ✓ Sistema de gestión de seguridad de la información

1.5.2. Variables Dependientes

- ✓ Riesgos de pérdida de información.

1.5.3. Dimensiones

- ✓ Política de seguridad de la información
- ✓ Plan de seguridad de la información
- ✓ Seguridad de la información
- ✓ Riesgo de confidencialidad de la información
- ✓ Riesgo de integridad de la información
- ✓ Riesgo de la disponibilidad de la información

1.5.4. Indicadores de las Variables

- ✓ Nivel de cumplimiento de las políticas
- ✓ % de implementación del plan

- ✓ Brechas de seguridad de la información
- ✓ Nivel de incidentes en la confidencialidad de la información
- ✓ Nivel de incidentes en la integridad de la información
- ✓ Nivel de incidentes en la disponibilidad de la información

1.5.5 Operacionalización de variables

Tabla 1*:*
Matriz de Operacionalización de Variables

VARIABLES	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
Sistema de gestión de seguridad de la información	Política de seguridad de la información	Nivel de cumplimiento de las políticas	Nunca A Veces Siempre
	Plan de seguridad de la información	% de implementación del plan	
	Seguridad de la información	Brechas de seguridad de la información	
Riesgos de pérdida de información	Riesgo de confidencialidad de la información	Nivel de incidentes en la confidencialidad de la información	Nunca A Veces Siempre
	Riesgo de integridad de la información	Nivel de incidentes en la integridad de la información	
	Riesgo de la disponibilidad de la información	Nivel de incidentes en la disponibilidad de la información	

Fuente: Elaboración propia

1.6. Justificación del estudio

Justificación Teórica

La presente investigación se desarrolla aplicando las teorías y conceptos concernientes a la seguridad de la información con el propósito de contribuir al conocimiento existente con calidad y eficacia en la mejora del control del riesgo de información. Para ello se requiere analizar y contrastar las diversas teorías e investigaciones con relación a la seguridad de la información el cual permitirá establecer resultados comparativos.

Justificación Práctica

El diseño del sistema de seguridad de la información permitirá tener la información integra, que se encuentre disponible al momento que sea requerida, garantizando la confiabilidad, aplicando controles de seguridad que permitan mantener los niveles de seguridad de tecnologías de la información alineadas a la institución

Justificación Legal

La seguridad de la información es un tema para tratar tanto para las instituciones públicas y privadas como para el estado, para ello la presente investigación se enmarca como referencia la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática, ley de protección de datos personales N° 29733 aprobada el 03 de julio del 2011, ley de delitos informáticos N° 30096 aprobada el 22 de octubre del 2013.

Justificación Económica

El proyecto permitirá salvaguardar el activo más importante de la institución como es la información, con ello la entidad podrá obtener beneficios económicos a través de

las políticas orientadas y destinadas a mejorar los procesos existentes en la institución.

Importancia del estudio

El sistema de gestión de seguridad de la información permite a la institución, con los constantes avances tecnológicos en un mundo globalizado, garantizar que los riesgos a los que está expuesto la información, sean controlados, de manera que puedan ser minimizados de manera estructurada y eficiente.

El sistema de gestión de seguridad de la información aportara las políticas, procedimientos necesarios basados en un modelo de buenas prácticas de seguridad como es la norma ISO 27001, para identificar y evaluar los riesgos y vulnerabilidades que está expuesto los activos de información, implantando controles adecuados sobre la confidencialidad, su disponibilidad y la integridad de la información protegiendo de esta manera la información en la institución.

En razón a lo anterior es de vital importancia para la institución la necesidad de contar con un sistema de gestión de seguridad de la información el cual permita reconocer, gestionar y reducir riesgos en la información de una forma organizada, sistemática y acorde a los cambios que pueda generar los riesgos permitiendo a los trabajadores del área informática obtener un adecuado y mejor nivel de servicio en calidad, funcionalidad y fluidez en seguridad de la información protegiendo a la institución de vulnerabilidades y riesgos al que puedan quedar expuesto la continuidad operacional.

La presente investigación es de gran importancia porque se puede asociar la teoría con la práctica complementando el desarrollo de la investigación obteniendo resultados que servirán de aporte en el ámbito tecnológico asegurando la protección de datos, información confidencial, etc.

1.7. Antecedentes nacionales e internacionales

1.7.1. Antecedentes internacionales

(Rainer, 2021) desarrollo la tesis “Evaluación del estado de seguridad de la información de una organización desde una perspectiva de gestión, Para obtener un título académico de Doctor en ciencias, Technische Universität Münche. Miunich – Alemania”.

Declaración del problema: a pesar de un creciente cuerpo de conocimiento en el área de investigación de la seguridad de la información y especialmente en la evaluación de la seguridad de la información, las organizaciones tienen dificultades para cuantificar su estado de seguridad de la información con el fin de tomar decisiones sobre un nivel de manejo. Por tanto, esta tesis aborda los siguientes retos en materia de información evaluación de la seguridad desde una perspectiva de gestión: (1) falta integral visión sobre la seguridad de la información, (2) las métricas disponibles no cumplen con los requisitos de gestión, (3) eslabón perdido entre las métricas técnicas y los objetivos de gestión, y (4) falta estándar integral de evaluación de la seguridad de la información. La tesis desarrolla un concepto tablero de evaluación de seguridad de la información para contribuir a una posible solución de los retos descritos.

Enfoque de investigación: El enfoque de investigación sigue el paradigma de la ciencia del diseño con tres iteraciones para desarrollar los resultados. Con respecto a este enfoque, múltiples metodologías se utilizaron para la recopilación de datos (búsqueda bibliográfica, entrevistas semiestructuradas a expertos, grupos focales), análisis de datos (análisis de literatura, codificación abierta-axial-

selectiva, análisis cualitativo análisis de contenido), desarrollo de artefactos (enfoque Objetivo-Pregunta-Métrica, seguridad de la información método de agregación de métricas) y evaluación (entrevistas semiestructuradas a expertos, grupos focales, simulación, argumento informado).

Resultados: Esta tesis proporciona varios hallazgos empíricos dentro de las tres iteraciones de la metodología de la ciencia del diseño. Comenzando con una revisión de la literatura disponible para distinguir términos que a menudo se usan como sinónimos, identificar corrientes de investigación y proponer una agenda de investigación en el campo de la evaluación de la seguridad de la información para introducir el problema.

Siguiendo la agenda de investigación, (1) la tesis sugiere 12 factores que influyen en la información decisiones de gestión de la seguridad y sus interrelaciones para generar un modelo. El desarrollo de (2) una metodología para agregar métricas de seguridad de la información de acuerdo con las necesidades de gestión combinado con una revisión de la información existente, las métricas de seguridad conducen al (3) desarrollo de una evaluación conceptual de la seguridad de la información cuadro de mando desde la perspectiva de la gestión.

Contribuciones: La tesis proporciona varias contribuciones a la teoría y la práctica, la delimitación de términos y el método de factores de seguridad de la información que influyen los tomadores de decisiones extienden el conocimiento de la seguridad de la información dentro de las organizaciones, los aspectos subyacentes e interdependencias. La tesis presenta una nueva forma de agregar métricas de seguridad de la información mediante la satisfacción de las necesidades de gestión. También contribuye a la investigación en el campo de la

evaluación de la seguridad de la información y ayuda a los profesionales con métricas existentes para presentarlas a la gerencia. El tablero en sí proporciona una visión integral, comparable, trazable, procesable y útil sobre el estado de seguridad de la información y contribuye a la teoría al mostrar una forma de reducir efectos sobre la calidad explicados por la teoría de la decisión, como la sobrecarga de información, asimetría de información y agregación de información.

Resumen y limitaciones del estudio: Los resultados de esta tesis están sujetos a limitaciones. La evaluación de los resultados se basa en entrevistas semiestructuradas a expertos y grupos focales y cubre solo un pequeño número de organizaciones e industrias con un enfoque en las grandes organizaciones. Por lo tanto, los resultados pueden tener una capacidad de generalización limitada. A pesar de las diferentes medidas para reducir los problemas de validez y confiabilidad, no todos los resultados se prueban con métodos cuantitativos experimentos y estudios y, por lo tanto, podría estar sesgado por los significados del sujeto de entrevistados o el juicio del investigador.

Investigación futura: en base a los hallazgos y limitaciones, esta tesis abre varias posibilidades de futuras investigaciones. Esto incluye la (1) evaluación cuantitativa y extensión del modelo integral sugerido de factores de seguridad de la información, (2) el uso de la metodología de agregación de seguridad de la información para desarrollar más herramientas de medición, y (3) la implementación del tablero conceptual de evaluación de la seguridad de la información para probar el desempeño mediante la toma de decisiones. Además, (4) la comparación de la información estado de seguridad de diferentes

organizaciones y (5) sistemas de recomendación basados en herramientas para apoyo a las decisiones.

(YiJie, 2021) desarrollo la tesis “Un enfoque sistemático para la gestión de riesgos de ciberseguridad, Para obtener el Master of Science in Engineering and Management, Universidad Nacional Chengchi. Taipei – Taiwan”.

En los últimos años, la preocupación por la ciberseguridad ha crecido de forma espectacular. Con todas las pautas y marcos existentes, y a veces en competencia, destinados a informar las estrategias de riesgo cibernético, las organizaciones enfrentan el problema de decidir cuál es el correcto para ellos. Para resolver la confusión, esta investigación propone una práctica y eficaz modelo que puede ser utilizado por organizaciones de cualquier tamaño o en cualquier industria para cyber gestión de riesgos. Proponemos una herramienta Cyber Risk Cube (CRC) diseñada para ser práctica para todas las partes de una organización, que examina tres pares fundamentales para analizando el riesgo cibernético: Interno/Externo, Medición/Gestión y Cualitativo/ Cuantitativo. La herramienta CRC se puede utilizar como un lenguaje común para compartir ideas y soluciones para la gestión del riesgo cibernético. En última instancia, la CRC proporciona detalles para implementar soluciones para gestionar los riesgos cibernéticos de forma concisa y estandarizada manera.

(Ruiz, 2018) desarrollo la tesis “Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) Bajo la Norma ISO/IEC 27001:2013, en la Cooperativa Multiactiva del Personal del SENA, en Bogotá, Para obtener el Título de

Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia UNAD. Bogotá – Colombia".

Este proyecto de grado presenta una descripción detallada de lo que es un Sistema de Gestión de Seguridad de la Información; Se específica para qué sirve, cuáles son sus objetivos, cuáles son sus ventajas, cuáles son sus componentes y cuáles son las metodologías más influyentes para lograr una buena y económica implementación.

Su desarrollo se basa en la investigación realizada en la infraestructura tecnológica de COOPSENA, con el fin de analizar la situación actual de la entidad desde la perspectiva de los procedimientos que se realizan con relación a la seguridad de la información, para ello hemos utilizado recursos como la observación, entrevista y análisis de documentos, así como la información obtenida de la norma ISO/IEC 27001:2013, escogida para el diseño y desarrollo del mencionado proyecto.

Para la etapa de planificación, que forma parte del modelo Deming integrado en el mencionado estándar, se ha optado por la metodología MAGERIT como herramienta del proceso de gestión de riesgos, lo que ha permitido realizar las actividades de desarrollo de una forma más sistemática. , gracias a las etapas en que se estructura.

- □ Identificación y valoración de activos corporativos.
- □ Identificación y evaluación de amenazas
- □ Determinación de salvaguardas, proceso apoyado en técnicas como las listas de verificación y la declaración de aplicabilidad (SOA).
- □ impacto residual

- □ riesgo residual

1.7.2. Antecedentes nacionales

(Silva, 2022) desarrollo la tesis “Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE – 2021, Para optar el Título Profesional de Ingeniero de Sistemas e Informática, Universidad Tecnológica del Perú. Lima – Perú”.

Según cifras de ENAHO, en 2020 las MYPES representaron el 95% de las empresas peruanas y empleaba al 26,6% de la Población Económicamente Activa - PEA, esto se debe a la actitud y capacidad emprendedora de los peruanos. “A su vez la información gestionada por las empresas es un factor clave para ellas, desde hace varios años la empresa ha sido considerada información como un activo por su importancia para las empresas, pero no todas las empresas le dan la misma importancia, por lo que muchas empresas presentan algún tipo de incidente o daño que afecta a los distintos activos de información que poseen, generando diversos problemas dentro de ellos. Por eso el objetivo de la presente investigación es implementar un Sistema de Gestión de Seguridad de la Información o SGSI, de esta manera mejorar la Seguridad de la Información o SI en una empresa MYPE”.

En el cual, se utilizó la NTP-ISO/IEC 27001:2014, “la cual establece una serie de lineamientos para gestionar adecuadamente el SGSI a través del ciclo de mejora y el enfoque de riesgos, consecuentemente, se logró mejorar el SI dentro de la empresa, esto debido a la implementación del SGSI, a través del compromiso de todas las personas involucrados y el cumplimiento de las pautas establecidas en la documentación requerido de este trabajo de investigación.

Asimismo, se concluye que la norma mencionada anteriormente proporciona pautas adecuadas para preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando así el SI dentro de la empresa".

(Garcia, 2020) desarrollo la tesis "Propuesta de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001 Para la Oficina de Tecnologías de Información del Gobierno Regional Piura; 2020, Para optar el título profesional de Ingeniero de Sistemas, Universidad Católica los Ángeles de Chimbote. Piura – Perú".

Esta tesis se desarrolló bajo la línea de investigación: Seguridad de la Información y Sistemas de Gestión de la Calidad, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; Su objetivo fue realizar una propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de la información del Gobierno Regional de Piura; 2020, para minimizar la pérdida de información, la investigación se desarrolló de forma cuantitativa bajo el diseño descriptivo de transcripción no experimental. La población de la muestra de la tesis estuvo constituida por los 23 trabajadores; de lo cual se obtuvo como resultado: El 91% de los trabajadores encuestados expresaron NO estar satisfechos con la situación actual; mientras que el 9% indicó que, SI están satisfechos con la situación actual, el 100,00% de los trabajadores encuestados expresaron SI necesitan seguridad de la información con la norma ISO 27001. El alcance abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para preservar la confidencialidad, integridad y

disponibilidad de la información en la oficina de tecnologías de la información del Gobierno Regional de Piura. Como conclusión se determinó que la propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de la información del Gobierno Regional de Piura mejoró sus procesos de seguridad de la información y las comunicaciones.

(Falcon, 2021) desarrollo la tesis "Propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información Basado en a Norma ISO 27001 Para una Empresa de Telecomunicaciones, 2021, Para optar el Título Profesional de Ingeniero de Sistemas, Universidad Nacional José Faustino Sánchez Carrión. Lima – Huacho".

Objetivo: Determinar la influencia de la implementación de un Sistema de Seguridad de la Información en la norma ISO 27001 para una empresa de telecomunicaciones, 2021.

Métodos: El siguiente tipo de investigación aplicada. El nivel de la investigación es Correlacional. La investigación tiene un diseño no experimental y transversal.

Resultados: Los resultados muestran que más del 80% de los encuestados están de acuerdo con la propuesta de Implantación del Sistema de Gestión de Seguridad de la Información basado en ISO 27001 para una empresa de telecomunicaciones, 2021.

Conclusión: Existe una correlación positiva significativa moderada entre el modelo de inteligencia empresarial y gestión administrativa (Rho = 0,697; p = 0,00 < 0,05).

1.8. Marco teórico

1.8.1. Seguridad informática

Es una disciplina que está conformada por políticas, estándares, modelos, procedimientos y mecanismos tecnológicos cuya acción está destinada a prevenir, detectar, anular o disminuir en cierto grado, las vulnerabilidades; y por tanto, las amenazas que se establecen contra las infraestructuras de Tecnologías de la información y las comunicaciones TIC'S, que son la base para el funcionamiento y desarrollo de las organizaciones.

La seguridad informática se ha estructurado en otros procesos como la seguridad en redes, seguridad en aplicaciones web, seguridad en base de datos, seguridad de los sistemas operativos, etc. Con el fin de gestionar acciones y procedimientos más seguros que permitan conservar, salvaguardar y proteger la información que es producida por los sistemas informáticos de las organizaciones, los cuales de manera constante están sometidos a una gran variedad de riesgos y amenazas que son originados, tanto desde la parte interna, como desde la parte externa de las mismas, debido a los siguientes factores:

- Factores humanos.
- Factores Ambientales

De acuerdo con estos factores, la seguridad informática se divide en dos grandes ramas:

- Seguridad física.
- Seguridad lógica.

Seguridad de la información

Es un proceso cuyo objetivo principal, es proteger y mantener la integridad de los activos críticos como la información, los aplicativos (software) y los servicios que soportan la razón de ser de una organización, los cuales dependen de las infraestructuras tecnológicas. Además, provee otras medidas de seguridad sobre los medios en donde esté disponible la Información como: cintas magnéticas, discos duros, impresiones en papel, videos e inclusive, sobre las personas que la manipulan o la conocen mediante procesos de concientización, es decir, asegura una mayor solidez a la confidencialidad, integridad y disponibilidad de la información.

Los procesos de seguridad de la información están orientados a hacer resistencia a las acciones que comprometan sus principios:

Confidencialidad

Garantiza que la información debe ser accedida solamente por las personas autorizadas. Una técnica de control asociada a este principio es la encriptación.

Integridad

Permite asegurar que los datos recibidos o recuperados son exactos y completos, es decir, que no han sufrido ningún tipo de modificación. Una de las técnicas que garantiza este principio son los algoritmos de cifrado.

Disponibilidad

Garantiza que la información debe ser accesible por las personas autorizadas en el momento de requerirla. Una de las técnicas aplicadas son los planes de contingencia.

Principios asociados a la seguridad de la información:

Autenticación

Garantiza la identidad de quien solicita acceso a la información. Una técnica aplicada, las firmas digitales.

Autorización

Garantiza el acceso y utilización de la información, solamente por las personas que tienen los permisos especiales o la exclusividad para hacerlo. Una técnica aplicada, los perfiles de usuario.

No repudio

Garantiza la aceptación de una persona como el actor, el responsable o participante de un evento informático. Por ejemplo: Un usuario que realiza la emisión de un mensaje no puede tener un argumento sólido para negar que lo generó y el usuario receptor tampoco podrá negar que lo recibió.

Gestión de la seguridad de la información - SGSI

"Es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización" (Suarez, 2016)

Un SGSI nos proporciona un modelo para verificar, sostener y aumentar la seguridad de los activos de información, así indica:

Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero si se pueden gestionar.

En este sentido, conviene destacar que en la práctica resulta imposible alcanzar al 100% y, por este motivo, algunos expertos prefieren hablar de la fiabilidad del sistema informático, entendiendo como tal la probabilidad de que el sistema se comporte tal y como se espera de él.

Podemos distinguir varias etapas o niveles de madurez den la gestión de la seguridad de la información en una organización:

- Implantación de medidas básicas de seguridad por "sentido común".
- Adaptación a los requisitos del marco legal y de las exigencias de los clientes.
- Gestión integral de la seguridad de la información.
- Certificación de la gestión de la seguridad de la información.

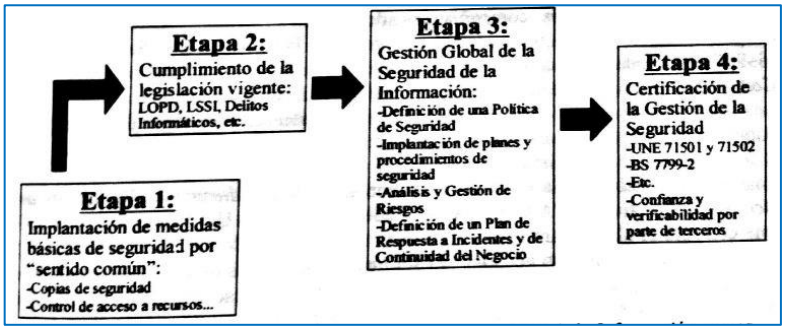


Figura 07. Niveles de madurez en la gestión de la seguridad de la información en una organización
Fuente: Enciclopedia de la seguridad informática 2da edición, Álvaro Gómez Vieites

En la mayoría de los países todavía no existe una legislación específica que obligue a las organizaciones públicas y privadas a implantar una serie de medidas para gestionar la seguridad de sus sistemas informáticos, salvo en lo que se refiere a la protección de los datos de carácter personal.

Sin duda una de las referencias legales más interesantes en este sentido es la ley Sarbanes-Oxley ("Sarbanes Oxley Act"), aprobada en 2002 en Estados Unidos. Esta ley fue promulgada a raíz de una serie de escándalos financieros que

afectaron a la credibilidad de varias compañías estadounidenses, siendo promovida por los congresistas Sarbanes y Oxley (de ahí el nombre de la ley). La ley Sarbanes-Oxley se aplica a todas las compañías que cotizan en la SEC (Securities Exchange Comission, comisión de la Bolsa de Valores de Estados Unidos) y a sus filiales, estableciendo un conjunto de medidas, requisitos y controles de seguridad que deben cumplir estas empresas para garantizar la fiabilidad de su información financiera.

Políticas de seguridad de la información

Las políticas de gestión de la seguridad de la información están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización.

Para implantar un sistema de gestión de gestión de seguridad e la información una organización debe contemplar los siguientes aspectos:

1. Formalizar la gestión de la seguridad de la información
2. Analizar y gestionar los riesgos.
3. Establecer procesos de gestión de la seguridad siguiendo la metodología PDCA:
4. Certificación de la gestión de la seguridad.

En todo proceso se debe contemplar un modelo que tenga en cuenta los aspectos tecnológicos, organizativos, el cumplimiento del marco legal y la importancia del factor humano.

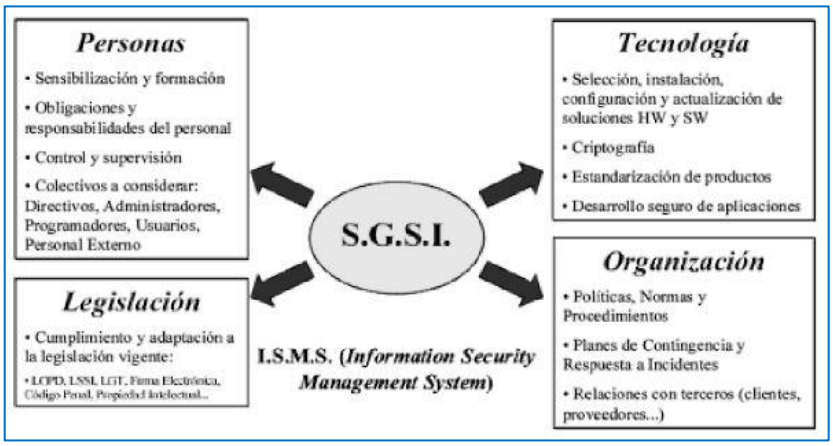


Figura 8. Modelo para la gestión de la seguridad de la información
Fuente: Enciclopedia de la seguridad informática 2da edición

Plan de Gestión de Seguridad Informática

Es un conjunto de herramientas, medidas administrativas, técnicas y de personal que están relacionadas.

Un plan de gestión de la seguridad informática es el documento básico que define los principios organizativos y funcionales de las actividades de seguridad informática de una entidad y establece todas las políticas seguridad y responsabilidad de los involucrados en el proceso informático, así como medidas y procedimientos para prevenir, detectar y responder a las amenazas que lo agobian.

ISO 27001

La Norma Estándar ISO 27001 tiene un enfoque sistemático utilizado para gestionar la información confidencial de una organización empresarial con el fin de mantener su integridad y confidencialidad. Este modelo de gestión de riesgos incluye a todo el personal, procesos internos, procesos externos y sistemas gestionados por el departamento de TI.

Mejora continua

La mejora continua en el SGSI se basa en el ciclo de Deming, conocido como PDCA (Plan, Do, Check, Act) o en español PHVA (Planear, Hacer, Verificar, Actuar) el cual contribuye a la mejora continua en las instituciones con el fin de obtener la eficacia del sistema por medio de la ejecución de acciones preventivas y correctivas, así indica:

Es habitual entender que los sistemas de gestión deben ajustarse al llamado ciclo de Deming (PDCA), habitual en sistemas de gestión de la calidad:

P – Plan – Se establecen objetivos y se preparan planes para alcanzarlos. Esto incluye analizar la situación de la Organización: dónde estamos y dónde queremos estar.

D – Do – Se ejecutan los planes.

C – Check – Se evalúan los resultados obtenidos para determinar en qué medida se han alcanzado los objetivos propuestos.

A – Act – A fin de estar cada día mejor (mejora continua), se actualizan los planes y su implantación.

Figura 09. Ciclo PDCA

Fuente: Magerit v3 – libro 1 método, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

1.13.4. Riesgo

El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas.

Los factores que lo componen son la amenaza y la vulnerabilidad.

Análisis de riesgo

"Es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados.

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza". (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 22)

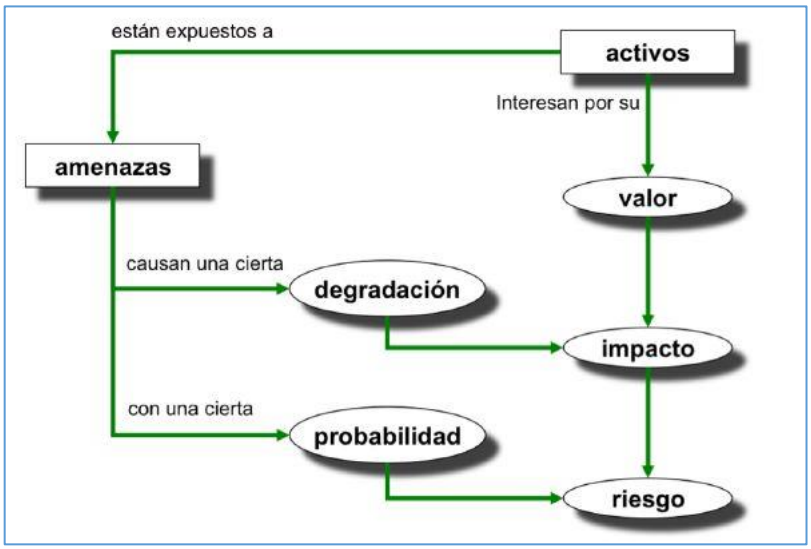


Figura 10. Elementos del análisis de los riesgos potenciales

Fuente: Magerit v3 – libro 1 método, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.

Paso 1: 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". (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 22)

Valoración

La valoración "se puede ver desde la perspectiva de la necesidad de proteger pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial". (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 24)

Dimensiones

Dimensiones de un activo

- **Confidencialidad:** Una propiedad que determina que la información no está disponible o divulgada a personas, organizaciones o procesos no autorizados.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo del activo de información.
- **Disponibilidad:** Una propiedad que determina que la información no está disponible o divulgada a personas, organizaciones o procesos no autorizados.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles).

Los criterios más importantes por respetar son:

- **La homogeneidad:** es importante poder comparar valores, aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra
- **La relatividad:** es importante poder relativizar el valor de un activo en comparación con otros activos.

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente “natural”.

El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

Amenaza

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 27)

Identificación de las amenazas

Presenta una relación de amenazas típicas.

- De origen natural
- Del entorno (de origen industrial)

- Defectos de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada

Determinación del impacto potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta

- Su valor acumulado (el propio más el acumulado de los activos que dependen de él)
- Las amenazas a que está expuesto

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta

- Su valor propio
- Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

Determinación del riesgo potencial

“Riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- Zona 1 – riesgos muy probables y de muy alto impacto
- Zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo
- Zona 3 – riesgos improbables y de bajo impacto
- Zona 4 – riesgos improbables, pero de muy alto impacto. “ (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 29)

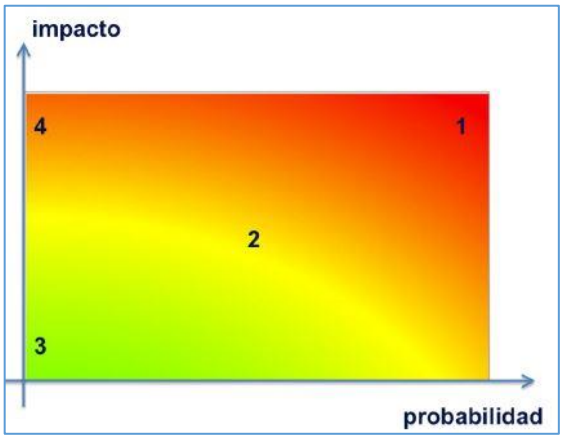


Figura 11. El riesgo en función del impacto y la probabilidad
Fuente: Magerit v3 – libro 1 método, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta

- El impacto acumulado sobre un activo debido a una amenaza y

- La probabilidad de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza. El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta

- El impacto repercutido sobre un activo debido a una amenaza
- La probabilidad de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Vulnerabilidades

"Es toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial" (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 35)

Evaluación: interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

Aceptación del riesgo

Al análisis de riesgos "debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión). (Dirección General de Modernización Administrativa, MAGERIT – versión 3.0., 2012, pág. 49)

Tratamiento del riesgo

El tratamiento del riesgo comprende tomar determinadas medidas para gestionar los riesgos que se puedan presentar en la seguridad de la información aplicando controles necesarios para protegerlas y de esta forma mitigar el riesgo. Así como indica:

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)

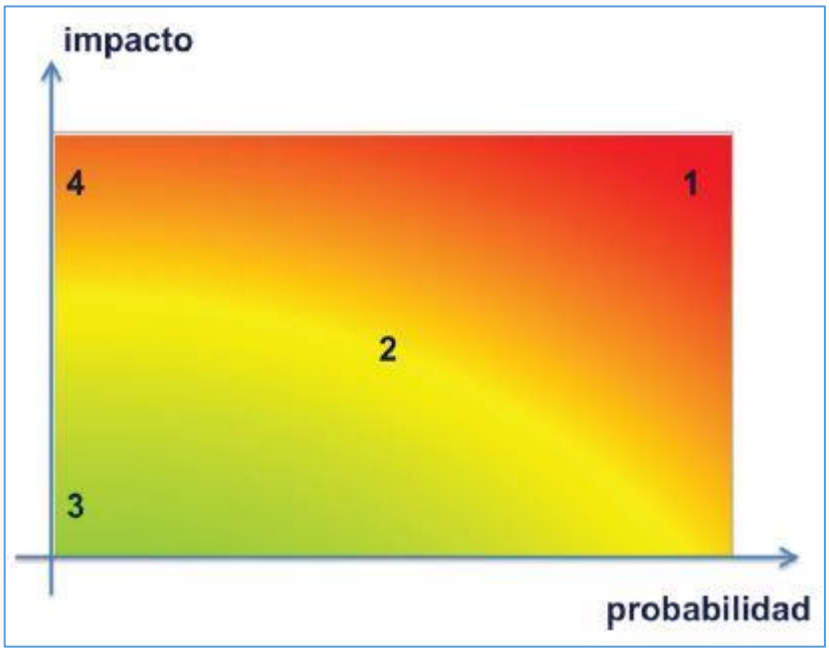


Figura 12. Zonas de riesgo

Fuente: Magerit v3 – libro 1 método, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.

En condiciones de riesgo residual medio, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la "norma". En términos de las zonas de riesgo que se expusieron anteriormente,

- Zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacar-los de esta zona
- Zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones
- Zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno

- Zona 4 – riesgos improbables, pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

1.9. Definición de términos básicos

1.9.1. 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" (Comité Técnico AEN/CTN 71 Tecnología de la Información, 2008).

1.9.2. Amenaza

"Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos" (Dirección General de Modernización Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.3. Ataque

"Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información" (Centro Superior de Información de la Defensa CESID, 1997).

1.9.4. Confidencialidad

"Característica que previene contra la divulgación no autorizada de activos del dominio" (Dirección General de Modernización Administrativa, Magerit -

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.5. Disponibilidad

"Característica que previene contra la denegación no autorizada de acceso a activos del dominio" (Dirección General de Modernización Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.6. Impacto

"Consecuencia que sobre un activo tiene la materialización de una amenaza." (Dirección General de Modernización Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.6. Integridad

"Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio" (Dirección General de Modernización Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.7. Riesgo

"Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización" (Dirección General de Modernización Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.8. Riesgo Residual

"Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real" (Dirección General de Modernización

Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.9. Seguridad de la información

"Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables" (Comité Técnico AEN/CTN 71 Tecnología de la Información, 2008).

1.9.10. Sistemas de Información

"Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información" (Dirección General de Modernización Administrativa, Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1, 1997).

1.9.11. 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. (Asociación Española de Normalización y Certificación, 2010)

II. METODO

2.1. Tipo y diseño de la investigación

Tipo de investigación

El tipo de investigación es básica

La investigación es de tipo básica. Según (Sánchez, Reyes, & Mejia, 2018) este tipo de investigación se centra en la búsqueda de nuevos conocimientos y campos de estudio que no tienen finalidad práctica, con el objetivo de crear nuevas teorías, orientadas a conocer y encontrar formas de resolver un problema.

Diseño de la investigación

El diseño de investigación es no experimental, puesto que no se manipula el SGSI.

"La investigación no experimental las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede

influir en ellas, porque ya sucedieron, al igual que sus efectos" (Hernández, Fernádez, & Baptista, 2014)

Nivel de la investigación

Para la presente tesis se aplica el nivel de investigación descriptiva.

"Tienen como objetivo indagar la incidencia de las modalidades o niveles de una o más variables en una población. El procedimiento consiste en ubicar en una o diversas variables a un grupo de personas, situaciones, etc., y proporcionar su descripción." (Hernández, Fernádez, & Baptista, 2014).

Nivel de Investigación Correlacional

"Este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto en particular." (Hernández, Fernádez, & Baptista, 2014)

Enfoque de la investigación

El enfoque cuantitativo es el aplicado en la presente investigación.

Representa, un conjunto de procesos es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar o eludir" pasos, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. (Hernández, Fernádez, & Baptista, 2014)

2.2. Población y muestra

- ✓ **Población**

La población está constituida por 30 funcionarios públicos que actúan como usuarios de los sistemas informáticos de CENARES.

Tabla 2.
Personal CENARES

N°	Oficina	N° de personas
1	Dirección general	1
2	Centro de adquisiciones y donaciones	12

3	Centro de gestión administrativa	14
4	Centro de almacén y distribución	8
5	Centro de programación	5
	Total	**30**

Fuente: Elaboración propia

✓ **Muestra**

(Hernández, Fernández, & Baptista, 2014). Mencionan que la muestra es en esencia un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a este conjunto definido en sus características al que se llama población (p. 175).

La selección de la muestra fue el total de la población constituida por los 30 funcionarios públicos.

2.3. Técnicas para la recolección de datos

✓ **Técnicas**

Las técnicas de recolección de datos son las distintas formas o maneras de obtener la información. Son ejemplos de técnicas; la encuesta en sus dos modalidades: oral o escrita (cuestionario), el análisis documental, análisis de contenido (Arias Odon, 2012).

Encuesta.

Se empleó la técnica de encuesta realizado al personal de CENARES conforme a la muestra en el cual se dispuso la conexión del sistema de gestión de seguridad de la información y la disminución de riesgos de perdida de información.

La encuesta “Se define la encuesta como una técnica que pretende obtener información que suministra un grupo o muestra de sujetos acerca de sí mismos, o en relación con un tema en particular”. (Arias Odon, 2012)

✓ **Instrumentos**

Los instrumentos “son los medios materiales que se emplean para recoger o almacenar la información. Ejemplo: fichas, formatos de cuestionario, guía de entrevista, lista de cotejo, escalas de actitudes u opinión, grabador, cámara fotográfica o de video, etc.” (Arias Odon, 2012)

Cuestionario.

El instrumento que se utilizó en la presente investigación para obtener resultados confiables y precisos fue el cuestionario.

El cuestionario “Es la modalidad de encuesta que se realiza de forma escrita mediante un instrumento o formato en papel contentivo de una serie de preguntas. Se le denomina cuestionario autoadministrado porque debe ser llenado por el encuestado, sin intervención del encuestador”. (Arias Odon, 2012)

2.4. Validez y confiabilidad de instrumentos

Validez del instrumento

La validación del contenido del instrumento se realizó mediante el Juicio de expertos, a profesionales con amplia trayectoria en asesoramiento de tesis y conocimiento de la temática de las variables de investigación.

Mg. Ing. Zarate Bocanegra Jhony Alex, Director de la escuela de posgrado – UPCI, obteniendo una calificación del 100% excelente, Magister en Gestión de Tecnología de la Información.

Mg. Ing. Corilla Baquerizo Eduardo Cancio, PMO en INEI, obteniendo una calificación del 85% excelente, Magister en Docencia e Investigación Universitaria.

Mg. Ing. Acosta Medina Lis Enrique, Gerente, en SYS4PERU SAC, obteniendo una calificación del 82% excelente, Ingeniero de Sistemas y magister en investigación y docencia.

Tabla 3.
Validez del instrumento – juicio de expertos

N°	Experto	Promedio
1	Mg. Ing. Zarate Bocanegra Jhony Alex	100%
2	Mg. Ing. Corilla Baquerizo Eduardo Cancio	85%
3	Mg. Ing. Acosta Medina Lis Enrique	82%
	Total	**89%**

Fuente: Elaboración propia

Criterio de confiabilidad de instrumento

La confiabilidad de la Encuesta será medida usando el coeficiente Alpha de Cronbach

$$\alpha = \frac{k}{(k-1)}\left(1 - \frac{\sum \sigma_i^2}{\sigma_X^2}\right)$$

Donde

K, es el número de ítems = 21

$(\sigma_i)^2$, varianza de cada ítem = 12.52667

$(\sigma_x)^2$, varianza del cuestionario total = 66.13333

Según lo mencionado por (Ñaupas, Mejia, Novoa, & Villagomez, 2014, pág 217) se dice que un instrumento es fiable cuando las mediciones no varían significativamente ni en tiempo ni en aplicación a diferentes personas. La confiabilidad es la prueba que genera confianza cuando, al aplicarse en condiciones iguales o similares los resultados son siempre los mismos.

Se sugieren los siguientes criterios para evaluar los coeficientes de alfa de Cronbach:

- Coeficiente alfa > 0.9 es excelente
- Coeficiente alfa > 0.8 es bueno
- Coeficiente alfa > 0.7 es aceptable
- Coeficiente alfa > 0.6 es cuestionable
- Coeficiente alfa > 0.5 es pobre
- Coeficiente alfa < 0.5 es inaceptable

El resultado de confiabilidad es bueno obteniendo da fue de 0.851, mayor a 0.7 que es lo mínimo aceptable. Dicho resultado demuestra que las preguntas realizadas con confiables para el estudio.

Tabla 4.
Resultado coeficiente Alpha de Cronbach

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,851	21

Fuente: Elaboración propia

2.5. Procesamiento y análisis de datos

La técnica de procesamiento y análisis de datos que se lograron son procesados en hoja de cálculo Excel, se realizó el análisis descriptivo, prueba de normalidad y contrastación de hipótesis haciendo uso del software SPSS, en el cual se buscó la relación entre el diseño del sistema de gestión de seguridad de la información y la disminución de riesgos de perdida de información.

2.6. Aspectos éticos

El trabajo de investigación se dio en el marco con lo dispuesto en el Reglamento de Grado de Bachiller y Título Profesional de la Universidad Peruana de Ciencias e Informática, aprobado por Resolución N° 373-2019-UPCI-R y cumpliendo con lo establecido en el artículo N° 45 de ley N° 30220 que indica “la obtención de grados y títulos se realiza de acuerdo con las exigencias académicas que cada universidad establezca”.

III. RESULTADOS

3.1. Resultados descriptivos

Tabla 5.
Nivel de frecuencia del sistema de gestión de seguridad de la información

Sistema de gestión de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	29	96,7	96,7	96,7
	Regular	1	3,3	3,3	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

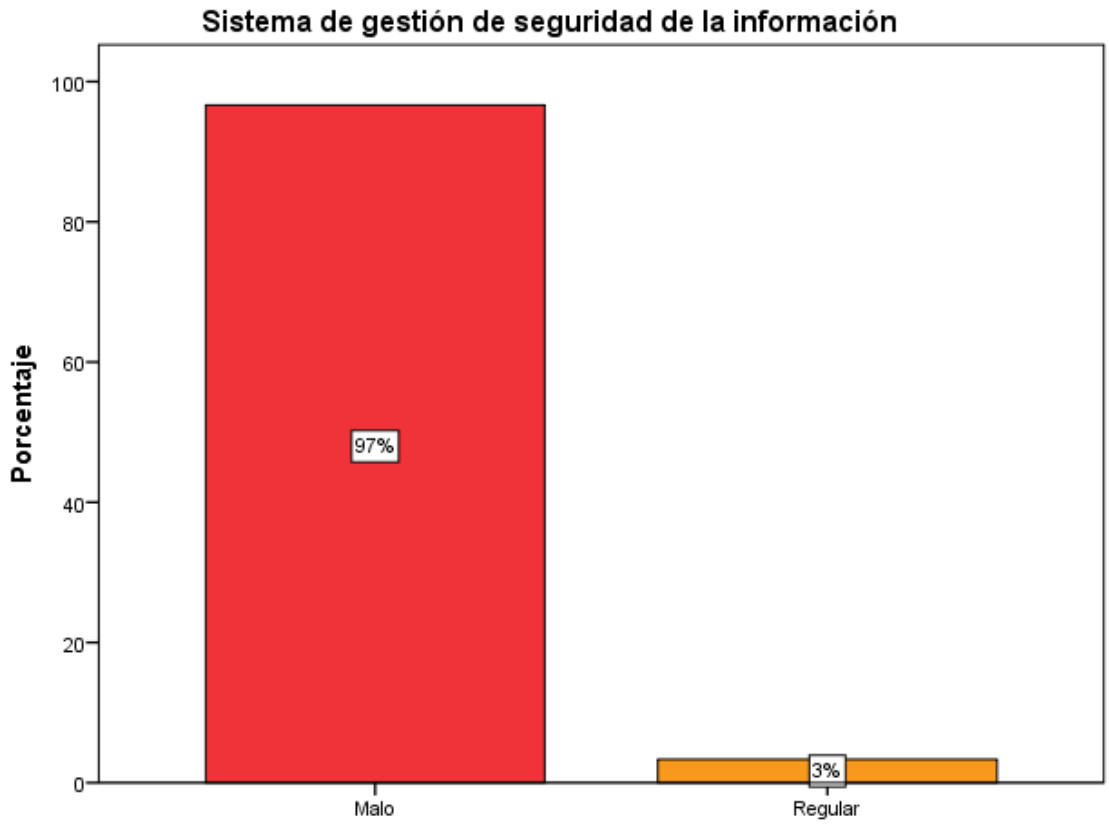


Figura 13: Nivel de frecuencia del sistema de gestión de seguridad de la información
Fuente: elaboración propia.

Interpretación: Observamos que del total de encuestados respondieron que el 97% Malo, y el 3% Regular, el nivel sistema de gestión de seguridad de la información.

Tabla 6.
Nivel de frecuencia política de seguridad de la información

Política de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	27	90,0	90,0	90,0
	Regular	3	10,0	10,0	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

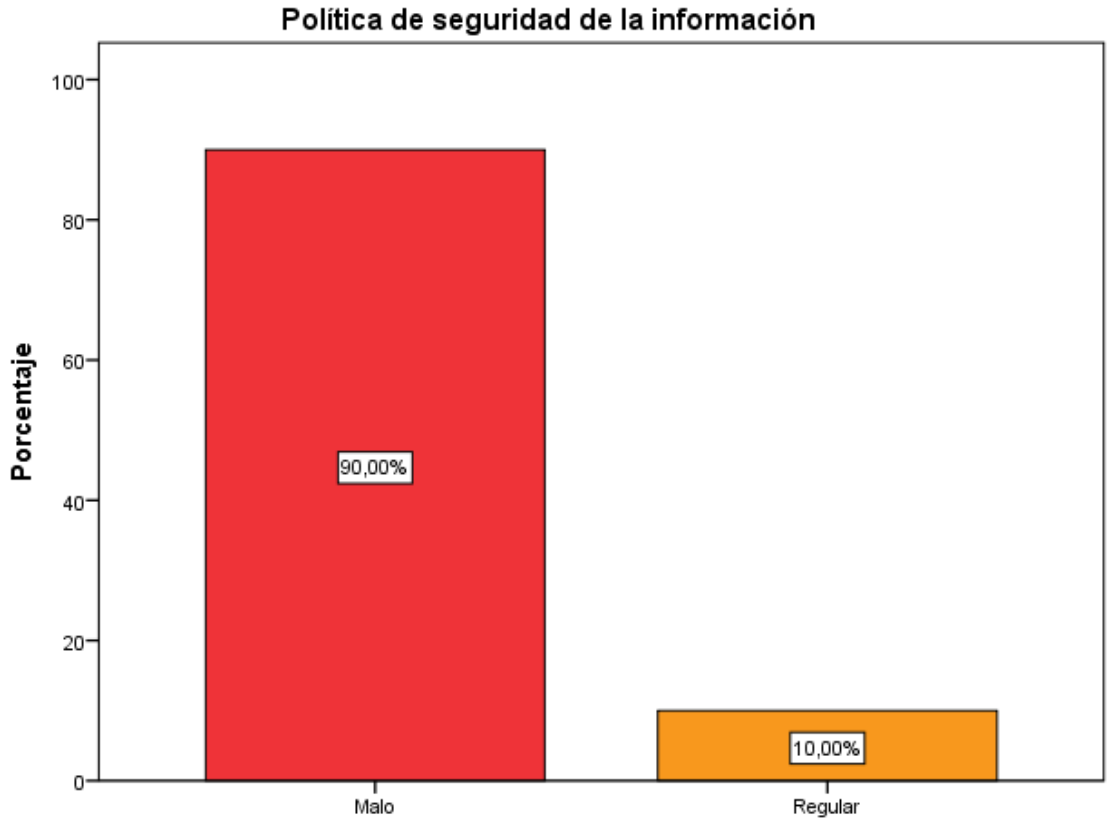


Figura 14. Nivel de frecuencia política de seguridad de la información
Fuente: elaboración propia

Interpretación: Observamos que del total de encuestados respondieron que el 90% Malo, y el 10% Regular, el nivel de la política de seguridad de la información.

.

Tabla 7.
Nivel de frecuencia plan de seguridad de la información

Plan de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	13	43,3	43,3	43,3
	Regular	17	56,7	56,7	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

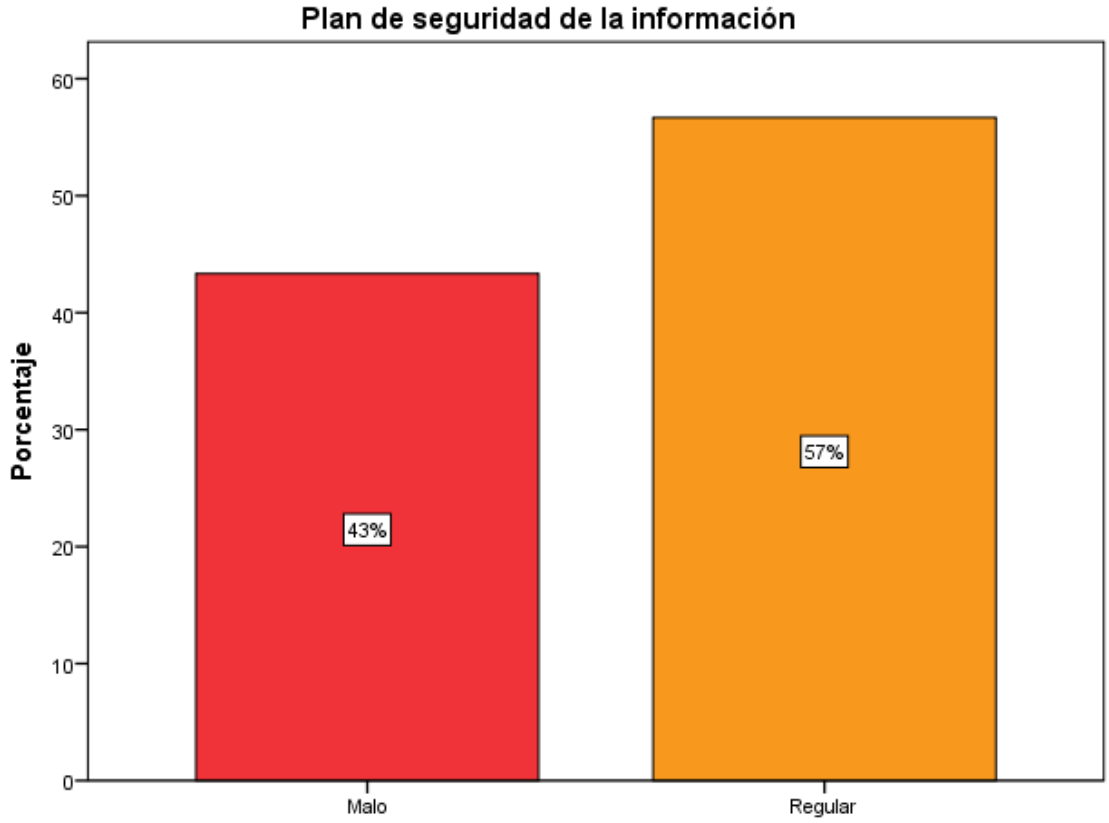


Figura 15. Nivel de frecuencia plan de seguridad de la información
Fuente: Elaboración propia

Interpretación: Observamos que del total de encuestados respondieron que el 43% Malo, y el 57% Regular, el nivel del plan de seguridad de la información.

Tabla 8.
Nivel de frecuencia de seguridad de la información

Seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	30	100,0	100,0	100,0

Fuente: Elaboración propia

Grafico

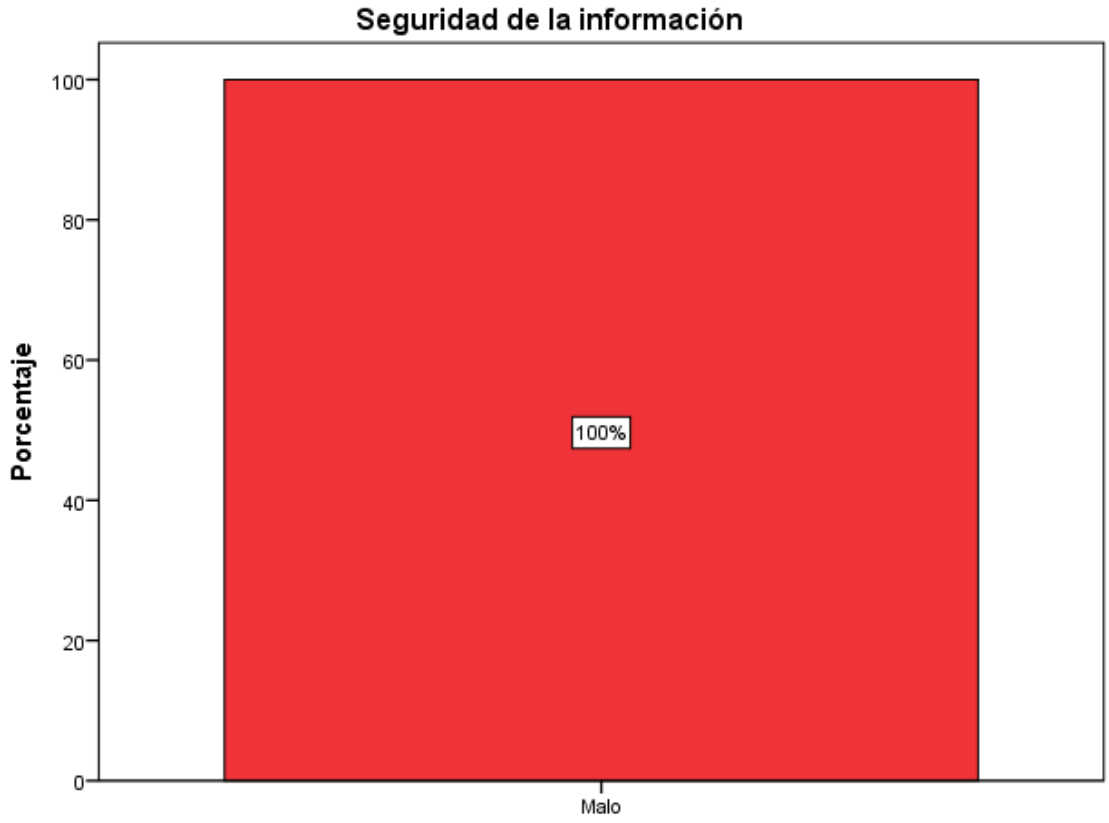


Figura 16. *Nivel de frecuencia de seguridad de la información*
Fuente: Elaboración propia

Interpretación: Observamos que del total de encuestados respondieron que el 100% Malo, el nivel de seguridad de la información.

Tabla 9.
Nivel de frecuencia de riesgos de pérdida de información

Riesgos de pérdida de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	27	90,0	90,0	90,0
	Regular	3	10,0	10,0	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

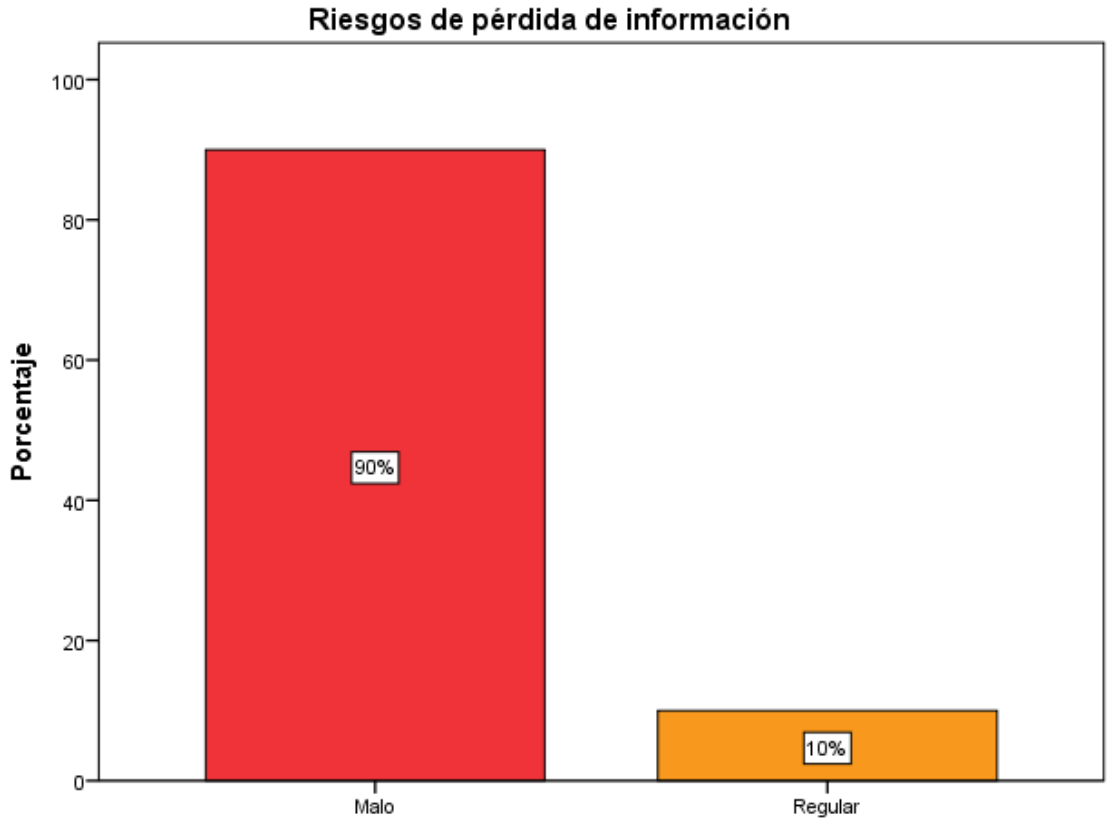


Figura 17. *Nivel de frecuencia de riesgos de pérdida de información*
Fuente: Elaboración propia

Interpretación: Observamos que del total de encuestados respondieron que el 90% Malo y el 10% Regular, el nivel de riesgos de pérdida de información.

Tabla 10.
Nivel de frecuencia de riesgo de confidencialidad de información

Riesgo de confidencialidad de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	29	96,7	96,7	96,7
	Regular	1	3,3	3,3	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

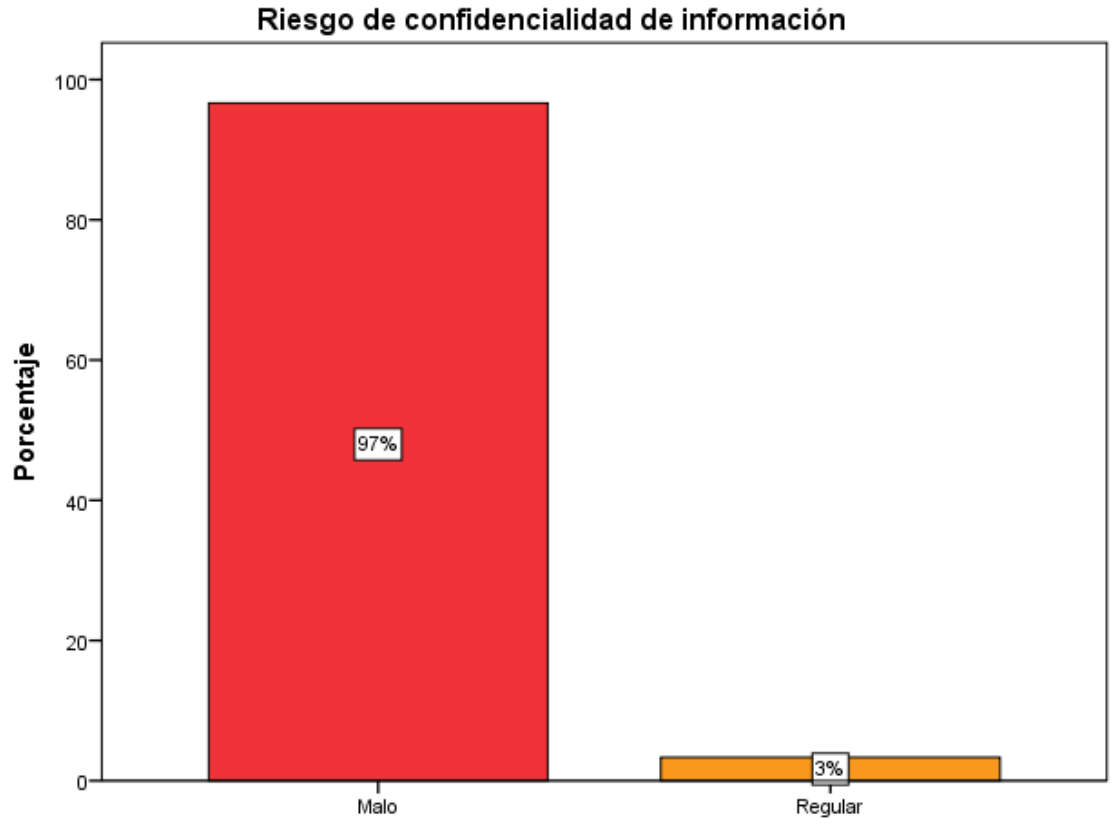


Figura 18. *Nivel de frecuencia de riesgo de confidencialidad de información*

Fuente: Elaboración propia

Interpretación: Observamos que del total de encuestados respondieron que el 97% Malo y el 3% Regular, el nivel de riesgo de confidencialidad de información.

Tabla 11.
Nivel de frecuencia de riesgo de integridad de información

Riesgo de integridad de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	28	93,3	93,3	93,3
	Regular	2	6,7	6,7	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

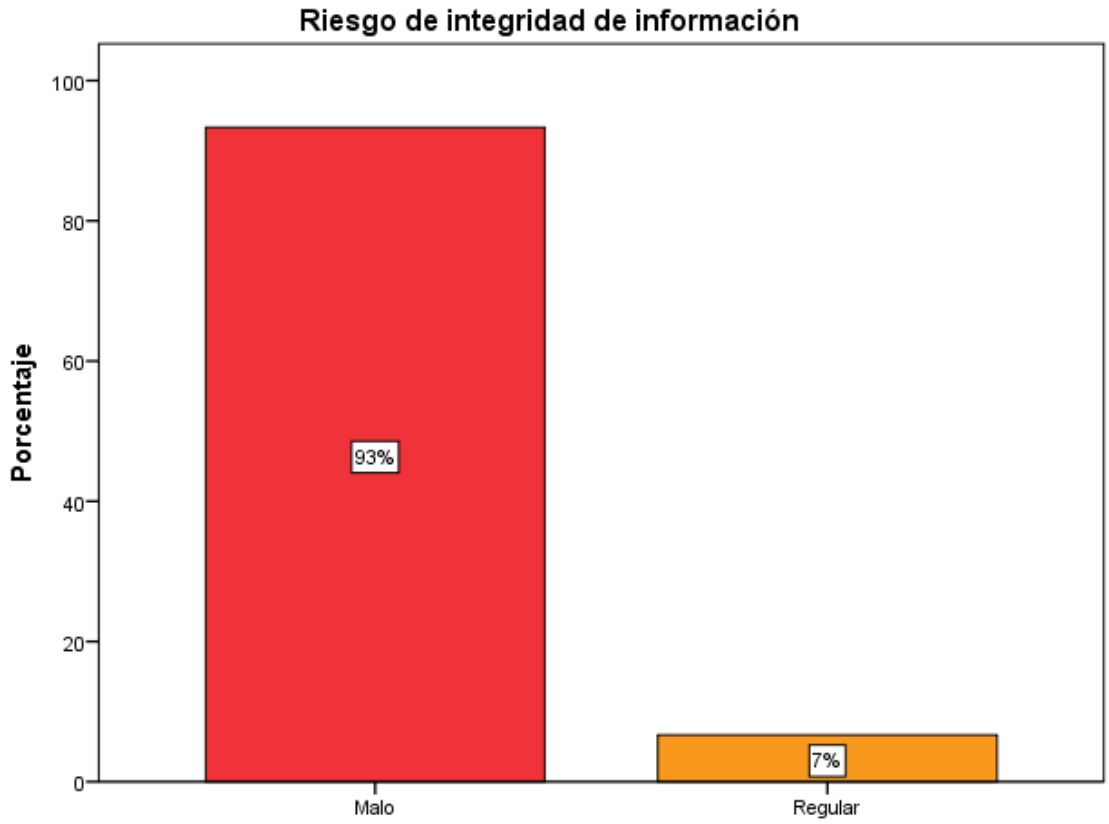


Figura 19. Nivel de frecuencia de riesgo de integridad de información
Fuente: Elaboración propia

Interpretación: Observamos que del total de encuestados respondieron que el 93% Malo y el 7% Regular, el nivel de riesgo de integridad de información.

Tabla 1.
Nivel de frecuencia del riesgo de disponibilidad de información

Riesgo de disponibilidad de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	24	80,0	80,0	80,0
	Regular	6	20,0	20,0	100,0
	Total	30	100,0	100,0	

Fuente: Elaboración propia

Grafico

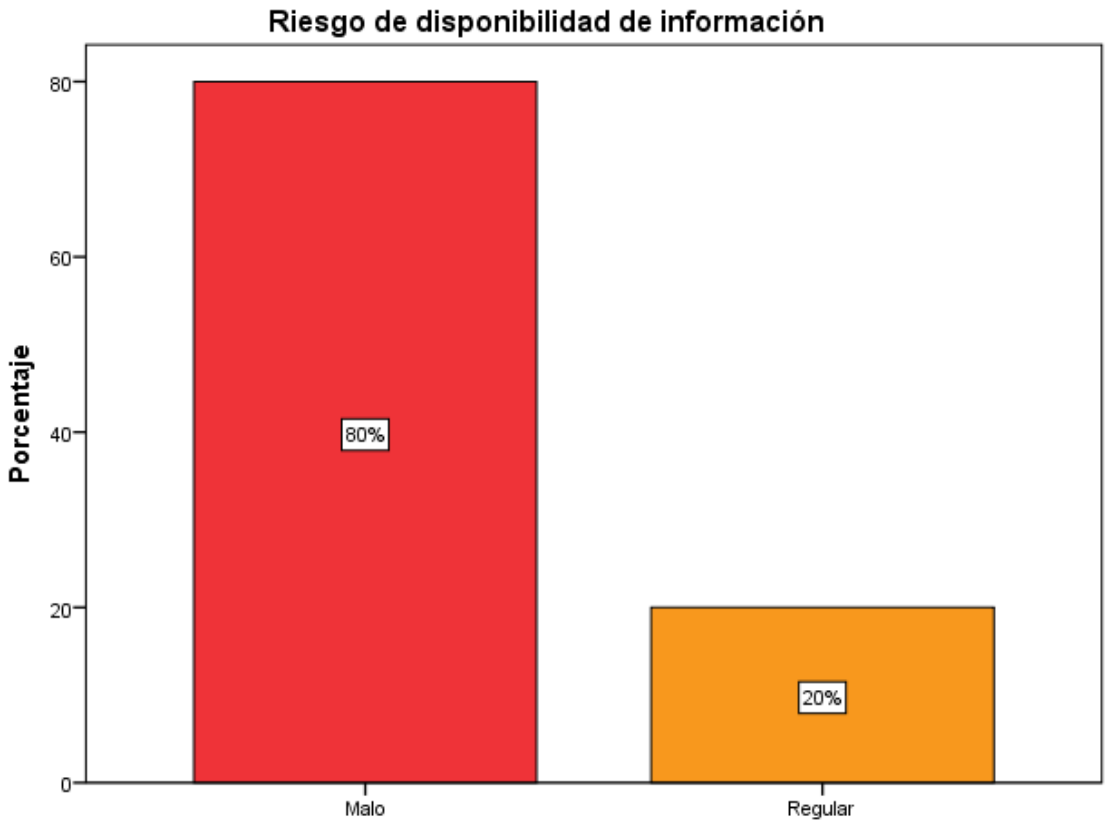


Figura 1. Nivel de frecuencia del riesgo de disponibilidad de información

Fuente: Elaboración propia

Interpretación: observamos que del total de encuestados respondieron que el 80% Malo y el 20% Regular, el nivel del riesgo de disponibilidad de información

3.2. Prueba de normalidad

Se efectuó la prueba de normalidad con el método estadístico de Shapiro-Wilk para determinar cuál es el comportamiento de las variables ya que la muestra es de 30 y debido a que la muestra es menor a 50.

Tabla 13.
Prueba de normalidad

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
V1_SGSI	,109	30	,200*	,977	30	,733
V2_RIESGOS_PI	,137	30	,156	,896	30	,007

Fuente: Elaboración propia

Se puede observar, que para la variable Sistema de gestión de seguridad de la información la significancia es de 0.733, como P= 0.733>0.05 entonces se acepta la H0 por lo tanto los datos provienen de una distribución normal.

Para la variable Riesgos de pérdida de información la significancia es de 0.007, como P= 0.007<0.05 entonces se rechaza H0 y se acepta la hipótesis alterna H1 por lo tanto los datos no provienen de una distribución normal.

3.3. Contrastación de las hipótesis

Para la validación de las hipótesis de estudio de la presente tesis se utilizó el coeficiente de correlación de Pearson para establecer el nivel de relación de las dos variables de investigación.

Contrastación de las hipótesis General

H0: Si no existe relación con el sistema de gestión de seguridad de la información, entonces no disminuye el riesgo de pérdida de información en CENARES.

H1: Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye el riesgo de pérdida de información en CENARES.

Tabla 14.
Contrastación de las hipótesis General

Correlaciones

		V1_SGSI	V2_RIESGOS_PI
V1_SGSI	Correlación de Pearson	1	,729**
	Sig. (bilateral)		,000
	N	30	30
V2_RIESGOS_PI	Correlación de Pearson	,729**	1
	Sig. (bilateral)	,000	
	N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia

Datos:
V1_SGSI: Sistema de gestión de seguridad de la información
V2_RIESGOS_PI: Riesgos de pérdida de información.

Interpretación

Observando los resultados la correlación es alta igual a 0.729 y la significancia bilateral es 0.000<0.05, se rechaza la hipótesis nula y aceptamos la hipótesis alternativa, en consecuencia, Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye el riesgo de pérdida de información en CENARES, existiendo una correlación directamente proporcional.

Contrastación de las hipótesis especifica 1

H0: Si no existe relación con el sistema de gestión de seguridad de la información, entonces no disminuye los riesgos de confidencialidad de la información.

H1: Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de confidencialidad de la información.

Tabla 15.
Contrastación de las hipótesis especifica 1

Correlaciones

		V1D1	V2D1
V1D1	Correlación de Pearson	1	,690**
	Sig. (bilateral)		,000
	N	30	30
V2D1	Correlación de Pearson	,690**	1
	Sig. (bilateral)	,000	
	N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).
Fuente: Elaboración propia

Datos:

V1D1: Política de seguridad de la información

V2D1: Riesgo de confidencialidad de información

Interpretación

Observando los resultados, la correlación es alta igual a 0.690 y la significancia bilateral es 0.000<0.05, se rechaza la hipótesis nula y aceptamos la hipótesis alternativa, en consecuencia, Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de confidencialidad de la información, siendo una correlación directamente proporcional.

Contrastación de las hipótesis especifica 2

H0: Si no existe relación con el sistema de gestión de seguridad de la información, entonces no disminuye los riesgos de integridad de la información.

H1: Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de integridad de la información.

Tabla 16.
Contrastación de las hipótesis especifica 2

Correlaciones

		V1D2	V2D2
V1D2	Correlación de Pearson	1	,590**
	Sig. (bilateral)		,000
	N	30	30
V2D2	Correlación de Pearson	,590**	1
	Sig. (bilateral)	,000	
	N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral)

Fuente: Elaboración propia

Datos:

V1D2: Plan de seguridad de la información

V2D2: Riesgo de integridad de información

Interpretación

Observando los resultados, la correlación es moderada igual a 0.590 y la significancia bilateral es 0.000<0.05, se rechaza la hipótesis nula y aceptamos la hipótesis alternativa, en consecuencia, Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de integridad de la información, existiendo una correlación directamente proporcional.

Contrastación de las hipótesis especifica 3

H0: Si no existe relación con el sistema de gestión de seguridad de la información, entonces no disminuye los riesgos de disponibilidad de la información

H1: Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de disponibilidad de la información.

Tabla 17.
Contrastación de las hipótesis especifica 3

Correlaciones

		V1D3	V2D3
V1D3	Correlación de Pearson	1	,593**
	Sig. (bilateral)		,001
	N	30	30
V2D3	Correlación de Pearson	,593**	1
	Sig. (bilateral)	,001	
	N	30	30

**. La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia

Datos:

V1D2: Seguridad de la información

V2D2: Riesgo de disponibilidad de información

Interpretación

Observando los resultados, la correlación es moderada igual a 0.593 y la significancia bilateral es 0.001<0.05, se rechaza la hipótesis nula y aceptamos la hipótesis alternativa, en consecuencia. Si existe relación con el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de disponibilidad de la información, existiendo una correlación directamente proporcional.

IV. DISCUSION

El objetivo de la presente investigación fue: “Determinar la relación entre el sistema de gestión de seguridad de la información y la disminución de riesgos de perdida de información en CENARES” obteniendo el resultado de la correlación fue alta igual a 0.729 y la significancia bilateral es 0.000<0.05, se rechaza la hipótesis nula y aceptamos la hipótesis alternativa, en consecuencia, Si existe relación entre el sistema de gestión de seguridad de la información, entonces disminuye el riesgo de pérdida de información en CENARES, existiendo una correlación directamente proporcional. De acuerdo con el trabajo de investigación presentado por (Flores, 2018), La presente tesis describe la necesidad de diseñar un sistema de gestión de seguridad de la información en una institución con los objetivos específicos de:

- Identificar y valorar los activos de información asociados a los procesos de negocios establecidos como alcance del SGSI
- Identificar, analizar y evaluar los riesgos a los que está expuesto los activos de mayor valor para la entidad.
- Seleccionar los controles que permitan gestionar y tratar los riesgos identificados.

Con ello se busca generar una herramienta que permita mejorar la seguridad en los activos de información y de esta manera poder mitigar el riesgo que pueda suscitar en el uso de ella en cuanto a la confiabilidad, integridad y disponibilidad.

En cuanto a la metodología se adopta el ciclo de Deming, conocida por las siglas en ingles PDCA (planear, hacer, verificar y actuar) el cual aplica a todos los procesos del SGSI.

Asimismo, del trabajo de investigación presentado por (Barrantes Porras & Hugo Herrera, 2022), La presente tesis tuvo el propósito de implementar un sistema de gestión de seguridad de la información (SGSI) tomando como referencia las normas ISO 27001:2018 teniendo como objetivos específicos:

- Implementar una política de Seguridad de información que sea desplegada a todos los colaboradores, proveedores y terceros involucrados en los procesos de tecnología.
- Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de la información, para reducirlos en un 80%.
- Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos, para reducirlos en un 90% de los riesgos a niveles aceptables.
- Formación y concientización al 100% de los colaboradores involucrados en los procesos de tecnología, en temas de seguridad de la información.
- Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras.
- Gestionar y controlar el 100% de los documentos de SGSI.

Una de las metodologías aplicadas en la presente tesis es la de Análisis y gestión de riesgo de los sistemas de información (MAGERIT) el cual se tomará como referencia para el desarrollo de la presente investigación.

Esta investigación permitió ampliar los conocimientos en el uso de metodologías y establecer el desarrollo del modelo PDCA, ciclo de Deming así como definir y establecer el análisis de riesgos y control de activos.

Ambos investigadores coinciden con nuestro objetivo.

CONCLUSIONES

1.- De los resultados obtenidos podemos concluir que existe una correlación alta en consecuencia, Si existe relación entre el sistema de gestión de seguridad de la información y la disminución del riesgo de pérdida de información en CENARES, existiendo una correlación directamente proporcional, por lo que se tiene que actualizar la política de seguridad de la información con el fin de garantizar la seguridad de los sistemas y minimizar el riesgo a niveles aceptables para la institución.

2.- Podemos concluir que existe una correlación alta en consecuencia, Si existe relación entre el sistema de gestión de seguridad de la información y la disminución de los riesgos de confidencialidad de la información existiendo una correlación directamente proporcional.

3.- Se concluye que existe una correlación moderada en consecuencia, Si existe relación entre el sistema de gestión de seguridad de la información y la disminución de los riesgos de integridad de la información, existiendo una correlación directamente proporcional.

4.- Podemos concluir que existe una correlación moderada en consecuencia, Si existe relación entre el sistema de gestión de seguridad de la información y la disminución de los riesgos de disponibilidad de la información, existiendo una correlación directamente proporcional.

V. RECOMENDACIONES

1.- Recomendar el mantenimiento del sistema de gestión de seguridad de la información, para lograr disminuir los riesgos de perdida de información en CENARES. Coordinar con los directivos de la institución para que se asigne el presupuesto correspondiente para mantener vigente el sistema de gestión de seguridad de la información y continuar disminuyendo los riesgos de perdida de información en CENARES.

2.- se recomienda continuar con una metodología para gestionar los riesgos y de esta manera tomar medidas de prevención para reducir su impacto.

3.- Recomendar la actualización periódica del sistema de gestión de seguridad de la información, para disminuir los riesgos de confidencialidad de la información en CENARES manteniendo una revisión continua de la política del SGSI y verificar el cumplimiento por parte de los trabajadores de la institución

4.- Recomendar un monitoreo y seguimiento del sistema de gestión de seguridad de la información, para disminuir los riesgos de integridad de la información en CENARES. Adoptando medidas correctivas para que de esta manera se asegure la integridad de la información que se almacena en los servidores de la institución.

5.- Recomendar la evaluación periódica del sistema de gestión de seguridad de la información en el proceso de disminuir los riesgos de disponibilidad de información en CENARES.

VII. REFERENCIAS BIBLIOGRÁFICAS

aguilar, a. s. (2004). *capacitacion y desarrollo del personal.* mexico DF, MEXICO: LIMUSA, S.A.

Arias Odon, F. G. (2012). *El Proyecto de Investigación - Introducción a la metodología científica.* Caracas: Editorial Episteme.

Asociación Española de Normalización y Certificación. (2010). *Gestión del riesgo.* Madid: Asociación Española de Normalización y Certificación.

Barrantes Porras, C. E., & Hugo Herrera, J. R. (2022). *Diseño e Implementación de un sistema de gestión de seguridad de la información en procesos tecnológicos (Tesis de Pregrado).* Universidad de San Martin de Porres, Lima.

Centro Superior de Información de la Defensa CESID. (1997). *Glosario de Términos de Criptología.* Madrid: Ministe-rio de Defensa 3° Edicion.

Comité Técnico AEN/CTN 71 Tecnología de la Información. (2008). *Metodología de análisis y gestión de riesgos para los sistemas de información.* Asociación Española de Normalización y Certificación. Madrid: AEONOR.

CONCYTEC. (2016). *I Censo Nacional de Investigación y Desarrollo a Centros de Investigación.* (T. e. Consejo Nacional de Ciencia, Ed.) Recuperado el 20 de Febrero de 2020, de https://portal.concytec.gob.pe/images/publicaciones/censo_2016/libro_censo_nacional.pdf

Dirección General de Modernización Administrativa, P. e. (1997). *Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Version 1.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0.* Madrid: administración electrónica.

Elizabeth, T. F. (2015). Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría aplicando la norma ISO/IEC 27001. *(Tesis para optar el título de Licenciado en sistema de información).* Escuela Superior Politécnica del litoral., Guayaquil, Ecuador. Obtenido de http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/30314/D-84631.pdf?sequence=-1&isAllowed=y

Falcon, F. J. (2021). Propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información Basado en a Norma ISO 27001 Para una Empresa de Telecomunicaciones, 2021. *Para optar el Título Profesional de Ingeniero de Sistemas.* Universidad Nacional José Faustino Sánchez Carrión, Lima - Huacho.

Fernanda, N. (2014). *Plan de gestión de riesgo para MADECO CIA LTDA (Tesis de Pregrado).* Universidad del Azuay, Cuenca – Ecuador. Obtenido de http://dspace.uazuay.edu.ec/bitstream/datos/3585/1/10269.pdf

Flores, L. C. (2013). *Diseño de un Sistema de Gestión de seguridad de información para un instituto educativo (Tesis de Pregrado).* Centro de Estudios: Pontificia Universidad Católica del Perú, Lima.

Francisco, G. P. (2018). *Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica ortega (Tesis de Maestria).* Universidad Nacional del Centro del Perú, Huancayo.

Garcia, C. R. (2020). Propuesta de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001 Para la Oficina de Tecnologías de Información del Gobierno Regional Piura; 2020. *Para optar el título profesional de Ingeniero de Sistemas.* Universidad Católica los Ángeles de Chimbote, Piura - Perú.

Hernández, R., Fernández, C., & Baptista, M. d. (2014). *Metodología de la investigación.* Mexico: Mc-Graw Hill/Interamericana Editores.

Hernández, S. R., Fernádez, C. C., & Baptista, L. P. (12 de 09 de 2014). *Metodología de la investigación* (sexta ed.). (M. G. S.A., Ed.) Mexico, Mexico: McGraw Hill.

Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). *Metodologìa de la Investigación.* Colombia: Ediciones de la U.

Perafan Ruiz, J. J., & Caicedo Cuchimba, M. (2014). *Análisis de Riesgos de la seguridad de la información para la Institución Universitaria Colegio Mayor del Cauca (Tesis de Pregrado).* Centro de Estudios: Universidad Nacional Abierta y a distancia UNAD, Popayán - Colombia. Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

Rainer, D. (2021). Assessing the Information Security Status of an Organization from a Management Perspective. *Para obtener un título académico de Doctor en ciencias.* Technische Universität München, Miunich - Alemania.

Ruiz, P. J. (2018). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) Bajo la Norma ISO/IEC 27001:2013, en la Cooperativa Multiactiva del Personal del SENA, en Bogotá. *Para obtener el Título de Especialista en Seguridad Informática.* Universidad Nacional Abierta y a Distancia UNAD, Bogotá - Colombia.

Sabino, C. (1996). *El proceso de investigación.* Caracas: Editorial Panapo.

Sampieri, R. H. (2014). *Metodologia de la investigacion sexta edicion.* Mexico D.F: INTERAMERICANA EDITORES, S.A. DE C.V.

Sánchez, C. H., Reyes, R. c., & Mejia, S. K. (2018). *Manual de ternminos de investigacion cientifica, tecnlógica y humanística.* Lima: Universidad Ricardo Palma.

Silva, G. A. (2022). "Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021". *Para optar el Título Profesional de Ingeniero de Sistemas e Informática.* Universidad Tecnológica del Perú, Lima – Peru.

Suarez, S. L. (16 de 10 de 2016). *Sistema de Gestión de la Seguridad de la Información (SGSI).* Obtenido de https://es.scribd.com/document/202912531/Modulo-SGSI-233003

Vieites, A. G. (2014). *Enciclopedia de la seguridad informatica 2da edicion actualizada.* Madrid, España: RA-MA .

YiJie, C. K. (2021). A Systematic Approach for Cybersecurity Risk Management. *Para obtener el Master of Science in Engineering and Management.* Universidad Nacional Chengchi, Taipei - Taiwan.

ANEXOS

Anexo 1: Matriz de Consistencia

Tabla 18:
Matriz de Consistencia

Problemas General	Objetivos General	Hipótesis General	Variables Independiente	Indicador V.I.	Variables Dependiente	Indicador V.D.
¿De qué manera el sistema de gestión de seguridad de la información disminuirá riesgos de perdida de información en CENARES?	Determinar la relación entre el sistema de gestión de seguridad de la información y la disminución de riesgos de perdida de información en CENARES.	Si existe relación entre el sistema de gestión de seguridad de la información, entonces disminuye el riesgo de pérdida de información en CENARES.	*Sistema de gestión de seguridad de la información*	--.--	*Riesgos de pérdida de información.*	--.--
Problemas Especifico	**Objetivos Específicos**	**Hipótesis Especificas**				
¿En qué medida el sistema de gestión de seguridad de la información disminuirá riesgos de confidencialidad de la información?	Determinar la relación entre el sistema de seguridad de la información y la disminución de riesgos de confidencialidad de la información.	Si existe relación entre el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de confidencialidad de la información.	Política de seguridad de la información	Nivel de cumplimiento de las políticas	Riesgo de confidencialidad de información	Nivel de incidentes en la confidencialidad de activos de información
¿En qué medida el sistema de gestión de seguridad de la información disminuirá riesgos de integridad de la información?	Determinar la relación entre el sistema de seguridad de la información y la disminución de riesgos de integridad de la información.	Si existe relación entre el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de integridad de la información.	Plan de seguridad de la información	% de implementación del plan	Riesgo de integridad de información	Nivel de incidentes en la integridad de activos de información
¿En qué medida el sistema de gestión de seguridad de la información disminuirá riesgos de disponibilidad de la información?	Determinar la relación entre el sistema de seguridad de la información y disminución de los riesgos de disponibilidad de la información.	Si existe relación entre el sistema de gestión de seguridad de la información, entonces disminuye los riesgos de disponibilidad de la información.	Seguridad de la información	Brechas de seguridad de la información	Riesgo de disponibilidad de información	Nivel de incidentes en la disponibilidad de activos de información

Elaboración propia

Anexo 2: Instrumento de recolección de datos

ENCUESTA	CÓDIGO	FOR -- 001
	VERSIÓN	01

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA DISMINUIR RIESGOS DE PERDIDA DE INFORMACION EN CENARES AÑO 2022

GENERALIDADDES: la presente información será utilizada en forma confidencial y anónima, por lo que se agradece proporcionar información veraz para el logro del objetivo

USUARIO: La presente encuesta está dirigida al personal de la institución CENARES
Edad: _____ **Sexo:** _____

OBJETIVO: Determinar la relación entre el sistema de gestión de seguridad de la información y la disminución de riesgos de perdida de información en CENARES.

PREGUNTAS

En función a las preguntas detalladas; se recomienda marcar con una "X" su respuesta, Donde:

ESCALA VALORATIVA

INTERVALO	PUNTUACION
Nunca	1
A Veces	2
Siempre	3

	PREGUNTAS	1	2	3
V1: SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION				
D1: Políticas de seguridad de la información				
1	¿Se ha establecido una política integral de seguridad de la información en CENARES?			
2	¿Existe controles de seguridad de la información para disminuir el riesgo de pérdida de información?			
3	¿Ud. Cree que actualmente la seguridad de información del CENARES se encuentra en riesgo?			
4	¿Existe algún control que impida el acceso al personal no autorizado a áreas restringidas?			
D2: Plan de seguridad de la información				
5	¿La seguridad física de los activos de información se encuentran vulnerables en CENARES?			
6	¿La seguridad lógica de los activos de información está expuesta a vulnerabilidades que tienen los sistemas informáticos de CENARES?			
7	¿La seguridad digital de los activos de información está expuesta a vulnerabilidades que tienen los sistemas informáticos de CENARES?			
8	¿Existe un plan de tratamiento de riesgos de la información?			

D3: Seguridad de la información				
9	¿Existe en CENARES un sistema de gestión de seguridad de la información que disminuya el riesgo de pérdida de información?			
10	¿Realizas copia de seguridad de la información que realizas?			
11	¿Existen controles para proteger los activos de información?			
12	¿Se realiza mantenimiento preventivo a los equipos de cómputo (hardware y software)?			
V2: RIESGOS DE PÉRDIDA DE INFORMACIÓN				
D1: Riesgo de confidencialidad de información				
1	¿El sistema de información en CENARES cumple con garantizar la confidencialidad de la información almacenados en medios físicos o digitales?			
2	¿Las contraseñas utilizadas tienen al menos 8 dígitos entre números letras?			
3	¿En CENARES existe control para la protección confidencial de datos personales?			
D2: Riesgo de integridad de información				
4	¿La integridad de la información se encuentra segura en la institución?			
5	¿En su oficina han evaluado los riesgos a los que está expuesta la integridad de la información de la institución?			
6	¿Su área de trabajo se encuentra protegida contra amenazas externas o condiciones ambientales que alteren la integridad de la información?			
D3: Riesgo de disponibilidad de información				
7	¿Existe un plan de contingencia en CENARES para mantener la disponibilidad de la información ante algún evento o interrupción no autorizado?			
8	¿Ha tenido dificultades para acceder a los sistemas informáticos?			
9	¿Ha sufrido perdida de información valiosa para la institución?			

¡MUCHAS GRACIAS POR SU COLABORACION!

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "sistema de gestión de seguridad de la información para disminuir riesgos de perdida de información en cenares año 2022"

PRESENTADO POR (Tesista): Bach. Hoces Roman Santiago Juan

I. DATOS GENERALES DEL EXPERTO N°: 1

1.1. Apellidos y Nombres : Zarate Bocanegra, Jhony Alex

1.2. Grado Académico : Magister en Gestión de Tecnologías de la Información

1.3. Cargo e Institución donde Labora: Director de la Escuela de Posgrado - UPCI

1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACION	Existe organización Lógica					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					X
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología					X
8. COHERENCIA	Entre índices, indicadores y dimensiones					X
9. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCION DE APLICABILIDAD : Excelente

III. PROMEDIO DE VALORACIÓN : 100%

IV. RECOMENDACIÓNES : Se puede aplicar el instrumento

Firma del experto:

Fecha: 07/11/2022

DNI : 09623461

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "sistema de gestión de seguridad de la información para disminuir riesgos de perdida de información en cenares año 2022"

PRESENTADO POR (Tesista): Bach. Hoces Roman Santiago Juan

I. DATOS GENERALES DEL EXPERTO N°: 2

1.1. Apellidos y Nombres : Corilla Baquerizo, Eduardo Cancio

1.2. Grado Académico : Magister en Docencia e Investigación Universitaria

1.3. Cargo e Institución donde Labora: PMO - INEI

1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACION	Existe organización Lógica					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					X
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología					X
8. COHERENCIA	Entre índices, indicadores y dimensiones					X
9. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCION DE APLICABILIDAD : Excelente

III. PROMEDIO DE VALORACIÓN : 85%

IV. RECOMENDACIÓNES : Se puede aplicar el instrumento

Firma del experto:

Fecha: 07/11/2022

DNI : 20037930

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "sistema de gestión de seguridad de la información para disminuir riesgos de perdida de información en cenares año 2022"

PRESENTADO POR (Tesista): Bach. Hoces Roman Santiago Juan

I. DATOS GENERALES DEL EXPERTO N°: 3

1.1. Apellidos y Nombres : Luis Enrique Acosta Medina

1.2. Grado Académico : Ingeniero de Sistemas y magister en investigación y docencia.

1.3. Cargo e Institución donde Labora: Gerente, en SYS4PERU SAC

1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado				X	
2. OBJETIVIDAD	Está expresado en conducta observable				X	
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACION	Existe organización Lógica				X	
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				X	
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología				X	
8. COHERENCIA	Entre Indices, indicadores y dimensiones					X
9. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCION DE APLICABILIDAD : APLICABLE

III. PROMEDIO DE VALORACIÓN : 82%

IV. RECOMENDACIÓNES :

Firma del experto: .....

Luis Enrique Acosta Medina
CEO
SYS4PERÚ

Fecha: 05/12/2022 DNI : 42810213

Anexo 3: Base de datos

Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2022

CODIGO	SEXO	EDAD	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21
1	M	38	1	1	3	1	3	3	3	1	1	1	1	1	1	1	2	1	1	1	1	3	1
2	M	36	1	1	3	1	3	1	1	1	1	1	1	1	1	3	1	3	1	1	1	1	2
3	F	53	1	1	2	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	M	42	2	2	3	3	3	3	3	2	3	3	2	1	1	3	3	3	3	2	3	3	3
5	M	44	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	M	40	2	1	3	1	1	3	3	3	1	1	1	1	1	3	3	1	1	1	1	3	3
7	F	58	1	3	2	1	3	3	3	2	1	1	1	1	1	1	1	1	1	1	1	1	2
8	M	32	1	2	3	1	1	3	2	2	1	1	1	1	1	1	1	1	1	1	1	3	1
9	M	35	3	1	1	3	3	3	3	2	3	1	1	3	1	3	1	3	3	3	3	3	3
10	M	28	1	1	3	1	3	1	1	2	1	1	3	1	1	1	1	1	1	1	1	1	1
11	M	56	3	1	3	1	1	3	3	2	1	3	1	1	1	1	1	1	1	1	1	1	1
12	M	37	1	1	2	1	3	3	3	1	3	1	1	1	3	1	1	1	1	1	1	3	3
13	F	40	2	2	3	1	3	3	3	2	1	3	3	1	3	1	3	3	1	3	3	3	3
14	M	29	2	1	1	1	1	3	3	1	3	2	1	1	1	1	1	1	1	1	1	3	3
15	M	42	1	1	3	1	3	1	3	1	1	1	1	1	1	1	2	1	1	1	1	1	1
16	M	42	3	1	3	3	3	3	1	3	1	3	2	1	3	1	1	1	3	1	1	3	3
17	M	54	1	1	2	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	1	3	2
18	F	52	1	2	3	1	3	3	3	2	2	1	2	3	3	1	2	3	1	2	2	3	3
19	M	39	2	1	1	1	3	1	1	1	1	1	1	1	2	1	1	1	3	1	1	3	2
20	M	47	1	1	3	1	3	3	3	3	1	3	1	1	1	1	1	1	3	1	2	1	3
21	M	39	1	2	3	2	3	3	3	1	1	2	3	3	1	1	3	1	1	1	3	3	3
22	M	42	2	1	1	1	3	3	3	2	1	1	1	1	1	1	1	1	1	1	1	1	1
23	F	53	1	1	3	1	3	1	1	1	3	3	1	1	1	1	1	3	2	1	1	1	1
24	F	38	2	1	3	1	3	3	3	2	1	1	2	1	2	1	3	1	1	1	1	1	3
25	M	42	1	1	3	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	2	3	3
26	F	40	1	1	1	1	3	3	3	1	1	3	2	1	1	1	2	1	2	1	1	3	3
27	M	44	1	1	3	1	3	3	3	2	1	1	1	1	1	1	1	1	1	1	1	1	1
28	M	38	3	3	3	3	3	3	3	1	1	1	1	1	3	3	3	1	1	1	1	3	3
29	F	51	1	1	2	3	3	3	3	1	1	3	1	1	1	1	1	1	1	1	1	3	3
30	M	36	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Anexo 4: Evidencia de similitud digital

Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2022

por Santiago Juan Hoces Román

Fecha de entrega: 20-ago-2023 12:46p.m. (UTC-0500)
Identificador de la entrega: 2148383538
Nombre del archivo: Tesis_Cuantitativa_-_HOCES_06_08_2023_vfinal.docx (2.99M)
Total de palabras: 16072
Total de caracteres: 85994

Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2022

INFORME DE ORIGINALIDAD

27%	23%	14%	19%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	openaccess.uoc.edu Fuente de Internet	2%
2	alejandria.poligran.edu.co Fuente de Internet	2%
3	ri.ues.edu.sv Fuente de Internet	2%
4	Submitted to Universidad Carlos III de Madrid Trabajo del estudiante	2%
5	Submitted to Universidad Nacional de Colombia Trabajo del estudiante	1%
6	Submitted to Instituto Especializado de Estudios Superiores Loyola Trabajo del estudiante	1%
7	repositorio.utelesup.edu.pe Fuente de Internet	1%

Anexo 5: Autorización de publicación en repositorio

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: HOCES ROMAN SANTIAGO JUAN

DNI: 41938313 Correo electrónico: sajuhoro@gmail.com

Domicilio: urb. LEONCIO PRADO MZ. N LOTE 4

Teléfono fijo: _____ Teléfono celular: 953251801

2.- IDENTIFICACIÓN DEL TRABAJO O TESIS

Facultad/Escuela: CIENCIAS E INGENIERÍA

Tipo: Trabajo de Investigación Bachiller ( ) Tesis (X)

Título del Trabajo de Investigación / Tesis:

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA DISMINUIR RIESGOS DE PERDIDA DE INFORMACION EN CENARES AÑO 2022

3.- OBTENER:

Bachiller ( ) Título (X) Mg. ( ) Dr. ( ) PhD. ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
( ) Sí, autorizo el depósito y publicación total.
(X) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 12 días del mes de DICIEMBRE de 2023.

Anexo 6: matriz de riesgo

Ítem	Nombre del Activo	Descripción del Activo	Tipo de Activo	Dueño del Activo
1	Servidores de TI [EXT]	Servidor dispuesto para las actividades de la institución	Arquitectura [ARCH]	Tecnología de la Información
2	PC, cableado red, switch	Equipo de cómputo dispuesto para actividades de la institución	Equipo informático [HW]	Tecnología de la Información
3	Sistemas de Información, navegador web, software y base de datos	SIGA, sicenares, Firma digital, antivirus	Software [SW]	Tecnología de la Información
4	Internet, red local,	Carpetas y archivos compartidos	Redes de comunicación [COM]	Tecnología de la Información
5	Cintas de Backup	Copia de seguridad de la información semanal	Datos/Información [D]	Tecnología de la Información
6	Oficina, Centro de datos	Espacio físico con equipamiento informático	Instalaciones [L]	Administración
7	Documentos en físico	Oficios, Informes, Memorandos, Resoluciones, Etc.	Dato/soporte de información [Media]	Oficinas
8	Administradores de sistema, soporte, Personal Administrativo	Personal con acceso a información de la institución	Personas [P]	RRHH

INVENTARIO DE ACTIVOS

VALORACION DE ACTIVOS SEGÚN METODOLOGIA DE MAGERIT

Valor		**Criterio**
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave a la organización
6-8	Alto	Daño grave a la organización
3-5	Medio	Daño importante a la organización
1-2	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Las dimensiones que se van a valorar son:

• [D] Disponibilidad: El activo puede ser usado por las entidades o procesos autorizados lo requieran.

• [I] Integridad de los datos: El activo no ha sido alterado por individuos, entidades o procesos no autorizados. Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

• [C] Confidencialidad: Es el aseguramiento de que la información es accesible sólo para aquellos individuos o entidades autorizados.

• [A] Autenticidad: La entidad que accede al activo es quien dice ser.

• [T]Trazabilidad: El acceso a la información protegida y la realización de operaciones debe ser registrada para evitar el repudio por parte de quien ejecuta dicha operación.

VALORACION DE ACTIVOS

Ítem	Nombre del Activo	Dueño del Activo	Dimensiones				
			D	I	C	A	T
1	Servidores de TI (HW/SW)	Tecnología de la Información	10	9	9	9	9
2	PC, cableado red, switch	Tecnología de la Información	4	4	4	5	6
3	Sistemas de Información, navegador web, software y base de datos	Tecnología de la Información	10	9	9	10	10
4	Internet, red local	Tecnología de la Información	1	5	5	5	7
5	Cintas de Backup	Tecnología de la Información	8	9	10	10	10
6	Centro de datos, instalaciones	Tecnología de la Información	10	9	9	9	9
7	Documentos en Físico	oficinas	5	4	4	5	4
8	Administradores	RRHH	1		6	4	

	de sistema, soporte, Personal Administrativo						

IDENTIFICACION Y VALORACION DE LA AMENAZA

En esta etapa se muestra el daño que puede causar una amenaza sobre los tipos de activos si ésta se materializa.

La metodología presenta un catálogo de amenazas posibles, pero éste no es definitivo.

La tabla 7 presenta los valores para la medir el daño o nivel de degradación que pueden presentar los activos se vean afectados por las amenazas que los acechan.

Valores para medir la degradacion

Valor	Descripción	
100%	MA	Muy alta
80%	A	Alta
50%	M	Media
20%	B	Baja
10%	MB	Muy baja

A continuación, se presenta la escala de valores que se usarán para medir la probabilidad de que una amenaza se materialice sobre un activo.

Valor	Descripción		
100	MF	Muy frecuente	A diario
10	F	Frecuente	Mensualmente
1	N	Normal	Una vez al año
1/10	P	Poco	Cada varios años
1/100	MP	Muy poco frecuente	Siglos

Para cumplir con este objetivo se toma el listado de amenazas que se presentan en el catálogo de elementos libro II Versión 3.0 de la metodología MAGERIT, las cuales están clasificadas en 4 categorías:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Las siguientes tablas muestran las amenazas sobre los activos identificados y la valoración de cada una de las dimensiones de los activos.

Valoración amenazas Servidores de TI (HW/SW)

Activo: Servidores de TI (HW/SW)						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	P	A				
[N.3] Desastre Natural	P	A				

Valoración amenaza equipo informático

[HW] EQUIPO INFORMATICO						
Activo: [PC] PC						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego						
[I.*] Desastres industriales	P	A				
[I.4] Contaminación electromagnética	P	A				
[I.5] Avería de origen físico o lógico	N	A				
[I.6] Corte del suministro eléctrico	N	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P	A				
[E.2] Errores del administrador	N	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P		A	A		
[A.23] Manipulación de los equipos	P			A		
[A.25] Robo	P			A		
[A.26] Ataque destructivo	P					
Activo: [LAN] Cableado red de área local						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.5] Avería de origen físico o lógico	N	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.23] Manipulación de los equipos	P	A				
[A.25] Robo	P	A				
[A.26] Ataque destructivo	P	A				
Activo: [SWITCH] Switch						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.5] Avería de origen físico o lógico	P	A				

[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[E.23] Errores de mantenimiento / actualización de equipos	N	A				
[E.25] Pérdida de equipos	P	A				
[A.23] Manipulación de los equipos	P	A				
[A.25] Robo	P	A				
[A.26] Ataque destructivo	P	A				

Valoración amenazas redes de comunicación

[COM] Redes de comunicaciones						
Activo: internet						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.8] Fallo de servicios de comunicaciones	N	A				
[E.2] Errores del administrador	N	M	M	M		
E.9] Errores de [re-]encaminamiento	P			A		
[E.10] Errores de secuencia	P		A			
[A.5] Suplantación de la identidad del usuario	P		A	A	A	
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.10] Alteración de secuencia	P		A			
[A.11] Acceso no autorizado	P		A	A		
[A.12] Análisis de tráfico	P			A		
[A.14] Interceptación de información	P			A		
[A.15] Modificación deliberada de la información	P		A			
Activo: [LAN] Red local						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.2] Errores del administrador	N	M	M	M		
E.9] Errores de [re-]encaminamiento	P			A		
[E.10] Errores de secuencia	P		A			
[A.5] Suplantación de la identidad del usuario	P		A	A	A	
[A.6] Abuso de privilegios de acceso	P	A	A	A		
[A.7] Uso no previsto	P	A	A	A		
[A.10] Alteración de secuencia	P		A			
[A.11] Acceso no autorizado	P		A	A		
[A.12] Análisis de tráfico	P			A		
[A.14] Interceptación de información	P			A		
[A.15] Modificación deliberada de la información	P		A			

Valoración amenazas a soporte de información

[Media] Soportes de información						
Activo: [PRINTED] Material impreso.						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				

[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[A.7] Uso no previsto	P	A		A		
[A.11] Acceso no autorizado	P			A		
[A.18] Destrucción de información	P	A				
[A.19] Divulgación de información	P			MA		
[A.25] Robo	P	A		MA		
[A.26] Ataque destructivo	P	A				

Valoración amenazas a Datos/Información

[D] Datos/Información						
Activo: [BACKUP] Copias de respaldo						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[I.4] Contaminación electromagnética	P	MB				
[I.5] Avería de origen físico o lógico	P	M				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MB				
[I.10] Degradación de los soportes de almacenamiento de la información	P	M				M
[E.1] Errores de los usuarios	N	B	B	B		
[E.2] Errores del administrador	P	M	M	M		
[E.3] Errores de monitorización	P		M			M
[E.4] Errores de configuración	N	M	M			M
[E.20] Vulnerabilidades de los programas	P	B				M
[A.6] Abuso de privilegios de acceso	P			M		M
[A.7] Uso no previsto	P			A		
[A.11] Acceso no autorizado	P			A		M
[A.15] Modificación deliberada de la información	P	M	A	M		
[A.18] Destrucción de información	P	M				M
[A.19] Divulgación de información	P		B	A		
[A.23] Manipulación de los equipos	P	M		A		M
[A.25] Robo	P	M		A		M
[A.26] Ataque destructivo	P	M				M

Valoración amenazas a software

[SW] Software						
Activo: [PRP] Desarrollo propio sistema institucional						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	M	A	A	A	A
[E.4] Errores de configuración	P	A		A	A	A
[E.19] Fugas de información	P			A		
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		

[A.6] Abuso de privilegios de acceso	P	A	A	A		A
[A.7] Uso no previsto	P	M	A	A		
[A.11] Acceso no autorizado	P	A	A	A		A
[A.15] Modificación deliberada de la información	P		A	A		
[A.18] Destrucción de información	P	A	A	A		A
[A.19] Divulgación de información	P		A	A	A	
[A.24] Denegación de servicio	P	A				
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		
Activo: [BROWSER] Navegador web						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[A.7] Uso no previsto	N			M		
[E.8] Difusión de software dañino	N		M			
Activo: [APP] Servidor de aplicaciones						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	M				
[E.4] Errores de configuración	P	M				
[E.21] Errores de mantenimiento / actualización de programas	P	A	A			
[E.23] Errores de mantenimiento / actualización de equipos	P	A				
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.6] Abuso de privilegios de acceso	P	M			A	A
[A.11] Acceso no autorizado	P		A	A		A
[A.15] Modificación deliberada de la información	P	M	A			M
[A.19] Divulgación de información	P			A		
[A.24] Denegación de servicio	P	A				
[A.25] Robo	P	A		A		
[A.26] Ataque destructivo	P	A				A
Activo: [DBMS] Sistema de gestión de bases de datos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.2] Errores del administrador	P	A	A	A	A	A
[E.4] Errores de configuración	P	A		A	A	A
[E.19] Fugas de información	P			A		
[E.20] Vulnerabilidades de los programas	N	A	M	M	A	A
[E.21] Errores de mantenimiento / actualización de programas	N	M	A			
[E.23] Errores de mantenimiento / actualización de equipos	P	A				
[E.24] Caída del sistema por agotamiento de recursos	N	A				
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		
[A.6] Abuso de privilegios de acceso	P	A	A	A		A
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P	A	A	A		A
[A.15] Modificación deliberada de la información	P		A	A		

[A.18] Destrucción de información	P	A	A	A		A
[A.19] Divulgación de información	P		A	A	A	
[A.25] Robo	P	A	A	A		
[A.26] Ataque destructivo	P	A	A	A		A
Activo: [AV] Anti virus						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.1] Errores de los usuarios	N	M				A
[E.2] Errores del administrador	P	A				A
[E.4] Errores de configuración	P	A			M	A
[A.11] Acceso no autorizado	P	A	A			A

Valoración amenazas Instalaciones

[L] Instalaciones						
Activo: [OFI] Oficina						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[N.1] Fuego	P	A				
[N.2] Daños por agua	MP	A				
[N.*] Desastres naturales	P	A				
[I.1] Fuego	P	A				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	A				
[I.5] Avería de origen físico o lógico	P	A				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A				
[I.11] Emanaciones electromagnéticas	P			A		
[E.15] Alteración accidental de la información	P		A			
[E.18] Destrucción de información	P	A				
[E.19] Fugas de información	P			A		
[A.7] Uso no previsto	P	A	A	A		
[A.11] Acceso no autorizado	P		A	A		
[A.15] Modificación deliberada de la información	P		A			
[A.18] Destrucción de información	P	M				
[A.19] Divulgación de información	P			A		
[A.26] Ataque destructivo	P	A				

Valoración amenazas personal

[P] Personal						
Activo: [ADM] Administradores de sistemas						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	N	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	N	M				
[A.29] Extorsión	P	B	A	A		
[A.30] Ingeniería social	p	B	A	A		
Activo: [SOP] Soporte						

Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	B				
[E.19] Fugas de información	P			M		
[E.28] Indisponibilidad del personal	N	A				
[A.29] Extorsión	P	B	A	A		
[A.30] Ingeniería social	p	B	A	A		
Activo: [UI] Usuarios internos						
Amenaza	Frecuencia	Dimensiones				
		D	I	C	A	T
[E.7] Deficiencias en la organización	P	B				
[E.19] Fugas de información	P			B		
[E.28] Indisponibilidad del personal	N	A				
[A.29] Extorsión	P	B	B	B		
[A.30] Ingeniería social	p	B	A	A		

Descripción de valores del riesgo

Riesgo	
Valor	Descripción
MA	Critico
A	Importante
M	Apeciable
B	Bajo
MB	despreciable

Valores de escala de cálculo de riesgo

Riesgo		Probabilidad				
		MP	P	N	F	MF
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Calculo de riesgo Servidores

Activo: Servidores de TI (HW/SW)	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	M	M
[N.2] Daños por agua	P	B	B
[N.3] Desastre Natural	P	B	B

Activo: [PC] PC	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*] Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.*] Desastres industriales	P	A	A
[I.4] Contaminación electromagnética	P	A	A
[E.2] Errores del administrador	N	A	A
[E.23] Errores de mantenimiento / actualización de equipos	N	A	A

[E.25] Pérdida de equipos	P	A	A
[A.6] Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.23] Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [LAN] Cableado red de área local	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*] Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*] Desastres industriales	P	A	A
[I.5] Avería de origen físico o lógico	N	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	A
[E.23] Errores de mantenimiento / actualización de equipos	N	A	A
[E.25] Pérdida de equipos	P	A	A
[A.23] Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [SWITCH] Switch	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*] Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*] Desastres industriales	P	A	A
[I.5] Avería de origen físico o lógico	P	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	A
[E.23] Errores de mantenimiento / actualización de equipos	N	A	A
[E.25] Pérdida de equipos	P	A	A
[A.23] Manipulación de los equipos	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: internet	Probabilidad	Impacto	Riesgo
[I.8] Fallo de servicios de comunicaciones	N	A	A
[E.2] Errores del administrador	N	M	M
E.9] Errores de [re-]encaminamiento	P	A	A
[E.10] Errores de secuencia	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6] Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.10] Alteración de secuencia	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.12] Análisis de tráfico	P	A	A
[A.14] Interceptación de información	P	A	A
[A.15] Modificación deliberada de la información	P	A	A
Activo: [LAN] Red local	Probabilidad	Impacto	Riesgo

[I.8] Fallo de servicios de comunicaciones	P	A	A
[E.2] Errores del administrador	N	M	M
E.9] Errores de [re-]encaminamiento	P	A	A
[E.10] Errores de secuencia	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6] Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.10] Alteración de secuencia	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.12] Análisis de tráfico	P	A	A
[A.14] Interceptación de información	P	A	A
[A.15] Modificación deliberada de la información	P	A	A
Activo: [PRINTED] Material impreso.	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*] Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*] Desastres industriales	P	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.18] Destrucción de información	P	A	A
[A.19] Divulgación de información	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [BACKUP] Copias de respaldo	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[I.4] Contaminación electromagnética	P	MB	MB
[I.5] Avería de origen físico o lógico	P	M	M
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MB	MB
[I.10] Degradación de los soportes de almacenamiento de la información	P	M	M
[E.1] Errores de los usuarios	N	B	B
[E.2] Errores del administrador	P	M	M
[E.3] Errores de monitorización	P	M	M
[E.4] Errores de configuración	N	M	M
[E.20] Vulnerabilidades de los programas	P	B	B
[A.6] Abuso de privilegios de acceso	P	M	M
[A.7] Uso no previsto	P	M	M
[A.11] Acceso no autorizado	P	A	A
[A.15] Modificación deliberada de la información	P	M	M
[A.18] Destrucción de información	P	M	M
[A.19] Divulgación de información	P	A	A
[A.23] Manipulación de los equipos	P	M	M
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [PRP] Desarrollo propio sistema institucional	Probabilidad	Impacto	Riesgo
[E.2] Errores del administrador	P	M	M
[E.4] Errores de configuración	P	A	A
[E.19] Fugas de información	P	A	A

[E.25] Pérdida de equipos	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6] Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	M	M
[A.11] Acceso no autorizado	P	A	A
[A.15] Modificación deliberada de la información	P	A	A
[A.18] Destrucción de información	P	A	A
[A.19] Divulgación de información	P	A	A
[A.24] Denegación de servicio	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [BROWSER] Navegador web	Probabilidad	Impacto	Riesgo
[A.7] Uso no previsto	N	B	B
[E.8] Difusión de software dañino	N	M	M
Activo: [APP] Servidor de aplicaciones	Probabilidad	Impacto	Riesgo
[E.2] Errores del administrador	P	M	M
[E.4] Errores de configuración	P	M	M
[E.21] Errores de mantenimiento / actualización de programas	P	A	A
[E.23] Errores de mantenimiento / actualización de equipos	P	A	A
[E.24] Caída del sistema por agotamiento de recursos	P	A	A
[A.6] Abuso de privilegios de acceso	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.15] Modificación deliberada de la información	P	M	M
[A.19] Divulgación de información	P	M	M
[A.24] Denegación de servicio	P	M	M
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [DBMS] Sistema de gestión de bases de datos	Probabilidad	Impacto	Riesgo
[E.2] Errores del administrador	P	A	A
[E.4] Errores de configuración	P	A	A
[E.19] Fugas de información	P	A	A
[E.20] Vulnerabilidades de los programas	N	A	A
[E.21] Errores de mantenimiento / actualización de programas	N	M	M
[E.23] Errores de mantenimiento / actualización de equipos	P	A	A
[E.24] Caída del sistema por agotamiento de recursos	N	A	A
[E.25] Pérdida de equipos	P	A	A
[A.5] Suplantación de la identidad del usuario	P	A	A
[A.6] Abuso de privilegios de acceso	P	A	A
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.15] Modificación deliberada de la información	P	A	A
[A.18] Destrucción de información	P	A	A
[A.19] Divulgación de información	P	A	A
[A.25] Robo	P	A	A
[A.26] Ataque destructivo	P	A	A
Activo: [AV] Anti virus	Probabilidad	Impacto	Riesgo
[E.1] Errores de los usuarios	N	M	M

[E.2] Errores del administrador	P	A	A
[E.4] Errores de configuración	P	A	A
[A.11] Acceso no autorizado	P	A	A
Activo: [OFI] Oficina	Probabilidad	Impacto	Riesgo
[N.1] Fuego	P	A	A
[N.2] Daños por agua	MP	A	M
[N.*] Desastres naturales	P	A	A
[I.1] Fuego	P	A	A
[I.2] Daños por agua	P	A	A
[I.*] Desastres industriales	P	A	A
[I.5] Avería de origen físico o lógico	P	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	A
[I.11] Emanaciones electromagnéticas	P	M	M
[E.15] Alteración accidental de la información	P	M	M
[E.18] Destrucción de información	P	M	M
[E.19] Fugas de información	P	M	M
[A.7] Uso no previsto	P	A	A
[A.11] Acceso no autorizado	P	A	A
[A.15] Modificación deliberada de la información	P	A	A
[A.18] Destrucción de información	P	M	M
[A.19] Divulgación de información	P	M	M
[A.26] Ataque destructivo	P	A	A
Activo: [ADM] Administradores de sistemas	Probabilidad	Impacto	Riesgo
[E.7] Deficiencias en la organización	N	B	B
[E.19] Fugas de información	P	M	M
[E.28] Indisponibilidad del personal	N	M	M
[A.29] Extorsión	P	B	B
[A.30] Ingeniería social	P	B	B
Activo: [SOP] Soporte	Probabilidad	Impacto	Riesgo
[E.7] Deficiencias en la organización	P	B	B
[E.19] Fugas de información	P	B	B
[E.28] Indisponibilidad del personal	N	A	A
[A.29] Extorsión	P	B	B
[A.30] Ingeniería social	P	B	B
Activo: [UI] Usuarios internos	Probabilidad	Impacto	Riesgo
[E.7] Deficiencias en la organización	P	B	B
[E.19] Fugas de información	P	B	B
[E.28] Indisponibilidad del personal	N	A	A
[A.29] Extorsión	P	B	B