UNIVERSIDAD SEÑOR DE SIPÁN

# FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

## ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

## TESIS

# DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS**

**Autor:**
**Bach. Méndez Gálvez, Cipriano**
**ORCID: https://orcid.org/0000-0003-0861-2610**

**Asesor:**
**Dr. Sánchez Chero, Manuel Jesús**
**ORCID: https://orcid.org/0000-0003-1646-3037**

**Línea de Investigación:**
**Infraestructura, Tecnología y Medio Ambiente**

**Pimentel - Perú 2020**

**APROBACIÓN DEL JURADO**

**DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS**

**Bachiller, Méndez Gálvez, Cipriano**
**Autor**

**MSc., Guerrero Millones, Ana María**
**Asesor**

**Dr., Sánchez Chero, Manuel Jesús**
**Presidente de Jurado**

**Mg., Bravo Ruiz, Jaime Arturo**
**Secretario de Jurado**

**MSc., Guerrero Millones, Ana María**
**Vocal de Jurado**

## DEDICATORIA

Gracias a **DIOS** por haberme regalado la vida y por darme los recursos necesarios para poder culminar mis metas profesionales y también doy gracias a mi familia por el apoyo constante que me brindaron para poder culminar de manera satisfactoria.

## AGRADECIMIENTOS

A mis compañeros de estudio por el apoyo constante, a mi asesor metodológico la Dra. Ana María Guerrero Millones, quien siempre se empeñó por brindar el mejor aporte, y a todas las personas que de un modo u otro me brindaron su apoyo.

## RESUMEN

En la actualidad las actividades de las empresas utilizan información y procesos los cuales tienen muchos riesgos, por lo consiguiente toda organización debe contar con medidas de control en la seguridad de la información y activos de la organización en todos los niveles jerárquicos. La disponibilidad de la información para los usuarios internos como externos desde cualquier medio y desde cualquier lugar es uno de los propósitos principales de una organización por lo cual, la seguridad es un elemento primordial y se debe dar la importancia necesaria para asegurar la confidencialidad, integridad y disponibilidad de la información y de los activos informáticos para prevenir las amenazas y vulnerabilidades los cuales puedan causar daños a una organización. La norma internacional ISO 27001 cuenta con una serie de medidas orientadas a proteger la información contra cualquier amenaza, garantizando la confidencialidad, integridad y disponibilidad de la información, así poder asegurar en todo momento la continuidad de las actividades de la organización.

El presente proyecto tiene como finalidad analizar y proponer el desarrollo de un plan de seguridad de la información dentro del área de tecnologías de la información de la empresa de seguros, mediante estándares internacionales como la ISO 27001, la norma en mención permite a cualquier organización a evaluar sus riesgos y poder aplicar los controles necesarios para su prevención o eliminación considerando como activo más importante la información de una organización. Asimismo, la norma establece procedimientos, guías y procesos para la gestión apropiada mediante el proceso de mejora continua.

Complementario a la norma IS27001, la metodología utilizada para evaluar los riesgos es MAGERIT, la metodología mencionada ayuda a poder determinar el nivel de impacto generado la no implementación de controles o medidas que necesita la organización, para proteger sus activos más críticos.

De acuerdo a los resultados obtenidos en la investigación la empresa se encuentra en una etapa inicial frente a los requerimientos y los controles del Anexo A de la norma ISO 27001.



**Palabras Claves:** Seguridad de la información, ISO 27001, MAGERIT, Amenazas

## ABSTRACT

Currently the activities of companies use information and processes which have many risks, therefore every organization must have control measures in the security of information and assets of the organization at all hierarchical levels. The availability of information for internal and external users from any medium and from any place is one of the main purposes of an organization, therefore, security is a primary element and the necessary importance must be given to ensure confidentiality, integrity and availability of information and computer assets to prevent threats and vulnerabilities which can cause damage to an organization. The international standard ISO 27001 has a series of measures aimed at protecting information against any threat, guaranteeing the confidentiality, integrity and availability of the information, thus ensuring the continuity of the organization's activities at all times.

The purpose of this project is to analyze and propose the development of an information security plan within the information technology area of the insurance company, through international standards such as ISO 27001, the mentioned standard allows any organization to evaluate its risks and be able to apply the necessary controls for their prevention or elimination, considering the information of an organization as the most important asset. Likewise, the standard establishes procedures, guides and processes for proper management through the continuous improvement process.

Complementary to the IS27001 standard, the methodology used to assess risks is MAGERIT, the aforementioned methodology helps to determine the level of impact generated by the non-implementation of controls or measures that the organization needs, to protect its most critical assets.

According to the results obtained in the investigation, the company is in an initial stage facing the requirements and controls of Annex A of the ISO 27001 standard.



**Keywords**: Information security, ISO 27001, MAGERIT, Threats

## Índice

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# I. INTRODUCCIÓN

## 1.1 Realidad Problemática.

La seguridad de la información es uno de los puntos más importantes dentro de una organización, de hecho la seguridad no es algo nuevo dentro de los negocios, en tiempos antiguos la protección de los activos se realizaba mediante barreras y guardas, pero en la actualidad se protege la información mediante contraseñas, certificados digitales, reconocimiento facial, reconocimiento dactilar, cifrado de datos y diversas maneras tanto tecnológicas como físicas, los dispositivos interconectados han redefinido lo que se entiende por seguridad y riesgos en la SI dentro de los negocios.

La ISO/IEC 27001 es una norma internacional ampliamente conocida que brinda una serie de requisitos para una gestión correcta en temas de seguridad de la información, definiendo un conjunto de políticas o reglas.

Al implementar un SGSI en una empresa le brinda muchos beneficios como pueden ser la reducción del impacto de los riesgos, garantiza la continuidad del negocio basándose en el Plan de Contingencias, mejora la imagen de la empresa, aumenta su valor comercial, incrementa los niveles de confianza de sus accionistas, socios, clientes y proveedores, mejora del retorno de sus inversiones, asimismo ayuda al cumplimiento contractual de las normas vigentes.

### Contexto internacional

(Arévalo, Bayona, & Rico, 2015), Según la investigación realizada en la ciudad de Ocaña Colombia menciona, que las empresas sin importar su tamaño ni el sector donde se encuentren deben ser creativas e innovadoras para ampliar su competitividad y poder mantenerse en el mercado ante la competencia y la globalización que crea nuevas reglas de comercio internacional.

Por lo cual diariamente se crean nuevos escenarios en lo que la información de la organización deja de ser confidencial y es accedido por muchas personas sin autorización.

La información es un activo con más importancia dentro de la organización y debe ser protegido ya que el funcionamiento y la operación de sus negocios dependerá de ello.

De acuerdo a la investigación se evidencia que las empresas de la ciudad de Ocaña tienen una brecha de Nivel tecnológico muy amplia entre organizaciones.

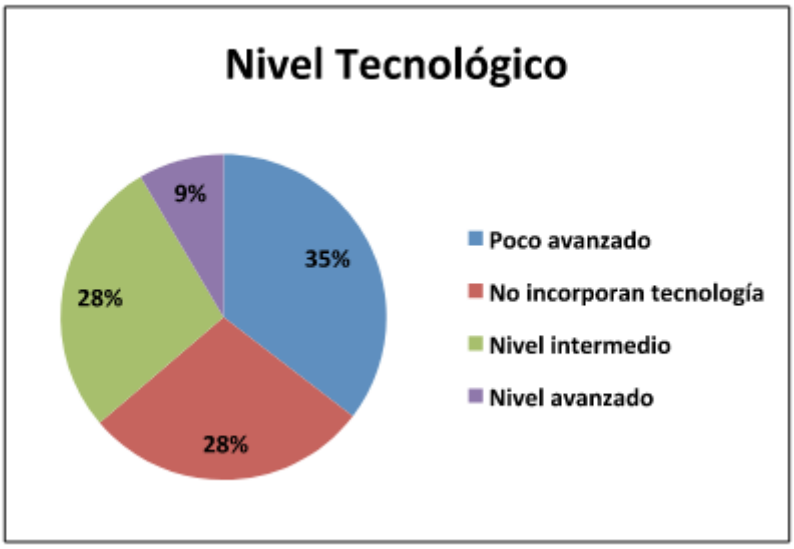



*Figura 1*. Nivel Tecnológico de la empresa en la ciudad de Ocaña-Colombia. Fuente: (Arévalo, Bayona, & Rico, 2015), Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001, 2015 – p.129

También menciona que las empresas trabajan con estrategias de seguridad de la información definidas pero su selección es empírica, por lo cual indica que la tecnología debe ser tomada con mucha importancia por cualquier organización, lo que les permitirá la eficiente optimización de costos, estandarización de sistemas, contar con información eficiente y oportuna. Por lo cual deben implementar normas que permitan mejorar la SI como la norma ISO27001 y le permitan tener una mejor imagen frente a otras empresas.

De acuerdo a la investigación actualmente el avance de las tecnologías ha traído consigo muchos amenazas y vulnerabilidades como la difusión de nuevas metodologías y técnicas de ataques más eficaces y avanzados

Las organizaciones invierten una cantidad de dinero muy alto, para evitar manipulaciones e intrusiones que pueden poner en riesgo sus operaciones y

afectar la integridad de la información de la organización.

Cárdenas, Martínez, & Becerra (2016), en la revisión bibliográfica indica que los incidentes y fallas en la seguridad cada vez son más frecuentes y sofisticados, en la mayoría de casos corresponden a temas técnicos como violaciones a las redes y sistemas de información. Las fallas de la SI generan muchas pérdidas y son difíciles de medir.

Las causas que generan los incidentes de la seguridad dentro de una organización, indica que es por el incumplimiento de las políticas de seguridad por parte de los empleados.

Nasser, (2017), En su investigación indica que la información es considerada como un activo fundamental de una empresa y para proteger la información se necesita contar con una serie de controles.

En la evaluación que realizó a la seguridad de la información de la Academia Yemení, se evidencia que el grado de madurez de la SI está en el nivel 2, el motivo es porque los controles con los que cuenta en la actualidad tiene muchas debilidades por lo consiguiente se necesita implementar un SGSI y mantener una cultura en gestión de la seguridad.

Khalid, Shamsul, Noor, Sapiee, & Kamaruddin (2019), en la investigación realizada mencionan que las causas principales que generan las vulnerabilidades de la información dentro de una organización se debe a las debilidades humanas, por lo cual se debe proponer un modelo de SI orientado a personas y a políticas de la organización.

Cuando una organización adopta políticas de seguridad de la información establece bases sólidas desde donde se puede difundir y dar cumplimiento a las mismas y dejar de ver al ser humano como la fuente del problema.

ESET, (2020), de acuerdo al reporte anual de la empresa ESET del año 2019 de las organizaciones encuestadas el 60% menciona que su principal preocupación es el acceso indebido a la información, el 55% indicó que es el robo de la información y el 53% la infección mediante códigos maliciosos. Aun así, las

empresas tienen una implementación baja de controles en la SI.


*Figura 2*. Incidentes en seguridad en empresas del Mundo. Fuente: (ESET, Security Report Latinoamérica, 2020)-p.10

**Contexto nacional**

Atencio, (2019), de acuerdo a su investigación efectuada en la ciudad de Pasco-Perú menciona que el diseño de un SGSI tomando como referencia la NTP ISO/IEC 27001:2014, mejorará significativamente la integridad, confidencialidad y disponibilidad de los activos de la información en la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión y minimizará el nivel de riesgos al aplicar controles.

ISO, (2019), Según la encuesta realizada por la organización www.iso.org en el año 2019 hubo un incremento considerable en obtener la certificación ISO 27001

por organizaciones de diversos sectores en el Perú, si bien es cierto que hubo un incremento en optar la certificación ISO27001, pero no es lo suficiente por lo consiguiente preservar y proteger la información debe ser primordial dentro de una organización sea pública o privada.

La norma ISO 27001 permite realizar una implementación de una serie de controles para mejorar la SI en cualquier tipo y tamaño de una empresa por lo cual muchas empresas están tomando conciencia e invirtiendo en la seguridad, en el siguiente cuadro se detalle las certificaciones por sector empresarial y año en el Perú.

Tabla 1.

*Certificación ISO por año y sector empresarial en el Perú*

| SECTOR | 2017 | 2018 | 2019 |
|---|---|---|---|
| Productos alimenticios, bebidas y tabaco | - | - | 3 |
| Textiles y productos textiles | - | - | 5 |
| Transporte, almacenamiento y comunicación | 2 | - | - |
| Intermediación financiera, inmobiliaria, renting | 2 | 2 | 1 |
| Tecnologías de la información | 24 | 83 | 144 |
| Otros Servicios | - | 10 | 21 |
| Sector desconocido | - | 10 | 21 |
| **Total** | **28** | **105** | **195** |

*Fuente:* (ISO, 2019)

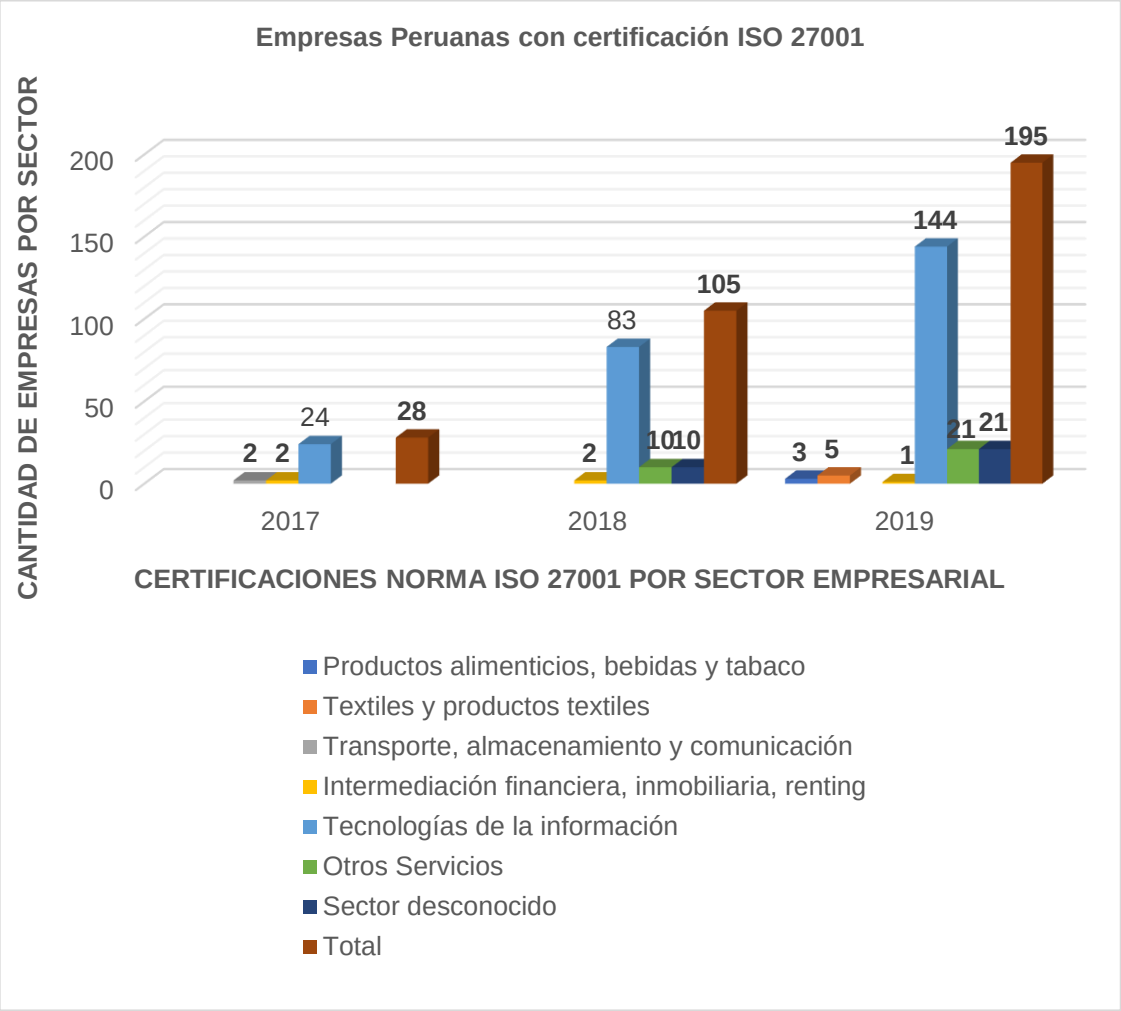



*Figura 3*. Certificación ISO por año y sector empresarial en el Perú. Fuente: *(ISO, 2019)*

ESET, (2020), Según el reporte realizado por ESET indica que la mayoría de las empresas muestra quejas recurrentes por la falta de presupuesto para el área de seguridad. La importancia de resguardar la información de una empresa es vital, por lo cual las empresas deben pensar en hacer un mayor esfuerzo de invertir en tiempo y recursos para lograr mejores resultados. Según el siguiente reporte el 22% considera que el presupuesto es suficiente, el 45% considera que es insuficiente y el 33% desconoce que hay un presupuesto.

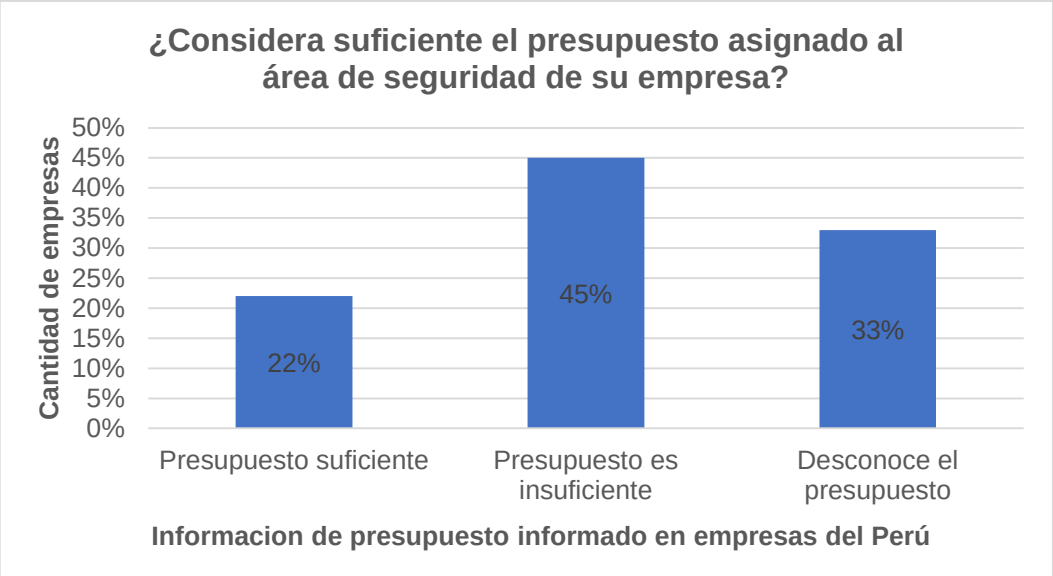



*Figura 4*. ¿Considera suficiente el presupuesto asignado al área de seguridad de su empresa?. Fuente: *(ESET, 2020)*-p.27

**Contexto local**

En la investigación se tomó como caso de estudio el área de sistemas de la empresa de seguros, el área mencionada es muy importante para que la organización continúe con el negocio y es necesario que cuente con un adecuado plan de seguridad de la información, basado en estándares internacionales que apoyen a su correcta implementación, actualmente la empresa cuenta con políticas de seguridad internas, pero no son cumplidas de manera adecuada.

Para cumplir con los objetivos de negocio, y brindar una solución al problema actual, se propone elaborar el plan de seguridad de la información basada en normas internacionales para la empresa de seguros, con la finalidad de cumplir con las regulaciones vigentes y la alineación de los objetivos de la empresa y del área de sistemas, con la finalidad de garantizar la SI en la empresa.

Para evaluar el nivel inicial de la seguridad de la información se utilizó una guía de observación y encuestas que se encuentra en el (Anexo 3).

Los empleados que participaron en la encuesta fueron en total 25, 19 empleados del área de Sistemas, 3 empleados de Contabilidad y 3 empleados del área de

Recursos Humanos y obteniendo los resultados como se muestra a continuación.

El 64% de empleados no informa los incidentes suscitados referentes a la SI, 48% desconoce las políticas de seguridad de la empresa, 44 % indican que la atención de incidentes es muy lento, 28 % no usa contraseñas seguras, 36% indica que los accesos a los lugares restringidos no tiene un control optimo, 12 % de los empleados no bloquean sus pantallas al momento de dejar el lugar, 16% de empleados dejan documentos importantes en sus escritorios o en la sala de impresión, el 40% de los empleados realizó la instalación de programas no autorizados.

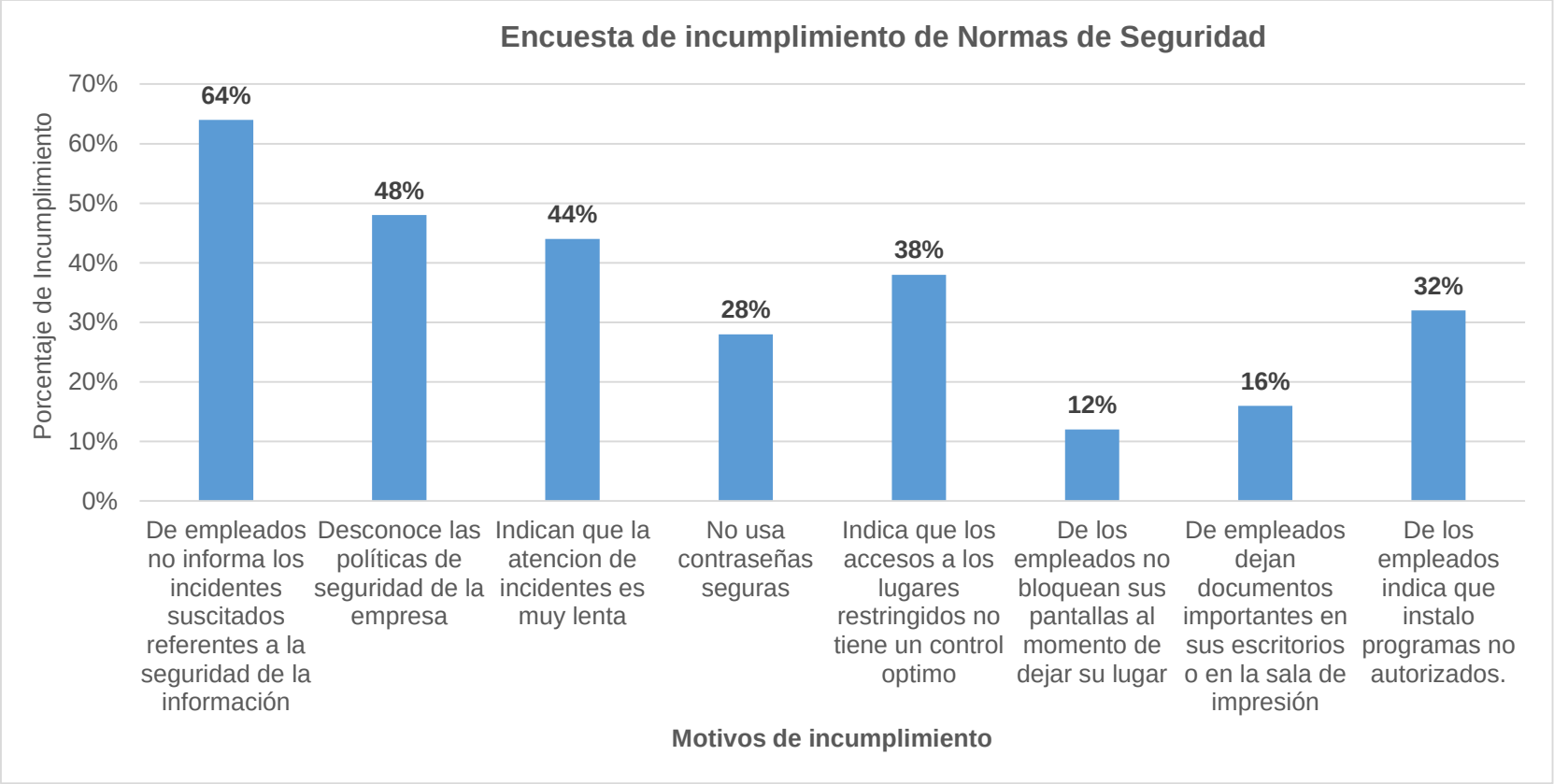



*Figura 5*. Encuesta incumplimiento seguridad de la información empresa de Seguros. Fuente: Elaboración propia

## 1.2 Antecedentes de estudio.

### Contexto internacional

Tsung-Han, Cheng-Yuan, & Man-Nung, (2016) en la Revista de investigación de riesgos indican que el SGSI juega un papel esencial para trazar la hoja de ruta de la seguridad de la información; por lo tanto, muchas metodologías teóricas y estándares se incorporan a este dominio. Sin embargo, muchos estándares y metodologías son demasiado engorrosos para ser adoptados por una organización. Además, no existe un marco unificado para manejar sistemáticamente las tediosas tareas de la gestión de la seguridad de la información. El estudio tiene como objetivo primordial diseñar un sistema integrado para la gestión de la seguridad de la información que tiene como objetivo utilizar metodologías y estándares actuales para resolver los problemas antes mencionados. Debido a que el análisis de impacto empresarial y el análisis de riesgos son las áreas más importantes dentro de este dominio, la investigación seleccionó de manera cuidadosa los métodos relacionados y luego se integró en un marco unificado, del cual depende el sistema integrado para la gestión de la seguridad de la información propuesto.

Cevallos, (2019), en su tesis titulada DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO, BASADO EN LA NORMA DE SEGURIDAD ISO/IEC 27002:2013, de la Universidad Internacional Sek Facultad de Arquitectura e Ingenierías, para optar el grado de Master en Tecnologías de la Información con Mención en Seguridad en Redes y Comunicación, propone la implementación de medidas para mejorar el control de las amenazas que puedan afectar las dimensiones de la SI. Para poder identificar y valorar las vulnerabilidades y amenazas a las que está expuesto la institución se utilizó la metodóloga MAGERIT para generar una matriz de riesgos. Se analizó la norma internacional ISO/IEC 27002:2013 que permite gestionar la SI en cualquier tipo de organización.

De acuerdo a la identificación de los riesgos en el área de TICS, se procedió a

seleccionar los controles necesarios que brinda la norma, con la finalidad minimizar los riesgos encontrados. Los controles que fueron seleccionados fueron presentados de protocolo de seguridad de la información con la finalidad de que la institución pueda implementarlo, ya que será muy útil para el correcto uso y manejo de los activos con los que cuenta el área de TICS.

Cardona, Carvajal, (2018), en la tesis titulada DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA FAMILIA DE NORMAS DE LA SERIE ISO/IEC 27000 PARA UNA ENTIDAD PÚBLICA COLOMBIANA, de la UNIVERSIDAD AUTÓNOMA DE MANIZALES, para optar el grado de MAESTRÍA EN GESTIÓN Y DESARROLLO DE PROYECTOS DE SOFTWARE, menciona que los activos de información de una organización tienen un gran valor, por lo consiguiente se genera una necesidad legal y organizacional de implementar una norma para proteger la SI, para que la organización asegure los dominios de la información.
Para solucionar la necesidad indicada en las entidades públicas, el Gobierno de Colombia realizó la implementación el Gobierno en Línea, basado en la buenas practicas que brinda la norma internacional ISO/IEC 27001.

Figueroa, (2018), en la tesis titulada DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO GERMÁN ARCINIEGAS I.E.D., BAJO LA NORMA TÉCNICA COLOMBIANA NTC ISO/IEC 27001:2013., de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD, para optar el título en ESPECIALISTA EN SEGURIDAD INFORMÁTICA. En la investigación indica que el diseño de un SGSI, para la institución bajo la norma NTC-ISO-IEC 27001:2013, permitirá mejorar la SI. Para lo cual realizó la evaluación de las necesidades de la institución como también las expectativas y la identificación de los interesados.

La importancia de que una organización cuente con un sistema de SI es esencial, según el estudio realizado en Colombia se registran a diario más de 542 mil ataques informáticos y en el último año, se presentaron más de 198 millones de incidentes, los ataques realizados pueden ser a grandes, medianas o pequeñas

empresas; empresas públicas o privadas o cualquier ciudadano. Si bien es cierto que el sector financiero fue el más afectado por los ataques informáticos en Colombia, el sector gubernamental ocupa el tercer puesto seguido del sector de telecomunicaciones el estudio realizado también revela que, hay cuatro ataques más comunes que reciben las organizaciones los cuales son: Malware, Pishing, DoS más conocido como denegación de servicio y los ataques basados en Web. La investigación también indica que el sector de servicios indicó que el 50% notó un aumento en ataques por malware, el 47% de ataques de Phishing, 39% de ataques de web y 18% en ataques de DoS, durante los años 2014, 2015, 2016 y al 10 de marzo del 2017, se recibieron 13.774 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país.

La finalidad del sistema es proveer medidas que puedan prevenir, aplicación de controles para la SI para garantizar la confiabilidad, disponibilidad e integridad de la información de la institución.

Barrera, (2019), en la tesis titulada PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDAD EDUCATIVA NUESTRA SEÑORA DE FÁTIMA., de UNIVERSIDAD TECNOLÓGICA ISRAEL, para optar el título en INGENIERO EN SISTEMAS INFORMÁTICOS, en su investigación menciona que la institución no cuenta con un SGSI por consiguiente sus activos con respecto a la SI, se encuentran en peligro.

El estudio tiene como objetivo proponer un SGSI basado en la norma internacional ISO/IEC 27001:2013, para lo cual se realizó una evaluación del estado actual de la organización frente a los requisitos obligatorios de la norma ISO/IEC 27001:2013, se realizó la evaluación de la factibilidad técnica y operativa con la finalidad de realizar una propuesta de implementación.

En la evaluación realizada se obtuvo que el 72% incumple los requisitos necesarios de la norma ISO 27001, y el 78% incumple los controles asociados al Anexo A de la norma.

La mayoría de riesgos detectados están ubicados en los niveles Alto y Muy Alto, también se detectó un alto índice de vulnerabilidades en los elementos asociados

al mantenimiento, transferencia de la información y la falta de documentación de los procesos asociados a la SI.

**Contexto nacional**

Benites, (2019), en su tesis titulada Implementación de un sistema de gestión de seguridad de la información - Norma ISO 27001 para la fábrica Radiadores Fortaleza de la Universidad Tecnológica del Perú, para optar el título de Ingeniero de Seguridad y Auditoría Informática. Menciona que el desarrollo de un Plan de SGSI traerá muchos beneficios empresa, uno de ellos puede ser a nivel técnico actualmente la empresa se basa en el uso de un Antivirus como técnica de defensa contra los diversos tipos de ataque que se generan a diario, sin embargo, la medida anterior no es la suficiente. Un SGSI propone la implementación de controles técnicos los cuales deben ir seguido de políticas claras en temas de SI con la finalidad de mantener y gestionar de manera correcta el SGSI

Lo cual permitirá reducir riesgos y amenazas que pueda sufrir la empresa en estudio.

Massco, (2017), en su tesis titulada PROPUESTA DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA DESYSWEB S.A.C. EN EL PERIODO 2017, de la Universidad Nacional Tecnológica de Lima Sur, para optar el título de Ingeniero de Sistemas. Indica que un plan de SI ayuda a identificar los activos de información, amenazas, vulnerabilidades, ocurrencias posibles y explotación de los puntos anteriores; con la finalidad minimizar, conocer y gestionar y los riesgos que pueda atentar la SI de la empresa, se debe establecer mecanismos de control los cuales deben estar alineados a la norma internacional ISO/IEC 27001.

Ccesa, (2017), en su tesis titulada DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA, 2016, de la Universidad Nacional de San Cristóbal de Huamanga, para optar el título de Ingeniero Informático. Menciona que en la actualidad la información dentro de una

organización es el activo más importante por lo consiguiente requiere de una protección adecuada.

Implementar un SGSI bajo la NTP ISO/IEC 27001:2014 permitirá realizar una adecuada gestión en la SI y ayudará a preservar sus respectivas dimensiones en la Municipalidad Provincial de Huamanga.

**Contexto local**

Vásquez, (2020), en su tesis titulada Diseño de un Sistema de Gestión de Seguridad de Información para la empresa Neointel SAC basado en la norma ISO/IEC 27001:2013, de la Universidad Peruana de Ciencias Aplicadas, para optar el título de Ingeniero de Sistemas. Indica que el diseño de un SGSI tomando como base al anexo A de la norma ISO/IEC 27001: 2013, permitirá reducir los riesgos a los que está expuesto los activos de información de la organización. También permitirá reducir las vulnerabilidades tecnológicas a las que se encuentra expuesta el Call Center.

## 1.3 Teorías relacionadas al tema.

### 1.3.1 Seguridad de la Información

Según ISO27001, la seguridad de la información se refiere a la confidencialidad, integridad y a la disponibilidad de la información y a todos los datos importantes para una empresa, sin importar el formato que tengan, los cuales pueden ser: Audios, Videos, medios electrónicos, en papel, etc.

Ramírez, (2014), menciona que la información satisface las necesidades de los clientes y permite el reconocimiento de las características de un determinado contexto y apoya los procesos de decisión, lo cual, garantiza ejecutar acciones institucionales en consonancia con los objetivos planteados por la organización. De la misma manera, (Disterer, 2013), reitera que la información en sí misma, junto a los sistemas que lo soportan, son una base importante para las organizaciones. Particularmente, cada vez la mayor transferencia de datos internos y entre empresas además del empleo de redes abiertas, aumenta el riesgo en la exposición de la información y los sistemas de información, por lo

cual, con el fin de reducir los riesgos y evitar daños a las empresas, se deben asumir determinadas consideraciones que garanticen adecuadamente la SI.

#### 1.3.1.1 Importancia de la seguridad de la información

ESAN, (2016), La seguridad de la información dentro de una organización consiste en preservar las dimensiones de la misma.

La información es un activo muy importante dentro de una organización y cumple un rol vital dentro de la misma.

Es como el oxígeno para el para el ser humano, debe fluir de manera adecuada y oportuna por todas las áreas de la empresa.

La certificación en un SGSI, basado en estándares internacionales tiene como finalidad ayudar a las organizaciones en la gestión y protección de su información. La base sobre la que rige la seguridad de la información es preservar la confidencialidad, la integridad y la disponibilidad.

#### 1.3.1.2 Objetivos principales de la seguridad de la información

Los objetivos principales de la SI más importantes son: disponibilidad, confidencialidad, integridad según (Romero, y otros, 2019).

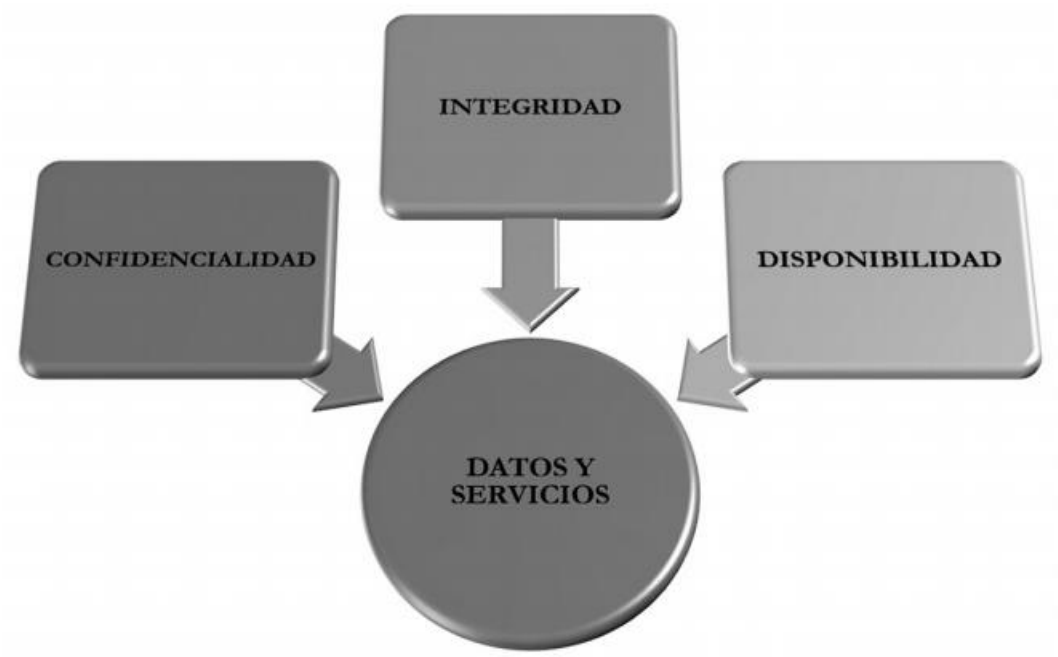



*Figura 6*. Objetivos de la Seguridad de la Información Fuente: (Romero, y otros,

2019).

#### 1.3.1.2.1 Confidencialidad de la Información

La información solo puede ser accedida por personas, entidades o procesos autorizados, (ISO27001, 2017).

#### 1.3.1.2.2 Integridad de la Información

Es una de las condiciones de la información que garantiza que la información no ha fue manipulada o alterada desde el momento de su creación por lo cual la información es válida y original, (ISO27001, 2017).

#### 1.3.1.2.3 Disponibilidad de la información

Acceso y uso de la información en el momento oportuno y necesario siguiendo procedimientos correctos y los canales adecuados, (ISO27001, 2017).

#### 1.3.1.2.4 Confiabilidad de la información

Se refiere a la credibilidad que pueda tener la información que son proporcionados por una fuente de información, (ISO27001, 2017).

### 1.3.1.3 Ciclo de vida de la información

La información como cualquier activo de la organización, cumple un ciclo desde el momento de su adquisición hasta cuándo debe ser desechada. Es importante asegurar la calidad de los procesos durante su ciclo, (SERMAN, 2013).

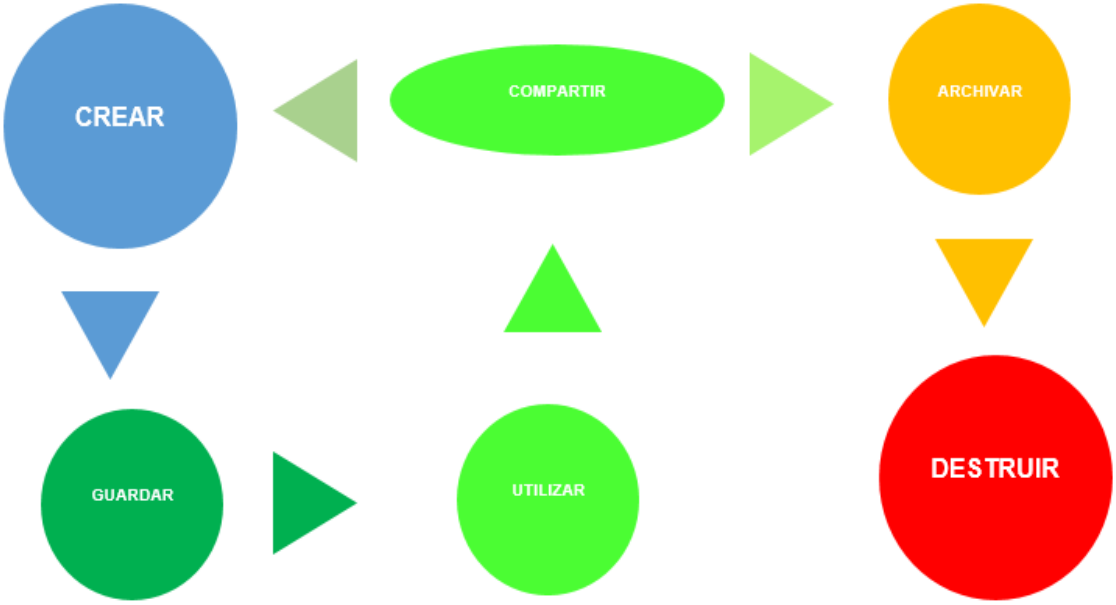



*Figura 7*. Ciclo de vida de la información, Fuente: (ISO27001, 2017).

#### 1.3.1.4 Activos de la información

Según (ISO27001, 2017), los activos de la información se refiere a los recursos del Sistema de Seguridad de la Información y pueden ser archivos, BD, contratos, manuales, software, aplicaciones y son necesarios para que la empresa funcione de manera adecuada, para conseguir los objetivos trazados por la alta dirección.

Los activos se encuentran expuestos a amenazas y vulnerabilidades

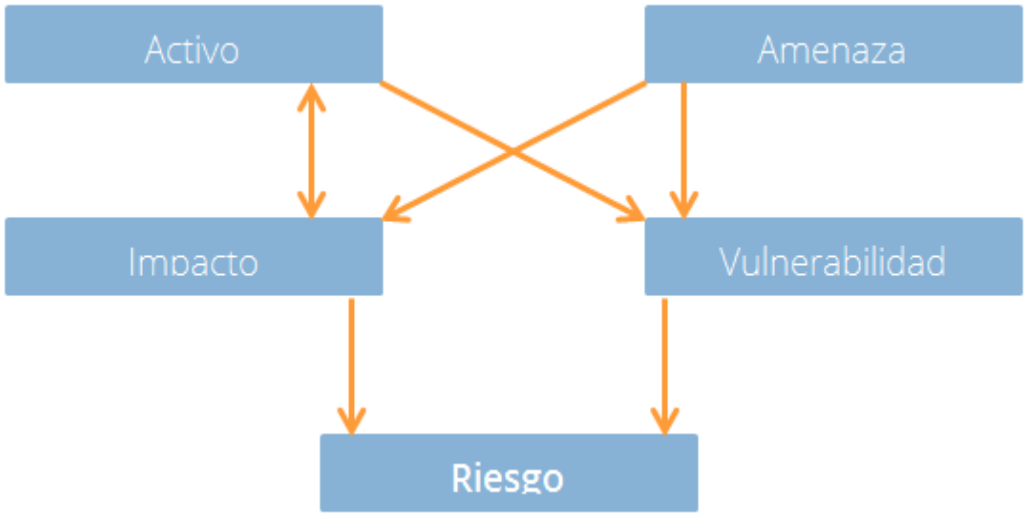



*Figura 8*. Activos de la Información, Fuente: (pmg-ssi, 2015).

#### 1.3.1.5 Vulnerabilidades

Joya & Sacristán, (2017), indican que según la norma ISO/IEC 27002 (2005), la vulnerabilidad es una fragilidad de algún activo, que puede ser explotado por una o más amenazas, incidiendo en la ruptura de uno o más principios de seguridad. Las vulnerabilidades están presentes en los propios activos, es decir, son inherentes a ellos, y pueden ser de orden tecnológico, humano, procesos y ambientes

#### 1.3.1.6 Amenazas

Las amenazas pueden provenir de diferentes formas, ya sean naturales o tecnológicas. La ISO/IEC 27002 (2005) define las amenazas de la SI que pueden generar un incidente no deseado, que puede dañar a un sistema o a la organización. Según esto, las amenazas son agentes o condiciones que causan incidentes que comprometen la información y sus activos a través de la explotación de vulnerabilidades.

#### 1.3.1.7 Incidentes de seguridad

Gómez,(2014), indica que de acuerdo a la norma ISO/IEC 27001:2013, un incidente de SI es reconocido como uno o más eventos inesperados y no deseados, y pueden tener la probabilidad de comprometer las operaciones o los procesos del negocio y amenazar la SI. Los incidentes son conceptuados como un acontecimiento que ocurre como consecuencia de la acción de una amenaza que explora una o más vulnerabilidades.

#### 1.3.1.8 Probabilidad

Konzen, (2013), define que en seguridad de la información la probabilidad es la posibilidad de que ocurra un incidente y asocia una escala de 0 a 1 a un evento que puede estar relacionado con una frecuencia de ocurrencia o un grado de confianza de que ocurrirá un evento.

#### 1.3.1.9 Impacto

Konzen, (2013), indica que el impacto se describe como el alcance de los daños

causados por un incidente de seguridad sobre uno o más procesos de negocio, en otras palabras, hace alusión directa a los posibles daños causados al negocio por un incidente de seguridad de la información. Estos perjuicios pueden significar pérdidas financieras, desgaste de la imagen, pérdida en la calidad de los servicios prestados, insatisfacción de los colaboradores y clientes, pérdida de recursos entre otros.

#### 1.3.1.10 Riesgos

La ISO/IEC 27001:2013, define el riesgo como la combinación de la probabilidad de un evento y de sus consecuencias. De esta manera, los riesgos pueden ser una oportunidad, una incertidumbre o una amenaza, (ISO27001, 2017).


*Figura 9*. Riesgos en la seguridad de la información. Fuente: (ISO27001, 2017).

### 1.3.2 Gestión de Riesgos en la Seguridad de la Información

De acuerdo a la investigación y a lo descrito en los puntos anteriores, se observa que las organizaciones a menudo están bajo riesgo. La presencia de estos, implica que las organizaciones deben gestionar los aspectos de la comunicación por sí mismos, identificando, analizando y posteriormente evaluando si dichos riesgos deben ser tratados o no.

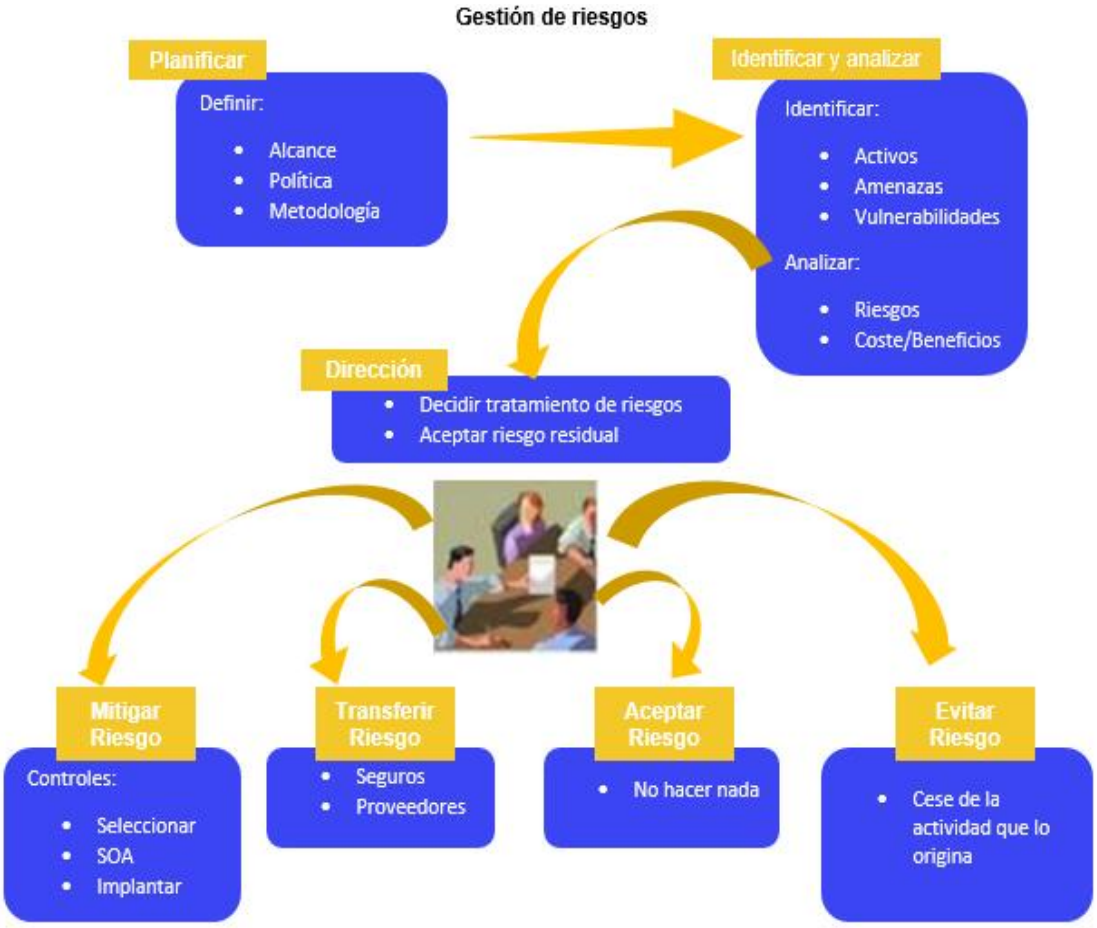



*Figura 10*. Gestión de riesgos. Fuente: (ISO27001, 2017).

### 1.3.3 Normativas para la gestionar la seguridad y los riesgos de la información

La importancia de la información dentro de una organización y su debida protección ante cualquier evento que puedan poner riesgo o peligro la continuidad de una organización, por lo cual se crearon normas que brinden una guía para la implementación de procesos para una correcta gestión de la SI y estas a su vez garanticen la SI mediante mejores prácticas.

Por lo consiguiente la ISO y IEC, crearon una familia de normas ISO/IEC 27000 las normas son un conjunto de estándares que describen procesos básicos para implantar un SGSI.

#### 1.3.3.1 Metodologías para el análisis de riesgos

Durante la implementación de un SGSI es muy importante seleccionar una

metodología para analizar y gestionar los riesgos el cual permite valorar los niveles de las amenazas y su impacto que puede ocasionar, para lo cual existen diversas metodologías como son Octave, MAGERIT, COSO, COBIT entre otras. La metodología MAGERIT sigue las siguientes fases, para la evaluación de los riesgos:

- Identificar activos más importantes de la empresa
- Identificar de manera clara las amenazas
- Crear un plan de control y salvaguardas
- Calcular los daños
- Calcular el riesgo

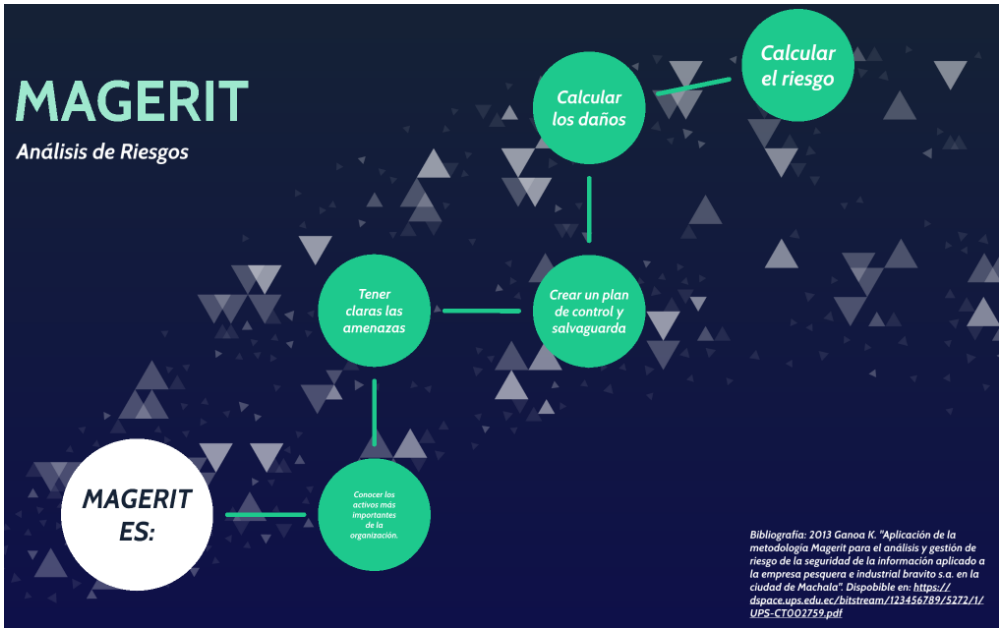



*Figura 11*. Análisis de Riesgos metodología MAGERIT. Fuente: *(Gaona, 2013)*

### 1.3.3.2 La familia de la norma ISO/IEC 27000

La ISO y la IEC, publicaron la primera versión de la familia de normas ISO/IEC 27000 el 01 de mayo del 2009, la norma mencionada es un conjunto de estándares de clase mundial, la cual, reemplazo a la norma BS7799-2.

La norma BS7799 fue un estándar publicado originalmente por BSI Group (BSI) en 1995 fue escrito por el Departamento de Comercio e Industria del Gobierno del Reino Unido (DTI).

La ISO/IEC 27000 tuvo varias modificaciones durante los siguientes años 2012, 2014, 2016, 2018, 2019 2020 siendo la última ISO/IEC 27000:2020, en la últimas modificaciones realizaron cambios a las siguientes normas ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27009 los cambios realizados fueron a temas de las especificaciones en los requisitos para acreditar a las organizaciones que brindan auditorías y certificación de SGSI el objetivo fue la refinación e la inclusión de los requisitos adicionales a los de la norma ISO/IEC 27001.

Mediante el uso de la familia de normas ISO/IEC 27000, cualquier organización puede implementar un marco para gestionar la seguridad de sus activos de información, como pueden ser: su información financiera, propiedad intelectual e información de los trabajadores o información que les confíen los clientes o terceros.

A continuación de muestra la evolución de la norma ISO 27001.


*Figura 12*. Historia de ISO 27001. Fuente: (ISO27001, 2017).

### 1.3.4 Objetivo del estándar ISO/IEC 27001

La ISO/IEC 27001 “En una norma internacional que permite asegurar, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan”, ISOTools (2019).

### 1.3.5 Gestión de la Calidad PDCA

La norma internacional ISO 27001 en su proceso de implementación está basado en el ciclo PDCA, más conocida como el ciclo de Deming, según (UNIR, 2019).

**(Planificar: Plan):** En esta etapa se establece el diseño del SGSI en donde se evalúa e identifica los riesgos asociados a la SI dentro de la organización.

**(Hacer: Do):** En esta etapa se implementa y se realiza la operación del SGSI definido.

**(Verificar: Check):** En esta etapa se realiza la revisión y evaluación de su eficacia y eficiencia. Si el cumplimiento no es el esperado se analiza las causas para determinar las mejoras.

**(Actuar: Act):** En esta etapa se mejora y mantiene la continuidad del SGSI.


*Figura 13*. Estructura general de la Norma ISO27001:2013. Fuente: (Mataracioglu, La versión 2013 de la norma ISO / IEC 27001, 2017).

La norma internacional ISO/IEC 27001, se compone de dos módulos relativamente distintos, en el primer módulo, se definen las reglas y los requisitos

que deben ser aplicables. Las Cláusulas del punto 4 al 10 son requisitos indispensables y no deben ser excluidas cuando la empresa declara conformidad con esta Norma. (ISO, 2014, pág. 10), El segundo módulo es el referente a los controles, designados como los puntos A.5 a A.18 en total 114 controles los cuales son directamente vinculados y alineados con el listado de la norma ISO/IEC 27002:2013, de las Cláusulas del 5 hasta el 18 (ISO, 2014, pág. 27). Estos objetivos de control enumerados en el Anexo A no todos son obligatorios y pueden ser utilizados de acuerdo a los objetivos y como controles adicionales, es decir la organización pueden usar los controles de acuerdo a sus riesgos identificados (ISO, 2014, pág. 16).

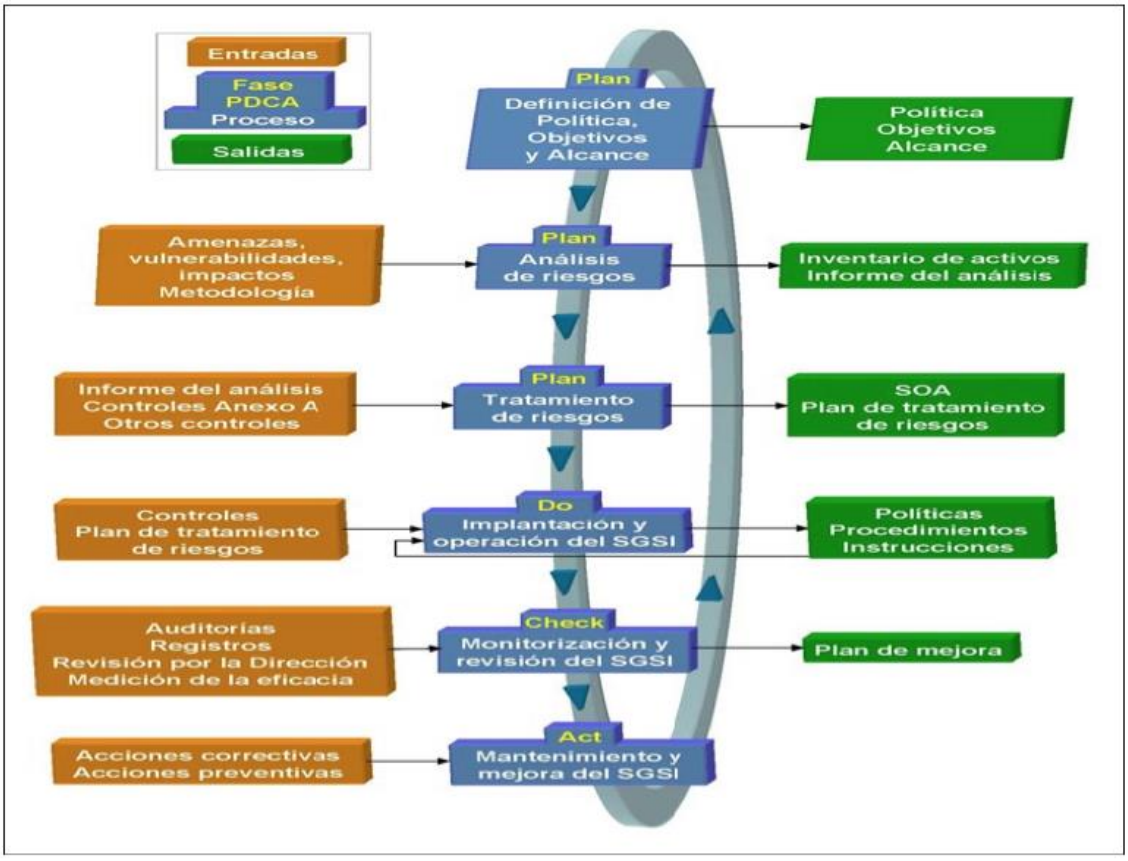



*Figura 14*. Proceso de planificación, ejecución, monitoreo y control con ISO 27001.Fuente: (Mantilla, Proceso de planificación, ejecución, monitoreo y control con ISO 27001, 2017, pág. 5).

### 1.3.6 Beneficios de la aplicabilidad de la norma ISO/IEC 27001

Al aplicar la norma ISO/IEC una organización puede tener muchos beneficios a continuación se puede mencionar algunos beneficios principales, (ISOTools,

2019).

#### 1.3.6.1 Cumplimiento

El cumplimiento es un acto de conformidad y es el primer beneficio que brinda la implementación de la norma 27001 dentro de la organización.

La norma ISO27001 es adecuada para apoyar al cumplimiento de los aspectos relaciones a la SI, (ISO27001, 2017).

#### 1.3.6.2 Ventaja competitiva

La competitividad es un aspecto muy importante dentro de una organización, la norma ISO 27001 ayuda a cumplir ese propósito a la organización. Una organización que dispone de SGSI conforme a la norma ISO 27001 le ofrece a la empresa tener una ventaja competitiva en cualquier ámbito como puede ser internacional, nacional, regional o local, (ISO27001, 2017).

#### 1.3.6.3 Descenso de los gastos por incidentes de seguridad

Para una correcta gestión de la SI es necesario establecer objetivos y medirlos. Cuando una organización establece objetivos claros son más fáciles medir y también se reduce en un porcentaje mayor en los incidentes generados en temas de seguridad de los activos de la organización.

La implementación adecuada de la norma ISO 27001 permite a la organización reducir los gastos por incidentes de SI, dichos beneficios no se evidencian en ganancias económicas, sino se evidencian cuando los gastos relacionados a los incidentes de seguridad disminuyen, (ISO27001, 2017).

### 1.3.7 Implementación de un SGSI

La implementación de un SGSI es la aplicación de estándares basados en buenas prácticas que incluyen la elaboración de documentación, procedimientos, instrucciones, herramientas y técnicas, además la elaboración de indicadores, registros y en la definición de un proceso educativo de concienciación de los empleados dentro de la organización (Córdoba, 2015).

El éxito de un SGSI comienza con la aplicación correcta de las recomendaciones de la norma ISO/IEC 27001:2013 y la alta dirección de la organización debe demostrar compromiso y liderazgo con respecto al SGSI, (ISO, 2013).

De acuerdo a la norma ISO,2014 el liderazgo y compromiso se debe demostrar dando cumplimiento a los siguientes puntos:

- Asegurar que los objetivos y las políticas de seguridad de la información, estén establecidos de manera clara y sean compatibles con los objetivos estratégicos de la empresa;
- Asegurar la integración de los requisitos del SGSI en los procesos de la empresa.
- Asegurar recursos necesarios para el SGSI estén disponibles.
- Difundir la importancia de la gestión de la seguridad de la información eficaz y de conformidad con los requisitos del SGSI.
- Asegurar que el SGSI alcance resultados deseados
- Orientar y apoyar a los empleados a que puedan contribuir a la eficacia del SGSI.
- Promover la mejora continua dentro de la empresa.

Teniendo en cuenta que la organización debe establecer, aplicar, mantener y mejorar de forma continua un SGSI, de acuerdo a los requisitos de la norma ISO/IEC 27001:2013, se debe aplicar un modelo de gestión que satisfaga este propósito (Córdoba, 2015).

El modelo PDCA (llamado ciclo de mejora continua de Deming), es una herramienta de gestión que favorece ese propósito, pues este modelo de gestión se basa en el ciclo de mejora continua.

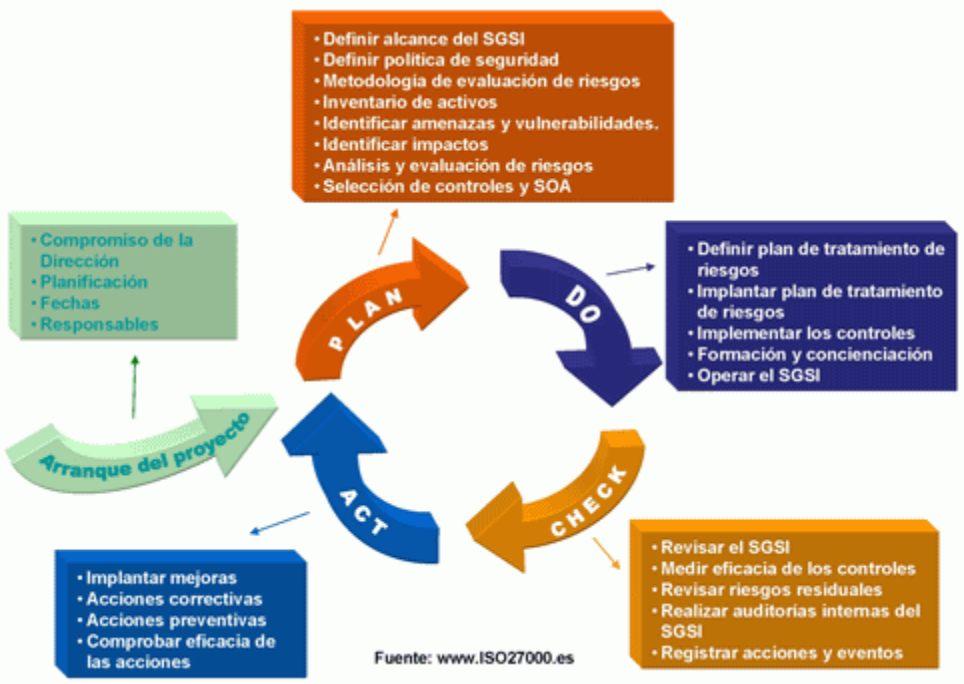



*Figura 15*. Proceso Implementación de SGSI. Fuente: (ISO27001, 2017).

### 1.3.8 Factores críticos para el éxito de la implementación de un SGSI

Al implementar un sistema de SI dentro de una empresa, debemos tener en cuenta que es un proceso transversal y participan todas las áreas de la organización.

Al ejecutar la implementación se estará difundiendo una imagen de cuidado en esta materia a todas las áreas de la organización para que tomen conciencia de la importancia de la SI y de esta manera disminuir cualquier riesgo al que puede estar sujeta la organización.

De esta manera la implementación de un sistema de SI cumplirá con los objetivos de la creación de una base de protección y confianza sobre la cual se desarrolla una actividad; señal clara e inequívoca de que la organización tiene preocupaciones fundamentales con la integridad y preservación de sus activos (ya sean procesos, servicios, información u otros).

**Norma técnica, ambiental, de seguridad, de gestión de riesgos**

**Norma Técnica**

En nuestro país la norma técnica peruana NTP–ISO/IEC 27001:2014 es una adecuación de la norma internacional ISO/IEC27001 la 2ª Edición, el órgano responsable es la OGEI (Oficina General de Estadística e Informática).

La norma mencionada tiene la finalidad de brindar los requisitos necesarios que permiten establecer, implementar, mantener y mejorar continuamente SGSI. La implementación de un SGSI es una decisión estratégica para una empresa.

**Impacto Ambiental**

La definición de políticas claras para la seguridad de la información dentro la empresa de seguros permitirá un ahorro significativo en los activos de la organización de esta manera la organización está comprometida al cuidado del medio ambiente cumpliendo la norma ISO 14001 – Sistemas de Gestión Ambiental.

**Gestión de riesgos**

**Seguridad y Salud Ocupacional**

La norma ISO27001 en su anexo A, específicamente en la sección A7(Seguridad relativa a los recursos humanos) al aplicar de manera correcta los controles de la SI de la sección A7.1(antes del Empleo), A7.2(durante el empleo) y A7.3 (después del empleo) la empresa cumplirá con las normas ISO 45001 referentes a la seguridad y salud ocupacional.

**Estado del Arte**

Cano & Almanza, (2020), de acuerdo al estudio realizado en Colombia para verificar la seguridad de la información, se observó que los siguientes sectores Financiero, Gobierno, Educación, Telecomunicaciones y Consultoría Especializada, tienen mayor interés por entender sus dinámicas en materia de seguridad y control.

El estudio también revela que las organizaciones sin importar el sector y tamaño, realizan inversiones de acuerdo a su realidad, el sector que realiza más asignaciones presupuestales es el financiero en relación con otros sectores de

la industria. La investigación también confirma que la tendencia de seguir asignando presupuestos al tema de SI se sostiene y que los montos mayoritariamente asignados en las pequeñas y medianas empresas en la realidad colombiana se encuentra por debajo de los $US 50.000 dólares y las grandes empresas con más de mil empleados se espera que sigan manejando montos por encima de los $US 100.000 dólares.

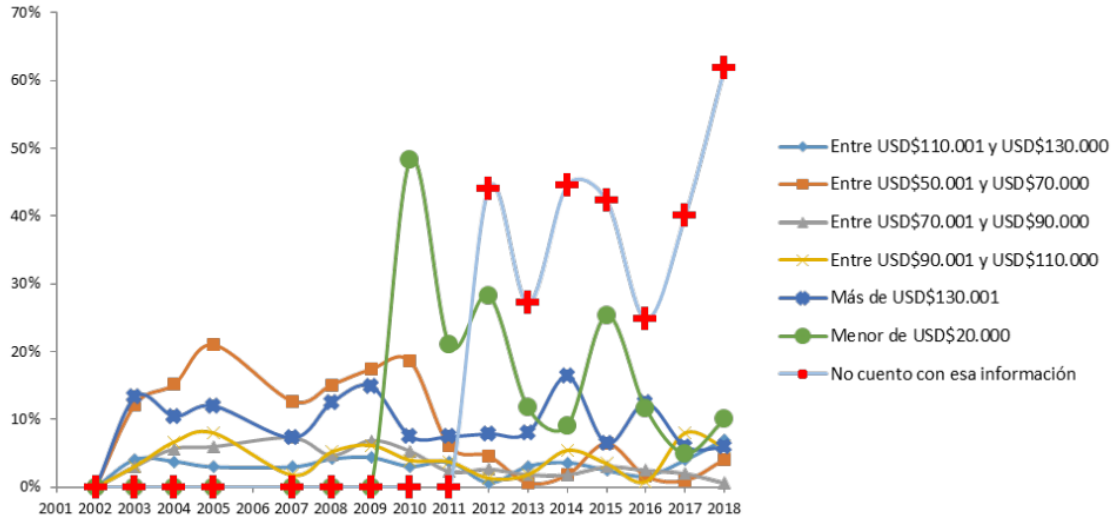



*Figura 16*. Ilustración de Presupuestos asignados-Colombia. Fuente: (Cano & Almanza, 2020, pág. 478).

Gil, (2019), en su artículo periodístico menciona que la ciberseguridad en el Perú avanza un paso, pero el cibercrimen avanza de manera más rápida de 2 a 3. En el año 2018 los ataques cibernéticos a las empresas crecieron en 600%, con respecto al año 2017, asimismo indica que el 70% de las empresas peruanas no ha realizado ningún análisis de vulnerabilidades a pesar del aumento de ataques.

También indica que las empresas han tomado con poca seriedad el tema de la SI, por lo cual una de cada cuatro empresas peruanas ha sufrido un ataque de virus.

Para poder contrarrestar el cibercrimen la implementación de la norma internacional de estandarización ISO27001 permitirá revisar y mejorar todos los procesos internos de la empresa para verificar que todo esté protegido.

**Definición de términos**

Tabla 2.

*Términos Seguridad de la Información*

| TERMINO | DESCRIPCIÓN |
|---|---|
| Activo | Recurso necesario que tiene la empresa con la finalidad de que estas funcionen de manera adecuada para conseguir los objetivos propuestos por la alta dirección.[a] |
| Amenaza | Cualquier acción que aprovecha la vulnerabilidad de un activo con la finalidad de causar daño. [b] |
| Control | Medio que permite gestionar los riesgos existentes para lo cual se incluyen las políticas, procedimientos y buenas prácticas que pueden ser técnicas, administrativas, gestiones contractuales. [c] |
| Declaración de aplicabilidad | Es un documento que permite establecer controles necesarios para gestionar los riesgos y es un requisito de la norma ISO/IEC27001. [d] |
| Impacto | El costo para una organización después de que un incidente se materialice y puede ser medido o no en términos estrictamente financieros o de imagen como puede ser la pérdida de reputación, implicaciones legales. [e] |
| Probabilidad | Frecuencia con que pueda ocurrir una amenaza. [f] |
| Riesgo | Posibilidad de que una amenaza se pueda materializar al aprovechar una vulnerabilidad con la finalidad de causar daño o pérdida en cualquier activo de la organización. [g] |
| Vulnerabilidad | Debilidad de un activo de una organización que puede ser aprovechada por una amenaza. [h] |

| | |
|---|---|
| SI | Seguridad de la información [i] |
| SGSI | Sistema de gestión de la seguridad de la información [j] |
| MINHAP | Ministerio de Hacienda y Administraciones Públicas [k] |

*Nota:* Tomado de [a] (OBS, 2020), [b] (ISOWin, 2020), [c] falta [d] (Escuela Europea de Excelencia, 2019), [e] (pmg-ssi, 2015), [f] (ESAN, 2018), [g] (NovaSec, 2018), [h] (INCIBE, 2017), [ij] (iso27000, 2020), [k] (PAE, 2020).

Tabla 3.

*Normas Internacionales*

| TERMINO | DESCRIPCIÓN |
|---|---|
| IEC | Comisión Electrotécnica Internacional. [a] |
| ISO | Organización Internacional de normalización. [b] |
| Estándar | Documentos o prácticas que contienen un fin en común con la finalidad de ser usado como regulación, guía para las necesidades que son demandadas en la sociedad, tecnología, etc. [c] |
| ISO27000 | Conjunto de normas desarrollados que están siendo modificados de manera constante por las organizaciones ISO e IEC, con la finalidad de proporcionar un marco de trabajo en la gestión de la SI para cualquier tipo y/o tamaño de organización. [d] |
| ISO27001 | Norma principal de la serie 27000 que contiene los requisitos para la gestión de los sistemas de SI. [e] |
| ISO27002 | Guía de buenas prácticas que contiene los objetivos de control y los controles necesarios y recomendables en cuanto a la seguridad de la información. [f] |
| ISO27005 | Guía que tiene la finalidad de proporcionar directrices para la gestión de riesgo en la seguridad de la información. [g] |

| | |
|---|---|
| Ley 29733 | La presente legislación instituye obligaciones sobre las organizaciones para que puedan brindar un adecuado tratamiento a los datos personales de sus empleados, clientes proveedores y otras personas vinculadas a su actividad. [h] |

*Nota*: Dato tomado de [a,b,c,d,e,g](ISO27000, 2020), [h] (CAL, 2020)

**Estudio Económico**

Actualmente la organización posee los recursos adecuados para la implementar el SGSI basado en los estándares de la norma ISO27001.

El objetivo primordial de la implementación es proteger la información de la empresa, por lo cual en la factibilidad económica se está considerando los costos que puedan generar la implementación y mantenimiento del mismo.

Los costos necesarios para la implementación serian en:

- Recursos Humanos
- Recursos Técnicos
- Normas Técnicas

## 1.4 Formulación del problema.

¿De qué manera el desarrollo de un plan de seguridad de la información basado en estándares internacionales ayudará en la seguridad de la información a la empresa de Seguros?

## 1.5 Justificación e importancia del estudio.

Dentro de una organización la información es un recurso clave para la toma de decisiones y es uno activo muy importante de la empresa de Seguros, por lo cual la seguridad de la información, es uno de los factores más importantes para asegurar la continuidad del negocio.

La empresa de seguros no cuenta con normas internacionales que permitan resguardar su información, por lo cual la investigación tiene como finalidad la

posibilidad de implementar la norma internacional de seguridad de la información ISO/IEC 27001. Que permitirá establecer metodologías, prácticas y procedimientos que ayudarán a proteger la información de la empresa como activo valioso, y también permitirá minimizar amenazas y riesgos a los que está expuesta la organización.

### 1.5.1 Justificación Tecnológica:

El estudio contribuye al uso de normas de seguridad con estándares internacionales actualizados e innovadores que permitirán mejorar la competitividad a la empresa; las empresas de seguros brindan diversos servicios y elaboran planes estratégicos con la finalidad de cumplir sus objetivos de negocio, pero la falta en la seguridad de la información puede ser muy perjudicial, por lo cual se debe considerar la implantación de controles que permitan garantizar la calidad en sus servicios y proteger información personal.

### 1.5.2 Justificación Operativa:

El estudio brinda una solución que entrega mejoras de manera continua, se recomienda que la empresa opte por un plan de seguridad de la Información basado en normas internacionales como la ISO27001, debido a que la norma ayuda a mejorar el control de amenazas y vulnerabilidades existentes de una empresa; por tanto, se puede ir mejorando varios aspectos de la seguridad de la información a medida que el sistema implementado tome mayor madurez.

### 1.5.3 Justificación Social:

Se justifica porque se podrá tener un enfoque más claro y en forma general de los aspectos relacionados a la seguridad de la información dentro de la empresa, en un futuro, resultaría adecuado, ya que de manera progresiva mejorará la SI al ampliar más controles que proporciona la norma ISO2700, pero también dependerá de la adaptación del cambio dentro de tal organización.

### 1.5.4 Justificación Económica:

La justificación económica es viable, ya que la empresa cuenta con los recursos necesarios y adecuados, en caso se necesite algún recurso complementario el

costo es factible y no excede los límites considerados.

## 1.6 Hipótesis.

Mediante el desarrollo del Plan de seguridad de la información basado en estándares internacionales se logrará mejorar la seguridad de la información en la empresa de seguros.

## 1.7 Objetivos.

### 1.7.1 Objetivo General

Desarrollar un plan de seguridad de la información basado en estándares internacionales para la empresa de seguros, que permitirá mejorar la integridad, confidencialidad y disponibilidad de la información en la empresa de Seguros.

### 1.7.2 Objetivos específicos

1. Evaluar el estado actual con respecto a las normas de seguridad de la información.
2. Identificar vulnerabilidades y amenazas en el área de sistemas
3. Elaborar el plan de seguridad de la información basado en normas internacionales para área de tecnologías de la información en beneficio de la empresa de seguros.

# II. MATERIAL Y MÉTODOS

## 2.1 Tipo y diseño de investigación.

### 2.1.1 Tipo de investigación:

La Investigación Aplicada se centra en la solución de problemas en un contexto determinado, es decir, busca la aplicación o utilización de conocimientos, desde una o varias áreas especializadas, con el propósito de implementarlos de forma práctica para satisfacer necesidades concretas, proporcionando una solución a problemas del sector social o productivo, según (CRAI, 2018).

Por lo antes mencionado, esta investigación es descriptiva y aplicada, porque tiene como propósito diseñar un plan de SGSI dentro de la empresa de seguros, tomando como base los riesgos de seguridad a los que está expuesto la empresa, la finalidad es brindar una solución innovadora, para la mejora de la seguridad de la información.

### 2.1.2 Diseño de la investigación:

La investigación corresponde al tipo de diseño cuasi experimental, debido a la relación de las variables presentes en la investigación como se muestra en cuadro de la operacionalización de variables, la investigación se apoyará en un análisis estadístico de la muestra en estudio.

## 2.2 Población y muestra

### 2.2.1 Población

En la investigación, la población estuvo conformado por el personal del área de sistemas y personal administrativo de la empresa de seguros.

### 2.2.2 Muestra

Se utilizó un muestreo de tipo no probabilístico, con juicio de experto, la cual estuvo conformado por los 25 trabajadores de la empresa de Seguros.

## 2.3 Variables y operacionalización.

| Variable | Definición Conceptual | Dimensión | Indicador | Técnicas De Recolección de información | Instrumentos de Recolección de información |
|---|---|---|---|---|---|
| **Independiente**<br><br>**Seguridad de la información** | La Seguridad de la Información se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, | Confidencialidad | Cantidad de información difundida<br>Cantidad de incidentes informados y atendidos<br>Tiempo de respuesta para la atención de incidentes | Encuesta<br><br>Observación | Cuestionario<br><br>Guía de observación |
| | | Disponibilidad | Cantidad de tiempo de que la información está disponible para el usuario | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | Identificar los activos críticos de la organización. Identificar riesgos que afectan los activos. | | |
| | | Integridad | Establecer controles en función de los riesgos detectados y mejoras en los sistemas | | |
| **Dependiente** **Estándares** | La ISO/IEC 27001 es una norma internacional de Seguridad de la Información que perite el aseguramiento **de la confidencialidad, integridad y disponibilidad de la** | Alcance | Cumple con la documentación para el Sistema de Gestión de Seguridad de la Información Respuesta ante incidentes | Encuesta Entrevista Análisis Documental | Cuestionario Guía de Entrevista Guía de Revisión documental |

| | | | |
|---|---|---|---|
| | **información** de una organización y de los sistemas y aplicaciones que los procesan, según (ISO27001, 2017). | Análisis de riesgo | Analizar riesgos |
| | | | Tratamiento de Riesgos |
| | | Controles de seguridad | Definir políticas de seguridad |
| | | | Establecer controles de seguridad |

**Fuente:** Elaboración propia

## 2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

### 2.4.1 Técnicas de recolección de información

Se utilizaron las siguientes técnicas de recolección de información:

- Observación
- Entrevistas
- Encuestas
- Revisión Documental

### 2.4.2 Instrumentos de recolección de Información

#### 2.4.2.1 Guía de Observación

a) Formato de observación de riesgos de la seguridad de la información
El formato permitió evaluar los riesgos actuales concernientes a la seguridad de la información de la empresa de seguros, se aplicó al área de sistemas en el proceso de control de accesos, escritorios limpios y seguridad física, la observación se realizó en dos oportunidades la frecuencia fue semanal. Ver Anexo 4.

#### 2.4.2.2 Guía de entrevista

a) La entrevista se realizó a un especialista en temas de Seguridad de la Información, para poder determinar aspectos de la propuesta relacionados a la norma internacional ISO27001.

#### 2.4.2.3 Cuestionarios

a) Se aplicó una encuesta diseñada en un formulario web que consta de 15 preguntas cerradas, a 25 empleados de la empresa la finalidad fue determinar los riesgos y vulnerabilidades a los que está expuesta la empresa de estudio. Ver (Anexo 3).

#### 2.4.2.4 Guía de Análisis Documental

a) Se realizó la revisión documental de la norma internacional ISO-IEC 27001:2013 es el instrumento guía para el desarrollo del diseño del Sistema de Gestión de Seguridad de la Información para la empresa de seguros.

### 2.4.3 Confiabilidad de los instrumentos

Los resultados obtenidos mediante los cuestionarios utilizando el método de medición de la escala Likert, se codificó y se preparó cuadros estadísticos correspondientes, para obtener valores absolutos y relativos, se trabajó en la hoja de cálculo de Microsoft Excel para efectuar los cálculos mediante el coeficiente de Alfa de Cronbach mediante la siguiente función, (González & Pazmiño, 2015, pág. 68).

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

Dónde:

α = Alfa de Cronbach

K = Número de Ítems

$V_i$ = Varianza de cada Ítem

$V_t$ = Varianza del total

El resultado obtenido fue de 0.70 lo que determina la confiabilidad del instrumento.

### 2.4.4 Validación de los instrumentos

Para la validación de los instrumentos se utilizó el juicio de expertos (profesionales de ingeniería de sistemas relacionados a temas de seguridad de informática.

## 2.5 Procedimiento de análisis de datos.

Para la evaluación del estado actual con respectos a las normas actuales de seguridad de la información de la empresa de Seguros, se utilizó una guía de observación tomando como referencia el documento ISO27k_ISMS_and_controls_status_with_SoA_and_gaps_Spanish.xlsx, pestaña-Req. Obligatorios SGSI los requisitos mencionados en el documento mencionado permite evaluar el estado inicial en cuanto a la norma ISO27001, asimismo se utilizó una guía de observación del Anexo 10, para realizar el inventario de activos del área de tecnología de información.

Para la identificación de las vulnerabilidades actuales a los que está expuesto la organización específicamente el área de sistemas, se utilizó un cuestionario con 15 preguntas cerradas. El cuestionario fue aplicado a 25 empleados de la empresa de seguros, mediante un formulario web. Ver Anexo 3.

Para del plan de seguridad de la información, basado en estándares internacionales, apropiados para el beneficio de la empresa de seguros, se realizó una entrevista a un especialista con conocimientos en la norma internacional ISO27001:2013 y también se realizó la revisión documental de la norma internacional ISO27001:2013.

## 2.6 Criterios éticos.

En la investigación, se aplicó principios éticos citados en el Informe Belmont, sobre los que se basan las normas de conducta ética.

### Ética de seleccionar problemas y modelos

Desde el punto de vista ético la información que se presenta en la investigación es verídica y la información obtenida es real, la recolección de datos se obtuvo en el lugar de estudio con el propósito de dar una solución al problema planteado.

### Principio de Beneficencia

La teoría principal de este principio es no hacer daño, se tomó en cuenta este principio para poder aplicar a la investigación por lo consiguiente se consideró el bienestar de los participantes en la investigación, por el contrario, los participantes en la investigación fueron beneficiados con nuevos conocimientos en normas internacionales referidos a la seguridad de la información.

### Principio de respeto a las personas

En la investigación se aplicó este principio, porque la investigación protege la autonomía de los participantes y se les trató con respeto y cortesía asimismo fueron informados cuales son los objetivos de la investigación, con la finalidad de que los participantes estén informados y puedan tomar una adecuada

decisión y de manera voluntaria.

**Principio de Justicia**

Este principio garantiza un trato justo y sin perjuicios a los participantes de la investigación. Por lo consiguiente en la investigación hubo una selección justa y no hubo ninguna discriminación de los participantes, todos tuvieron un trato justo y equitativo durante el desarrollo de la investigación.

## 2.7 Criterios de rigor científico

En la investigación se consideraron los siguientes criterios de rigor científico

**Validez:** La adecuada operacionalización de las preguntas de investigación, de forma que las variables que se estudian sea relevantes y abarquen todas las dimensiones que incorporan las preguntas de la investigación, (Méndez, 2018).

**Fiabilidad:** Mediante los instrumentos utilizados en la investigación se podrán obtener las mismas respuestas en más de una oportunidad.

**Replicabilidad:** La investigación se puede volver a repetir sin que los resultados se contradigan.

# III. RESULTADOS

## 3.1 Resultados en Tablas y Figuras

### 3.1.1 Estado actual con respecto a las normas de seguridad de la información de la empresa de seguros.

Para verificar el estado actual de la seguridad de la información en la empresa de seguros, frente a los requerimientos obligatorios de la norma ISO 27001:2013, se realizó mediante una encuesta que se encuentra ubicado en el Anexo 3 del documento a 25 empleados y una guía de observación, tomando como base los requisitos exigidos por la norma internacional en seguridad de la información ISO27001 y los resultados de la evaluación se presentaron de dos maneras (Descriptiva y Cuantitativa) Ver Tabla 4.

El resultado de la Tabla 4 se obtuvo al realizar el análisis de la información de la evaluación inicial que se encuentra en el Anexo 4.

Tabla 4.

*Evaluación del estado inicial de la empresa de seguros con respecto a los requerimientos obligatorios de la norma internacional 27001:2013*

| SECCIÓN | REQUERIMIENTOS ISO 27001 | % CUMPLIMIENTO |
|---|---|---|
| 4 | Contexto de la organización [a] | 20% |
| 5 | Liderazgo [b] | 25% |
| 6 | Planificación [c] | 20% |
| 7 | Soporte [d] | 30% |
| 8 | Operación [e] | 15% |
| 9 | Evaluación del desempeño [f] | 20% |
| 10 | Mejora [g] | 25% |

*Nota:* Tomado de [a,b,c,d,e,f,g](ISOTools, 2020).

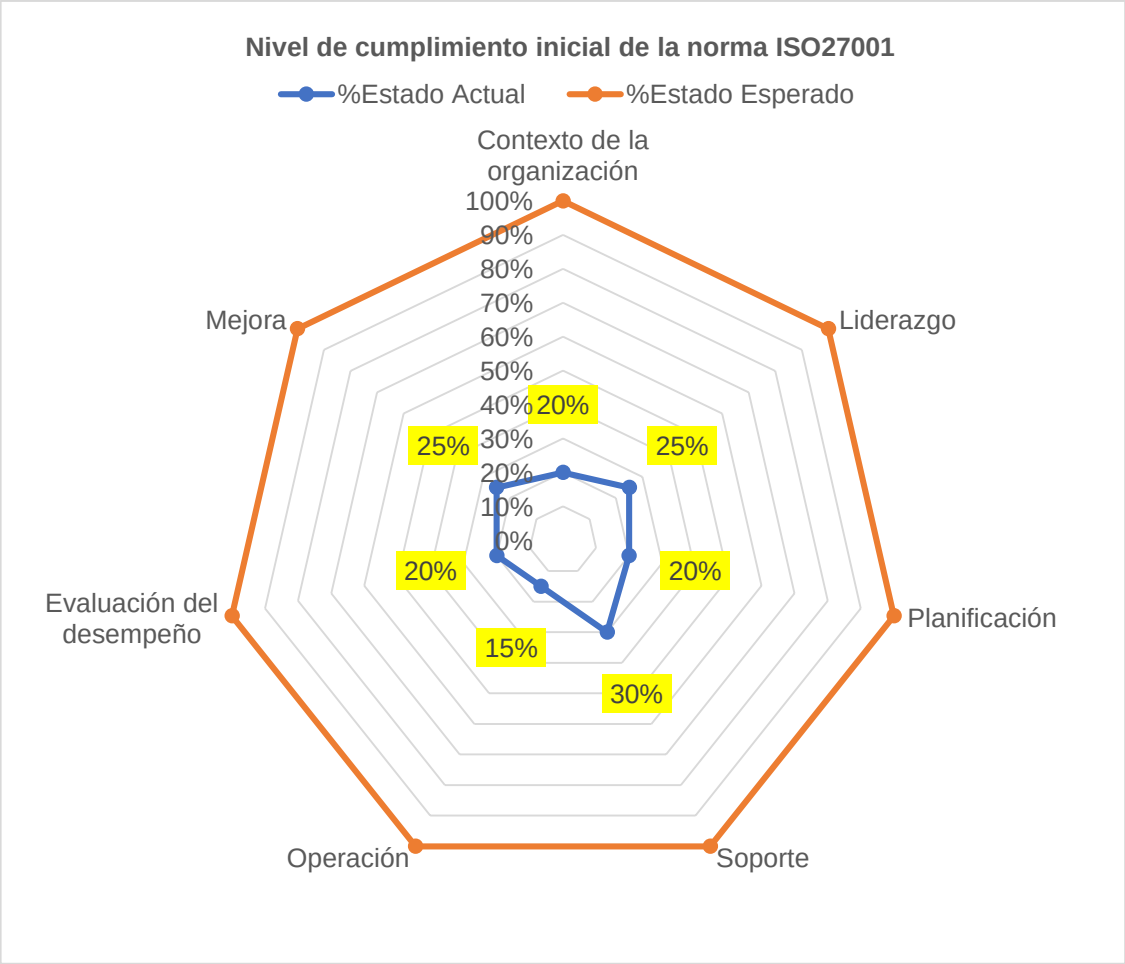



*Figura 17*. Cumplimiento de los requerimientos de la norma ISO27001. Fuente: Elaboración propia con datos tomados de (ISOTools, 2020).

Los resultados del grafico anterior muestran que la empresa de seguros al no contar con un plan de seguridad de la información, tiene un porcentaje mínimo en el cumplimiento de los requerimientos obligatorios de la norma ISO27001:2013.

Para medir el nivel inicial en la aplicación de controles de la norma ISO27001, se analizaron los resultados obtenidos mediante la encuesta a los 25 empleados, se muestran en la siguiente tabla.

Tabla 5.

*Evaluación inicial de controles aplicados de la norma ISO27001*

| Sección | Controles de Seguridad de la Información | Estado Actual | GAP | Estado Esperado | Nivel |
|---|---|---|---|---|---|
| A5 | Políticas de seguridad de la información | 10% | 90% | 100% | Repetible |
| A6 | Organización de la seguridad de la información | 10% | 90% | 100% | Repetible |
| A7 | Seguridad relativa a los recursos humanos | 40% | 60% | 100% | Repetible |
| A8 | Gestión de activos | 15% | 85% | 100% | Repetible |
| A9 | Control de acceso | 60% | 40% | 100% | Definido |
| A10 | Criptografía | 10% | 90% | 100% | Repetible |
| A11 | Seguridad física y del entorno | 20% | 80% | 100% | Repetible |
| A12 | Seguridad de las operaciones | 50% | 50% | 100% | Definido |
| A13 | Seguridad de las comunicaciones | 20% | 80% | 100% | Repetible |
| A14 | Adquisición, desarrollo y mantenimiento de los sistemas de información | 20% | 80% | 100% | Repetible |
| A15 | Relación con proveedores | 20% | 80% | 100% | Repetible |
| A16 | Gestión de incidentes de seguridad de la información | 50% | 50% | 100% | Definido |
| A17 | Aspectos de seguridad de la información para la gestión de la continuidad de negocio | 15% | 85% | 100% | Repetible |
| A18 | Cumplimiento | 20% | 80% | 100% | Repetible |

| | | |
|---|---|---|
| Promedio de Clausulas | 26% | Repetible |

*Nota:* Datos tomados de (ISO27002, 2013). Fuenta: Elaboración propia.

Según los resultados de la tabla anterior la empresa tiene un promedio de cumplimiento al 26% de los controles del anexo A de la norma ISO27001.

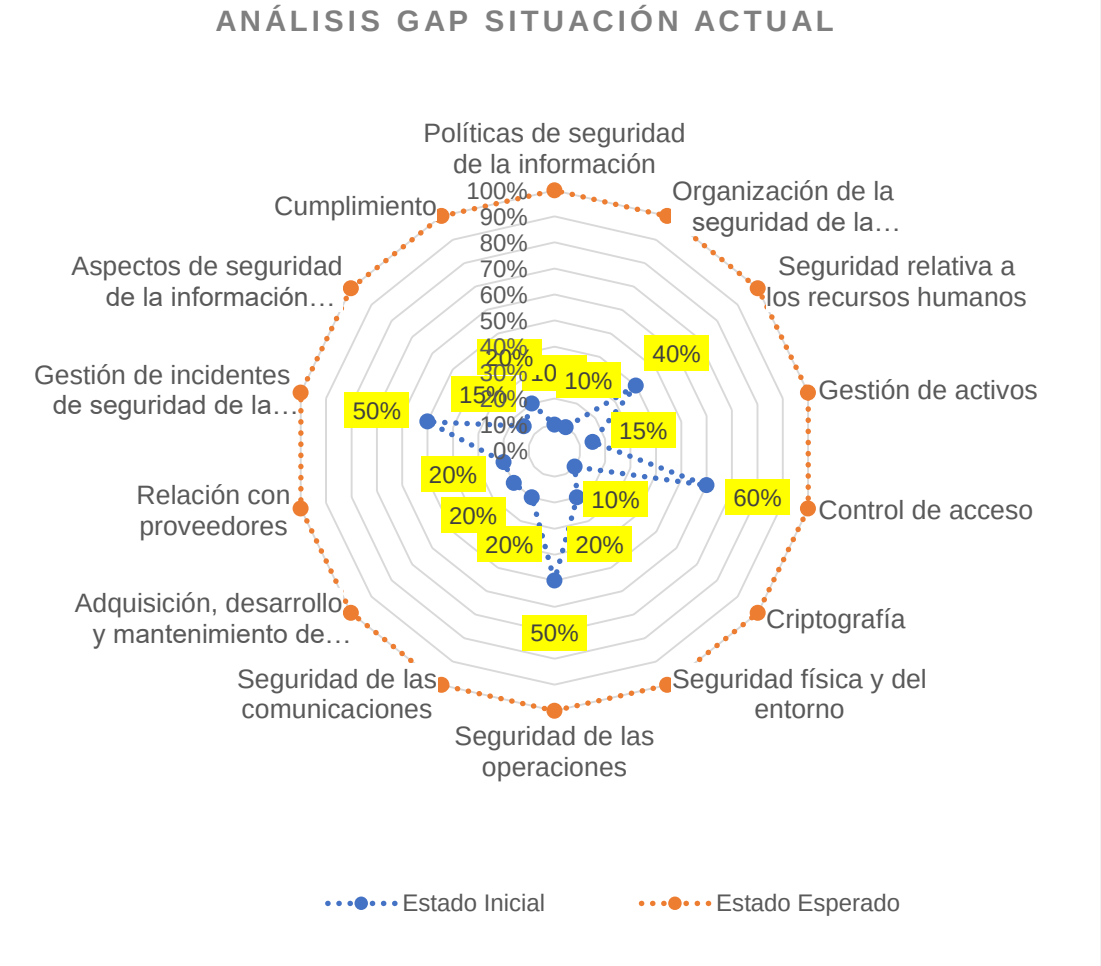



*Figura 18.* Análisis Inicial de brecha en seguridad de la información. Fuente: Elaboración propia con datos tomados de la norma (ISO27002, 2013).

Los resultados que muestra la figura anterior evidencian que algunos dominios del anexo A, tienen controles implementados en un porcentaje alto, como en los dominios de control de acceso, seguridad de las operaciones y gestión de incidentes de la seguridad.

Los controles que cuenta con un porcentaje mínimo de cumplimiento se debe al desconocimiento de la norma y por lo consiguiente es necesario seguir

mejorando en la aplicación de los demás controles de manera escalonada hasta completar el nivel esperado de acuerdo a la declaración de aplicabilidad que se encuentra en el Anexo 15, con la finalidad de mejorar la seguridad de la información dentro de la empresa.

Para la evaluación de riesgos, amenazas y vulnerabilidades a los que está expuesto los activos ubicados en el área se sistemas.

Se realizó el levantamiento de la información mediante la guía de observación, el documento mencionado ayudó a realizar el inventario de los activos de la empresa el documento se encuentra en el Anexo 10 y también se analizó la información de la encuesta del Anexo 3.
Para poder evaluar los riesgos, vulnerabilidades y amenazas a las que está expuesto los activos de la empresa se realizó mediante la siguiente metodología.

### 3.1.2 Metodología para el análisis de riesgos, vulnerabilidades y amenazas de los activos del área de sistemas

Para realizar el análisis de los riesgos, vulnerabilidades y amenazas a lo que están expuestos los activos de la empresa, se utilizó la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), el cual permite medir los niveles de impacto, criterios para aceptar el riesgo y tipos de impacto y otros elementos a evaluar.

La metodología MAGERIT, considera los siguientes objetivos principales

Tabla 6.

*Objetivos de la Metodología MAGERIT control de riesgos.*

| Objetivos | Descripción |
|---|---|
| Directos | Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos. [a]<br>Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC). [b] |

| | |
|---|---|
| | Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos. [c] |
| Indirectos | Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. [d] |

*Nota:* Datos tomados de [a,b,c,d]MINHAP Libro I Magerit versión 3.0, (2012, pág. 8)

La metodología MAGERIT considera dos importantes tareas:

- Analizar los riesgos (Califica el riesgo de acuerdo a la cantidad de las consecuencias)
- Tratar los riesgos encontrados (Que acciones se necesita para mitigar los riesgos encontrados)

**Inventario de activos de la empresa**

La metodología MAGERIT indica que para poder llevar a cabo una evaluación de los riesgos, amenazas y vulnerabilidades se necesita conocer los tipos de activos con las que cuenta la empresa, con la finalidad de realizar la valoración correspondiente y de acuerdo al valor establecido se debe evaluar cómo afectaría a la organización su pérdida o degradación.

La metodología MAGERIT clasifica los activos que cuenta la empresa mediante una serie de identificadores en la siguiente tabla, se muestra la clasificación de activos por tipo.

Tabla 7.

*Tipos de Activos*

| **Tipos de activos** | |
|---|---|
| [D] | Datos/Información |
| [K] | Claves Criptográficas |
| [S] | Servicios |
| [SW] | Software - Aplicaciones informáticas |
| [HW] | Equipamiento informático (hardware) |

| | |
|---|---|
| [COM] | Redes de comunicaciones |
| [Media] | Soportes de información |
| [AUX] | Equipamiento auxiliar |
| [L] | Instalaciones |
| [P] | Personal |

*Nota***:** Datos tomados de MINHAP, Libro II MAGERIT versión 3.0., (2012, págs. 8-13).

Para poder dar valoración a los activos es necesario tener en cuenta las dimensiones de valoración, los cuales hacen valioso a un activo.

Las dimensiones son utilizadas para valorar la consecuencia de materialización de una amenaza, la valoración que recibe un activo en una dimensión determinada es la medida de perjuicio para la empresa si el activo sufre algún daño en dicha dimensión.

Tabla 8.

*Dimensiones de valoración de la seguridad de la información*

| **Dimensiones de la seguridad** | |
|---|---|
| [D] | Disponibilidad |
| [I] | Integridad de los datos |
| [C] | confidencialidad |
| [A] | Autenticidad |
| [T] | Trazabilidad |

*Nota*: Datos tomados de MINHAP, Libro II MAGERIT versión 3.0., (2012, págs. 15-16).

**Valorar Activos**

La metodología MAGERIT clasifica de dos maneras la valoración de los activos, la cualitativamente y cuantitativamente. La cualitativa permite realizar el cálculo del valor del activo en base al impacto que pueda causar a la organización y la cuantitativa estima el costo del activo.

**Identificar amenazas**

Las amenazas son acciones que aprovechan vulnerabilidades de un activo con la finalidad de causar daños a los activos de la empresa.

MAGERIT cuenta con un catálogo de amenazas más comunes que puedan afectar la SI, en la siguiente tabla se muestran las amenazas más comunes.

Tabla 9.

*Listado de amenazas de los activos*

| | **Amenazas** | **Dimensiones Afectadas** |
|---|---|---|
| **[N]** | **Desastres naturales** | |
| [N.1] | Fuego | [D] |
| [N.2] | Daños por agua | [D] |
| [N.*] | Desastres naturales | [D] |
| **[I]** | **De origen industrial** | |
| [I.1] | Fuego | [D] |
| [I.2] | Daños por agua | [D] |
| [I.*] | Desastres industriales | [D] |
| [I.3] | Contaminación mecánica | [D] |
| [I.5] | Avería de origen físico o lógico | [D] |
| [I.6] | Corte del suministro eléctrico | [D] |
| [I.7] | Condiciones inadecuadas de temperatura o humedad | [D] |
| [I.8] | Fallo de servicios de comunicaciones | [D] |
| [E] | Errores y fallos no intencionados | |
| [E.1] | Errores de los usuarios | [C], [I], [D] |
| [E.2] | Errores del administrador | [C], [I], [D] |
| [E.3] | Errores de monitorización (log) | [I], [T] |
| [E.4] | Errores de configuración | [I] |
| [E.7] | Deficiencias en la organización | [D] |
| [E.8] | Difusión de software dañino | [C], [I], [D] |
| [E.15] | Alteración accidental de la información | [I] |

*Nota:* Datos tomados de MINHAP, Libro II MAGERIT versión 3.0., (2012, págs. 15-36).

**Valorar amenazas**

La metodología MAGERIT, para poder determinar una valoración apropiada de las amenazas, es necesario establecer la frecuencia que ocurre dicho evento, para lo cual se establece una escala con su respectiva valoración en la siguiente tabla.

Tabla 10.

*Probabilidad de ocurrencia de amenazas*

| Abreviatura | Frecuencia | Rango | Valor |
|---|---|---|---|
| MA | Muy frecuente | A diario | 100 |
| A | Frecuente | Semanalmente | 75 |
| M | Normal | Mensualmente | 50 |
| B | Poco frecuente | Semestralmente | 10 |
| MB | Muy Poco Frecuente | Anualmente | 5 |

*Nota:* Datos tomados de MINHAP, Libro I MAGERIT versión 3.0., (2012, pág. 28).

Se considera riesgo a la medida del daño posible sobre un sistema. Al conocer el impacto de una amenaza sobre uno o más activos, es claro derivar el riesgo sin necesidad de tener en cuenta la probabilidad de que ocurra.

Para poder medir cuál es el nivel probable de daño se realiza el siguiente calculo.

Riesgo=Probabilidad x Impacto

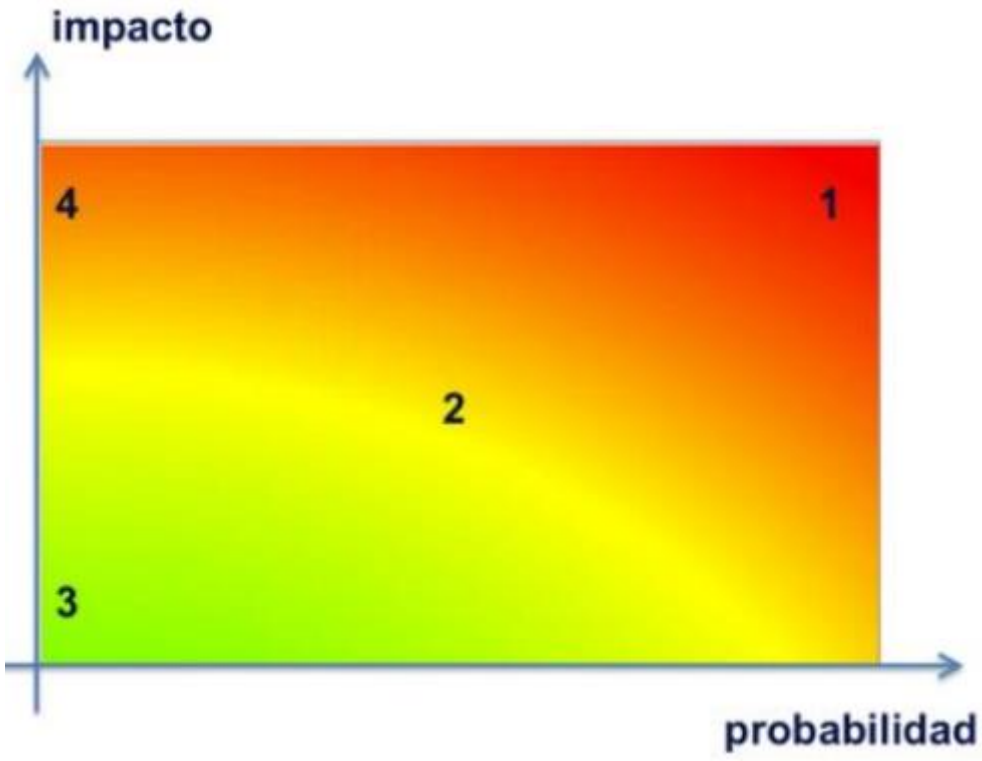



*Figura 19*. El riesgo en función del impacto y la probabilidad. Fuente: (MINHAP, Libro I MAGERIT versión 3.0., El riesgo en función del impacto y la probabilidad 2012, pág. 30)

El riesgo aumenta con el impacto y la probabilidad de ocurrencia, por lo cual la metodología de evaluación de riesgos MAGERIT, clasifica en cuatro zonas el tratamiento de los riesgos.

Zona 1 – riesgos muy probables y de muy alto impacto(MA), (MINHAP, 2012, pág. 29).
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 (M), (MINHAP, 2012, pág. 29).
Zona 3 – riesgos improbables y de bajo impacto (B, MB), (MINHAP, 2012, pág. 30).
Zona 4 – riesgos improbables, pero de muy alto impacto(A), (MINHAP, 2012, pág. 30).

Para evaluar el impacto y la probabilidad de los riesgos se hará uso de la siguiente matriz de riesgos.

Tabla 11.

*Matriz de estimación cualitativa de riesgos*

| **RIESGO** | | **PROBABILIDAD** | | | | |
|---|---|---|---|---|---|---|
| | | MB | B | M | A | MA |
| 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 |

*Nota:* Datos tomados de MINHAP, Libro III MAGERIT versión 3.0., (2012, pág. 7)

**Salvaguardas**

Las salvaguardas son un conjunto de medidas preventivas que se pueden realizar mediante procedimientos o instrumentos tecnológicos con la finalidad de reducir los riesgos.

Tabla 12.

*Clasificación de Salvaguardas*

| IDENTIFICADOR | DESCRIPCIÓN |
|---|---|
| H | Protecciones generales |
| D | Protección de los datos / información |
| K | Protección de las claves criptográficas |
| S | Protección de los servicios |
| SW | Protección de las aplicaciones (software) |
| HW | Protección de los equipos (hardware) |
| COM | Protección de las comunicaciones |
| IP | Protección en los puntos de interconexión con otros sistemas |
| MP | Protección de los soportes de información |
| AUX | Protección de los elementos auxiliares |
| L | Seguridad física – Protección de las instalaciones |
| PS | Protecciones relativas al personal |
| G | Protecciones de tipo organizativo |
| BC | Continuidad de operaciones |
| E | Externalización |
| NEW | Adquisición y desarrollo |

*Nota:* Datos tomados de MINHAP, Libro II MAGERIT versión 3.0., (2012, págs. 53-57).

Después de la definición de los pasos y la metodología para el tratamiento de los riesgos utilizando MAGERIT, como primer paso se identificó y clasifico los activos del área de tecnologías de la información los cuales encuentran en el Anexo 13.

Después de la identificación y clasificación de los activos se realizó una valoración de los mismos de acuerdo a los impactos indicados de acuerdo a la metodología MAGERIT según se muestra en la siguiente tabla.

Tabla 13.

*Valoración de activos informáticos*

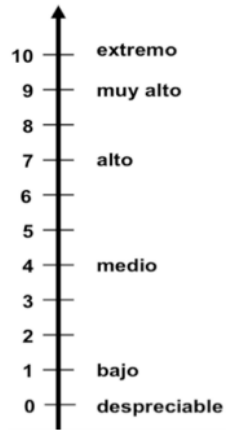
| Impacto | Valor | Descripción |
|---|---|---|
| MUY ALTO(MA) | 10 | El daño causado a la empresa sería grave e irreversible |
| ALTO(A) | 7-9 | El daño causado a la organización sería muy grave |
| MEDIO (M) | 4-6 | El daño tiene consecuencias relevantes para la organización y su operación |
| BAJO (B) | 1-3 | El daño tiene consecuencias relevantes, pero no afecta una gran parte de la organización |
| MUY BAJO(MB) | 0 | El daño no contiene consecuencias relevantes para la organización |

*Nota:* Datos tomados de MINHAP, Libro II MAGERIT versión 3.0., (2012, pág. 19)

En el Anexo 11, se muestra la valoración de los activos identificados y clasificados en el inventario, de acuerdo a la escala de valores que se encuentran en la Tabla 13.

**Valoración de activos por Dimensión de Seguridad**

Al finalizar la identificación y clasificación de los activos, se procedió a realizar la valoración de los activos frente a los riesgos de acuerdo a su dimensión, se utiliza la escala de valores de 0 a 10, donde 0 representa un valor despreciable, como se puede ver en la siguiente figura.




| *valor* | | *criterio* |
|---|---|---|
| 10 | extremo | daño extremadamente grave |
| 9 | muy alto | daño muy grave |
| 6-8 | alto | daño grave |
| 3-5 | medio | daño importante |
| 1-2 | bajo | daño menor |
| 0 | despreciable | irrelevante a efectos prácticos |

*Figura 20*.Criterios de valoración de los activos de acuerdo a su dimensión.

Fuente: (MINHAP, Libro II MAGERIT versión 3.0., Criterios de valoración 2012, pág. 19).

#### 3.1.2.1 Valoración de activos frente a los riesgos por tipo y dimensiones de seguridad.

Con los valores indicados en la figura 21 se realizó la valoración de los activos que tiene el área de tecnologías e información y se encuentra en el Anexo 12.

Para la elaboración de las siguientes figuras, se tomó los datos del Anexo 12.

**Tipo de Activo: Datos/Información**

Valoración de los activos de tipo **Datos/Información** por sus dimensiones

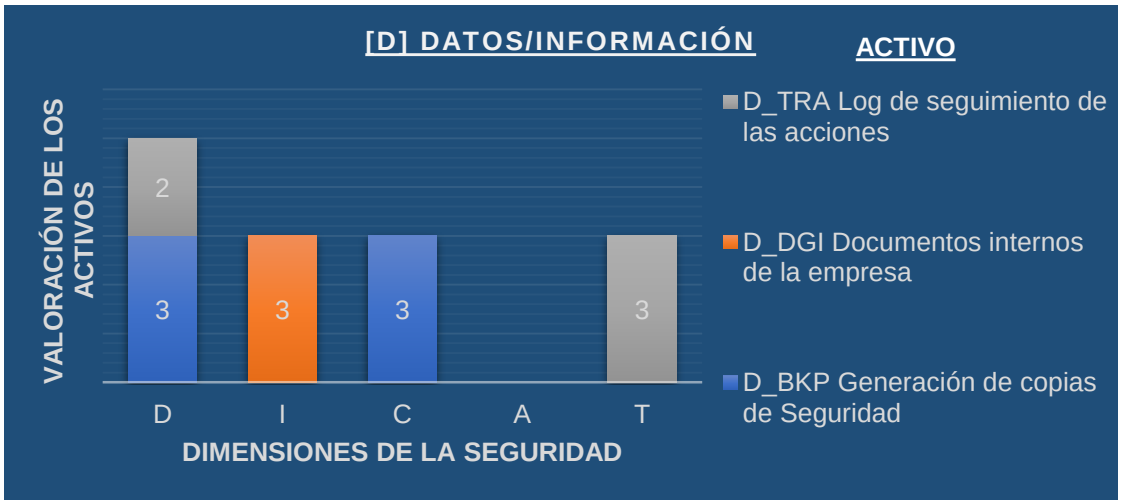



*Figura 21*.Valoración de activos Datos/Información por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor mínimo el 2 y máximo 3, de acuerdo a los

criterios de valoración indicados por la metodología MAGERIT el primer valor indica que el daño que puede ocasionar menor y el valor 3 indica que el daño causado puede ser importante.

**Tipo de Activo: Servicios**

Valoración de los activos de tipo **Servicios** por sus dimensiones

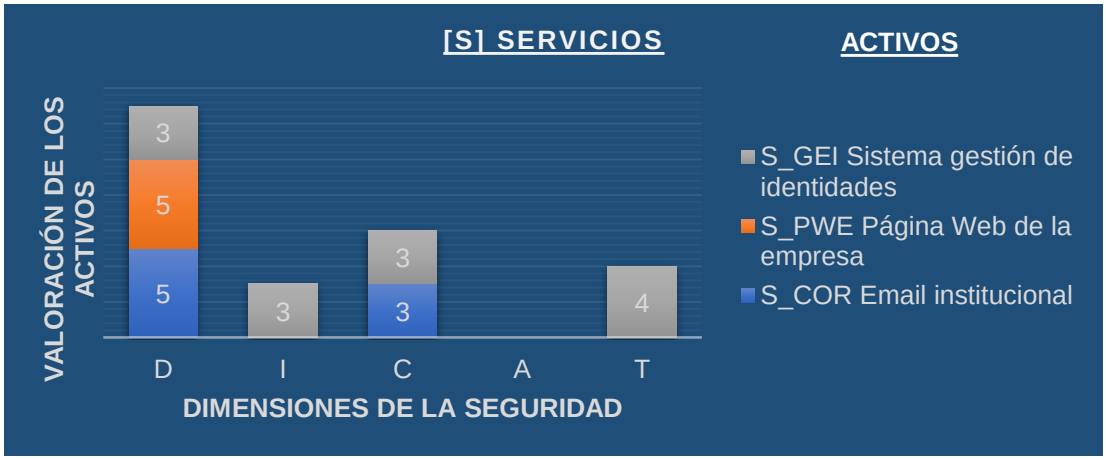



*Figura 22*. Valoración del activo Servicios por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor mínimo el 3 y máximo 5, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT los valores dentro de ese indican que le daño causado a la organización puede ser importante.

**Tipo de Activo: Software**

Valoración de los activos de tipo **Software** por sus dimensiones

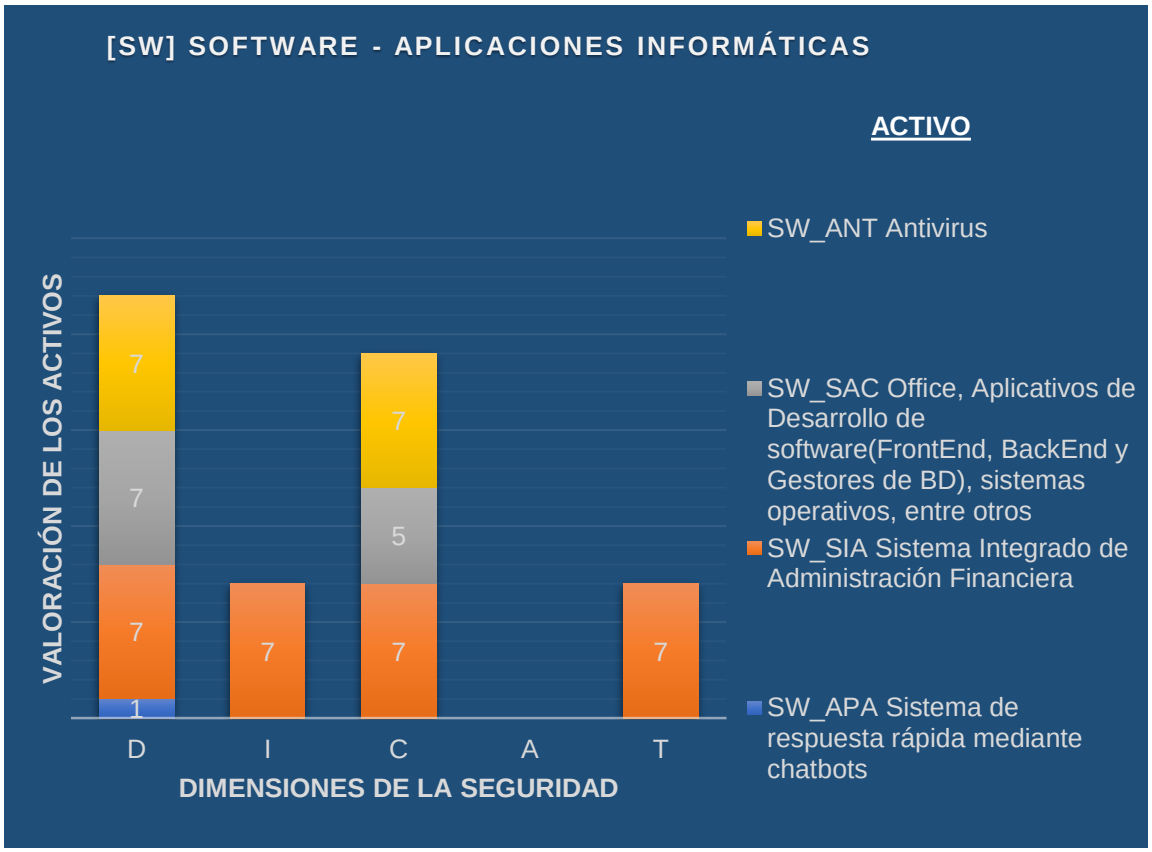



*Figura 23.* Valoración del activo Software por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor mínimo el 5 y máximo 7, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el primer valor indica que el daño causado puede ser importante y el valor 7 indica que el daño causado puede ser grave.

**Tipo de Activo: Hardware**

Valoración de los activos **Hardware** por sus dimensiones

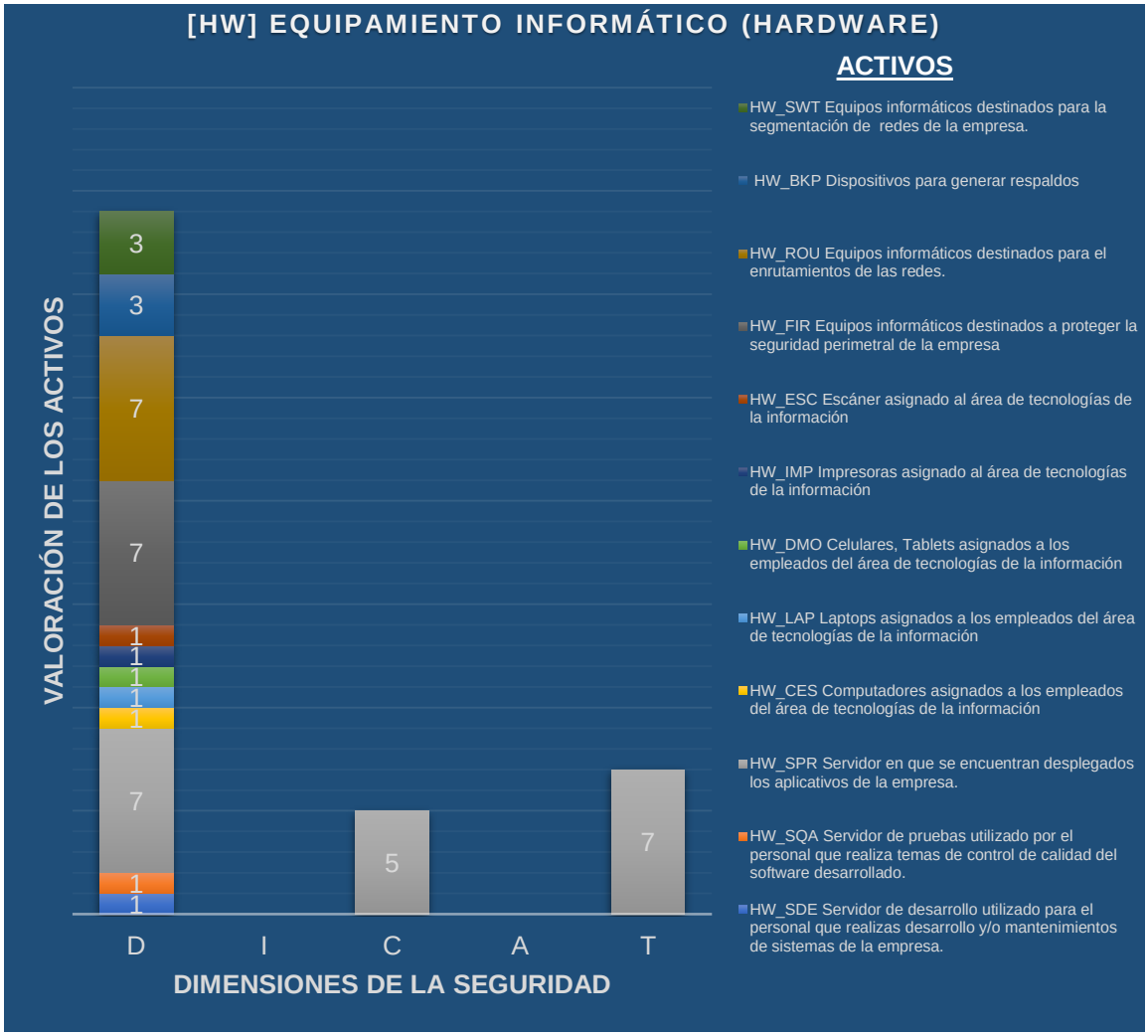



*Figura 24.* Valoración del activo Hardware por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor mínimo el 1, valor medio de 3 a 5 y el máximo 7, de acuerdo a los criterios de valoración indicados por la metodología

MAGERIT el primer valor indica que el daño causado puede ser menor, los valores en el rango de 3 a 5 indica que el daño causado puede ser importante y el valor 7 indica que el daño causado puede ser grave.

**Tipo de Activo: Criptografía**

Valoración de los activos de **Criptografía** por sus dimensiones


*Figura 25.* Valoración del activo Criptografía por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor 3, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el primer valor 3 indica que el daño causado puede ser importante.

**Tipo de Activo: Comunicaciones**

Valoración de los activos de **Comunicaciones** por sus dimensiones

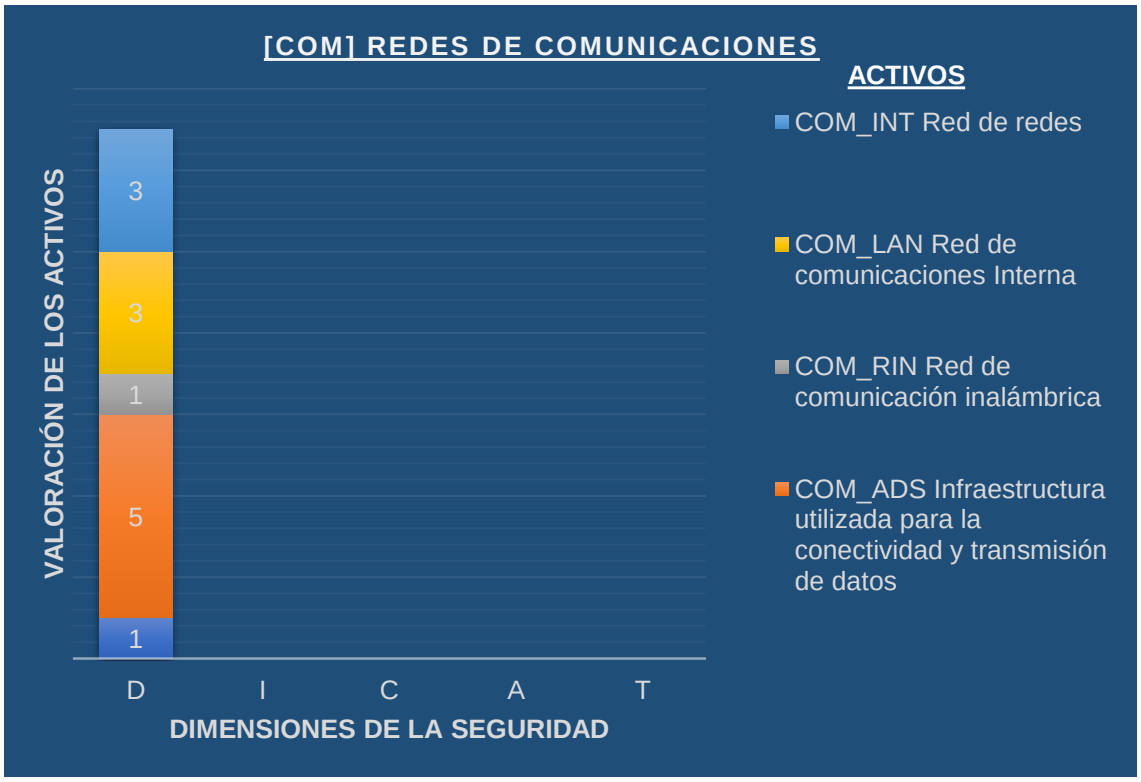



*Figura 26.* Valoración del activo Comunicaciones por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la seguridad de la información como son los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor mínimo el 1 y máximo 5, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el primer valor indica que el daño que puede ocasionar menor y los valores en el rango de 3 a 5 indica que el daño causado puede ser importante.

**Tipo de Activo: Media**

Valoración de los activos de **Media** por sus dimensiones

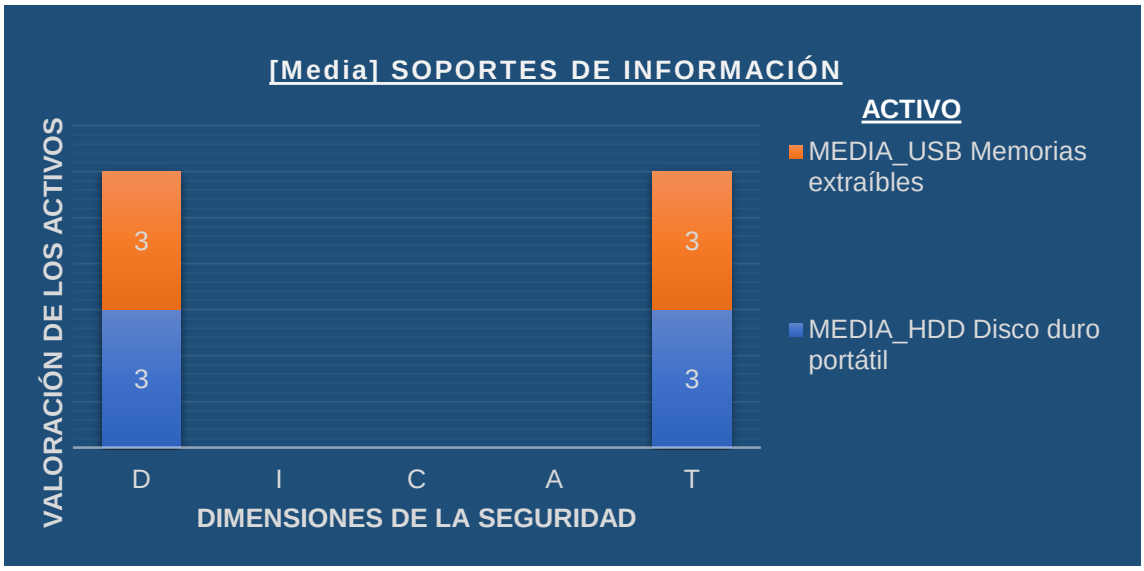



*Figura 27.* Valoración del activo Media por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor 3, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el primer valor 3 indica que el daño causado puede ser importante.

**Tipo de Activo: Auxiliares**

Valoración de los activos **Auxiliares** por sus dimensiones

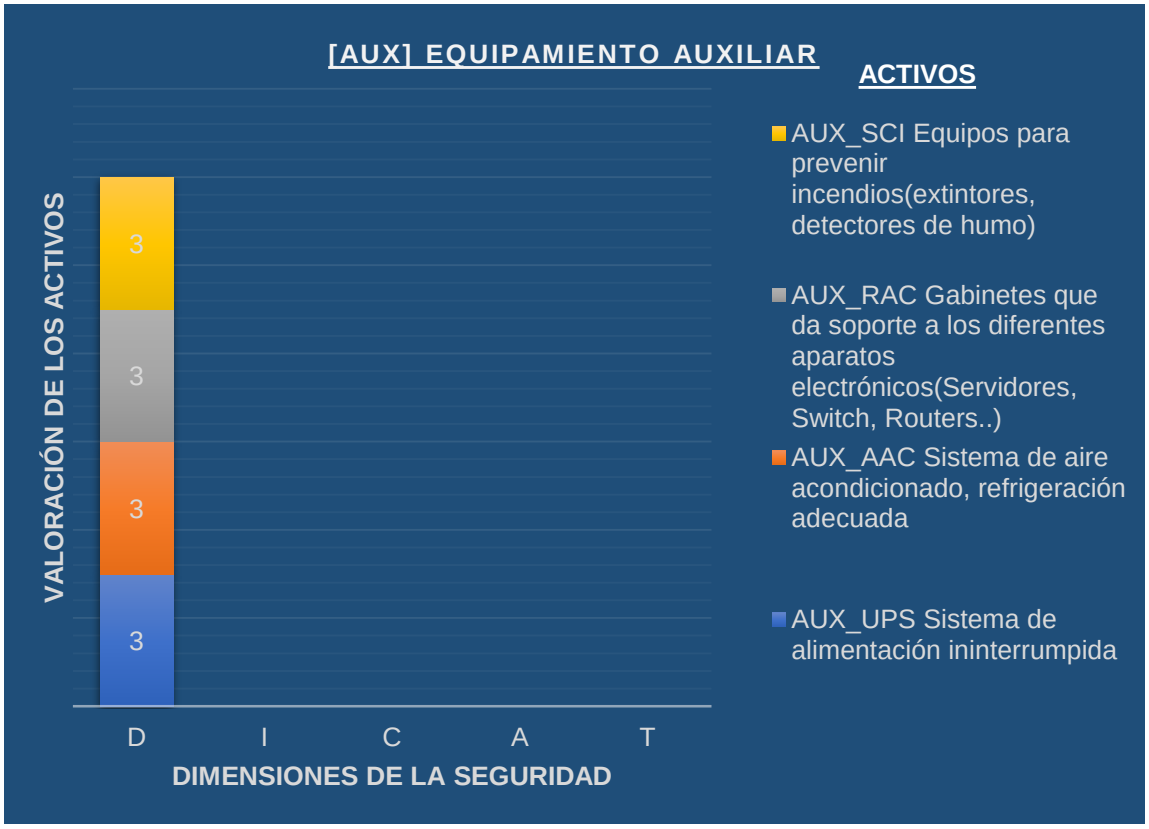



*Figura 28*. Valoración del activo Auxiliares por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor 3, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el primer valor 3 indica que el daño causado puede ser importante.

**Tipo de Activo: Local**

Valoración de los activos de tipo **LOCAL** por sus dimensiones


*Figura 29.* Valoración del activo Instalaciones por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:
La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor el 7, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el valor 7 indica que el daño causado puede ser grave.

**Tipo de Activo: PERSONAL**

Valoración de los activos de tipo **PERSONAL** por sus dimensiones

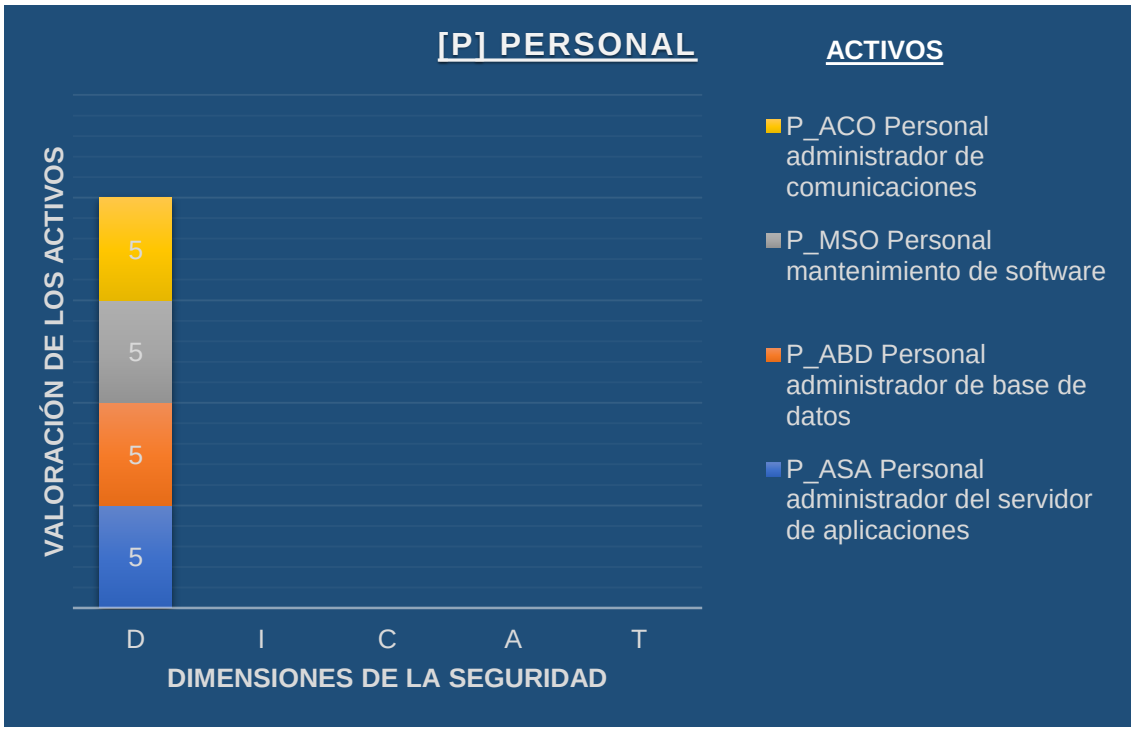



*Figura 30.* Valoración del activo Personal por dimensiones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Dimensiones de valoración 2012, pág. 15-16).

Los resultados del grafico anterior muestran la valoración de los activos lo que indica la importancia del activo dentro de la organización y el problema que puede causar su indisponibilidad lo cual puede afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la valoración realizada a los activos se interpreta de la siguiente manera:

La indisponibilidad de los activos puede afectar las dimensiones de la seguridad en el grafico anterior tiene como valor el 5, de acuerdo a los criterios de valoración indicados por la metodología MAGERIT el valor 7 indica que el daño causado puede ser importante.

De acuerdo a los resultados mostrados en las figuras anteriores la valoración de los activos permite tomar las medidas necesarias para mitigar los riesgos a los cuales está asociado cada activo, todos los valores son muy importantes pero los valores mayores a 2 se debe priorizar la implementación de controles del anexo A, de la norma ISO 27001:2013.

**Identificar y valorar amenazas de los activos**

después de haber realizado la valoración de los activos identificados del área de sistemas, en este punto se realizará la valoración de las amenazas a las que está expuesto los activos, para lo cual se utilizó un rango de presentación de amenazas con frecuencia (mensual, semestral y anual).

La valoración % de que ocurra una amenaza dentro de la empresa de seguros y el impacto es las dimensiones se muestra en las siguientes figuras.

**Tipo Activo: Datos/Información**

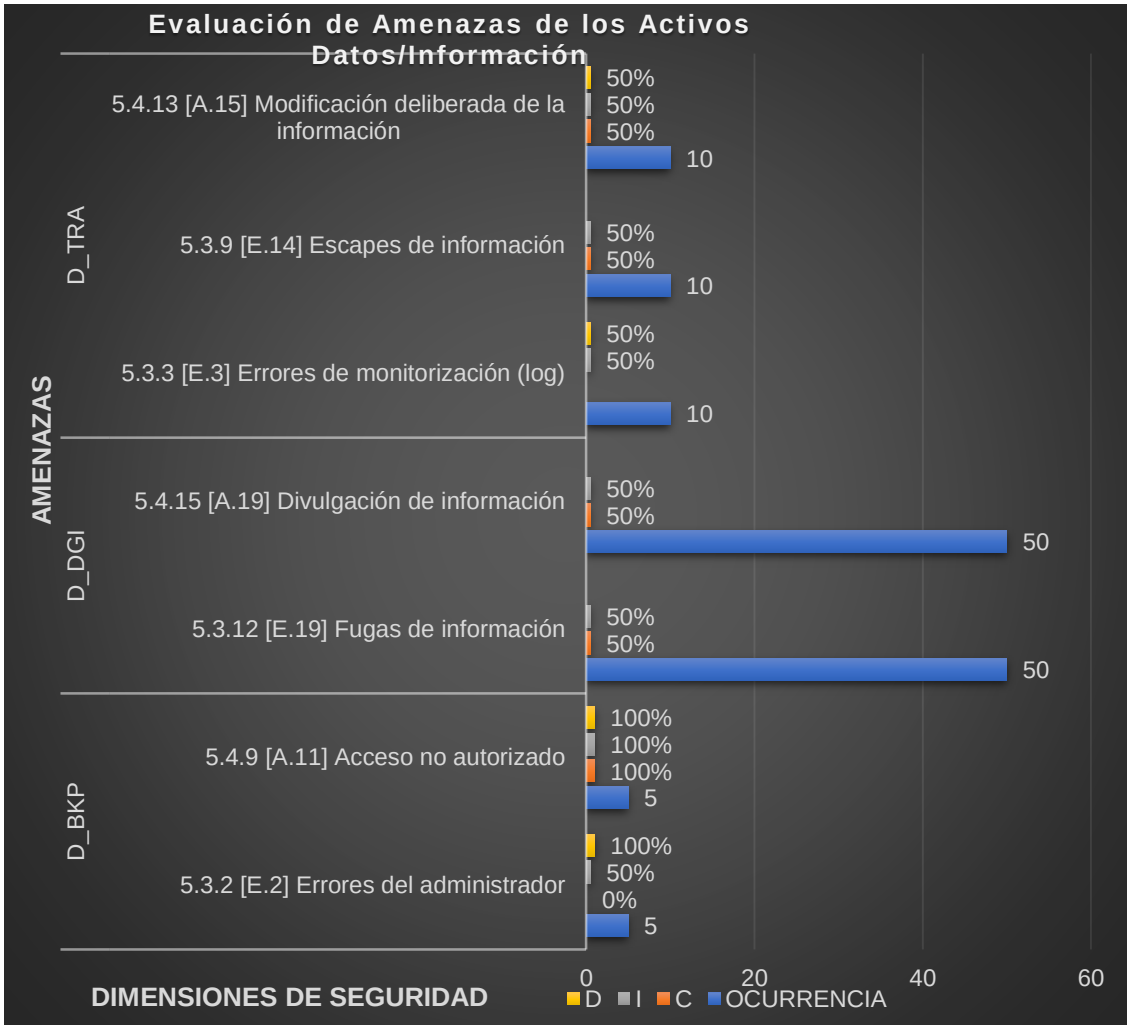



*Figura 31*. Evaluación de Amenazas de los Activos Datos/Información. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Datos/Información tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual y como valor máximo se tiene 50 que equivale que la amenaza puede generarse de manera Normal que equivale al rango mensual.

**Tipo Activo: Servicio**

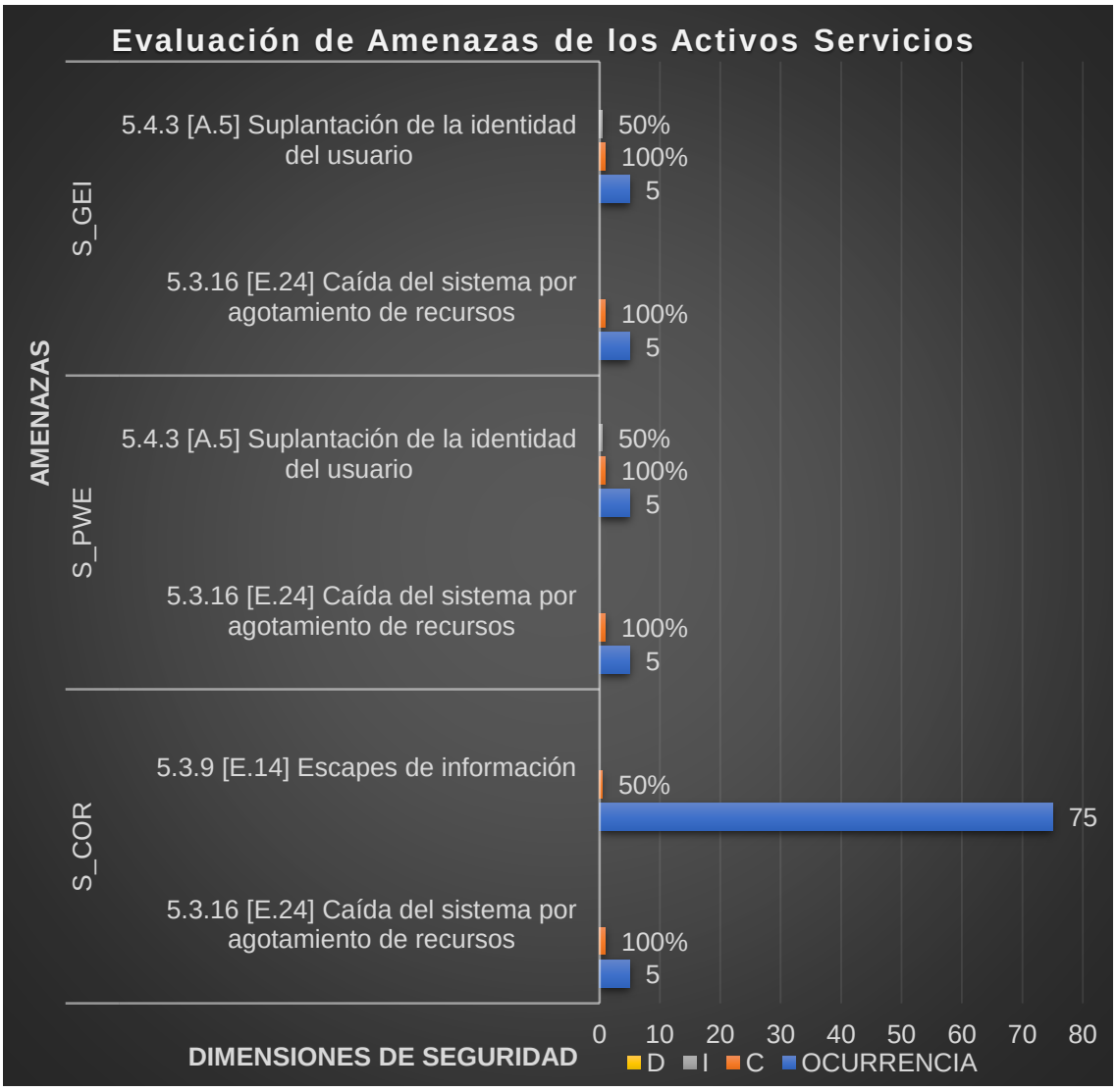



*Figura 32.* Evaluación de Amenazas de los Activos Servicios. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Servicio tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual y como valor máximo se tiene 75 que equivale que la amenaza puede generarse de manera Frecuente que equivale al rango Semanal.

**Tipo Activo: Software**

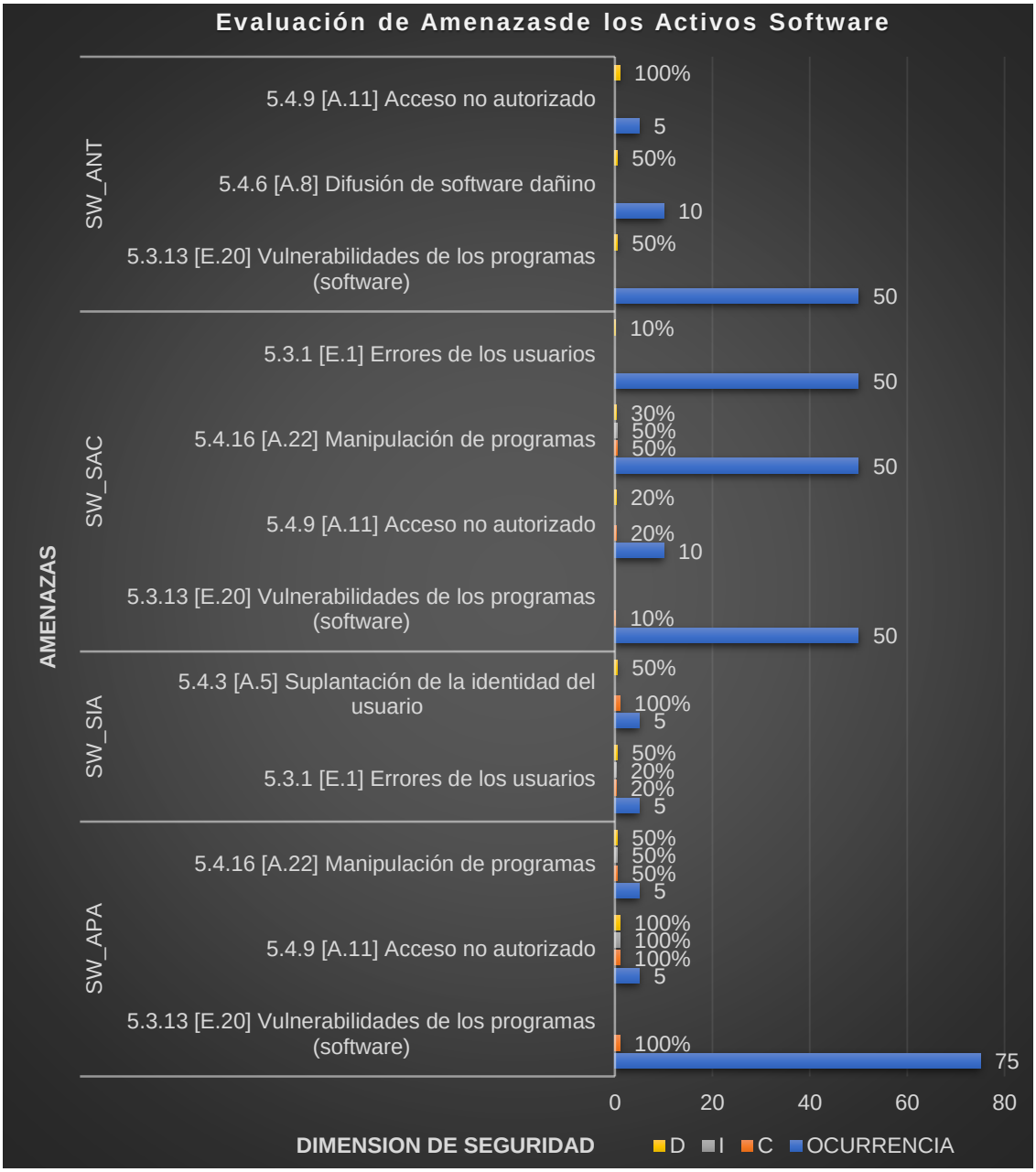



*Figura 33.* Evaluación de Amenazas de los Activos Software. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Software tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y

equivale al rango anual y como valor máximo se tiene 75 que equivale que la amenaza puede generarse de manera Frecuente que equivale al rango Semanal.

**Tipo Activo: Hardware**

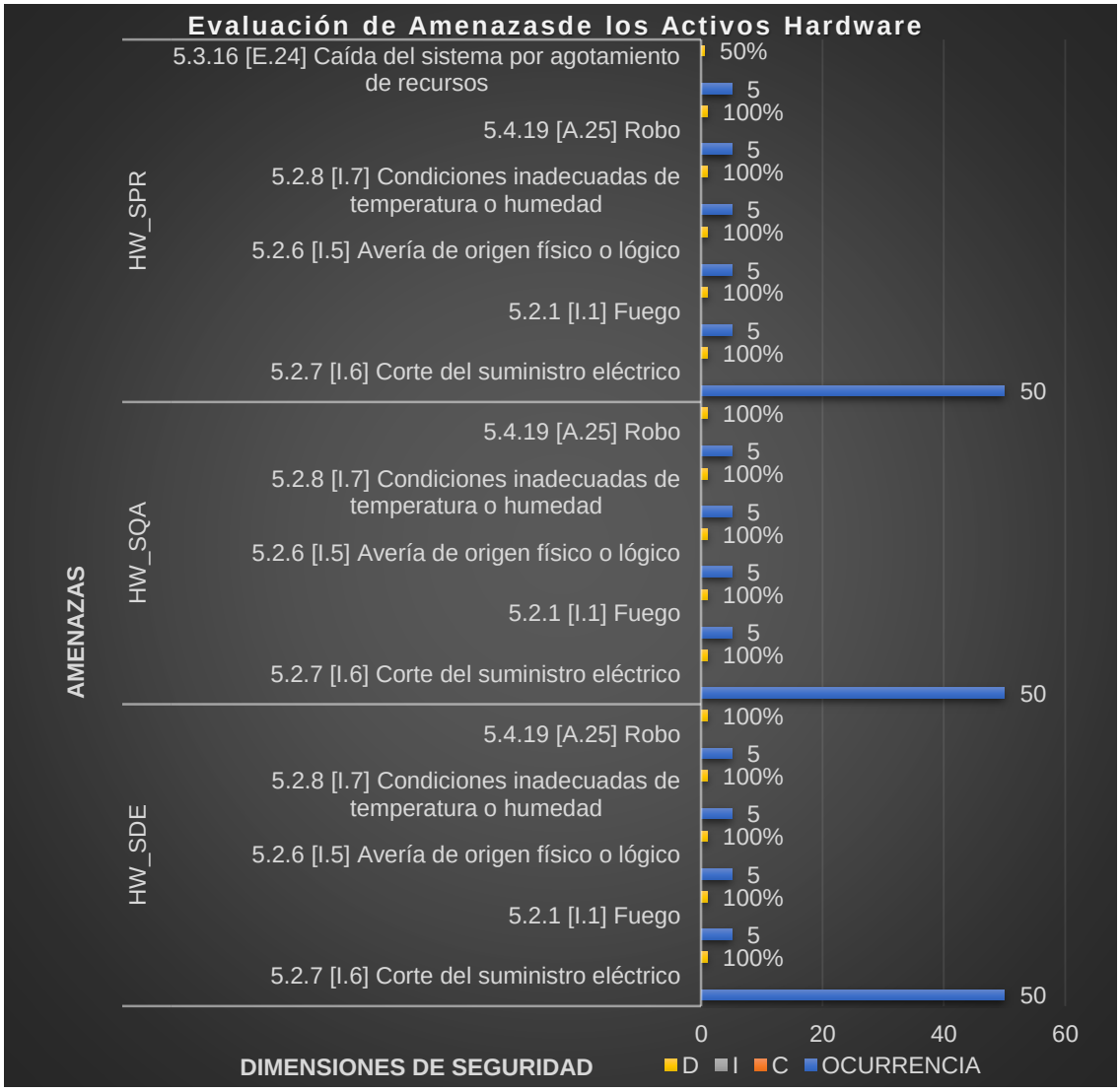



*Figura 34.* Evaluación de Amenazas de los Activos Hardware-Parte1. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

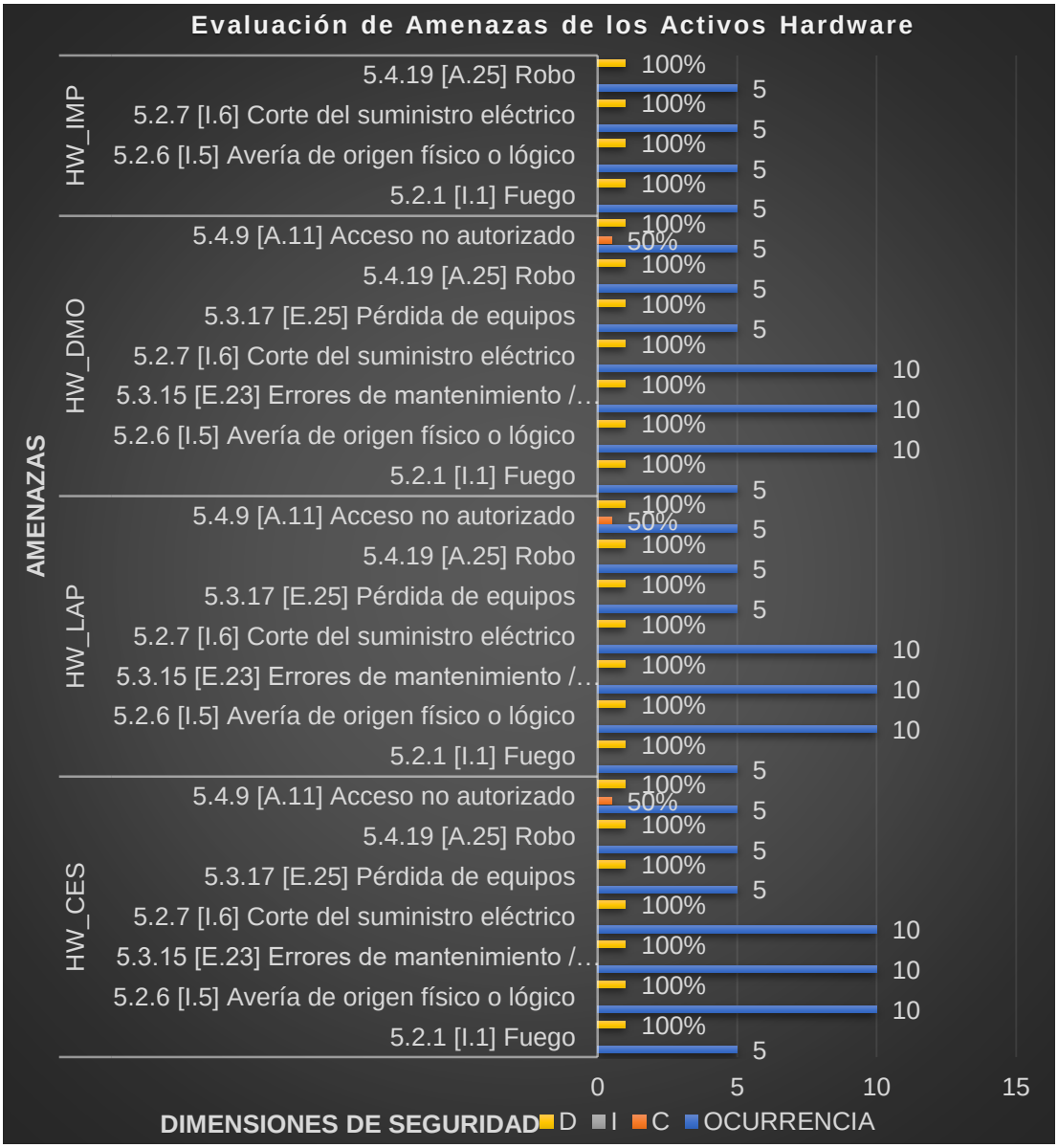



*Figura 35.* Evaluación de Amenazas de los Activos Hardware-Parte 2. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

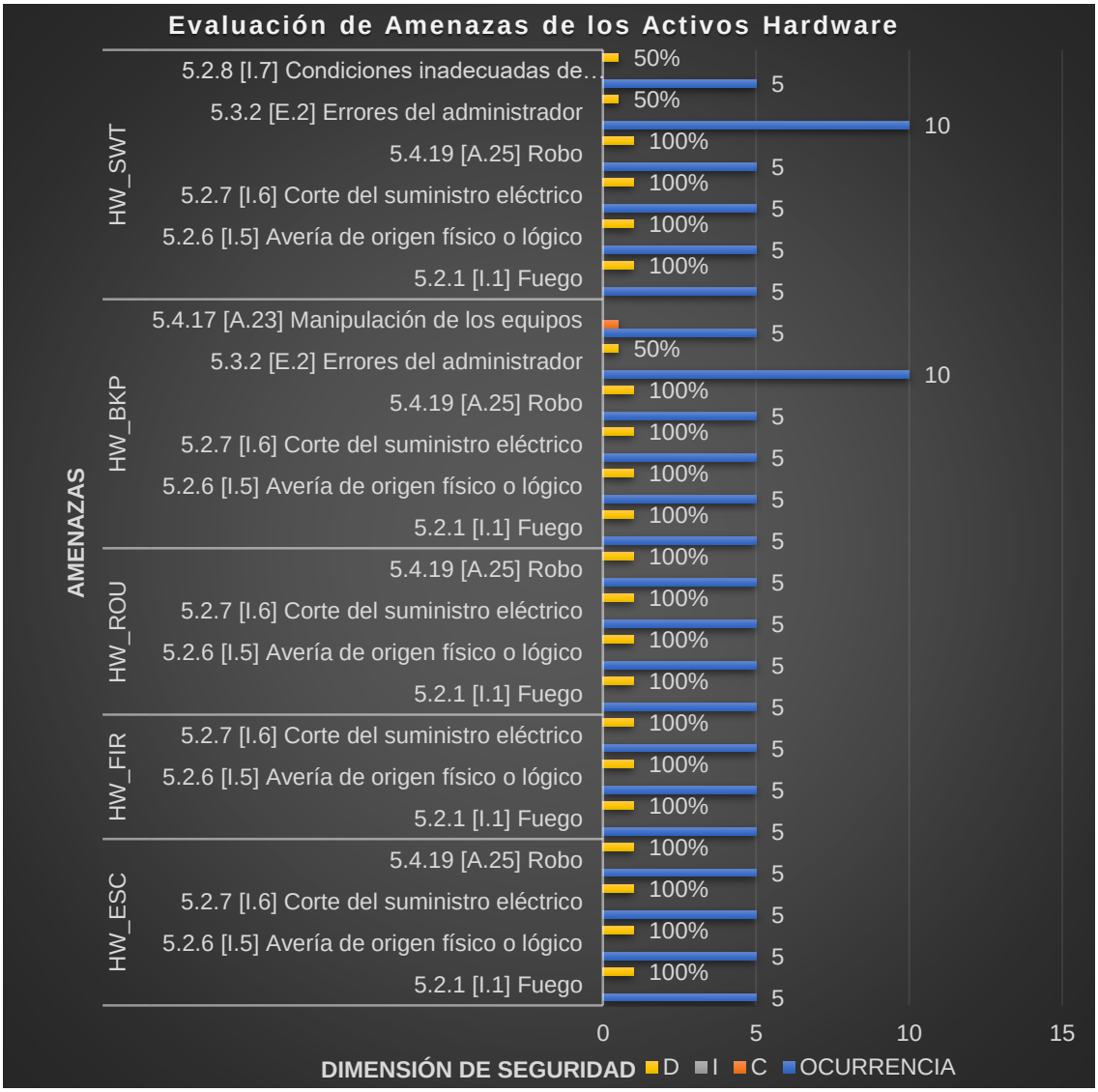



*Figura 36.* Evaluación de Amenazas de los Activos Hardware-Parte 3. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Hardware tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual y como valor máximo se tiene 10 que equivale que la amenaza puede generarse de manera Poco Frecuente que equivale al rango

Semestral.

**Tipo Activo: CRIPTOGRAFÍA**

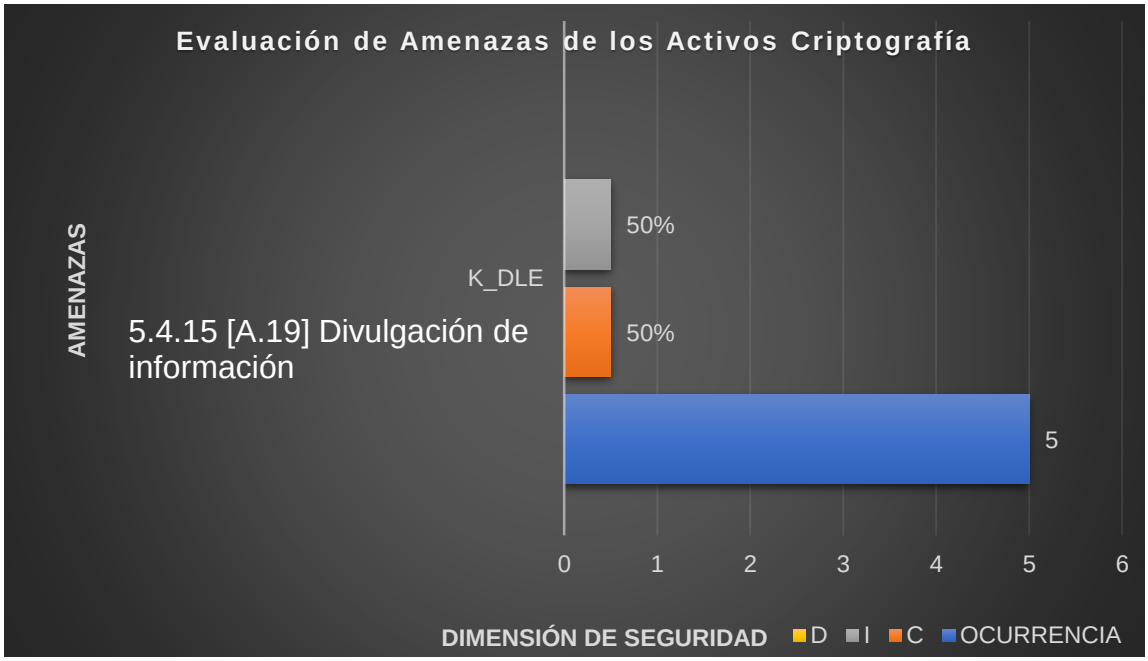



*Figura 37.* Evaluación de Amenazas de los Activos Criptografía. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Criptografía tiene como valor 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual.

**Tipo Activo: COMUNICACIONES**

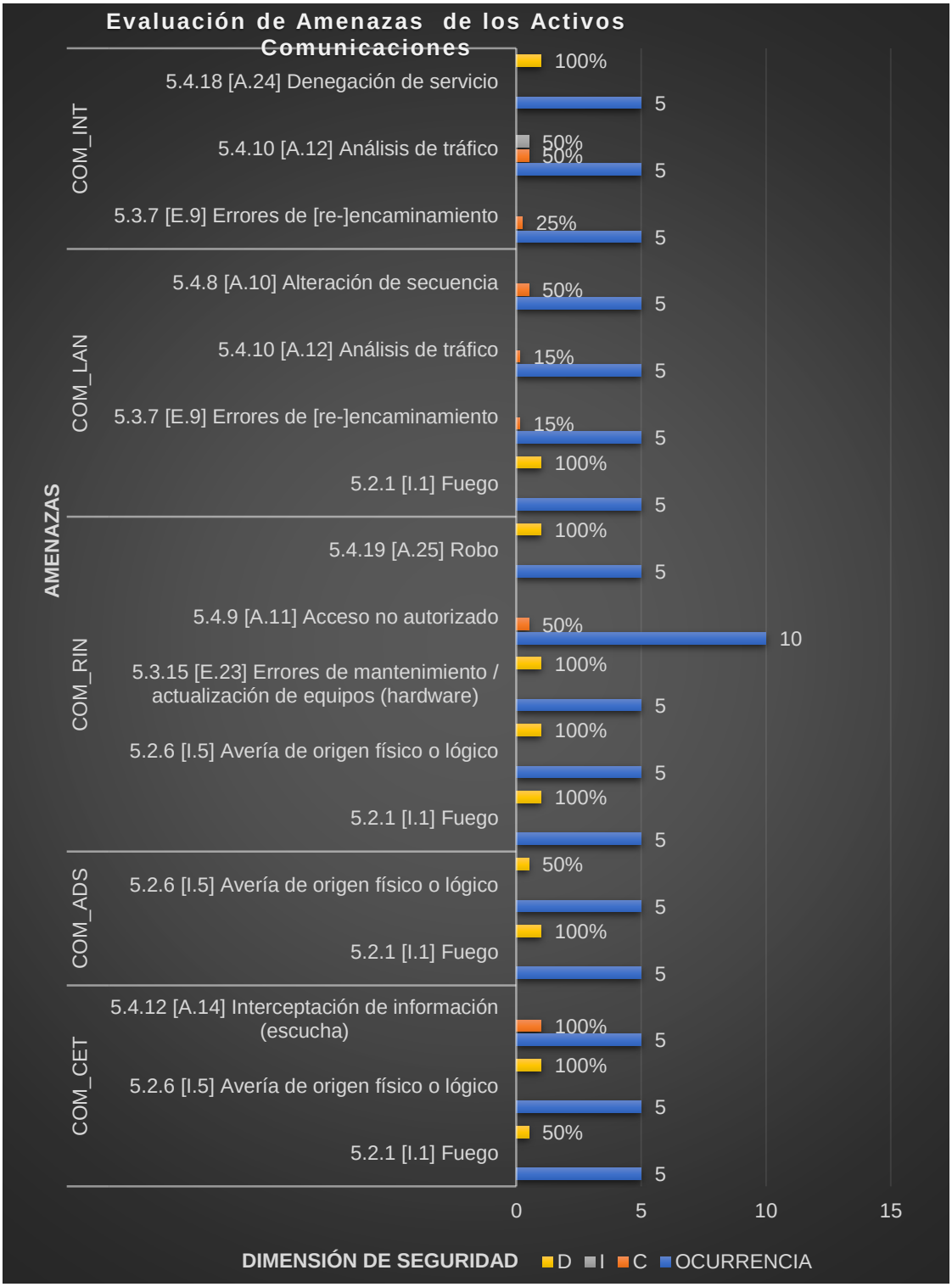



*Figura 38.* Evaluación de Amenazas de los Activos Comunicaciones. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0.,

Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.
En la evaluación realizada los activos Comunicaciones tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual y como valor máximo se tiene 10 que equivale que la amenaza puede generarse de manera Poco Frecuente que equivale al rango Semestral.

**Tipo Activo: Media**

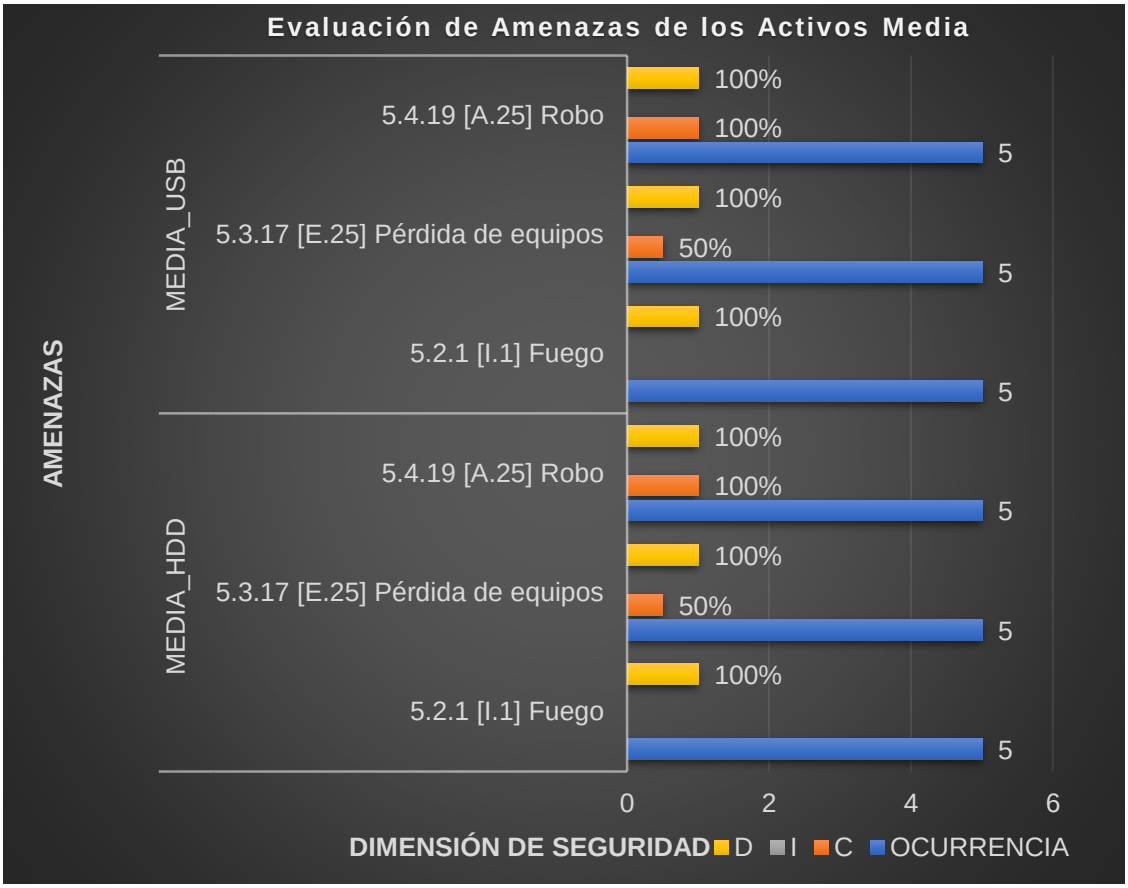



*Figura 39*.Evaluación de Amenazas de los Activos Media. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de

amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Media tiene como valor 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual.

**Tipo Activo: Auxiliares**

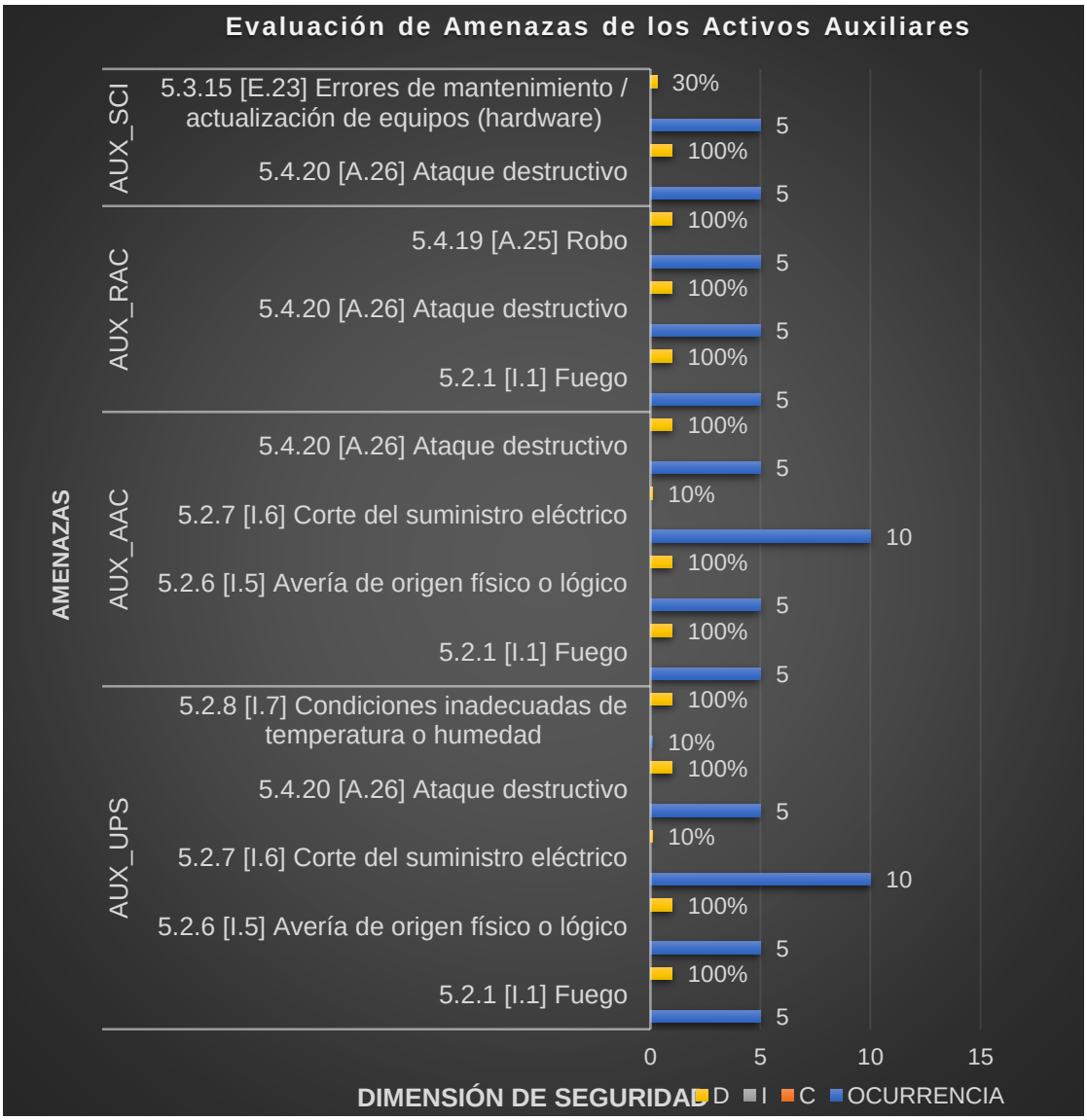



*Figura 40*. Evaluación de Amenazas de los Activos Auxiliares. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de

amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Auxiliares tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual y como valor máximo se tiene 10 que equivale que la amenaza puede generarse de manera Poco Frecuente que equivale al rango Semestral.

**Tipo Activo: Local**

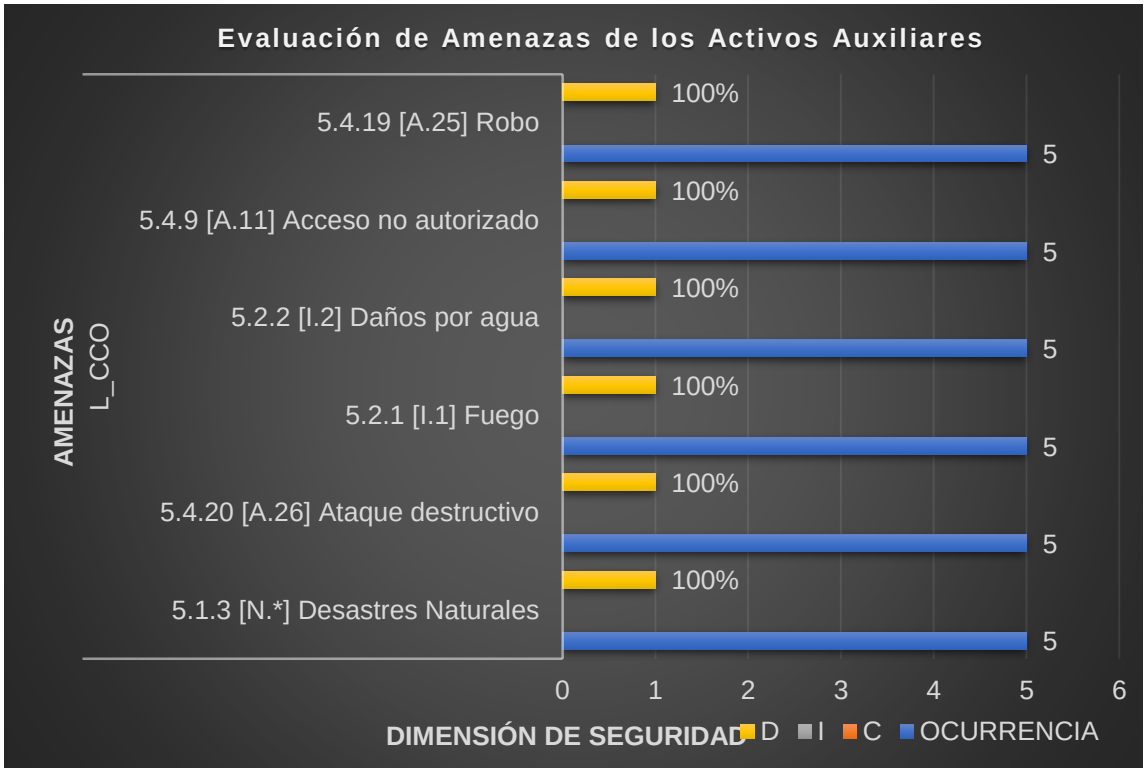



*Figura 41.* Evaluación de Amenazas de los Activos Local. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.
En la evaluación realizada los activos Auxiliares tiene como valor 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual.

**Tipo Activo: Personal**

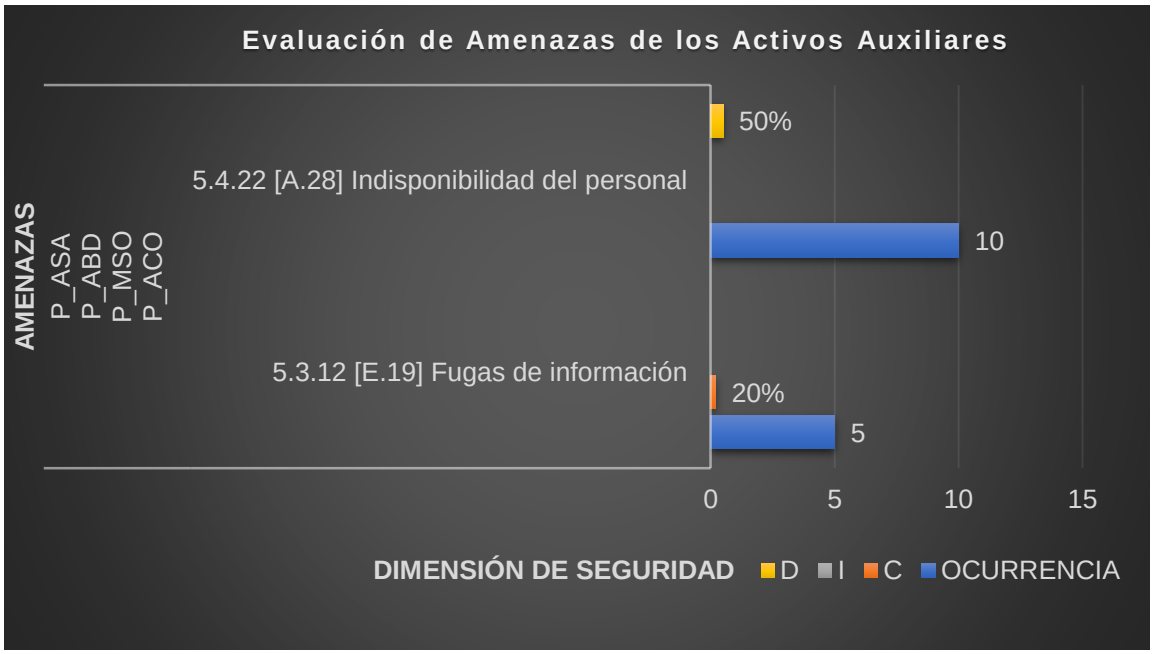



*Figura 42.* Evaluación de Amenazas de los Activos Personal. Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., Amenazas de activos 2012, pág. 25-47).

Los resultados del grafico anterior, muestran la valoración de la ocurrencia de amenazas a los cuales están expuestos los activos y que pueden afectar los dominios de la SI que se encuentran detallados en la Tabla 8.

En la evaluación realizada los activos Auxiliares tiene como valor mínimo 5 que equivale a que la amenaza puede generarse de manera Muy Poco Frecuente y equivale al rango anual y como valor máximo se tiene 10 que equivale que la amenaza puede generarse de manera Poco Frecuente que equivale al rango Semestral.

Para verificar las vulnerabilidades y amenazas a los que está expuesta el área de sistemas en temas de la seguridad de la información, se tomó en cuenta los datos obtenidos mediante la encuesta del Anexo 3, la encuesta consta de 15 preguntas cerradas y fue realizada a 25 empleados de la empresa, asimismo se consultó el grado de aceptación de la posibilidad del desarrollo de un plan de seguridad de la información.

En la siguiente tabla se muestra los resultados de manera consolidada de la encuesta aplicada al personal del área de sistemas y administrativo de la empresa de seguros, la información completa se encuentra en el Anexo 5..

Tabla 14.

*Resultado de encuesta para verificar las vulnerabilidades y amenazas en el área de sistemas*

| Ítem | Nunca | Casi nunca | Regularmente | Casi Siempre | Siempre |
|---|---|---|---|---|---|
| 1. ¿Tiene conocimiento de las políticas relacionadas a la seguridad de la información que debe aplicar en su puesto de trabajo? | 0% | 48% | 48% | 0% | 4% |
| 2. ¿La empresa brinda capacitaciones a los empleados para concientizar sobre la importancia de la seguridad de la información en la empresa? | 0% | 60% | 40% | 0% | 0% |
| 3. ¿Tiene conocimiento si la empresa ha sufrido algún ataque informático durante estos 3 últimos años? | 100% | 0% | 0% | 0% | 0% |
| 4. ¿Ha tenido algún percance o incidente referente a la seguridad de la información en su puesto de trabajo? | 40% | 56% | 4% | 0% | 0% |
| 5. ¿Si tuvo algún percance o incidente, fue informado? | 0% | 64% | 16% | 12% | 8% |
| 6. ¿El activo entregado para sus labores en este caso una Laptop u otro dispositivo, al sufrir algún incidente, la respuesta o la atención para solucionar el incidente fue inmediato? | 0% | 44% | 48% | 8% | 0% |
| 7. ¿Hace uso de contraseñas seguras Ejm: 8 Caracteres Alfanuméricos entre los cuales debe haber una Mayúscula, un número y un signo? | 16% | 12% | 28% | 4% | 40% |

| Ítem | Nunca | Casi nunca | Regularmente | Casi Siempre | Siempre |
|---|---|---|---|---|---|
| 8. ¿Tu equipo asignado tuvo algún mantenimiento preventivo hace un año? | 40% | 28% | 28% | 4% | 0% |
| 9. ¿Hace uso de medios extraíbles como USB, Disco Externo, etc. para el traslado de alguna información? | 16% | 36% | 28% | 16% | 4% |
| 10. ¿Los accesos a lugares restringidos tienen una medida adecuada de seguridad? | 8% | 28% | 64% | 0% | 0% |
| 11. ¿Al realizar impresiones de documentos confidenciales, en algún momento se olvidó en su escritorio o en la impresora? | 48% | 36% | 16% | 0% | 0% |
| 12. ¿Ud. Realiza el bloqueo de su computadora cuando se retira de su puesto de trabajo? | 0% | 12% | 40% | 24% | 24% |
| 13. ¿La disponibilidad de los aplicativos para los clientes es continua? | 0% | 0% | 0% | 4% | 96% |
| 14. ¿Tuvo la necesidad de instalar programas nuevos en su equipo asignado? | 8% | 60% | 20% | 8% | 4% |
| 15. ¿La implementación de un plan de seguridad de la información basado en normas internacionales, ayudara a mejorar la seguridad de la información en la empresa? | 0% | 0% | 0% | 0% | 100% |

Fuente: Elaboración Propia

**IDENTIFICACIÓN DE VULNERABILIDADES Y AMENAZAS Y CLASIFICACIÓN DE RESULTADO POR TIPO DE ACTIVO Y DIMENSIÓN DE LA SEGURIDAD DE INFORMACIÓN**

Tabla 15.

*Identificación de Vulnerabilidades y Amenazas y Clasificación de resultados por Dimensión de la Seguridad de información*

| TIPO ACTIVO | CÓDIGO | VULNERABILIDAD | AMENAZA | RIESGO | DIMENSION | PREGUNTA |
|---|---|---|---|---|---|---|
| **DATO INFORMACION** | V1 | Documentos al alcance de personas no autorizadas | Uso indebido de los documentos | Puede afectar la reputación de un individuo o la organización | C | 11 |
| | V2 | Desconocimiento de políticas internas | Incumplimiento de la política | Realizar acciones que van en contra de la políticas internas | C, I, D | 1,2 |
| | V3 | No informar los incidentes | Puedo volver a ocurrir el mismo incidente | Perdida de activos | D | 5 |
| **HARDWARE** | V4 | Falla de equipos por falta de mantenimiento | Perdida de información | Personal sin herramienta de trabajo | D | 8 |

| TIPO ACTIVO | CÓDIGO | VULNERABILIDAD | AMENAZA | RIESGO | DIMENSION | PREGUNTA |
|---|---|---|---|---|---|---|
| **SOFTWARE** | V5 | Fallas en los aplicativos | Indisponibilidad de los aplicativos | Mala imagen ante los clientes internos y externos | C , D | 13 |
| | V6 | Instalación de software libre no autorizado | Aplicativos no verificados pueden contener virus | Ataque mediante malware, DoS | C, I, D | 14 |
| | V7 | Acceso a aplicativos sin autorización | Acceso a información sensible | Perdida de información | C, I | 12 |
| | V8 | Contraseñas débiles | Acceso a algún sistema por parte de usuarios no autorizados | Perdida de información confidencial y mala imagen | C, I, D | 7 |
| MEDIA | V9 | Uso inadecuado de dispositivos removibles | Infección de virus | Indisponibilidad del activo | I ,D | 9 |

| TIPO ACTIVO | CÓDIGO | VULNERABILIDAD | AMENAZA | RIESGO | DIMENSION | PREGUNTA |
|---|---|---|---|---|---|---|
| LOCAL | V10 | Control de acceso inadecuado a oficinas | Acceso de personal no autorizado | Perdida de información, robo de activos | C, I, D | 10 |
| C=Confiabilidad, I=Integridad, D=Disponibilidad | | | | | | |

Fuente: Elaboración Propia

**Interpretación**:

Los resultados de la Tabla 18 muestran que, de los 25 empleados encuestados, al 100%, el 52% afirma que tiene conocimiento de las políticas de seguridad que debe aplicar en su puesto de trabajo, el 60% indica que la organización no cuenta con un plan de capacitaciones en seguridad de la información, el 60% indicó que en algún momento tuvo un incidente referente a la seguridad de la información en su puesto de trabajo, solamente el 36% informa de manera oportuna los incidentes que se presentaron en su puesto de trabajo, el 44% indico que la atención a sus activos no se realiza de manera oportuna, el 28% indico que no usa contraseñas seguras, el, el 68% indico que no sus equipos asignados no tuvieron un mantenimiento en el transcurso de un año, el 48% hace uso de medios extraíbles para trasladar su información, el 36% indicó que la seguridad de accesos físicos no tienen una medida adecuada de seguridad, el 16% indicó que en algún momento dejó documentos confidenciales al alcance de otras persona, el 12% no realiza el bloqueo de su computadora de manera adecuada, el 4% indicó que en una oportunidad los aplicativos y/o sistemas no estuvieron disponibles, el 40% realiza la instalación de programadas en sus equipos asignado y el 100% está de acuerdo con contar con un plan de un seguridad de la información basado en normas internacionales en el área de tecnologías de información.

### 3.1.3 Elaboración del plan de seguridad de la información basado en normas internacionales para el beneficio de la empresa de seguros.

Para lograr de este objetivo se realizó una entrevista virtual a un especialista en temas de seguridad de la información en la norma ISO 27001:2013, el documento de la entrevista se encuentra en el Anexo 9.

El especialista indica que la implementación de un SGSI en una organización es muy importante porque ofrece una serie de controles y buenas practicas con la finalidad de mejorar la seguridad de la información.

También menciona que al no contar con un SGSI la empresa no tiene manera de medir los riesgos o amenazas a las que pueda estar expuesto la organización, también recalca la importancia de concientizar a los empleados de una empresa en termas de seguridad de la información ya que estarán más preparados para afrontar a situaciones que puedan perjudicar a la organización.

El especialista concluye indicando que la implementación de la norma ISO27001 ayudará a disminuir riesgos y amenazas a la seguridad de la información que pueda sufrir la organización y recomienda que las empresas que no cuenten con un sistema de seguridad de la información deberían hacer un gran esfuerzo en su implementación de lo contrario podrían sufrir pérdidas económicas y daño en la imagen de la organización.

Asimismo, para cumplir el tercer objetivo de la investigación se tomó en cuenta los datos obtenidos en la evaluación del estado inicial de la organización, la valoración de activos, evaluación de amenazas a las que está expuesta los activos de la empresa y la evaluación de los riesgos y vulnerabilidades de la empresa referente a temas de la seguridad de la información.

## 3.2 Discusión de resultados

**Objetivo 1:**

En la evaluación inicial del estado actual de la empresa con respecto a las normas de seguridad de la información.

Los resultados obtenidos en la Tabla 4 frente a los requisitos en temas de seguridad de la información indican que el 93% de los requisitos que exige la norma ISO27001:2013 se encuentran en una etapa inicial el 7% de los requisitos se encuentra en una etapa repetible.

La norma ISO27001:2013 considera que la etapa inicial se refiere a que las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad. La etapa repetible se refiere a que La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.

Estos resultados al ser comparados con el estudio realizado por (Barrera, 2019), en su tesis titulada PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDAD EDUCATIVA NUESTRA SEÑORA DE FÁTIMA. quien en su investigación concluye que el incumplimiento de los requisitos formales de la norma es del 72%, ya que la mayoría de riesgos detectados están ubicados en los niveles Alto y Muy Alto, también se detectó un alto índice de vulnerabilidades en los elementos asociados al mantenimiento, transferencia de la información y la falta de documentación de los procesos asociados a la SI.

La implementación de un plan de seguridad de la información basado en la norma ISO27001:2013 ayudará a que los objetivos principales de la información como son disponibilidad, confidencialidad e integridad se cumplan de manera adecuada, según (Romero, y otros, 2019).

**Objetivo 2:**

En la identificación de las vulnerabilidades y amenazas en el área de sistemas, los resultados de la Tabla 5 muestran que 48% de empleados que no aplican de manera adecuada las políticas de seguridad en su puesto de trabajo, el 60% de empleados indican que la empresa no cuenta con un adecuado plan de capacitación en temas de seguridad de la información y concientización al personal, el 48% de empleados indican que la empresa no cuenta con un adecuado plan de mantenimiento de activos, es necesario

implementar normas de seguridad basado en la norma ISO27001, aplicando controles del anexo A, para mitigar y mejorar la seguridad de la información.

El anexo A, de la norma ISO27001:2013 cuenta con 14 dominios y 114 controles los cuales pueden apoyar en mejorar la seguridad de la información aplicando controles de acuerdo a las necesidades y prioridades de la empresa para mejorar los temas de plan de capacitación, concientización, plan de mantenimiento de activos.

Estos resultados al ser comparados con el estudio realizado por (Figueroa, 2018), en su tesis titulada DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO GERMÁN ARCINIEGAS I.E.D., BAJO LA NORMA TÉCNICA COLOMBIANA NTC ISO/IEC 27001:2013. en su investigación realizado en el país de Colombia indica que a diario se registran 542 mil ataques informáticos y en el último año, los ataques se realizan a cualquier tamaño de empresas, la investigación también indica que en el sector de Servicios aumento en 50% los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de DoS, la investigación evidencia la vulnerabilidad a las que está expuesta cualquier organización en temas de SI, por lo cual la norma ISO27001 mediante su anexo A, ayuda a mejorar la seguridad de la información.

El anexo A, de la norma internacional ISO/IEC 27001:2013 cuenta con 14 dominios y 114 controles designados como los puntos A.5 a A.18 los controles ayudan a mejorar la SI dentro de la organización.

**Objetivo 3:**

El desarrollo de un plan de seguridad de la información basado en normas internacionales para área de tecnologías de la información en beneficio de la empresa de seguros.

La implementación de un plan de seguridad de la información basado en la norma ISO27001:2013 mediante la aplicación de los controles del Anexo A mejorará de manera significativa la seguridad de la información dentro de la organización.

Estos resultados al ser comparados con el estudio realizado por (Benites, 2019), en su tesis titulada Implementación de un sistema de gestión de seguridad de la información - Norma ISO 27001 para la fábrica Radiadores Fortaleza. En su investigación menciona que el desarrollo de un plan de SGSI, traerá beneficios a la empresa. Ya que un SGSI propone que controles deben ir acompañados de políticas correctas en la seguridad, lo cual ayuda a que la empresa pueda prevenir en gran porcentaje posibles problemas en temas de seguridad de la información.

La implementación de un plan de seguridad de la información basado en la norma ISO27001:2013 ayuda a conseguir los niveles adecuados en los dominios de la SI dentro de la empresa, con la finalidad de asegurar la continuidad operacional de los procesos y servicios, mediante el SGSI.

## 3.3 Aporte práctico

Elaboración del plan de seguridad de la información basado en la norma internacional ISO 27001:2013 los documentos relacionados al plan son los siguientes:

Plan de seguridad de la información empresa de seguros.docx

Plan de mantenimiento preventivo activos informaticos.docx

Plan de concientización de seguridad de la información.docx

Políticas de seguridad de la informacion.docx

Los documentos mencionados se encuentran como anexos.

# IV. CONCLUSIONES Y RECOMENDACIONES

## 4.1 Conclusiones

Se realizó la evaluación de la situación actual de la seguridad de la información de la empresa de seguros evidenciando falencias y determinando el nivel de seguridad actual frente a los requisitos de la norma ISO27001:2013, abordando controles para mejorar la seguridad de la información.

Debido a la existencia de una serie de incumplimientos de la política actual de la seguridad de la información la empresa presenta amenazas y vulnerabilidades en la seguridad de la información, los cuales pueden provocar riesgos en la seguridad de la información, para una correcta gestión de la seguridad de la información la implementación de controles del anexo A de la norma ISO 27001:2013, contribuye de manera significativa en la protección de los activos de la empresa.

Se desarrolló un plan de seguridad de la información basado en la norma ISO 27001:2013, lo que permite a la empresa implementar los controles del anexo A, priorizando sus necesidades, para eliminar y/o reducir las amenazas y vulnerabilidades a las que está expuesto.

## 4.2 Recomendaciones

Se recomienda a la empresa de seguros considerar la presente investigación que le ayudará a mejorar la seguridad de la información de manera significativa, debido al desarrollo de un plan de seguridad de la información basado en la norma ISO27001:2013.

El área de sistemas debe contar con los recursos necesarios y el liderazgo en la ejecución de las cláusulas de la norma ISO27001:2013, debe haber un compromiso efectivo se debe comunicar los roles y responsabilidades de la seguridad de la información.

Los empleados de la empresa deben tener conocimiento de las buenas prácticas y recomendaciones que brinda la norma ISO 27001:2013, el cumplimiento de los controles se debe realizar de manera adecuada, para minimizar los riesgos a los que está expuesto la empresa.

La implementación de la norma ISO27001:2013 considerando cada una de las clausulas y los controles establecidos en el anexo A de la norma y contar con los documentos necesarios indicados por el estándar ayudará de manera significativa en la mitigación de riesgos a los que pueda estar expuesto la empresa.

**REFERENCIAS**


Arévalo, A., Bayona, T., & Rico, B. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura*, 123-134. doi:http://dx.doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10.

Atencio, E. (2019). Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú. *Tesis de Maestro.* Universidad Nacional Daniel Acides Carrión, Pasco-Perú. Obtenido de http://repositorio.undac.edu.pe/handle/undac/1474

Barrera, A. (2019). PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDAD EDUCATIVA NUESTRA SEÑORA DE FÁTIMA. *(Tesis de Grado).* UNIVERSIDAD TECNOLÓGICA ISRAEL, Quito-Ecuador. Obtenido de http://repositorio.uisrael.edu.ec/handle/47000/1901

Benites, D. (2019). Implementación de un Sistema de Gestión de Seguridad de la Información-Norma ISO 27001 para la FábricaRadiadores Fortaleza. *(Tesis de Grado).* Universidad Tecnológica del Perú, Lima-Perú. Obtenido de http://repositorio.utp.edu.pe/handle/UTP/1933

CAL. (20 de Noviembre de 2020). *Ley de Protección de Datos 29733*. Obtenido de Colegio de Abogados de Lima – CAL: https://www.cal.org.pe/v1/ley-de-proteccion-de-datos-29733/

Cano, M., & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 470-483.

Cárdenas, S., Martínez, A., & Becerra, A. (2016). Gestión de seguridad de la información. *Profesional de la Información*, 931-948. doi:https://doi.org/10.3145/epi.2016.nov.10

Cardona, L., & Carvajal, P. (2018). DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA FAMILIA DE NORMAS DE LA SERIE ISO/IEC 27000 PARA UNA ENTIDAD PÚBLICA

COLOMBIANA. *(Tesis de Magister).* UNIVERSIDAD AUTÓNOMA DE MANIZALES, Manizales-Colombia.

Ccesa, Q. (2017). Diseño de un sitema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. *(Tesis de Grado).* Universidad Nacional San Cristóbal de Huamanga, Ayacucho-Perú. Obtenido de http://repositorio.unsch.edu.pe/handle/UNSCH/1751

Cevallos, J. (2019). ISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TICS DEL INSTITUTO TECNOLÓGICO SUPERIOR CENTRAL TÉCNICO, BASADO EN LA NORMA DE SEGURIDAD ISO/IEC 27002:2013. *Tesis Master.* UNIVERSIDAD INTERNACIONAL SEK, Quito-Ecuador.

Córdoba, S. (2015). Diseño e implementación de un SGSI para el área de informática de la Curaduría Urbana segunda de PASTO bajo la norma ISO/IEC 27001. *(Tesis de Grado).* Universidad Nacional Abierta Y Distancia "UNAD", Pasto, Colombia. Obtenido de https://repository.unad.edu.co/handle/10596/3627

CRAI. (2018). *¿Cuál es el propósito de la Investigación Aplicada?* Obtenido de CRAI-Centro de recursos para el aprendizaje y la investigación: http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

Disterer, G. (2013). ISO / IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información. *Investigación Científica, 4*(2), 92-100. doi:10.4236 / jis.2013.42011

ESAN. (11 de Mayo de 2016). *Importancia y beneficios de contar con un Sistema de Gestión de Seguridad de Información*. Obtenido de ESAN: https://www.esan.edu.pe/apuntes-empresariales/2016/05/importancia-y-beneficios-de-contar-con-un-sistema-de-gestion-de-seguridad-de-informacion/

ESAN. (07 de Noviembre de 2018). *¿Cómo construir un escenario de riesgos, amenazas y vulnerabilidades?* Obtenido de ESAN: https://www.esan.edu.pe/apuntes-empresariales/2018/11/como-construir-un-escenario-de-riesgos-amenazas-y-vulnerabilidades/

Escuela Europea de Excelencia. (Agosto de 2019). *Qué es y para qué sirve la Declaración de Aplicabilidad en ISO 27001*. Obtenido de Escuela Europea de Excelencia: https://www.escuelaeuropeaexcelencia.com/2019/08/que-es-y-para-que-sirve-la-declaracion-de-aplicabilidad-en-iso-27001

ESET. (2020). *Security Report Latinoamérica 2020.* Argentina: ESET. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Figueroa, C. (2018). Diseño de un sistema de gestión de seguridad de la información para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC ISO/IEC 27001:2013. *(Tesis de grado).* Universidad Nacional Abierta y a Distancia UNAD, Bogotá-Colombia. Obtenido de https://repository.unad.edu.co/handle/10596/25633

Gaona, V. (2013). APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A. EN LA CIUDAD DE MACHALA. *(Tesis de Grado).* Universidad Politécnica Salesiana Sede Cuenca, Machala-Ecuador. Obtenido de https://dspace.ups.edu.ec/handle/123456789/5272

Gil, M. (26 de Marzo de 2019). *Menos de 150 empresas peruanas cuentan con certificación en seguridad de la información*. Obtenido de Gestión: https://gestion.pe/tecnologia/150-empresas-peruanas-cuentan-certificacion-cibercrimen-262366-noticia/

Gómez, Á. (2014). *Respuesta a incidentes de Seguridad y planes para la continuidad del Negocio.* Madrid: RA-MA, S.A. Editorial y Publicaciones.

González, A., & Pazmiño, S. (2015). Cálculo e interpretación del Alfa de Cronbach para el caso de validación de la consistencia interna de un cuestionario, con dos posibles escalas tipo Likert. *Publicando, 2*(1), 68. Obtenido de https://www.ssoar.info/ssoar/bitstream/handle/document/42382/ssoar-revpublicando-2015-1-gonzalez_alonso_jorge_et_al-Calculo_e_interpretacion__del.pdf

INCIBE. (20 de Marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido de Institulo Nacional de Ciberseguridad:

https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

ISO. (Octubre de 2013). *ISO / IEC 27001: 2013*. Obtenido de Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos: https://www.iso.org/standard/54534.html

ISO. (2019). *09. Encuesta ISO de certificaciones para estándares de sistemas de gestión - Resultados completos.* ISO. Obtenido de https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse

ISO27000. (2020). *Glosario*. Obtenido de ISO27000.es: https://www.iso27000.es/glosario.html

iso27000. (26 de Noviembre de 2020). *ISO27000.es*. Obtenido de SGSI: https://www.iso27000.es/sgsi.html

ISO27001. (2017). *NORMA ISO 27001*. Obtenido de ISO27001: https://normaiso27001.es/referencias-normativas-iso-27000/

ISO27002. (Octubre de 2013). *CONTROLES DE SEGURIDAD*. Obtenido de Modelo de declaración de aplicabilidad (SoA) en 5 idiomas distintos : https://www.iso27000.es/iso27002.html

ISOTools. (11 de Enero de 2019). *5 beneficios de implementar un sistema de gestión de seguridad de la información*. Obtenido de ISOTools: https://www.isotools.org/2019/01/11/5-beneficios-implementar-sistema-gestion-seguridad-informacion/

ISOTools. (2020). *Estructura de la norma ISO 27001*. Obtenido de ISOTools: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOWin. (2020). *Las Amenazas en la norma ISO 27001 2017*. Obtenido de ISOWin: https://isowin.org/blog/amenazas-ISO-27001/

Joya, C., & Sacristán, H. (2017). *Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para la Empresa Javesalud I.P.S.* Universidad Católica De Colombia, Bogotá-Colombia. Obtenido de http://hdl.handle.net/10983/15405

Khalid, A., Shamsul, K., Noor, S., Sapiee, J., & Kamaruddin, M. (2019). A policy driven, human oriented information security model: a case study in UAE

banking sector. *IEEE Conference on Application, Information and Network Security (AINS)*. doi:10.1109/AINS47559.2019.8968705

Konzen, M. (2013). GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA. *(Grado de Maestro).* Universidad Federal de Santa María, Santa María-Brasil. Obtenido de http://repositorio.ufsm.br/handle/1/8276

Mantilla, G. (2017). Gestión de seguridad de la información con la norma ISO 27001:2013. *Espacios, 39*(18), 5. Obtenido de https://www.revistaespacios.com/a18v39n18/18391805.html

Massco, T. (2017). Propuesta De Un Plan De Seguridad De La Información Basado En La Norma ISO 27001 Para La Empresa Desysweb S.A.C. En El Periodo 2017. *(Tesis de Grado).* Universidad Nacional Tecnológica de Lima Sur, Lima-Perú. Obtenido de http://repositorio.untels.edu.pe/handle/UNTELS/260

Mataracioglu, T. (2017). Propuesta para la próxima versión de la norma ISO / IEC 27001. *ISACA, 4*, 1-2.

Méndez, G. (2018). ANALISIS DE MODELO DE GOBIERNO CON ENFOQUE EN SEGURIDAD DE LA INFORMACIÓN. *(Tesis de Grado).* Universidad Señor de Sipán, Pimentel, Perú. Obtenido de https://hdl.handle.net/20.500.12802/5935

MINHAP. (2012). *Libro I MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: © Ministerio de Hacienda y Administraciones Públicas. Obtenido de http://administracionelectronica.gob.es/

MINHAP. (2012). *Libro II MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: © Ministerio de Hacienda y Administraciones Públicas.

MINHAP. (2012). *Libro III MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: © Ministerio de Hacienda y Administraciones Públicas. Obtenido de http://administracionelectronica.gob.es/

Nasser, A. (2017). Análisis de brechas de seguridad de la información basado en ISO 27001: 2013 estándar: A estudio de caso de la Academia Yemení de

Estudios de Posgrado, Sana'a, Yem. *Revista Internacional de Investigación Científica en Estudios multidisciplinarios*, 4-13.

NovaSec. (01 de Septiembre de 2018). *ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI*. Obtenido de NovaSec: https://www.novasec.co/en/blog/62-gestion-integral-de-la-seguridad-de-la-informacion

OBS. (2020). *Que son activos de una empresa*. Obtenido de OBS Business School: https://www.obsbusiness.school/blog/que-son-los-activos-de-una-empresa-y-como-se-valoran

PAE. (02 de Diciembre de 2020). *Portal Institucional del Ministerio de Hacienda*. Obtenido de Portal Administrativo Electronico: https://www.hacienda.gob.es/es-ES/Paginas/Home.aspx

pmg-ssi. (13 de Abril de 2015). *ISO 27001: El impacto en los Sistemas de Gestión de Seguridad de la Información*. Obtenido de pmg-ssi: https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

pmg-ssi. (30 de Marzo de 2015). *ISO 27001: Los activos de información*. Obtenido de pmg-ssi: https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

Ramírez, C. (2014). Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013. *(Grado de Master).* Universitat Oberta de Catalunya, Calalunya-España.

Romero, M., Araujo, G., Mestre, A., Galindo, O., Rueda, C., Bracho, T., & Quintero, T. (2019). *TECNOLOGÍA INTERCULTURALIDAD Y NATURALEZA.* Bogotá-Colombia: Ibáñez.

SERMAN. (22 de Octubre de 2013). *Qué es el ciclo de vida de la información*. Obtenido de SERMAN: https://serman.com/blog-recuperacion-datos/que-es-el-ciclo-de-vida-de-la-informacion/

Tsung-Han, Y., Cheng-Yuan, K., & Man-Nung, L. (2016). Un sistema integrado para la gestión de la seguridad de la información con el marco unificado. *Journal of Risk Research, 1*(19), 21-41. doi:10.1080/13669877.2014.940593

UNIR. (11 de Diciembre de 2019). *Gestión de la calidad PDCA*. Obtenido de UNIR La universidad en internet: https://www.unir.net/ingenieria/revista/iso-27001/

Vásquez. (2020). Diseño de un Sistema de Gestión de Seguridad de Información para la empresa Neointel SAC basado en la norma ISO/IEC 27001:2013. *(Tesis de Grado).* Universidad Peruana de Ciencias Aplicadas (UPC), Lima-Perú. doi:http://doi.org/10.19083/tesis/652123

## ANEXOS

**Anexo 1.** Resolución de aprobación del trabajo de investigación

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO**
**RESOLUCIÓN N°2136-2020/FIAU-USS**

Pimentel, 22 de septiembre de 2020

**VISTO:**
El Acta de reunión N°2109 - 2020, de fecha 21 de septiembre de 2020 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS, para la ejecución de la Tesis: **"DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS"**, presentado por **MENDEZ GALVEZ CIPRIANO,** del Programa de estudios **INGENIERÍA DE SISTEMAS**, y;

**CONSIDERANDO:**

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48º que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24º señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, en el Acta de reunión N°2109 - 2020 de fecha 21 de septiembre de 2020, del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS, se indica entre los acuerdos la aprobación del tema de la Tesis denominado "DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS" de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de MENDEZ GALVEZ CIPRIANO en condición de egresado, del Programa de estudios INGENIERÍA DE SISTEMAS.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

**SE RESUELVE:**

**ARTÍCULO 1°: APROBAR,** el tema de la Tesis denominado **"DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS",** perteneciente a la línea de investigación de **INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE**, a cargo de **MENDEZ GALVEZ CIPRIANO**, del Programa de estudios **INGENIERÍA DE SISTEMAS.**

**ARTÍCULO 2°: ESTABLECER,** que la inscripción del Título de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

**ARTÍCULO 3°: DEJAR SIN EFECTO,** toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

**REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE**

Dr. Mario Fernando Ramos Morcil
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Mtra. María Noelia Sialer Rivera
Secretaria Académica - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

*Cc: Interesado, Archivo*

**Anexo 2.** Carta de aceptación de la institución para la recolección de datos.

**SOLICITO: PERMISO PARA LA RECOLECCION DE DATOS**

Sr. Víctor Martin Adrianzén Lizama
Representante Legal - Vinculaperu Corredores de Seguros E.I.R.L.

Yo Cipriano Méndez Gálvez identificado con DNI N° 25860501 con domicilio en el A.H. Francisco Bolognesi Mza. J. Lt. 9 –Callao, ante su representada respetuosamente me presento y expongo.

Que siendo bachiller de la carrera Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán, solicito a su representada me conceda el permiso para la recolección de datos para mi proyecto de investigación titulado "DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS" ya que es necesario para la presentación del trabajo final.

Por lo expuesto
Ruego a usted acceder a mi petición

Callao 02 de diciembre de 2020

**Firma del Investigador**
Cipriano Méndez Gálvez

**Firma del Representante**
Victor M. Adrianzén Lizama

Vinculaperu Corredores de Seguros E.I.R.L.

Callao, 10 de diciembre de 2020

Quien suscribe

Sr. Víctor Martín Adrianzén Lizama
Representante Legal-Vinculaperu Corredores de Seguros E.I.R.L.

**AUTORIZA:** Permiso para recojo de información pertinente en función del proyecto de investigación, denominado: **"DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS".**

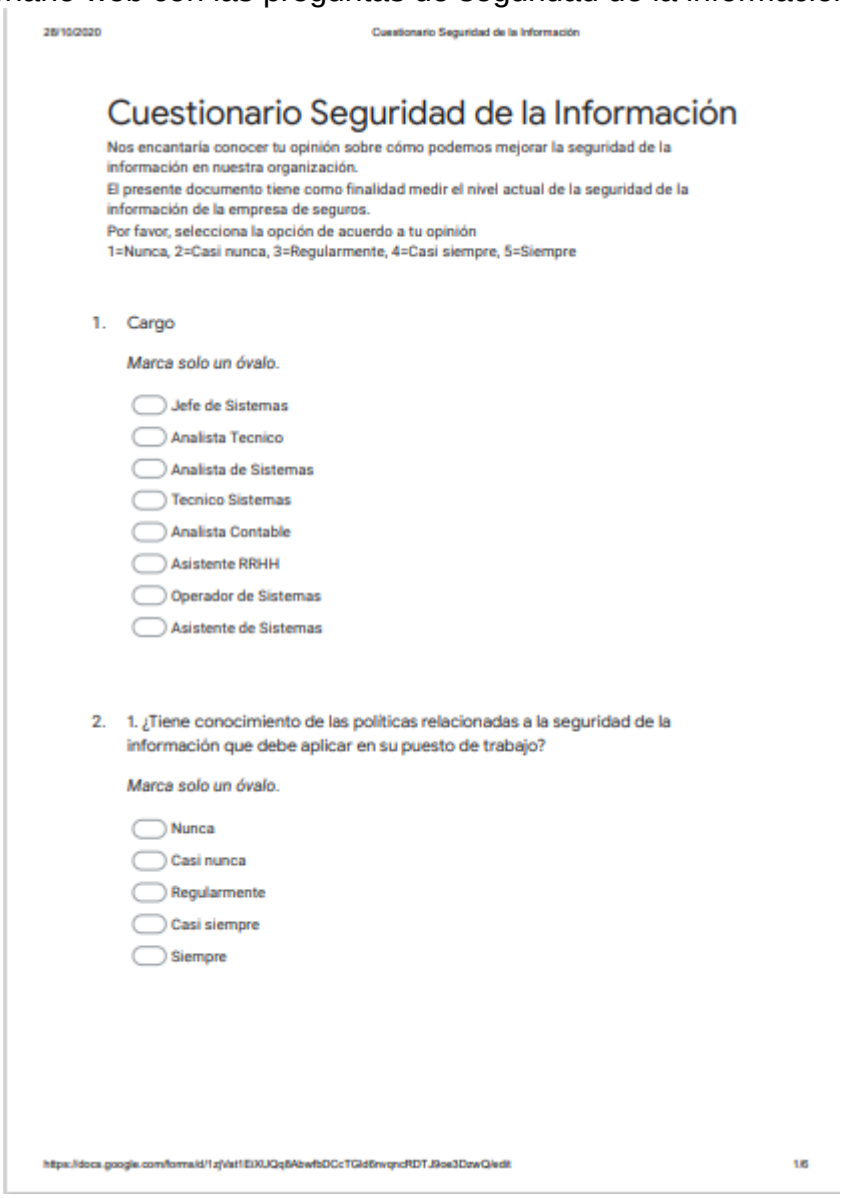
Por el presente, el que suscribe, Sr, Víctor Martín Adrianzén Lizama representante legal de la empresa Vinculaperu Corredores de Seguros E.I.R.L., AUTORIZO al estudiante Cipriano Méndez Gálvez identificado con DNI N° 25860501 de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán y autor del trabajo de investigación denominado: **"DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS. CASO DE ESTUDIO: EMPRESA DE SEGUROS"**, al uso de la información concerniente para el caso, para efectos exclusivamente de la elaboración de la tesis de grado enunciado líneas arriba de quien solicita se garantice la absoluta confidencialidad de la información solicitada.

Atentamente.

Víctor Martín Adrianzén Lizama
DNI N° 46803768
Jefe Dpto. de Informática

**Anexo 3:** Encuesta para medir el nivel actual de la seguridad de la información

Cuestionario web con las preguntas de seguridad de la información



28/10/2020 Cuestionario Seguridad de la Información

# Cuestionario Seguridad de la Información

Nos encantaría conocer tu opinión sobre cómo podemos mejorar la seguridad de la información en nuestra organización.
El presente documento tiene como finalidad medir el nivel actual de la seguridad de la información de la empresa de seguros.
Por favor, selecciona la opción de acuerdo a tu opinión
1=Nunca, 2=Casi nunca, 3=Regularmente, 4=Casi siempre, 5=Siempre

1. Cargo

*Marca solo un óvalo.*

- Jefe de Sistemas
- Analista Tecnico
- Analista de Sistemas
- Tecnico Sistemas
- Analista Contable
- Asistente RRHH
- Operador de Sistemas
- Asistente de Sistemas

2. 1. ¿Tiene conocimiento de las políticas relacionadas a la seguridad de la información que debe aplicar en su puesto de trabajo?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

https://docs.google.com/forms/d/1zjVat1EiXUQq8AbwfbDCcTGld0nvqncRDTJ9oe3DzwQ/edit 1/6

3. 2. ¿La empresa brinda capacitaciones a los empleados para concientizar sobre la importancia de la seguridad de la información en la empresa?

   *Marca solo un óvalo.*

   - ◯ Nunca
   - ◯ Casi nunca
   - ◯ Regularmente
   - ◯ Casi siempre
   - ◯ Siempre

4. 3. ¿Tiene conocimiento si la empresa ha sufrido algún ataque informático durante estos 3 últimos años?

   *Marca solo un óvalo.*

   - ◯ Nunca
   - ◯ Casi nunca
   - ◯ Regularmente
   - ◯ Casi siempre
   - ◯ Siempre

5. 4. ¿Ha tenido algún percance o incidente referente a la seguridad de la información en su puesto de trabajo?

   *Marca solo un óvalo.*

   - ◯ Nunca
   - ◯ Casi nunca
   - ◯ Regularmente
   - ◯ Casi siempre
   - ◯ Siempre

6. 5. ¿Si tuvo algún percance o incidente, fue informado?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

7. 6. ¿El activo entregado para sus labores en este caso una Laptop u otro dispositivo, al sufrir algún incidente, la respuesta o la atención para solucionar el incidente fue inmediato?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

8. 7. ¿Hace uso de contraseñas seguras Ejm: 8 Caracteres Alfanuméricos entre los cuales debe haber una Mayúscula, un número y un signo?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

9. 8. ¿Tu equipo asignado tuvo algún mantenimiento preventivo hace un año?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

10. 9. ¿Hace uso de medios extraíbles como USB, Disco Externo, etc.. para el traslado de alguna información?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

11. 10. ¿Los accesos a lugares restringidos tienen una medida adecuada de seguridad?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

12. 11. ¿Al realizar impresiones de documentos confidenciales, en algún momento se olvidó en su escritorio o en la impresora?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

13. 12. ¿Ud. Realiza el bloqueo de su computadora cuando se retira de su puesto de trabajo?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

14. 13. ¿La disponibilidad de los aplicativos para los clientes es continua?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

15. 14. ¿Tuvo la necesidad de instalar programas nuevos en su equipo asignado?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

16. 15. ¿La implementación de un plan de seguridad de la información basado en normas internacionales, ayudara a mejorar la seguridad de la información en la empresa?

*Marca solo un óvalo.*

- Nunca
- Casi nunca
- Regularmente
- Casi siempre
- Siempre

**Anexo 4: Resultados de evaluación inicial a alto nivel**

**FORMATO DE OBSERVACION REQ. OBLIGATORIOS ISO 27001**

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| **4** | **Contexto de la organización** | | |
| **4.1** | **Comprensión de la organización y de su contexto** | | La empresa de Seguros actualmente tiene documentos de su Misión, Visión, Matriz FODA y Estrategias. La empresa debe establecer objetivos en temas de seguridad de la Información que estén alineados con sus objetivos estratégicos. |
| 4.1 | Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia | Inicial | |
| **4.2** | **Comprensión de las necesidades y expectativas de las partes interesadas** | | La empresa de seguros, debe determinar las partes interesadas y los requisitos de las mismas. |
| 4.2 (a) | Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc. | Inicial | |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| 4.2 (b) | Determinar los requerimientos y obligaciones relevantes de seguridad de la información | Inicial | |
| **4.3** | **Determinación del alcance del SGSI** | | La empresa de seguros, actualmente cuenta con una política seguridad interna pero no tiene determinado los límites y la aplicabilidad, por lo cual la empresa debe determinar los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la información para establecer su alcance. |
| 4.3 | Determinar y documentar el alcance del SGSI | Repetible | |
| **4.4** | **SGSI** | | La empresa de seguros, no cuenta con un plan de mejoramiento continuo en temas de SGSI, por lo cual debe establecer, implementar, mantener y mejorar de manera continua un Sistema de gestión de la seguridad de la información, de acuerdo a la norma ISO27001:2013. |
| 4.4 | Establecer, implementar, mantener y mejorar de forma continua | Inicial | |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| | el SGSI acorde al estándar | | |
| **5** | **Liderazgo** | | |
| **5.1** | **Liderazgo y compromiso** | | Actualmente la empresa de seguros, cuenta con personal responsable de cada área, pero el personal no cuenta con roles con autoridad y responsabilidades en temas de SGSI, por lo cual la alta dirección, debe mostrar liderazgo y compromiso respecto al SGSI. Por ende, debe asignar roles y responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información, por lo cual es importante establecer, una Política de Seguridad de la Información, y los objetivos de seguridad de la información acorde al propósito de la organización. |
| 5.1 | La administración debe demostrar liderazgo y compromiso por el SGSI | Inicial | |
| **5.2** | **Política** | | Actualmente la empresa de seguros cuenta con políticas de seguridad interna, pero esas políticas no se cumplen, por lo cual es necesario establecer y mejorar la Políticas de |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| | | | Seguridad de la Información acorde al propósito empresa. |
| 5.2 | Documentar la Política de Seguridad de la Información | Inicial | |
| **5.3** | **Roles, responsabilidades y autoridades en la organización** | | La empresa de seguros no cuenta con personal especialista en SGSI, por lo cual la alta dirección debe garantizar que las responsabilidades y la autoridad para los roles relevantes en temas de seguridad de la información sean asignadas y comunicadas a toda la organización. |
| 5.3 | Asignar y comunicar los roles y responsabilidades de seguridad de la información | Inicial | |
| **6** | **Planificación** | | La empresa de seguros no tiene procedimientos para la valoración de riesgos en temas de seguridad de la información, por lo cual es necesario que la empresa adopte, planifique y documente un procedimiento de valoración y tratamiento de riesgos de la seguridad de la información y estos deben estar conforme a los propósitos de la empresa. |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| **6.1** | **Acciones para tratar los riesgos y oportunidades** | | |
| 6.1.1 | Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades | Inicial | |
| 6.1.2 | Definir e implementar un proceso de análisis de riesgos de seguridad de la información | Inicial | |
| 6.1.3 | Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información | Inicial | |
| **6.2** | **Objetivos de seguridad de la información y planificación para su consecución** | | |
| 6.2 | Establecer y documentar los planes y objetivos | Inicial | |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| | de la seguridad de la información | | |
| **7** | **Soporte** | | La empresa de seguros no asigna un presupuesto adecuado para temas de seguridad de la información, al implementar un SGSI, la organización de asignar un presupuesto para la implementación, mantenimiento y mejora continua del SGSI. |
| **7.1** | **Recursos** | | |
| 7.1 | Determinar y asignar los recursos necesarios para el SGSI | Inicial | |
| **7.2** | **Competencia** | | |
| 7.2 | Determinar, documentar hacer disponibles las competencias necesarias | Inicial | |
| **7.3** | **Concienciación** | | |
| 7.3 | Implementar un programa de concienciación de seguridad | Inicial | |
| **7.4** | **Comunicación** | | |
| 7.4 | Determinar la necesidades de comunicación | Inicial | |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| | internas y externas relacionadas al SGSI | | |
| **7.5** | **Información documentada** | | |
| 7.5.1 | Proveer documentación requerida por el estándar más la requerida por la organización | Inexistente | |
| 7.5.2 | Proveer un título, autor, formato consistente, revisión y aprobación a los documentos | Inexistente | |
| 7.5.3 | Mantener un control adecuado de la documentación | Inexistente | |
| **8** | **Operación** | | Actualmente la empresa de seguros no cuenta con un SGSI implementado, pero al realizar la implementación del SGSI, se debe planificar, controlar y documentar los procesos necesarios para cumplir con los requisitos de seguridad de la información y estar seguros de que los procesos se llevan a cabo acorde a lo planeado. |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| **8.1** | **Planificación y control operacional** | | |
| 8.1 | Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos) | Inicial | |
| **8.2** | **Apreciación de los riesgos de seguridad de la información** | | |
| 8.2 | Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios | Inexistente | |
| **8.3** | **Tratamiento de los riesgos de seguridad de la información** | | |
| 8.3 | Implementar un plan de tratamiento de riesgos y | Inexistente | |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| | documentar los resultados | | |
| **9** | **Evaluación del desempeño** | | Actualmente la empresa de seguros no cuenta con un SGSI implementado, pero al realizar la Implementación del SGSI se debe y elaborar un plan para realizar la evaluación de manera periódica el funcionamiento del SGSI y garantizar correcto funcionamiento y las evaluaciones deben ser documentadas. |
| **9.1** | **Seguimiento, medición, análisis y evaluación** | | |
| 9.1 | Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles | Inexistente | |
| **9.2** | **Auditoría interna** | | |
| 9.2 | Planificar y realizar una auditoria interna del SGSI | Inexistente | |
| **9.3** | **Revisión por la dirección** | | |
| 9.3 | La administración realiza una revisión periódica del SGSI | Inexistente | |

| Sección | Requerimientos ISO 27001 | Estado | Comentarios |
|---|---|---|---|
| **10** | **Mejora** | | Actualmente la empresa de seguros no cuenta con un SGSI implementado, al realizar la implantación el SGSI y se debe elaborar un plan de mejora continua para mejorar el SGSI de acuerdo a los nuevos cambios en la organización, tecnologías, nuevas amenazas, para mantener los riesgos controlados. |
| **10.1** | **No conformidad y acciones correctivas** | | |
| 10.1 | Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones | Inicial | |
| **10.2** | **Mejora continua** | | |
| 10.2 | Mejora continua del SGSI | Inicial | |

Nota: Datos tomados del documento (ISO27k_ISMS_and_controls_status_with_SoA_and_gaps_Spanish.xlsx, pestaña-Req. Obligatorios SGSI) de requisitos obligatorios de SGSI, ISO27001. Fuente: Elaboración Propia.

**Anexo 5: Descripción de las preguntas de la encuesta para identificar las vulnerabilidades y amenazas.**

Pregunta 1:

¿Tiene conocimiento de las políticas relacionadas a la seguridad de la información que debe aplicar en su puesto de trabajo?

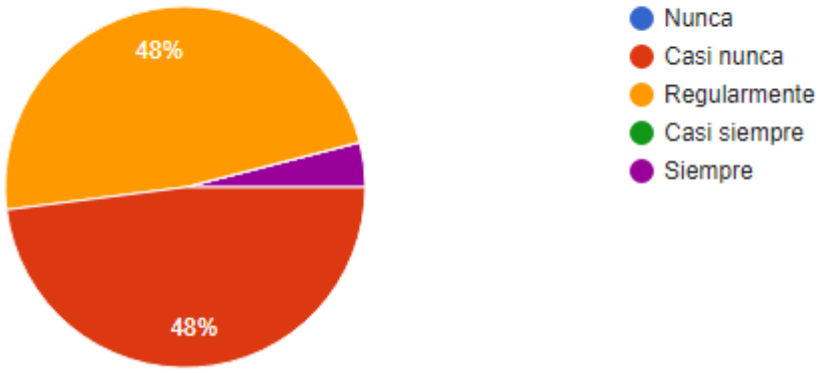



*Figura 43*. ¿Tiene conocimiento de las políticas relacionadas a la seguridad de la información que debe aplicar en su puesto de trabajo?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 48% indico que tiene poco conocimiento, el 48% tiene conocimiento medio y que solo el 4% tiene conocimiento de las políticas relacionadas que debe aplicar en su puesto de trabajo, por lo cual es importante el desarrollo de un plan de seguridad de la información para reforzar los temas de concientización.

Pregunta 2:

¿La empresa brinda capacitaciones a los empleados para concientizar sobre la importancia de la seguridad de la información en la empresa?

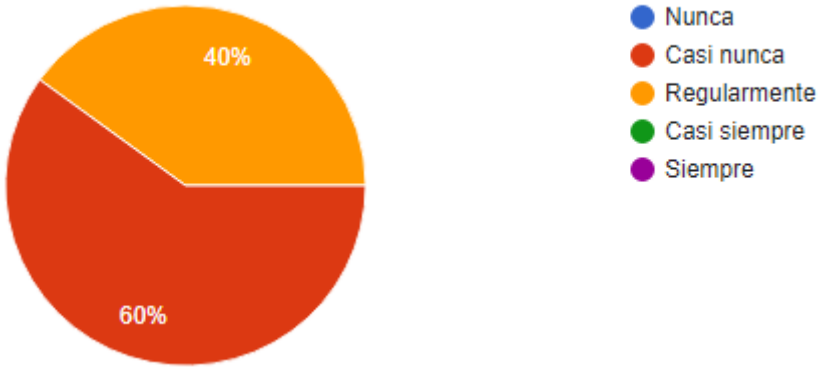



*Figura 44*. ¿La empresa brinda capacitaciones a los empleados para concientizar sobre la importancia de la seguridad de la información en la empresa?. Fuente: Elaboración Propia

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 60% indicó que se realiza capacitaciones en temas de seguridad de la información de manera muy esporádica, el 40% indicó haber recibido de alguna manera una capacitación en termas de seguridad de la información, por lo cual es importante el desarrollo de un plan en seguridad de la información.

Pregunta 3:
¿Tiene conocimiento si la empresa ha sufrido algún ataque informático durante estos 3 últimos años?


*Figura 45.* ¿Tiene conocimiento si la empresa ha sufrido algún ataque informático durante estos 3 últimos años?. Fuente: Elaboración Propia

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 100% desconoce que la empresa haya sufrido algún ataque a sus activos informáticos, este punto es muy importante para la organización ya que la empresa ha sabido proteger su información, pero es necesario que cuente con controles más adecuados para mejorar la protección.

Pregunta 4:

¿Ha tenido algún percance o incidente referente a la seguridad de la información en su puesto de trabajo?

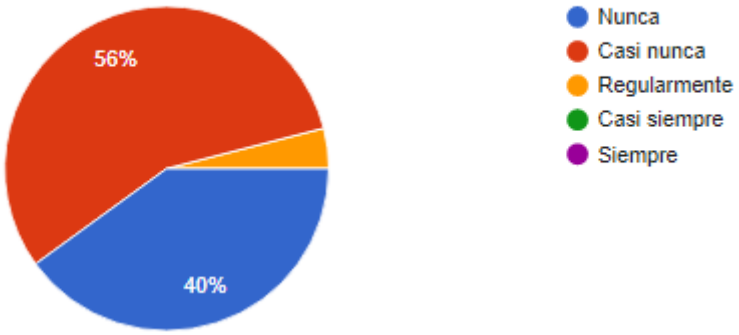



*Figura 46*. ¿Ha tenido algún percance o incidente referente a la seguridad de la información en su puesto de trabajo?. Fuente: Elaboración Propia

Pregunta 5:

¿Si tuvo algún percance o incidente, fue informado?

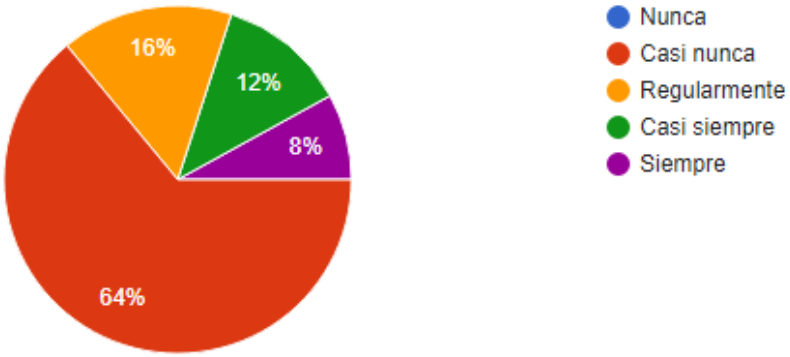



*Figura 47.* ¿Si tuvo algún percance o incidente, fue informado?. Fuente: Elaboración Propia

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 64% no informa en el momento adecuado sobre el incidente o percance que tuvo durante sus labores, el 16% informó de manera regular, el 12% indicó que informa casi en totalidad y solo el 8% informa de manera adecuada y oportuna, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se debe tomar puntos en temas de concientización del personal en temas de seguridad.

Pregunta 6:

¿El activo entregado para sus labores en este caso una Laptop u otro dispositivo, al sufrir algún incidente, la respuesta o la atención para solucionar el incidente fue inmediato?

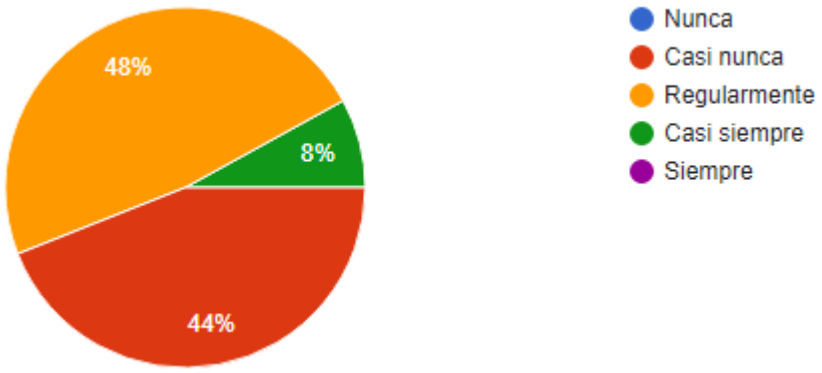



Figura 48. ¿El activo entregado para sus labores en este caso una Laptop u otro dispositivo, al sufrir algún incidente, la respuesta o la atención para solucionar el incidente fue inmediato?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 44% indicó que la atención a los incidentes suscitados a sus equipos es muy lenta, el 48% manifestó que la atención se realiza de manera regular y el 8% informó que la atención se realiza de manera casi inmediata, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique el tema de gestión de activos.

Pregunta 7:

¿Hace uso de contraseñas seguras Ejm: 8 Caracteres Alfanuméricos entre los

cuales debe haber una Mayúscula, un número y un signo?

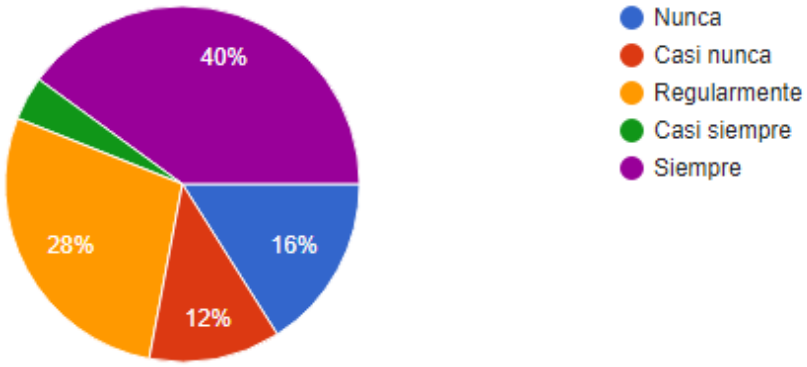



*Figura 49*. ¿Hace uso de contraseñas seguras Ejm: 8 Caracteres Alfanuméricos entre los cuales debe haber una Mayúscula, un número y un signo?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 16% no utiliza contraseñas seguras, el 12% indicó que a veces utiliza contraseñas seguras, el 28% usa contraseñas seguras de manera regular y el 4% utiliza casi siempre contraseñas seguras y solo el 40% sigue utiliza contraseñas seguras, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de Seguridad de la Información.

Pregunta 8:

¿Tu equipo asignado tuvo algún mantenimiento preventivo hace un año?

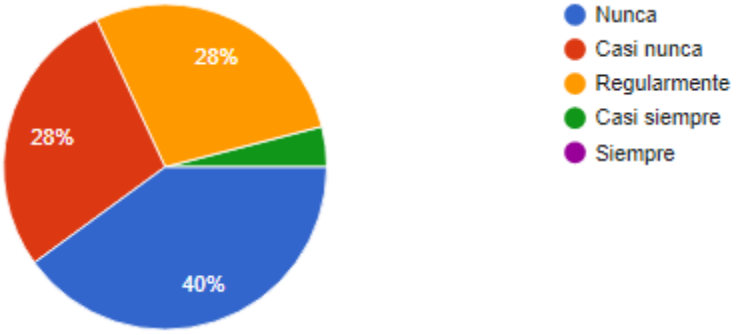



*Figura 50*. ¿Tu equipo asignado tuvo algún mantenimiento preventivo hace un año?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 40% mencionó que sus equipos asignados no

tuvieron mantenimiento en el transcurso de un año, el 28% indicó que en algún momento si realizaron mantenimiento a su equipo asignado, el 28% indicó que el mantenimiento de sus equipos se realiza de manera regular y el 4% indicó que el mantenimiento a su equipo se realizó en el momento oportuno, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique la gestión de activos.

Pregunta 9:

¿Hace uso de medios extraíbles como USB, Disco Externo, etc. para el traslado de alguna información?

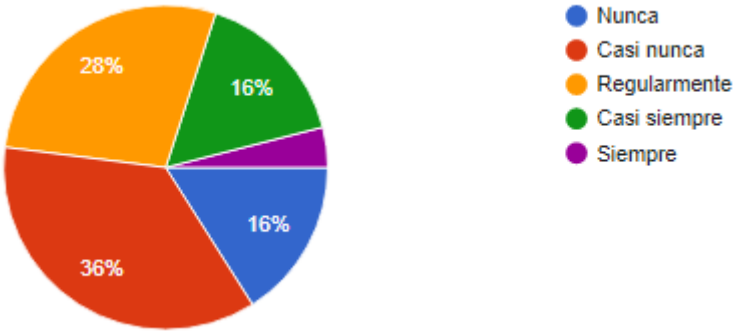



*Figura 51*. ¿Hace uso de medios extraíbles como USB, Disco Externo, etc. para el traslado de alguna información?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 16% no hace uso de medios extraíbles para trasladar la información, el 36% indicó que hizo uso del medio extraíble en alguna oportunidad, el 28% indicó que usa medios extraíbles para de manera regular, el 16% indicó que casi siempre utiliza un medio extraíble y el 4% hace uso de los medios extraíbles en todo momento, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de clasificación de la información.

Pregunta 10:

¿Los accesos a lugares restringidos tienen una medida adecuada de seguridad?

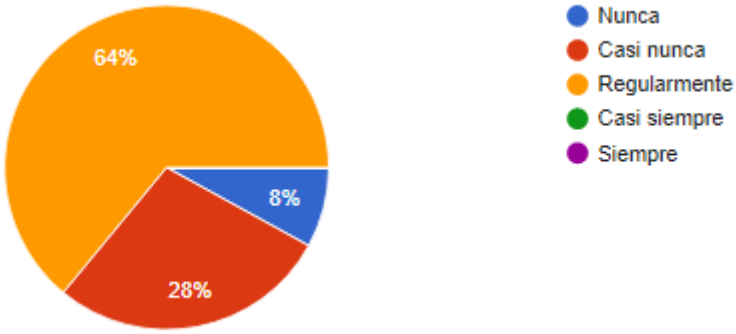



*Figura 52.* ¿Los accesos a lugares restringidos tienen una medida adecuada de seguridad?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 8% indicó que los accesos a lugares restringidos no cuentan con medidas adecuadas, el 28% indicó que los accesos a lugares restringidos no tienen una medida adecuada, el 64% indicó que regularmente el acceso a los lugares restringidos si está seguro, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de acceso para minimizar los riesgos.

Pregunta 11:
¿Al realizar impresiones de documentos confidenciales, en algún momento se olvidó en su escritorio o en la impresora?

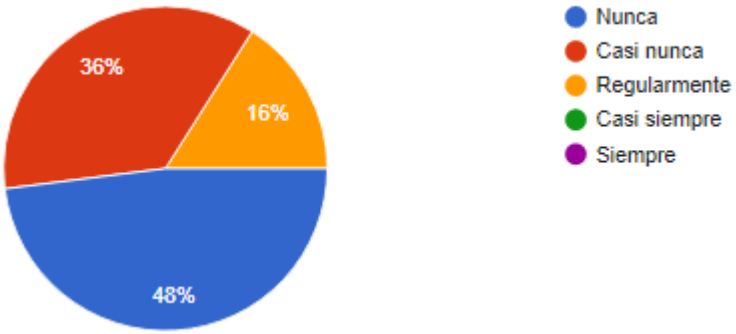



*Figura 53.* ¿Al realizar impresiones de documentos confidenciales, en algún momento se olvidó en su escritorio o en la impresora?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 48% indicó tener conocimiento de la importancia de los documentos confidenciales por lo cual tienen mucho cuidado al momento de exponer los documentos en lugares públicos, el 36% indicó que a veces se olvida los documentos impresos, el 16% indicó que en algunas oportunidades se olvidó el documento en la sala de impresión o en su lugar de trabajo, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de concientización al personal.

Pregunta 12:

¿Ud. Realiza el bloqueo de su computadora cuando se retira de su puesto de trabajo?

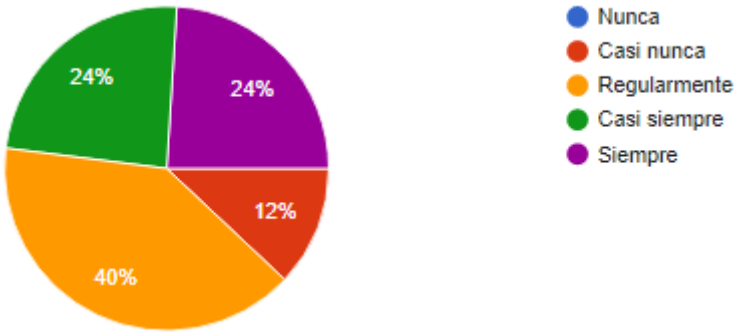



*Figura 54.* ¿Ud. Realiza el bloqueo de su computadora cuando se retira de su puesto de trabajo?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 12% en alguna oportunidad no realizó el bloqueo de su equipo al momento de retirarse de su lugar de trabajo, el 40% indicó que a veces se olvida de bloquear su equipo, el 14% indicó que casi siempre bloquean sus equipos y el 24% si realiza el bloqueo de su equipo asignado, por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de concientización al personal.

Pregunta 13:

¿La disponibilidad de los aplicativos para los clientes es continua?

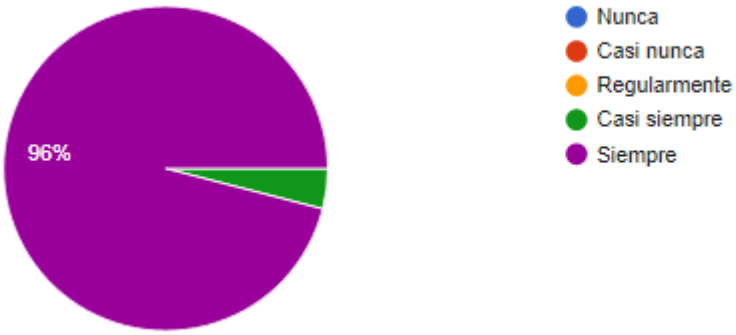



*Figura 55.* ¿La disponibilidad de los aplicativos para los clientes es continua?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 4% indico que en una oportunidad no hubo disponibilidad de los aplicativos, el 96% indicó la disponibilidad de los aplicativos es continua, para que la disponibilidad sea al 100% es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de gestión de incidentes de seguridad de la información.

Pregunta 14:
¿Tuvo la necesidad de instalar programas nuevos en su equipo asignado?

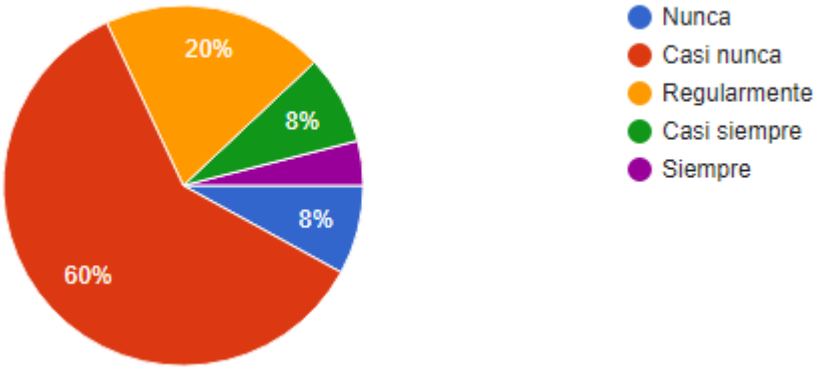



*Figura 56.* ¿Tuvo la necesidad de instalar programas nuevos en su equipo asignado?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 8% indicó que nunca realizó la instalación de

programas nuevos por necesidades del trabajo, el 60% indicó que en alguna oportunidad realizó la instalación de algún software, el 20% indicó que instala software de manera regular, el 8% indico que casi siempre instala software nuevo y el 8% manifestó que siempre instala algún software por lo cual es importante el desarrollo de un plan de seguridad de la información donde se aplique Controles de gestión de activos.

Pregunta 15:

¿La implementación de un plan de seguridad de la información basado en normas internacionales, ayudaría a mejorar la seguridad de la información en la empresa?


*Figura 57.* ¿La implementación de un plan de seguridad de la información basado en normas internacionales, ayudara a mejorar la seguridad de la información en la empresa?. Fuente: Elaboración Propia.

De acuerdo a la figura anterior, los resultados evidencian que, de los 25 empleados encuestados el 100% indicó que está de acuerdo con el desarrollo de un plan de seguridad de la información dentro de la organización, ya que ayudara a mejorar la seguridad de la información.

**Anexo 6: MATRIZ DE CONSISTENCIA**

<table>
<tr><td>Titulo</td><td colspan="4">DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS.<br>CASO DE ESTUDIO: EMPRESA DE SEGUROS</td></tr>
<tr><td rowspan="3"></td><td>Problema</td><td>Variables</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>¿De qué manera el desarrollo de un plan de seguridad de la información basado en estándares internacionales ayudará en la seguridad de la información a la empresa de Seguros de Lima?</td><td>V. Independiente:<br>Seguridad de la Información<br><br>V.Dependiente:<br>Estándares</td></tr>
<tr><td>Hipótesis</td><td>Objetivo General</td><td>Objetivos específicos</td><td>Método propuesto</td></tr>
<tr><td>Mediante el desarrollo de Plan de seguridad de la información basado en estándares internacionales se logrará mejorar la seguridad de la información en la empresa de seguros de Lima.</td><td>Desarrollar un plan de seguridad de la información basado en estándares internacionales para la empresa de seguros, que permitirá mejorar la integridad, confidencialidad y disponibilidad de la información en la empresa de Seguros.</td><td>1. Evaluar el estado actual con respecto a las normas de seguridad de la información.<br>2. Identificar vulnerabilidades y amenazas en el área de sistemas<br>3. Elaborar el plan de seguridad de la información basado en normas internacionales para área de tecnologías de la información en beneficio de la empresa de seguros.</td><td>Evaluar el estado actual con respecto a las normas de seguridad<br>Identificar vulnerabilidades y amenazas en el área de sistemas<br>Desarrollar un plan de seguridad de la información basado en la norma ISO27001.</td></tr>
</table>

*Fuente:* Elaboración propia.

**Anexo 7:** Archivo con las respuestas de las encuestas

Encuesta Seguridad de la Información.xls

## Anexo 8: Archivo datos tabulados para generar alfa de CRONBACH

| Encuestados | Preguntas Tabuladas | | | | | | | | | | | | | | | Suma |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **P1** | **P2** | **P3** | **P4** | **P5** | **P6** | **P7** | **P8** | **P9** | **P10** | **P11** | **P12** | **P13** | **P14** | **P15** | |
| Jefe de Sistemas | 5 | 3 | 1 | 2 | 4 | 4 | 5 | 4 | 2 | 3 | 1 | 5 | 4 | 2 | 5 | 50 |
| Analista Técnico | 3 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 2 | 5 | 5 | 2 | 5 | 45 |
| Técnico Sistemas | 3 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 5 | 2 | 5 | 44 |
| Analista Contable | 3 | 3 | 1 | 2 | 3 | 3 | 2 | 2 | 4 | 3 | 2 | 3 | 5 | 2 | 5 | 43 |
| Analista Contable | 3 | 3 | 1 | 1 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 3 | 5 | 2 | 5 | 39 |
| Asistente RRHH | 2 | 2 | 1 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 5 | 2 | 5 | 39 |
| Técnico Sistemas | 3 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 5 | 2 | 5 | 44 |
| Técnico Sistemas | 2 | 2 | 1 | 2 | 4 | 4 | 4 | 3 | 4 | 3 | 2 | 4 | 5 | 5 | 5 | 50 |
| Analista de Sistemas | 3 | 3 | 1 | 1 | 2 | 2 | 5 | 2 | 4 | 2 | 2 | 4 | 5 | 4 | 5 | 45 |
| Analista de Sistemas | 3 | 3 | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 5 | 3 | 5 | 40 |
| Técnico Sistemas | 2 | 2 | 1 | 2 | 2 | 2 | 3 | 1 | 5 | 2 | 3 | 2 | 5 | 2 | 5 | 39 |
| Analista Contable | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 4 | 5 | 2 | 5 | 33 |
| Analista Técnico | 2 | 2 | 1 | 1 | 2 | 2 | 5 | 1 | 3 | 3 | 3 | 3 | 5 | 4 | 5 | 42 |
| Analista Técnico | 3 | 3 | 1 | 1 | 2 | 3 | 4 | 3 | 3 | 3 | 1 | 4 | 5 | 3 | 5 | 44 |
| Analista de Sistemas | 3 | 2 | 1 | 1 | 5 | 2 | 5 | 3 | 1 | 1 | 1 | 5 | 5 | 3 | 5 | 43 |
| Operador de Sistemas | 2 | 2 | 1 | 1 | 2 | 3 | 1 | 3 | 1 | 1 | 1 | 4 | 5 | 1 | 5 | 33 |
| Operador de Sistemas | 2 | 2 | 1 | 2 | 2 | 2 | 1 | 1 | 1 | 2 | 1 | 2 | 5 | 2 | 5 | 31 |
| Operador de Sistemas | 2 | 2 | 1 | 1 | 2 | 3 | 5 | 2 | 2 | 3 | 1 | 2 | 5 | 2 | 5 | 38 |
| Analista de Sistemas | 3 | 2 | 1 | 2 | 5 | 3 | 5 | 1 | 2 | 2 | 1 | 5 | 5 | 2 | 5 | 44 |
| Analista de Sistemas | 3 | 2 | 1 | 2 | 2 | 3 | 5 | 2 | 2 | 3 | 1 | 3 | 5 | 2 | 5 | 41 |
| Asistente de Sistemas | 2 | 2 | 1 | 1 | 2 | 2 | 5 | 1 | 2 | 3 | 1 | 5 | 5 | 1 | 5 | 38 |
| Asistente de Sistemas | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 1 | 2 | 3 | 1 | 3 | 5 | 2 | 5 | 37 |
| Asistente RRHH | 2 | 2 | 1 | 2 | 4 | 2 | 5 | 1 | 4 | 3 | 3 | 5 | 5 | 3 | 5 | 47 |
| Asistente RRHH | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 2 | 1 | 3 | 5 | 2 | 5 | 31 |
| Analista Técnico | 3 | 3 | 1 | 3 | 2 | 3 | 3 | 1 | 3 | 3 | 3 | 4 | 5 | 3 | 5 | 45 |
| **Varianza** | **0.48** | **0.24** | **0** | **0.3104** | **0.9504** | **0.3904** | **2.1504** | **0.8384** | **1.1264** | **0.4064** | **0.5376** | **0.96** | **0.0384** | **0.8** | **0** | |

Fuente: Elaboración propia

Resultado de confiabilidad de alfa de CRONBACH de acuerdo al cuadro anterior

| | |
|---|---|
| A=Alfa Cronbach | 0.70025740 |
| K=Numero Items | 15 |
| Vi=Varianza de cada Item | 9.2288 |
| Vt=Varianza Total | 26.64 |

Fuente: Elaboración propia

## Anexo 9: Entrevista a especialista de seguridad de la información

### FORMATO DE ENTREVISTA SEGURIDAD DE LA INFORMACION ISO 27001

Entrevistada: Sofía S.

Entrevistador: Cipriano Méndez

Fecha :

**Pregunta 1:**

**¿Porque es importante que una empresa cuente con un sistema de gestión de la seguridad de la información?**

El SGSI es muy importante dentro de una organización, porque nos ofrece una forma de trabajo y nos brinda una serie de controles y buenas prácticas que ayudaran a mejorar la seguridad de la información.

**Pregunta 2:**

**¿Qué consecuencias puede tener una organización que no cuente con un SGSI?**

Al no contar con un SGSI no hay manera de medir los riesgos o amenazas que pueda tener la organización.

**Pregunta 3:**

**¿Cuáles son los beneficios de la concientización a los empleados en temas de seguridad dentro de una organización?**

Un empleado concientizado en temas de seguridad de la información es una persona capacitada toma las precauciones necesarias antes de realizar una acción que pueda perjudicar a la organización.

**Pregunta 4:**

¿Cómo ayuda la implementación de la norma ISO27001 en una organización?

Ayuda a disminuir riesgos y amenazas que puede sufrir la organización mediante controles y buenas prácticas.

**Pregunta 5:**

¿Cuál es la sugerencia que se le debería dar a una empresa que no cuente con un SGSI?

Las empresas que no cuenten con sistemas de seguridad de la información, deberían hacer un gran esfuerzo en la implementación de manera escalonada, de lo contrario podría traerle perdidas económicas y daño de la imagen de la organización.

**Anexo 10: Ficha de observación de los activos informáticos**

**GUIA DE VERIFICACION DE ACTIVOS DE AREA TECNOLOGÍAS DE LA INFORMACIÓN**

El documento permite realizar el levantamiento de información de los activos que se encuentran ubicados en el área de tecnologías de la información de la empresa de seguros.

Observador :

Lugar :

Fecha :

Marcar con una **X** si la institución cuenta con el tipo de activo

| TIPO DE ACTIVOS | Cant. | SI | NO |
|---|---|---|---|
| DATO/INFORMACIÓN | | | |
| Se generan backups de la información | | X | |
| Cuentan con credenciales (Ejem. Contraseñas, tarjetas magnéticas) | | X | |
| Documentos de gestión interna | | X | |
| Registro de actividad o log de los sistemas de información | | X | |
| TIPO SERVICIO | | | |
| Tiene aplicativos que brindan servicios en línea | | X | |
| Proveedor de correo | | X | |
| TIPO SOFTWARE Y APLICACIONES | | | |
| Página web | | X | |
| **Aplicación de atención en línea** | | X | |
| SIAF | | X | |
| Servidor de máquinas virtuales | | X | |
| Aplicaciones comerciales | | X | |
| TIPO CLAVES CRIPTOGRÁFICAS | | | |
| Documento con valor legal firmados digitalmente | | X | |
| TIPO EQUIPOS INFORMATICOS | | | |
| Servidores de ambiente de Desarrollo, Prueba y Producción | 7 | X | |
| Laptops | 20 | X | |

| TIPO DE ACTIVOS | Cant. | SI | NO |
|---|---|---|---|
| Computadora de escritorio | 10 | X | |
| Dispositivos móviles | 15 | X | |
| Impresoras | 3 | X | |
| Escáner | 2 | X | |
| Firewall | 2 | X | |
| Routers | 2 | X | |
| Switchs | 3 | X | |
| Redes de Comunicaciones | | | |
| Central Telefónica | 1 | X | |
| ADSL | | X | |
| Red inalámbrica | 4 | X | |
| Red local | | X | |
| Internet | | X | |
| Soportes de Información | | | |
| Disco duro externo | 10 | X | |
| Memorias | 8 | X | |
| Equipamiento auxiliar | | | |
| UPS | 3 | X | |
| Aire acondicionado | 2 | X | |
| Racks | 2 | X | |
| Sistema contraincendios | | X | |
| Instalaciones | | | |
| Centro de computo | | X | |
| Personal | | | |
| Usuarios Externos | | X | |
| Usuarios Internos | | X | |
| Proveedores | | X | |

Fuente: Elaboración propia

**Anexo 11: Valoración de impacto en los activos del área de tecnologías de la información**

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| [D] | D_BKP | Generación de copias de Seguridad | MA | La generación de copias de seguridad son muy importantes para la recuperación de datos si hubiera algún desastre |
| | D_DGI | Documentos internos de la empresa | MA | Documentos confidenciales con datos de la empresa. |
| | D_TRA | Log de seguimiento de las acciones | MA | Archivos que registran la traza de las acciones que realiza un determinado usuario, es muy importante para poder realizar el seguimiento de las fallas |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | | | para poder dar tratamiento al mismos. |
| [S] | **S_COR** | Email institucional | MA | El uso de correos son muy importantes para lo comunicaciones entres usuario internos y externos. |
| | **S_PWE** | Página Web de la empresa | MA | Disponibilidad de la información de los servicios que brinda la empresa, para realizar consultas, reclamos, etc. |
| | **S_GEI** | Sistema gestión de identidades | MA | Sistema que brinda los accesos de acuerdo a los roles asignados. |
| [SW] | **SW_APA** | Sistema de respuesta | B | Sistema que |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | rápida mediante chatbots | | permite la ayuda en línea a los clientes para responder a consultas básicas. |
| | **SW_SIA** | Sistema Integrado de Administración Financiera | MA | El Sistema es muy importante para la empresa porque soporta la administración financiera son de la organización. |
| | **SW_SAC** | Office, Aplicativos de Desarrollo de software(FrontEnd, BackEnd y Gestores de BD), sistemas operativos, entre otros | MA | Los aplicativos, SO, BD, son muy importantes para la continuidad de la organización. |
| | **SW_ANT** | Antivirus | A | Aplicativo utilizado para prevenir amenazas de software |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | | | malintencionado |
| [HW] | **HW_SDE** | Servidor de desarrollo utilizado para el personal que realiza desarrollo y/o mantenimientos de sistemas de la empresa. | M | Servidor utilizado por el personal para desarrollar nuevos requerimientos o modificarlos |
| | **HW_SQA** | Servidor de pruebas utilizado por el personal que realiza temas de control de calidad del software desarrollado. | M | Servidor utilizado por el personal Tester para realizar las pruebas de los requerimientos o modificarlos por el equipo de desarrollo. |
| | **HW_SPR** | Servidor en que se encuentran desplegados los aplicativos de la empresa. | MA | Servidor utilizado para el despliegue de las aplicaciones que serán utilizadas por el personal interno y |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | | | externo de la empresa. |
| | **HW_CES** | Computadores asignados a los empleados del área de tecnologías de la información | M | Dispositivos utilizados por el personal para el desarrollo de sus labores. |
| | **HW_LAP** | Laptops asignados a los empleados del área de tecnologías de la información | M | Dispositivos utilizados por el personal para el desarrollo de sus labores. |
| | **HW_DMO** | Celulares, Tablets asignados a los empleados del área de tecnologías de la información | M | Dispositivos utilizados por el personal para el desarrollo de sus labores. |
| | **HW_IMP** | Impresoras asignado al área de tecnologías de la información | B | Dispositivos utilizados por el personal para la impresión de documentos. |
| | **HW_ESC** | Escáner asignado al área de tecnologías de la información | B | Dispositivos utilizados por el personal para la digitalización |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | | | de documentos. |
| | **HW_FIR** | Equipos informáticos destinados a proteger la seguridad perimetral de la empresa | MA | Dispositivos que tienen la finalidad de filtran los paquetes input y output, son muy importantes para la seguridad. |
| | **HW_ROU** | Equipos informáticos destinados para el enrutamientos de las redes. | MA | Dispositivos que permiten realizar el enrutamiento de datos tanto internos como externos, también sirven como Gateway, para el acceso a internet. |
| | **HW_BKP** | Dispositivos para generar respaldos | MA | Dispositivos que guardan las copias de seguridad y son necesario en caso de |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | | | sufrir algún desastre. |
| | **HW_SWT** | Equipos informáticos destinados para la segmentación de redes de la empresa. | MA | Equipos esenciales dentro de la empresa que permiten la administración y segmentación de redes. |
| [K] | **K_DLE** | Firmas electrónicas con valor legal | MA | Firmas electrónicas necesarias para documentos digitales con valor legal. |
| [COM] | **COM_CET** | Red de comunicación IP | A | Equipos utilizados para la comunicación de la empresa |
| | **COM_ADS** | Infraestructura utilizada para la conectividad y transmisión de datos | MA | Infraestructura necesaria para la transmisión de grandes volúmenes de datos |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | **COM_RIN** | Red de comunicación inalámbrica | M | Equipo utilizado para la conexión de dispositivos móviles de los empleados como los visitantes |
| | **COM_LAN** | Red de comunicaciones Interna | MA | Infraestructura importante para la trasmisión de datos para el funcionamiento de los servicios de la empresa. |
| | **COM_INT** | Red de redes | MA | Acceso a la red de redes para la transmisión de datos de la empresa. |
| [Media] | **MEDIA_HDD** | Disco duro portátil | A | Dispositivos que permite transportar datos y software |
| | **MEDIA_US** | Memorias extraíbles | A | Dispositivos |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | **B** | | | que permite transportar datos y software |
| [AUX] | **AUX_UPS** | Sistema de alimentación ininterrumpida | MA | Son equipos necesarios para el correcto funcionamiento de los equipos de la empresa |
| | **AUX_AAC** | Sistema de aire acondicionado, refrigeración adecuada | MA | Son equipos necesario que tiene la finalidad de mantener el ambiente con un clima adecuado para los equipos. |
| | **AUX_RAC** | Gabinetes que da soporte a los diferentes aparatos electrónicos(Servidores, Switch, Routers..) | MA | Equipos necesarios para soportar los equipos como switch, router, servidores, etc.. de manera ordenada. |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | **AUX_SCI** | Equipos para prevenir incendios(extintores, detectores de humo) | MA | Equipos necesarios para proteger los equipos de incendios |
| [L] | **L_CCO** | Oficina principal de procesamiento donde reside la infraestructura para soporta la operación del negocio | MA | Esencial para el funcionamiento de la organización. |
| [P] | **P_ASA** | Personal administrador del servidor de aplicaciones | MA | Personal que administran las diferentes aplicaciones que tiene la empresa |
| | **P_ABD** | Personal administrador de base de datos | MA | Personal que administra los diversos gestores de base de datos que tiene la empresa. |
| | **P_MSO** | Personal mantenimiento de software | MA | Personal encargado de realizar el desarrollo y pruebas del software. |
| | **P_ACO** | Personal | MA | Personal |

| ACTIVO | CÓDIGO | DESCRIPCIÓN | IMPACTO | MOTIVO |
|---|---|---|---|---|
| | | administrador de comunicaciones | | encargado de la administración y el soporte para el correcto funcionamiento de las todas las comunicaciones de la empresa |

Fuente: Elaboración propia con datos tomados MINHAP Libro II Magerit versión 3.0, (2012, pág. 8-13)

## Anexo 12: Valoración de riesgos en los activos de la Información por tipo y por dimensiones

Tabla 16.

*Valoración de los activos Datos/Información*

| **ACTIVO: [D] DATOS-INFORMACÓN** | | | | | | |
|---|---|---|---|---|---|---|
| **CÓDIGO** | **DESCRIPCIÓN** | **DIMENSIONES** | | | | |
| **ACTIVO** | | [D] | [I] | [C] | [A] | [T] |
| **D_BKP** | Generación de copias de Seguridad | 3 | | 3 | | |
| **D_DGI** | Documentos internos de la empresa | | 3 | | | |
| **D_TRA** | Log de seguimiento de las acciones | 2 | | | | 3 |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 17.

*Análisis de la valoración de los activos Datos/Información*

| **CÓDIGO ACTIVO** | **DIMENSIÓN** | **DESCRIPCIÓN** |
|---|---|---|
| **D_BKP** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |
| | [C] | 3.lg: Probablemente afecte negativamente a las relaciones internas de la Organización |
| **D_DGI** | [I] | 3.pi1: probablemente afecte a un individuo |
| **D_TRA** | [D] | 2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización |
| | [T] | 3.si: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 18.

*Valoración de los activos Servicios*

| ACTIVO: [S] SERVICIOS | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **S_COR** | Email institucional | 5 | | 3 | | |
| **S_PWE** | Página Web de la empresa | 5 | | | | |
| **S_GEI** | Sistema gestión de identidades | 3 | 3 | 3 | | 4 |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 19.

*Análisis de la valoración de los activos Servicios*

| **CÓDIGO ACTIVO** | **DIMENSIÓN** | **DESCRIPCIÓN** |
|---|---|---|
| **S_COR** | [D] | 5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización |
| | [C] | 3.lg: Probablemente afecte negativamente a las relaciones internas de la Organización |
| **S_PWE** | [I] | 5.adm:probablemente impediría la operación efectiva de más de una parte de la Organización |
| **S_GEI** | [D] | 3.adm:probablemente impediría la operación efectiva de una parte de la Organización |
| | [I] | 3.pi1: probablemente afecte a un individuo |
| | [C] | 3.lg: Probablemente afecte negativamente a las relaciones internas de la Organización |
| | [T] | 4.crm: Dificulte la investigación o facilite la comisión de delitos |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 20.

*Valoración de los activos Software*

| ACTIVO-[SW] SOFTWARE | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **SW_APA** | Sistema de respuesta rápida mediante chatbots | 1 | | | | |
| **SW_SIA** | Sistema Integrado de Administración Financiera | 7 | 7 | 7 | | 7 |
| **SW_SAC** | Office, Aplicativos de Desarrollo de software(FrontEnd, BackEnd y Gestores de BD), sistemas operativos, entre otros | 7 | | 5 | | |
| **SW_ANT** | Antivirus | 7 | | 7 | | |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 21.

*Análisis de la valoración de los activos Software*

| **CÓDIGO ACTIVO** | **DIMENSIÓN** | **DESCRIPCIÓN** |
|---|---|---|
| **SW_APA** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **SW_SIA** | [D],[I],[C] | 7.adm: probablemente impediría la operación efectiva de la Organización |
| | [T] | 7.cei.c: causa de graves pérdidas económicas |
| **SW_SAC** | [D] | 7.adm: probablemente impediría la operación efectiva de la Organización |

| | | |
|---|---|---|
| | [C] | 5.da: Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones |
| **SW_ANT** | [D], [C] | 7.adm:probablemente impediría la operación efectiva de la Organización |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 22.

*Valoración de los activos Hardware*

| **ACTIVO-[HW] HARDWARE** | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| **ACTIVO** | | [D] | [I] | [C] | [A] | [T] |
| **HW_SDE** | Servidor de desarrollo utilizado para el personal que realizas desarrollo y/o mantenimientos de sistemas de la empresa. | 1 | | | | |
| **HW_SQA** | Servidor de pruebas utilizado por el personal que realiza temas de control de calidad del software desarrollado. | 1 | | | | |
| **HW_SPR** | Servidor en que se encuentran desplegados los aplicativos de la empresa. | 7 | | 5 | | 7 |
| **HW_CES** | Computadores asignados a los empleados del área de tecnologías de la información | 1 | | | | |
| **HW_LAP** | Laptops asignados a los empleados del área de tecnologías de la información | 1 | | | | |
| **HW_DMO** | Celulares, Tablets asignados a los | | | | | |

| | | |
|---|---|---|
| | empleados del área de tecnologías de la información | 1 |
| **HW_IMP** | Impresoras asignado al área de tecnologías de la información | 1 |
| **HW_ESC** | Escáner asignado al área de tecnologías de la información | 1 |
| **HW_FIR** | Equipos informáticos destinados a proteger la seguridad perimetral de la empresa | 7 |
| **HW_ROU** | Equipos informáticos destinados para el enrutamientos de las redes. | 7 |
| **HW_BKP** | Dispositivos para generar respaldos | 3 |
| **HW_SWT** | Equipos informáticos destinados para la segmentación de redes de la empresa. | 3 |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 23.

*Análisis de la valoración de los activos Hardware*

| **CÓDIGO ACTIVO** | **DIMENSIÓN** | **DESCRIPCIÓN** |
|---|---|---|
| **HW_SDE** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_SQA** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_SPR** | [D] | 7.adm: probablemente impediría la operación efectiva de la Organización |

| | | |
|---|---|---|
| | [C] | 5.da: Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones |
| | [T] | 7.cei.c: causa de graves pérdidas económicas |
| **HW_CES** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_LAP** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_DMO** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_IMP** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_ESC** | [D] | 1.adm: pudiera impedir la operación efectiva de una parte de la Organización |
| **HW_FIR** | [D] | 7.da2: Probablemente tenga un gran impacto en otras organizaciones |
| **HW_ROU** | [D] | 7.da2: Probablemente tenga un gran impacto en otras organizaciones |
| **HW_BKP** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |
| **HW_SWT** | [D] | 3.da: Probablemente cause la interrupción de actividades propias de la Organización |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 24.

*Valoración de los activos Criptografía*

| **ACTIVO-[K] CRIPTOGRAFÍA** | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| **ACTIVO** | | [D] | [I] | [C] | [A] | [T] |
| **K_DLE** | Firmas electrónicas con valor legal | | | 3 | | |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuente: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 25.

*Análisis de la valoración de los activos Criptografía*

| CÓDIGO ACTIVO | DIMENSIÓN | DESCRIPCIÓN |
|---|---|---|
| **K_DLE** | [D] | 3.pi1 probablemente afecte a un individuo |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 26.

*Valoración de los activos Comunicaciones*

| ACTIVO-[COM] COMUNICACIONES | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **COM_CET** | Red de comunicación IP | 1 | | | | |
| **COM_ADS** | Infraestructura utilizada para la conectividad y transmisión de datos | 5 | | | | |
| **COM_RIN** | Red de comunicación inalámbrica | 1 | | | | |
| **COM_LAN** | Red de comunicación local | 3 | | | | |
| **COM_INT** | Red de comunicación internet | 3 | | | | |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 27.

*Análisis de la valoración de los activos Comunicaciones*

| CÓDIGO ACTIVO | DIMENSIÓN | DESCRIPCIÓN |
|---|---|---|
| **COM_CET** | [D] | 1.da: Pudiera causar la interrupción de actividades propias de la Organización |
| **COM_ADS** | [D] | 5.da: Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones |
| **COM_RIN** | [D] | 1.da:Pudiera causar la interrupción de actividades propias de la Organización |
| **COM_LAN** | [D] | 3.da: Probablemente cause la interrupción de actividades propias de la Organización |
| **COM_INT** | [D] | 3.adm probablemente impediría la operación efectiva de una parte de la Organización |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 28.

*Valoración de los activos Media*

| **ACTIVO-[Media]** | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **MEDIA_HDD** | Disco duro portátil | 3 | | | | 3 |
| **MEDIA_USB** | Memorias extraíbles | 3 | | | | 3 |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 29.

*Análisis de la valoración de los activos Media*

| CÓDIGO ACTIVO | DIMENSIÓN | DESCRIPCIÓN |
|---|---|---|
| **MEDIA_HDD** **MEDIA_USB** | [D] | 3.lg: Probablemente afecte negativamente a las relaciones internas de la Organización |
| | [T] | 3.si: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 30.

*Valoración de los activos Auxiliares*

| ACTIVO-[AUX] AUXILIARES | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **AUX_UPS** | Sistema de alimentación ininterrumpida | 3 | | | | |
| **AUX_AAC** | Sistema de aire acondicionado, refrigeración adecuada | 3 | | | | |
| **AUX_RAC** | Gabinetes que da soporte a los diferentes aparatos electrónicos(Servidores, Switch, Routers..) | 3 | | | | |
| **AUX_SCI** | Equipos para prevenir incendios(extintores, detectores de humo) | 3 | | | | |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 31.

*Análisis de la valoración de los activos Auxiliares*

| CÓDIGO ACTIVO | DIMENSIÓN | DESCRIPCIÓN DE RIESGO |
|---|---|---|
| **AUX_UPS** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |
| **AUX_AAC** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |
| **AUX_RAC** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |
| **AUX_SCI** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |
| **AUX_UPS** | [D] | 3.adm: probablemente impediría la operación efectiva de una parte de la Organización |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 32.

*Valoración de los activos Local*

| ACTIVO [L] - LOCAL | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **L_CCO** | Oficina principal de procesamiento donde reside la infraestructura para soporta la operación del negocio | 7 | | | | |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 33.

*Análisis de la valoración de los activos Local*

| CÓDIGO ACTIVO | DIMENSIÓN | DESCRIPCIÓN |
|---|---|---|
| **L_CCO** | [D] | 7.adm: probablemente impediría la operación efectiva de la Organización |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Tabla 34.

*Valoración de los activos Personal*

| ACTIVO-[P] PERSONAL | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO ACTIVO** | **DESCRIPCION** | **DIMENSIONES** | | | | |
| | | [D] | [I] | [C] | [A] | [T] |
| **P_ASA** | Personal administrador del servidor de aplicaciones | 5 | | | | |
| **P_ABD** | Personal administrador de base de datos | 5 | | | | |
| **P_MSO** | Personal mantenimiento de software | 5 | | | | |
| **P_ACO** | Personal administrador de comunicaciones | 5 | | | | |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

Análisis de resultados de riesgos de los activos de la seguridad por dimensiones de acuerdo a la metodología MAGERIT v3.0

Tabla 35.

*Análisis de la valoración de los activos Personal*

| CÓDIGO ACTIVO | DIMENSIÓN | DESCRIPCIÓN |
|---|---|---|
| **P_ASA** | [D] | 5.adm: probablemente impediría la operación |

| | | |
|---|---|---|
| | | efectiva de más de una parte de la Organización |
| **P_ABD** | [D] | 5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización |
| **P_MSO** | [D] | 5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización |
| **P_ACO** | [D] | 5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización |

*Nota:* Datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23). Fuenta: Elaboración propia.

**Anexo 13: Inventario de activos del área de tecnologías de la información**

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| 1. | Backup | Generación de copias de Seguridad | Dato/Información | Sala de computo | D_BKP |
| 2. | Documentos de Gestión interna | Documentos internos de la empresa | Dato/Información | Servidor de archivos, Sala de computo | D_DGI |
| 3. | Documentos Trazabilidad | Log de seguimiento de las acciones | Dato/Información | Servidores, Sala de computo | D_TRA |
| 4. | Credenciales de los usuario (password) | Credenciales de usuarios para ingresar a los recursos tecnológicos y fisicos | Dato/Información | Servidor active Directory, Sala de computo | D_PAS |
| 5. | Correo | Email institucional | Servicio | Servidor de correo, Sala de computo | S_COR |
| 6. | Página Web | Página Web de la empresa | Servicio | Servidor de aplicaciones, Sala de computo | SW_PWE |
| 7. | Gestión de identidades | Sistema gestión de identidades | Servicio | Sala de computo | S_GEI |
| 8. | Aplicación de atención | Sistema de respuesta rápida | Software/Aplicaciones | Servidor de | SW_APA |

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| | en línea | mediante chatbots | informática | aplicaciones, Sala de computo | |
| 9. | SIAF | Sistema Integrado de Administración Financiera | Software/Aplicaciones informática | Servidor de aplicaciones, Sala de computo | SW_SIA |
| 10. | Aplicaciones Comerciales | Office, Aplicativos de Desarrollo de software(FrontEnd, BackEnd y Gestores de BD), sistemas operativos, entre otros | Software/Aplicaciones informática | Computadoras Personales, área de tecnologías de la información | SW_SAC |
| 11. | Antivirus | Software antivirus | Software/Aplicaciones informática | Servidores, Sala de computo Computadores personales, oficinas | SW_ANT |
| 12. | Servidores de desarrollo | Servidor de desarrollo utilizado para el personal que realizas desarrollo y/o mantenimientos | Equipos informáticos | Servidores de aplicaciones y Servidor de base de datos, Sala | HW_SDE |

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| | | de sistemas de la empresa. | | de computo. | |
| 13. | Servidores de prueba | Servidor de pruebas utilizado por el personal que realiza temas de control de calidad del software desarrollado. | Equipos informáticos | Servidores de aplicaciones y Servidor de base de datos, Sala de computo. | HW_SQA |
| 14. | Servidores de producción | Servidor en que se encuentran desplegados los aplicativos de la empresa. | Equipos informáticos | Servidores de aplicaciones y Servidor de base de datos, Sala de computo. | HW_SPR |
| 15. | Computadores de escritorio usuarios | Computadores asignados a los empleados del área de tecnologías de la información | Equipos informáticos | Área de tecnologías de la información | HW_CES |
| 16. | Laptops | Laptops asignados a los empleados del área de tecnologías de la | Equipos informáticos | Área de tecnologías de la información | HW_LAP |

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| | | información | | | |
| 17. | Dispositivos Móviles | Celulares, Tablets asignados a los empleados del área de tecnologías de la información | Equipos informáticos | Área de tecnologías de la información | HW_DMO |
| 18. | Impresoras | Impresoras asignado al área de tecnologías de la información | Equipos informáticos | Área de tecnologías de la información | HW_IMP |
| 19. | Escáner | Escáner asignado al área de tecnologías de la información | Equipos informáticos | Área de tecnologías de la información | HW_ESC |
| 20. | Firewall | Equipos informáticos destinados a proteger la seguridad perimetral de la empresa | Equipos informáticos | Centro computo | HW_FIR |
| 21. | Router | Equipos informáticos destinados para el enrutamientos de las redes. | Equipos informáticos | Centro computo | HW_ROU |
| 22. | Generadore | Dispositivos para | Equipos | Centro | HW_BKP |

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| | s Backup | generar respaldos | informáticos | computo | |
| 23. | Switchs | Equipos informáticos destinados para la segmentación de redes de la empresa. | Equipos informáticos | Centro computo | HW_SWT |
| 24. | Firmas electrónicas | Firmas electrónicas con valor legal | Criptografía | Centro de computo | K_DLE |
| 25. | Central Telefónica | Red de comunicación IP | Redes de Comunicaciones | Área de tecnologías de la información | COM_CET |
| 26. | ADSL | Infraestructura utilizada para la conectividad y transmisión de datos | Redes de Comunicaciones | Área de tecnologías de la información | COM_ADS |
| 27. | Red inalámbrica | Red de comunicación inalámbrica | Redes de Comunicaciones | Área de tecnologías de la información | COM_RIN |
| 28. | Red local | Red de comunicaciones cableada | Redes de Comunicaciones | Oficina de la empresa | COM_LAN |
| 29. | Internet | Red de redes | Redes de Comunicacio | www | COM_INT |

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| | | | nes | | |
| 30. | Disco duro externo | Disco duro portátil | Soportes de Información | Área de tecnologías de la información | MEDIA_HDD |
| 31. | Memorias | USB | Soportes de Información | Área de tecnologías de la información | MEDIA_USB |
| 32. | Respaldo de energía UPS | Sistema de alimentación ininterrumpida | Equipamiento auxiliar | Área de tecnologías de la información | AUX_UPS |
| 33. | Aire acondicionado | Sistema de aire acondicionado, refrigeración adecuada | Equipamiento auxiliar | Área de tecnologías de la información | AUX_AAC |
| 34. | Racks | Gabinetes que da soporte a los diferentes aparatos electrónicos(Servidores, Switch, Routers.) | Equipamiento auxiliar | Área de tecnologías de la información | AUX_RAC |
| 35. | Sistema contraincendios | Equipos para prevenir incendios(extintor | Equipamiento auxiliar | Área de tecnologías de la | AUX_SCI |

| N° | Nombre | Descripción | Tipo | Ubicación | Código |
|---|---|---|---|---|---|
| | | es, detectores de humo) | | información | |
| 36. | Centro de computo | Oficina principal de procesamiento donde reside la infraestructura para soporta la operación del negocio | Instalaciones | Local empresa de seguros | L_CCO |
| 37. | Usuarios Externos | Usuarios que hacen uso de los servicios online de la empresa. | Personal | Usuarios Externos | P_UEX |
| 38. | Usuarios Internos | Empleados de la empresa | Personal | Oficinas empresa de seguros | P_UIN |
| 39. | Proveedores | Proveedores de tecnología y comunicaciones | Personal | Externo | P_UEP |

Fuente: Elaboración propia

**Anexo 14: Valoración de amenazas de los activos**

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| **DATOS-INFORMACÓN** | | | | | |
| **D_BKP** | 5.3.2 [E.2] Errores del administrador | 5 | | 50% | 100% |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | 100% | 100% | 100% |
| **D_DGI** | 5.3.12 [E.19] Fugas de información | 50 | 50% | 50% | |
| | 5.4.15 [A.19] Divulgación de información | 50 | 50% | 50% | |
| **D_TRA** | 5.3.3 [E.3] Errores de monitorización (log) | 10 | | 50% | 50% |
| | 5.3.9 [E.14] Escapes de información | 10 | 50% | 50% | |
| | 5.4.13 [A.15] Modificación deliberada de la información | 10 | 50% | 50% | 50% |
| **SERVICIOS** | | | | | |
| **S_COR** | 5.3.16 [E.24] Caída del sistema por agotamiento de recursos | 5 | 100% | | |
| | 5.3.9 [E.14] Escapes de información | 75 | 50% | | |
| **S_PWE** | 5.3.16 [E.24] Caída | 5 | 100% | | |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | del sistema por agotamiento de recursos | | | | |
| | 5.4.3 [A.5] Suplantación de la identidad del usuario | 5 | 100% | 50% | |
| S_GEI | 5.3.16 [E.24] Caída del sistema por agotamiento de recursos | 5 | 100% | | |
| | 5.4.3 [A.5] Suplantación de la identidad del usuario | 5 | 100% | 50% | |
| **SOFTWARE** | | | | | |
| SW_APA | 5.3.13 [E.20] Vulnerabilidades de los programas (software) | 75 | 100% | | |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | 100% | 100% | 100% |
| | 5.4.16 [A.22] Manipulación de programas | 5 | 50% | 50% | 50% |
| SW_SIA | 5.3.1 [E.1] Errores de los usuarios | 5 | 20% | 20% | 50% |
| | 5.4.3 [A.5] Suplantación de la identidad del | 5 | 100% | | 50% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | usuario | | | | |
| SW_SAC | 5.3.13 [E.20] Vulnerabilidades de los programas (software) | 50 | 10% | | |
| | 5.4.9 [A.11] Acceso no autorizado | 10 | 20% | | 20% |
| | 5.4.16 [A.22] Manipulación de programas | 50 | 50% | 50% | 30% |
| | 5.3.1 [E.1] Errores de los usuarios | 50 | | | 10% |
| SW_ANT | 5.3.13 [E.20] Vulnerabilidades de los programas (software) | 50 | | | 50% |
| | 5.4.6 [A.8] Difusión de software dañino | 10 | | | 50% |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | | | 100% |
| HARDWARE | | | | | |
| HW_SDE | 5.2.7 [I.6] Corte del suministro eléctrico | 50 | | | 100% |
| | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.8 [I.7] Condiciones inadecuadas de temperatura o | 5 | | | 100% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | humedad | | | | |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| HW_SQA | 5.2.7 [I.6] Corte del suministro eléctrico | 50 | | | 100% |
| | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| HW_SPR | 5.2.7 [I.6] Corte del suministro eléctrico | 50 | | | 100% |
| | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| | 5.3.16 [E.24] Caída del sistema por agotamiento de recursos | 5 | | | 50% |
| HW_CES | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de | 10 | | | 100% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | origen físico o lógico | | | | |
| | 5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (hardware) | 10 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 10 | | | 100% |
| | 5.3.17 [E.25] Pérdida de equipos | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | 50% | | 100% |
| **HW_LAP** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 10 | | | 100% |
| | 5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (hardware) | 10 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 10 | | | 100% |
| | 5.3.17 [E.25] Pérdida de equipos | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | 50% | | 100% |
| **HW_DMO** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de | 10 | | | 100% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | origen físico o lógico | | | | |
| | 5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (hardware) | 10 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 10 | | | 100% |
| | 5.3.17 [E.25] Pérdida de equipos | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | 50% | | 100% |
| **HW_IMP** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| **HW_ESC** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| **HW_FIR** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 5 | | | 100% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| HW_ROU | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| HW_BKP | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| | 5.3.2 [E.2] Errores del administrador | 10 | | | 50% |
| | 5.4.17 [A.23] Manipulación de los equipos | 5 | 50% | | |
| HW_SWT | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| | 5.3.2 [E.2] Errores del administrador | 10 | | | 50% |
| | 5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad | 5 | | | 50% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| **CRIPTOGRAFÍA** | | | | | |
| **K_DLE** | 5.4.15 [A.19] Divulgación de información | 5 | 50% | 50% | |
| **COMUNICACIONES** | | | | | |
| **COM_CET** | 5.2.1 [I.1] Fuego | 5 | | | 50% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.4.12 [A.14] Interceptación de información (escucha) | 5 | 100% | | |
| **COM_ADS** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 50% |
| **COM_RIN** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (hardware) | 5 | | | 100% |
| | 5.4.9 [A.11] Acceso no autorizado | 10 | 50% | | |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| **COM_LAN** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.3.7 [E.9] Errores de [re-]encaminamiento | 5 | 15% | | |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | 5.4.10 [A.12] Análisis de tráfico | 5 | 15% | | |
| | 5.4.8 [A.10] Alteración de secuencia | 5 | 50% | | |
| COM_INT | 5.3.7 [E.9] Errores de [re-]encaminamiento | 5 | 25% | | |
| | 5.4.10 [A.12] Análisis de tráfico | 5 | 50% | 50% | |
| | 5.4.18 [A.24] Denegación de servicio | 5 | | | 100% |
| **[Media]** | | | | | |
| MEDIA_HDD | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.3.17 [E.25] Pérdida de equipos | 5 | 50% | | 100% |
| | 5.4.19 [A.25] Robo | 5 | 100% | | 100% |
| MEDIA_USB | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.3.17 [E.25] Pérdida de equipos | 5 | 50% | | 100% |
| | 5.4.19 [A.25] Robo | 5 | 100% | | 100% |
| **AUXILIARES** | | | | | |
| AUX_UPS | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 10 | | | 10% |
| | 5.4.20 [A.26] Ataque destructivo | 5 | | | 100% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | 5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad | 10% | | | 100% |
| **AUX_AAC** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.6 [I.5] Avería de origen físico o lógico | 5 | | | 100% |
| | 5.2.7 [I.6] Corte del suministro eléctrico | 10 | | | 10% |
| | 5.4.20 [A.26] Ataque destructivo | 5 | | | 100% |
| **AUX_RAC** | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.4.20 [A.26] Ataque destructivo | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| **AUX_SCI** | 5.4.20 [A.26] Ataque destructivo | 5 | | | 100% |
| | 5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (hardware) | 5 | | | 30% |
| **LOCAL** | | | | | |
| **L_CCO** | 5.1.3 [N.*] Desastres Naturales | 5 | | | 100% |
| | 5.4.20 [A.26] Ataque destructivo | 5 | | | 100% |
| | 5.2.1 [I.1] Fuego | 5 | | | 100% |
| | 5.2.2 [I.2] Daños por | 5 | | | 100% |

| CÓDIGO ACTIVO | AMENAZA | OCURRENCIA | DIMENSIONES | | |
|---|---|---|---|---|---|
| | | | C | I | D |
| | agua | | | | |
| | 5.4.9 [A.11] Acceso no autorizado | 5 | | | 100% |
| | 5.4.19 [A.25] Robo | 5 | | | 100% |
| **PERSONAL** | | | | | |
| **P_ASA**<br>**P_ABD**<br>**P_MSO**<br>**P_ACO** | 5.3.12 [E.19] Fugas de información | 5 | 20% | | |
| | 5.4.22 [A.28] Indisponibilidad del personal | 10 | | | 50% |

Fuente: Elaboración propia con datos tomados (MINHAP, Libro II MAGERIT versión 3.0., criterios de valoración 2012, pág. 19-23).

**Anexo 15: Declaración de aplicabilidad de controles del anexo a de la norma ISO 27001:2013**

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| **A5** | **Políticas de seguridad de la información** | | |
| **A5.1** | **Directrices de gestión de la seguridad de la información** | | |
| A5.1.1 | Políticas para la seguridad de la información | Aplicar | Establecer y comunicar políticas de seguridad de la información |
| A5.1.2 | Revisión de las políticas para la seguridad de la información | Aplicar | Las políticas de información no se revisan y no se evalúan |
| **A6** | **Organización de la seguridad de la información** | | |
| **A6.1** | **Organización interna** | | |
| A6.1.1 | Roles y responsabilidades en seguridad de la información | Aplicar | Falta definir roles y responsabilidades |
| A6.1.2 | Segregación de tareas | Aplicar | Se debe elaborar matriz RACI para la asignación de responsabilidades |
| A6.1.3 | Contacto con las autoridades | Aplicar | El contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar está en un nivel inicial |
| A6.1.4 | Contacto con grupos de interés especial | Aplicar | Actualmente no hay contacto regular, con grupos especiales de interés, foros, etc. |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A6.1.5 | Seguridad de la información en la gestión de proyectos | Aplicar | La identificación de los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos se encuentra en una etapa inicial |
| **A6.2** | **Los dispositivos móviles y el teletrabajo** | | |
| A6.2.1 | Política de dispositivos móviles | Aplicar | La políticas controles seguridad relacionados con los usuarios móviles no existen |
| A6.2.2 | Teletrabajo | Aplicado | Los controles para temas de teletrabajo se encuentran en una etapa inicial, hay una gestión adecuada en tema de permisos y uso de VPN |
| **A7** | **Seguridad relativa a los recursos humanos** | | |
| **A7.1** | **Antes del empleo** | | |
| A7.1.1 | Investigación de antecedentes | Aplicado | En la evaluación previa al empleo se toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo |
| A7.1.2 | Términos y condiciones del empleo | Aplicar | Las responsabilidades en temas de seguridad de la información son especificadas de acuerdo a la naturaleza de los roles |
| **A7.2** | **Durante el empleo** | | |
| A7.2.1 | Responsabilidades de gestión | Aplicar | No existe un programa de concientización |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A7.2.2 | Concienciación, educación y capacitación en seguridad de la información | Aplicar | Aun no existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para el personal de la empresa |
| A7.2.3 | Proceso disciplinario | Aplicar | El personal que incumple políticas de seguridad de la información, tiene un proceso disciplinario. |
| **A7.3** | **Finalización del empleo o cambio en el puesto de trabajo** | | |
| A7.3.1 | Responsabilidades ante la finalización o cambio | Aplicar | Para las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos se sigue un proceso. |
| **A8** | **Gestión de activos** | | |
| **A8.1** | **Responsabilidad sobre los activos** | | |
| A8.1.1 | Inventario de activos | Aplicar | El inventario de activos es realizado por el personal a cargo jefe del área de sistemas |
| A8.1.2 | Propiedad de los activos | Aplicar | Los activos tienen dueños y propietarios de los riesgos |
| A8.1.3 | Uso aceptable de los activos | Aplicar | El personal está comprometido en cuidar y hacer uso adecuado del activo asignado |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A8.1.4 | Devolución de activos | Aplicar | El personal que cuenta con un activo, sigue procedimientos para realizar la devolución |
| **A8.2** | **Clasificación de la información** | | |
| A8.2.1 | Clasificación de la información | Aplicar | Los activos son clasificados de acuerdo a la información que contiene |
| A8.2.2 | Etiquetado de la información | Aplicar | El etiquetado de los activos se realiza de manera correcta y clara |
| A8.2.3 | Manipulado de la información | Aplicar | Los niveles de clasificación de los activos asignados está en una etapa inicial |
| **A8.3** | **Manipulación de los soportes** | | |
| A8.3.1 | Gestión de soportes extraíbles | Aplicar | Existe un registro de activos completo y actualizado de dispositivos extraíbles |
| A8.3.2 | Eliminación de soportes | Aplicar | No existe una política de cómo se debe eliminar los soportes |
| A8.3.3 | Soportes físicos en tránsito | Aplicar | Aun no se cuenta con mecanismos de cifrado adecuado durante el proceso de transferencia |
| **A9** | **Control de acceso** | | |
| **A9.1** | **Requisitos de negocio para el control de acceso** | | |
| A9.1.1 | Política de control de acceso | Aplicar | Existe  políticas de control de acceso, pero se cumple de manera |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| | | | parcial |
| A9.1.2 | Acceso a las redes y a los servicios de red | Aplicar | El acceso a las redes y servicios de red de la empresa, se hace uso de autenticación y permisos |
| **A9.2** | **Gestión de acceso de usuario** | | |
| A9.2.1 | Registro y baja de usuario | Aplicar | Se hace uso de un ID de usuario único para cada usuario, para las gestiones necesarias relacionados al usuario |
| A9.2.2 | Provisión de acceso de usuario | Aplicar | Los accesos a sistemas y servicios de información se brindan de acuerdo a las necesidades del negocio |
| A9.2.3 | Gestión de privilegios de acceso | Aplicar | Se realiza revisión periódica de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios |
| A9.2.4 | Gestión de la información secreta de autenticación de los usuarios | Aplicar | Al momento de entregar las contraseñas de acceso a los usuarios para que ingresen a los sistemas se efectúa de manera personal y se le indica que puedan cambiar inmediatamente después de su entrega. |
| A9.2.5 | Revisión de los derechos de acceso de usuario | Aplicar | Se realiza la revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones |
| A9.2.6 | Retirada o reasignación de los derechos de acceso | Aplicar | El proceso de ajuste de derechos de acceso, se encuentra en una etapa inicial |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| **A9.3** | **Responsabilidades del usuario** | | |
| A9.3.1 | Uso de la información secreta de autenticación | Aplicar | La confidencialidad de las credenciales de autenticación es comunicado al personal |
| **A9.4** | **Control de acceso a sistemas y aplicaciones** | | |
| A9.4.1 | Restricción del acceso a la información | Aplicar | Los acceso a los sistemas e información son controlados de acuerdo al rol del personal de la empresa. |
| A9.4.2 | Procedimientos seguros de inicio de sesión | Aplicar | Al momento de ingresar a los sistemas se muestran pantalla con advertencias de inicio de sesión de manera segura y se realiza el registro de sesión. |
| A9.4.3 | Sistema de gestión de contraseñas | Aplicar | Al momento de crear contraseñas se sugiere al personal, que al momento de crear su contraseña lo realice de manera segura |
| A9.4.4 | Uso de utilidades con privilegios del sistema | Aplicar | El jefe del área de sistemas verifica los privilegios de accesos a los sistemas |
| A9.4.5 | Control de acceso al código fuente de los programas | Aplicar | El código fuente se guarda en repositorios como SVN, Harvest, GitHub |
| **A10** | **Criptografía** | | |
| **A10.1** | **Controles criptográficos** | | |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A10.1.1 | Política de uso de los controles criptográficos | Aplicar | No existe una política que cubra el uso de controles criptográficos |
| A10.1.2 | Gestión de claves | Aplicar | No existe políticas de criptografía que abarque el ciclo de vida de la gestión de claves. |
| **A11** | **Seguridad física y del entorno** | | |
| **A11.1** | **Áreas seguras** | | |
| A11.1.1 | Perímetro de seguridad física | Aplicar | Los accesos a lugares físicos se realiza mediante tarjetas de proximidad y también hay personal de seguridad que custodia el lugar |
| A11.1.2 | Controles físicos de entrada | Aplicar | El acceso a lugares físicos solo está permitido al personal que cuente con los privilegios y que cuente con la tarjeta de proximidad |
| A11.1.3 | Seguridad de oficinas, despachos y recursos | Aplicar | Los accesos cuentan con CCTV |
| A11.1.4 | Protección contra las amenazas externas y ambientales | Aplicar | El plan de continuidad del negocio se encuentra en una etapa inicial Se cuenta con sistema contraincendios |
| A11.1.5 | El trabajo en áreas seguras | Aplicar | Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación |
| A11.1.6 | Áreas de carga y descarga | Aplicar | Existen lugares exclusivos para realizar la carga y descarga |
| **A11.2** | **Seguridad de los equipos** | | |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A11.2.1 | Emplazamiento y protección de equipos | Aplicar | Los equipos relacionado se encuentran en áreas adecuadamente protegida |
| A11.2.2 | Instalaciones de suministro | Aplicar | Se cuenta con el sistema UPS proporciona una potencia adecuada, confiable y de alta calidad<br>Se cuenta con detectores de temperatura con alarmas de temperatura |
| A11.2.3 | Seguridad del cableado | Aplicar | Se cuenta con la protección física adecuada para cables externos, cajas de conexiones |
| A11.2.4 | Mantenimiento de los equipos | Aplicar | Se realiza el mantenimiento de manera parcial, no se cuenta con un plan de mantenimiento de activos |
| A11.2.5 | Retirada de materiales propiedad de la empresa | Aplicar | Se cuenta con procedimientos relativos al traslado de activos de información |
| A11.2.6 | Seguridad de los equipos fuera de las instalaciones | Aplicar | No se cuenta con políticas para el manejo de equipos fuera de la empresa |
| A11.2.7 | Reutilización o eliminación segura de equipos | Aplicar | No existe políticas de eliminación segura de equipos |
| A11.2.8 | Equipo de usuario desatendido | Aplicar | No todo el personal realiza la suspensión de las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción |
| A11.2.9 | Política de puesto de trabajo | Aplicar | No existen políticas, normas, procedimientos y directrices para |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| | despejado y pantalla limpia | | mantener las zonas de trabajo limpias y despejada |
| **A12** | **Seguridad de las operaciones** | | |
| **A12.1** | **Procedimientos y responsabilidades operacionales** | | |
| A12.1.1 | Documentación de procedimientos operacionales | Aplicar | La documentación de los procedimientos para las operaciones relativas a la seguridad de la información de cada uno de los activos, se encuentra en una etapa inicial |
| A12.1.2 | Gestión de cambios | Aplicar | No existe una política de gestión de cambios |
| A12.1.3 | Gestión de capacidades | Aplicar | No existe una política de gestión de capacidades |
| A12.1.4 | Separación de los recursos de desarrollo, prueba y operación | Aplicar | La empresa cuenta con entornos de TIC para el equipo de desarrollo, prueba y operacionales |
| **A12.2** | **Protección contra el software malicioso (malware)** | | |
| A12.2.1 | Controles contra el código malicioso | Aplicar | No existen políticas y procedimientos asociados a controles antimalware |
| **A12.3** | **Copias de seguridad** | | |
| A12.3.1 | Copias de seguridad de la información | Aplicar | Existen políticas y procedimientos asociados a las copias de seguridad |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| **A12.4** | **Registros y supervisión** | | |
| A12.4.1 | Registro de eventos | Aplicar | No existen políticas y procedimientos para el registro de eventos |
| A12.4.2 | Protección de la información del registro | Aplicar | Los controles para el acceso a los registros para su control adecuado, autorizado y monitoreado se encuentra en una etapa inicial |
| A12.4.3 | Registros de administración y operación | Aplicar | Se realiza el registro de los eventos relacionados con la seguridad de la información para la generación de las evidencias. |
| A12.4.4 | Sincronización del reloj | Aplicar | Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión |
| **A12.5** | **Control del software en explotación** | | |
| A12.5.1 | Instalación del software en explotación | Aplicar | Existe una política acerca de la instalación de software, pero no se cumple |
| **A12.6** | **Gestión de la vulnerabilidad técnica** | | |
| A12.6.1 | Gestión de las vulnerabilidades técnicas | Aplicar | No existe una política para la gestión de vulnerabilidades técnicas |
| A12.6.2 | Restricción en la instalación de software | Aplicar | La instalación de programas solo debe ser realizado por el personal autorizado |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| **A12.7** | **Consideraciones sobre la auditoria de sistemas de información** | | |
| A12.7.1 | Controles de auditoría de sistemas de información | Aplicar | No existe una política sobre auditorias de seguridad de la información |
| **A13** | **Seguridad de las comunicaciones** | | |
| **A13.1** | **Gestión de la seguridad de las redes** | | |
| A13.1.1 | Controles de red | Aplicar | Los dispositivos se autentican mediante algoritmos fuerte y cifrados<br>Se utiliza la segmentación de redes adecuada usando cortafuegos, VLAN, VPN, etc.<br>Se controlan los puertos y servicios utilizados para funciones de administración de sistemas |
| A13.1.2 | Seguridad de los servicios de red | Aplicar | El acceso a la red es monitoreado y controlado |
| A13.1.3 | Segregación en redes | Aplicar | Las redes están segmentadas en VLAN y el acceso es restringido |
| **A13.2** | **Intercambio de información** | | |
| A13.2.1 | Políticas y procedimientos de intercambio de información | Aplicar | No existen políticas y procedimientos relacionados con la transmisión segura de información |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A13.2.2 | Acuerdos de intercambio de información | Aplicar | Los acuerdos de intercambio de información se encuentra en una etapa inicial |
| A13.2.3 | Mensajería electrónica | Aplicar | Existe controles de seguridad adecuados para el intercambio de datos mediante el correo electrónico, para asegurar la autenticidad, la confidencialidad de los mensajes. |
| A13.2.4 | Acuerdos de confidencialidad o no revelación | Aplicar | Existe acuerdos contractuales con el personal donde se establece el compromiso de confidencialidad de la información. |
| **A14** | **Adquisición, desarrollo y mantenimiento de los sistemas de información** | | |
| **A14.1** | **Requisitos de seguridad en los sistemas de información** | | |
| A14.1.1 | Análisis de requisitos y especificaciones de seguridad de la información | Aplicar | Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software |
| A14.1.2 | Asegurar los servicios de aplicaciones en redes públicas | Aplicar | Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio |
| A14.1.3 | Protección de las transacciones de servicios de aplicaciones | Aplicar | Las transacciones se realizan de manera segura, con la finalidad de garantizar la confidencialidad e integridad de la información |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| **A14.2** | **Seguridad en el desarrollo y en los procesos de soporte** | | |
| A14.2.1 | Política de desarrollo seguro | Aplicar | Los ambiente de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios |
| A14.2.2 | Procedimiento de control de cambios en sistemas | Aplicar | Se cuenta con procedimientos y registros relacionados de la gestión de control de cambios |
| A14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | Aplicar | Se realiza las validaciones y evaluaciones de riesgo después de un cambio o mantenimiento a los sistemas |
| A14.2.4 | Restricciones a los cambios en los paquetes de software | Aplicar | El proveedor del software es el encargado de brindar el soporte tras los cambios al software |
| A14.2.5 | Principios de ingeniería de sistemas seguros | Aplicar | Se realiza capacitaciones al personal de desarrollo para brindarles el conocimiento adecuado necesario de prácticas seguras al momento de la programación |
| A14.2.6 | Entorno de desarrollo seguro | Aplicar | Los entornos de desarrollo se encuentran aislados y el software modificado es verificado por el personal del ambiente de pruebas. |
| A14.2.7 | Externalización del desarrollo de software | Aplicar | Se realiza la evaluación de seguridad del software desarrollado por proveedores y se solicita el código fuente. |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A14.2.8 | Pruebas funcionales de seguridad de sistemas | Aplicar | Existe procedimientos de pruebas técnicas y funcionales del software desarrollado |
| A14.2.9 | Pruebas de aceptación de sistemas | Aplicar | Se realizan pruebas de aceptación de usuario antes de ser desplegado en el ambiente productivo |
| **A14.3** | **Datos de prueba** | | |
| A14.3.1 | Protección de los datos de prueba | Aplicar | Se utilizan mecanismos de enmascaramiento para proteger la información para las pruebas |
| **A15** | **Relación con proveedores** | | |
| **A15.1** | **Seguridad en las relaciones con proveedores** | | |
| A15.1.1 | Política de seguridad de la información en las relaciones con los proveedores | Aplicar | Existe políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI pero se encuentran en una etapa inicial |
| A15.1.2 | Requisitos de seguridad en contratos con terceros | Aplicar | Los contratos y acuerdos formales con proveedores se encuentran documentados |
| A15.1.3 | Cadena de suministro de tecnología de la información y de las comunicaciones | Aplicar | Existe acuerdos documentados con los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados. |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| **A15.2** | **Gestión de la provisión de servicios del proveedor** | | |
| A15.2.1 | Control y revisión de la provisión de servicios del proveedor | Aplicar | Existe acuerdos documentados con los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados. |
| A15.2.2 | Gestión de cambios en la provisión del servicio del proveedor | Aplicar | Existe acuerdos documentados con los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados. |
| **A16** | **Gestión de incidentes de seguridad de la información** | | |
| **A16.1** | **Gestión de incidentes de seguridad de la información y mejoras** | | |
| A16.1.1 | Responsabilidades y procedimientos | Aplicar | No existen políticas, procedimientos para la gestión de incidentes |
| A16.1.2 | Notificación de los eventos de seguridad de la información | Aplicar | Los incidentes reportados, son evaluados y documentados, para establecer los procedimientos a seguir para dar la solución. |
| A16.1.3 | Notificación de puntos débiles de la seguridad | Aplicar | El personal debe realizar el reporte de cualquier tipo de ocurrencia inusual |
| A16.1.4 | Evaluación y decisión sobre los eventos de seguridad de | Aplicar | Los incidentes reportados, deben ser evaluadas por el jefe del área de sistemas |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| | información | | |
| A16.1.5 | Respuesta a incidentes de seguridad de la información | Aplicar | Los incidentes deben ser registrados en formatos, para que el responsable de la solución respectiva |
| A16.1.6 | Aprendizaje de los incidentes de seguridad de la información | Aplicar | Se debe realizar la documentación respectiva de los incidentes de seguridad de la información y se debe especificar las vulnerabilidades, amenaza y el riesgo al que está expuesto el activo, con la finalidad de implementar los controles de seguridad. |
| A16.1.7 | Recopilación de evidencias | Aplicar | Elaboración de formatos y documentos para la recopilación de las evidencias, para que personal responsable pueda realizar su verificación |
| **A17** | **Aspectos de seguridad de la información para la gestión de la continuidad de negocio** | | |
| **A17.1** | **Continuidad de la seguridad de la información** | | |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información | Aplicar | No existe un plan de continuidad de negocio |
| A17.1.2 | Implementar la continuidad de la seguridad de la información | Aplicar | Se debe crear controles de seguridad adecuados para la continuidad del negocio |
| A17.1.3 | Verificación, revisión y evaluación | Aplicar | Se debe crear métodos de pruebas del plan de continuidad |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| | de la continuidad de la seguridad de la información | | |
| **A17.2** | **Redundancias** | | |
| A17.2.1 | Disponibilidad de los recursos de tratamiento de la información | Aplicar | Se debe identificar los requisitos de disponibilidad de servicios |
| **A18** | **Cumplimiento** | | |
| **A18.1** | **Cumplimiento de los requisitos legales y contractuales** | | |
| A18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Aplicar | Existe una política para dar cumplimiento a los requisitos de las normas legales vigentes |
| A18.1.2 | Derechos de Propiedad Intelectual (DPI) | Aplicar | Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual. |
| A18.1.3 | Protección de los registros de la organización | Aplicar | Los registros de la empresa están protegidos físicamente para evitar la alteración, modificación, pérdida y acceso de usuarios no autorizados. |
| A18.1.4 | Protección y privacidad de la información de carácter personal | Aplicar | Los datos personales son guardados y protegidos de acuerdo a las regulaciones y leyes vigentes |

| Sección | Controles de Seguridad de la Información | Estado | Comentarios |
|---|---|---|---|
| A18.1.5 | Regulación de los controles criptográficos | Aplicar | No existe una políticas que cubra actividades relacionadas a la criptografía |
| **A18.2** | **Revisiones de la seguridad de la información** | | |
| A18.2.1 | Revisión independiente de la seguridad de la información | Aplicar | No existe políticas de auditorías internas |
| A18.2.2 | Cumplimiento de las políticas y normas de seguridad | Aplicar | No existe políticas de auditorías internas, para evaluar el cumplimiento de las normas de seguridad de la información. |
| A18.2.3 | Comprobación del cumplimiento técnico | Aplicar | No se lleva a cabo escaneos de vulnerabilidades de red y pruebas de intrusión. |

Nota: Datos tomados del anexo A de la norma ISO27001:2013, (2017). Fuente: Elaboración propia.