**UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA**

**FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

# "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"


**Tesis presentado por:**

Bach. Mercedes Ccesa Quincho


**Para optar el título profesional de:**

Ingeniero Informático


**Asesor:**

Ing. Manuel A. Lagos Barzola


Ayacucho, mayo de 2017

## Dedicatoria

A Dios por ser el motor de mi vida y el que guía mi camino.

A la Virgen María por cuidarme y protegerme siempre.

A mis padres Modesto Julio y Sixta Alejandría, por brindarme su amor y apoyo incondicional y por enseñarme a luchar por un mundo mejor.

A mis hermanos: Maritza y Julio por su aliento y consejo.

## Agradecimientos

A Dios por darme salud y permitirme terminar esta etapa de mi vida.

A mis padres y hermanos por su amor, confianza, paciencia, aliento y apoyo incondicional.

A mi amiga Ana Lucila López por su amistad incondicional y generosidad.

Al Ing. Manuel Lagos Barzola por su asesoría

A mis amigos de la Subgerencia de Sistemas y Tecnología de la Municipalidad Provincial de Huamanga por dedicarme su tiempo y brindarme todo el apoyo para la realización de mi tesis.

# Contenido

## Lista de tablas

## Lista de figuras

# Resumen

La información es considerada hoy en día el mayor activo que posee cualquier organización y en consecuencia requiere de una protección adecuada.

En el Perú, con el objetivo de establecer una adecuada gestión de la seguridad de la información que ayude a preservar la confidencialidad, integridad y disponibilidad de la misma, se exige a las entidades públicas integrantes del sistema nacional de informática la implementación de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 (Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información), pero el desconocimiento por parte de la alta dirección, la falta de presupuesto y falta de personal especializado ha ocasionado que no se cumplan con el cronograma establecido por el estado para su implementación.

Se escogió como caso de estudio a la Municipalidad Provincial de Huamanga y para realizar el diseño de su SGSI se dividió la investigación en tres fases: en la primera fase se realizó el diagnóstico inicial de la entidad con respecto a la NTP ISO/IEC 27001:2014 y su posibilidad de aceptación, en la segundad fase se estudió a la organización y su contexto; se identificó el proceso crítico; se definió la política de seguridad, el alcance y se identificó al comité de seguridad de la información de la organización, en la tercera fase, siguiendo la metodología de análisis y gestión de riesgos adoptada, se identificó y valoró los activos de información, se identificó las amenazas, se realizó el cálculo del impacto y del riesgo, se identificaron las medidas de control necesarias para mitigar los riesgos a un nivel aceptable y finalmente se elaboró un documento denominado declaración de aplicabilidad que contiene la justificación de qué controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementados en la organización.



**Palabras Clave:** NTP ISO/IEC 27001:2014, sistema de gestión de seguridad de la Información, seguridad MPH, activo de información, impacto, riesgo, control de seguridad.

# Capítulo I

# Planteamiento del problema

## 1.1. Diagnóstico y enunciado del problema

Hoy en día, muchas empresas invierten en Tecnologías y Sistemas de información con el fin de satisfacer las necesidades del negocio, tener un control de sus operaciones y sobresalir en un mercado cada vez más competitivo y de constante evolución tecnológica.

> Desde una perspectiva de negocios, los sistemas de información forman parte de una serie de actividades que agregan valor para adquirir, transformar y distribuir la información que los gerentes pueden usar para mejorar la toma de decisiones, el desempeño de la organización y, en última instancia, incrementar la rentabilidad de la empresa. (Laudon y Laudon, 2012, p.25)

De acuerdo a lo mencionado, la información, tanto digital como física, cumple un papel muy importante ya que actúa como activo principal y genera valor económico real para una organización. Si una empresa no administra, protege o asegura adecuadamente su información estará expuesta a riesgos que perjudicarán la continuidad de su negocio. Es por ello, que toda información debe ser protegida, para que se encuentre accesible en tiempo y forma o, desde el punto de vista de la seguridad de información, conserve sus características de confidencialidad, integridad y disponibilidad.

Es así que desde tiempos inmemorables las organizaciones han puesto los medios necesarios para evitar el robo y manipulación de su información confidencial, pero con el desarrollo e incorporación de nuevas tecnologías de información y comunicaciones (TICs) han aumentado también los riesgos de nuevas amenazas a los que se exponen las organizaciones.

Hoy en día es relativamente fácil tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida, con poco esfuerzo y conocimientos, causando graves perjuicios para la organización; asimismo la poca

concientización a los trabajadores en temas de seguridad de información hace aún más vulnerable a las empresas u organizaciones.

Por otro lado, en el Perú, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) como ente rector del Sistema Nacional de Informática, ha venido publicando (en su página web y en Diario Oficial el Peruano) desde el año 2004 normas relacionas a la seguridad de información —a saber las Normas Técnicas Peruanas NTP ISO/IEC 17799:2004, NTP ISO/IEC 17799:2007, NTP ISO/IEC 27001:2008 y la NTP ISO/IEC 27001/2014 (que reemplaza a la NTP ISO/IEC 27001:2008)— para ayudar a las entidades del estado a proteger su información sensible mediante la implementación de un sistema de gestión de seguridad de la información.

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al sistema nacional de informática, el diseño e implementación de un sistema de gestión de seguridad de la información (SGSI), basándose en la norma técnica peruana (NTP) ISO/IEC 27001:2014 aprobada mediante la resolución ministerial Nº 004-2016-PCM el 8 de enero de 2016.

Una de las entidades integrantes del sistema nacional de informática son los órganos de informática de las municipalidades (Oficina Nacional de Gobierno Electrónico e Informática, 2016). En el caso de la provincia de Huamanga se ha observado que las municipalidades desconocen de la existencia de esta norma, y no han establecido lineamientos de seguridad de la información de acuerdo a los estándares, que les ayude tanto en la prevención como recuperación ante desastres o ataques (internos y externos) que pudieran afectar a la información que manejan.

Así también cabe mencionar que una municipalidad (como institución del estado) tiene como finalidad ser una instancia de representación, promotora del desarrollo integral sostenible y una instancia prestadora de servicios públicos que contribuyan a satisfacer las aspiraciones y necesidades del ciudadano, en el ámbito de su competencia de acuerdo a lo dispuesto en la Ley Orgánica de Municipalidades Ley N° 27972 (Instituto de Estudios Peruanos, 2016).

En su esfuerzo de brindar mejores servicios y estar acorde con el avance tecnológico la Municipalidad Provincial de Huamanga ha experimentado un crecimiento constante de su plataforma tecnológica, además de sus activos, tales como la información, el hardware y software, equipos de cómputo, equipos de red y telecomunicaciones, recurso humano entre otros, y estos pueden estar expuestos a situaciones de inseguridad.

Para proteger a la Municipalidad Provincial de Huamanga de las amenazas a las que se enfrenta, es necesario conocerlas para afrontarlas de una manera adecuada, así mismo conocer los activos a los que afecta. Para ello se debe establecer la metodología adecuada e implementar controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia.

Bajo este contexto, se presenta como alternativa de solución al problema identificado el diseño de un sistema de gestión de seguridad de la información alineado a la normativa peruana vigente para cubrir las necesidades de los procesos institucionales críticos de la MPH, de tal forma, que el documento resultante sirva como referencia de implementación de la norma NTP ISO/IEC 27001:2014 en dicha institución.

## 1.2. Formulación del problema de investigación

### 1.2.1. Problema principal

¿Cuáles son las características del 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?

### 1.2.2. Problemas secundarios

a. ¿Cuál es el alcance del diseño del SGSI para la Municipalidad Provincial de Huamanga?
b. ¿Cuáles son los resultados del análisis de riesgos del diseño del SGSI para la Municipalidad Provincial de Huamanga?
c. ¿Qué controles de seguridad son aplicables para el diseño del SGSI para la Municipalidad Provincial de Huamanga?

## 1.3. Objetivos de la investigación

### 1.3.1. Objetivo general

Determinar las características del 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.

### 1.3.2. Objetivos específicos

a. Analizar las áreas funcionales y definir el alcance del diseño del SGSI para la Municipalidad Provincial de Huamanga
b. Realizar la evaluación de riesgos de seguridad de información para la Municipalidad Provincial de Huamanga
c. Elaborar la lista de controles de seguridad para mitigar los riesgos identificados en el diseño del SGSI para la Municipalidad Provincial de Huamanga.

## 1.4. Hipótesis de la investigación

Para Hernández, Fernández y Baptista (2014), no todas las investigaciones cuantitativas plantean hipótesis. La formulación de hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas cuyo alcance de estudio es exploratorio, no se formula hipótesis; si es descriptivo, sólo se formulan hipótesis cuando se pronostica un hecho o dato; si es correlacional, formulan hipótesis correlacionales; y si es explicativo, formulan hipótesis causales.

El presente trabajo tiene un nivel de investigación descriptivo y no pronostica ningún hecho o dato por lo que no se formulará una hipótesis.

## 1.5. Justificación y delimitación de la investigación

### 1.5.1. Importancia del tema

Con este proyecto de investigación la Municipalidad Provincial de Huamanga da un primer paso en la implantación de un sistema de gestión de seguridad de la Información bajo la NTP ISO/IEC 27001:2014.

### 1.5.2. Justificación

Asegurar los activos de información es de vital importancia dentro de cualquier organización. En palabras de Pallas (2009):

> La seguridad de la información, no es un activo a comprar, ni un fin en sí mismo, tampoco un estado a alcanzar haciendo una determinada inversión; debe gestionarse, debe existir una meta concreta, criterios generales de evaluación y de decisión, y debe poder medirse. Es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan comparar conscientemente y lo más objetivamente posible, escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos disponibles. (p.2)

En este sentido la norma ISO/IEC 27001:2013 sirve como modelo para el establecimiento, implementación, seguimiento y mejora de un sistema de gestión de seguridad de la información en cualquier tipo de organización basándose en sus propios objetivos y requerimientos de seguridad y usando, además, los controles sugeridos en la norma ISO/IEC 27002.

Asimismo, el Perú a través de la Oficina de Gobierno Electrónico e Informática (ONGEI) como ente rector del sistema nacional de informática ha venido aprobando desde el 2004 los estándares tecnológicos para asegurar las medidas de seguridad de la información en las entidades de la administración pública.

La presente tesis responde a la necesidad creada por la ONGEI al declarar el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición, en todas las entidades integrantes del sistema nacional de informática (con fecha de publicación 14 de enero del 2016 en el Diario Oficial el Peruano) con la finalidad de cooperar con la infraestructura de gobierno electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo.

Una de los miembros del sistema nacional de informática son los órganos de informática de las municipalidades (Oficina Nacional de Gobierno Electrónico e Informática, 2016). En el caso de Huamanga se ha observado que las subgerencias, oficinas de Sistemas e Informática y en su defecto las que hacen las partes de éstas, no tienen conocimiento de esta norma, ni un diseño, ni mucho menos implementado un sistema de gestión de seguridad de la información, retrasando de este modo uno de los objetivos (el relacionado con la seguridad de la información) de la actual política nacional de gobierno electrónico 2013-2017, el mismo que busca garantizar la integridad, confidencialidad y disponibilidad de la información en la administración pública mediante mecanismos de seguridad de la información gestionada, así como articular los temas de ciberseguridad en el Estado. Para esto recomienda que deben establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano.

Es así que el diseño e implementación de un adecuado sistema de gestión de seguridad de la información demuestra el compromiso de la organización hacia la seguridad de la información y le proporciona a la entidad las herramientas y elementos necesarios para alcanzar de manera efectiva los siguientes objetivos:

- Reducir los riesgos relacionados con la confidencialidad, disponibilidad e integridad de la información, mediante un análisis de riesgos y establecimiento de controles.
- Dar cumplimiento a la legislación que regula la protección de información confidencial, de sistemas de información y demás datos sensibles.
- Reducir los costes comerciales debido a la menor cantidad de incidentes y una adecuada inversión en tecnologías.
- Permite la elaboración formal de planes de contingencia.

Asimismo, un SGSI proporciona indicadores (en base los controles establecidos en el anexo A de la NTP ISO/IEC 27001:2014) para medir, cuantificar y mejorar la seguridad de la información.

### 1.5.3. Delimitación

La investigación se realizó en la Municipalidad Provincial de Huamanga el año 2016, en la Subgerencia de Sistemas y Tecnología, por ser ésta la responsable de formular, proponer y ejecutar normas internas para el desarrollo y aplicación de políticas, prácticas, procedimientos y funciones que aseguren los niveles adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información, los datos y de las comunicaciones de la Municipalidad (Municipalidad Provincial de Huamanga, 2016a).

# Capitulo II

# Marco de referencia de la investigación

## 2.1. Antecedentes de la investigación

Ponemon Institute (2016), en su artículo “Flipping the Economics of Attacks” concluye que hay que tener en cuenta la motivación y el entorno económico de los ataques, y no sólo enfocarnos en soluciones técnicas a los problemas de seguridad, debido a que los atacantes se desvían hacia otros objetivos (organizaciones) cuando romper la seguridad de una organización le toma más tiempo del que han previsto. Por eso recomienda crear una estrategia integral de ciberseguridad, que se centre en los tres componentes importantes de un programa de seguridad: personas, procesos y tecnología, así como construir un equipo fuerte de operaciones de seguridad con políticas claras en lugar de responder eficazmente a los incidentes de seguridad.

Guzmán (2015), en su trabajo de investigación “Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso”, concluyó que el diseño de un sistema de gestión de seguridad de la información basado en un modelo de mejoras prácticas y lineamientos de seguridad, como es la norma ISO/IEC 27001:2013, es un herramienta de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta cuando las organizaciones deciden establecer un modelo de seguridad de la información, ya que si las organizaciones logran cumplir al pie de la letra lo establecido en la norma ISO/IEC 27001:2013, pueden llegar a forjar en el tiempo un adecuado y sostenible SGSI, aunque dicha labor depende del tamaño y naturaleza de la entidad y de la cultura de la misma en torno a la seguridad de la información. Asimismo, menciona que es indispensable contar con el apoyo de la alta directiva, para poder concebir un modelo de seguridad de la información que realmente apoye y apalanque la misión y visión de la organización; y es fundamental contar con este apoyo antes de comenzar a diseñar un SGSI, ya que si esto no se logra conseguir, es casi seguro que cualquier iniciativa de seguridad no alcancen los resultados esperados.

Justino (2015), en su tesis “Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la NORMA ISO/IEC

27001:2013”, concluyó que el papel de la alta dirección es muy importante en el SGSI, porque además de tomar las decisiones estratégicas más importantes de la organización, su compromiso será fundamental para llevar a cabo el SGSI e imprescindible para la implementación de los controles. Menciona también la importancia de establecer políticas de seguridad de información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas y mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad, asimismo considera importante establecer roles y responsabilidades que ayuden a garantizar el cumplimiento de las políticas y el monitoreo de los riesgos a los que se encuentra expuesta la información.

Aguirre (2014), en su tesis “Diseño de un sistema de gestión de seguridad de información para Servicios Postales del PERÚ S.A.” concluyó que el apoyo de la alta gerencia fue imprescindible para concientizar a los jefes de área y dueño de los procesos de la institución, así como para el levantamiento de información, asimismo hace énfasis en la necesidad de difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

Sandoval (2014), en su tesis “Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa”, concluyó que: la puesta en funcionamiento de un SGSI basado en la norma ISO/IEC 27001 garantiza la ejecución de un conjunto de procesos que gestionen la accesibilidad de la información en la empresa, asimismo señala que realizar esta implementación siguiendo las cuatro fases fundamentales (Planificar, Hacer Verificar y Actuar) del Ciclo de Deming, permite desarrollar una metodología de trabajo clara y estructurada, y que la revisión periódica de los controles seleccionados e implementados reduce los riesgos de pérdida, robo o corrupción de la información en la empresa.

Suárez (2013), en su tesis “Estudio de la seguridad de la información aplicado a Recursos Humanos, Adquisiciones y Cómputo para empresas del Sector Pesquero”, concluyó que la prioridad que posee el área de seguridad en las tecnologías de información, se afirma en que las empresas están en la obligación, incluso de aspecto legal, de certificarse y mantener las mejores prácticas ofrecidas en las Normas Internacionales, estipuladas en la ISO 27000, ISO 27001, cuyos estándares permitirán, después de su correcta y verificada implementación y puesta en marcha de controles minuciosos y continuos, que la empresa desarrolladora obtenga un agregado de confianza y solidez.

López (2011), en su tesis “Diseño de un plan de gestión de seguridad de la información. Caso: dirección de informática de la alcaldía del municipio Jiménez del estado Lara”, concluyó que el diseño del SGSI (una vez implantado) brindará un esquema de seguridad más sólido y eficiente en el uso de los sistemas de información.

Barragán, Góngora y Martínez (2011), en su tesis “Implementación de Políticas de Seguridad Informática para la Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002”, concluyeron que la forma de conseguir mayor beneficio en la seguridad de la información es contar con una adecuada evaluación de riesgos, que orienten las inversiones y que minimicen el impacto en casos de incidentes. Asimismo, mencionan que la organización debe entender la seguridad como un proceso que nunca termina.

Villena (2006), en su tesis “Sistema de gestión de seguridad de información para una institución financiera”, concluyó que no necesariamente la tecnología de información por sí sola garantiza la seguridad de la información. Se vuelve imperativo gestionarla de acuerdo siempre a los objetivos de negocio. Asimismo, afirma que de nada sirve contar con los últimos adelantos tecnológicos, si no se da la importancia debida a la protección de la información, la cual se verá reflejada en el cumplimiento de todas las políticas de seguridad de la información, siempre actualizadas de acuerdo a los cambios constantes propios de una institución.

## 2.2. Marco teórico

A continuación, se presenta la definición de algunos conceptos claves que deben estar claros para la comprensión del tema.

### 2.2.1. Información

La información "comprende los datos y conocimientos que se usan en la toma de decisiones" (Ferrell y Geoffrey, 2004, p.121).

> Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones. (Chiavenato, 2006, p.110)

La información es también, un activo que tiene valor para la organización y que requiere una protección adecuada frente a la constante exposición a distintas amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Sea cual sea la forma que tome la información, o medio en que se almacene o comparta, siempre tiene que estar apropiadamente protegida (INDECOPI, 2007).

### 2.2.2. Seguridad

La Real Academia Española (2014) define a la seguridad como la cualidad de que algo (o alguien) esté libre y exento de riesgo.

La seguridad viene a ser la protección de los activos frente a acciones o situaciones no deseadas, mediante la implantación de los controles, lo que suele suponer una inversión y un esfuerzo. Todo ello se lleva a cabo en las entidades con el objetivo de proteger los intereses de los accionistas, de los empleados, de los clientes, de los proveedores y de los ciudadanos afectados según el sector (Peso y Ramos, 2004).

### 2.2.3. Seguridad de la información

La seguridad de la información es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran. Así también puede involucrar otras propiedades como la autenticidad, no repudio y confiabilidad. La seguridad de la información protege a la información (implantando un conjunto adecuado de controles —que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware—, monitoreándolos, revisándolos y mejorándolos donde sea necesario) de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio (INDECOPI, 2007).

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma. Diferenciando el concepto de seguridad de la información con el de seguridad informática, en que este último sólo se encarga de la seguridad en el medio informático (Fitzgerald, 2007).

### 2.2.4. Sistema de gestión de la seguridad de la información

Gómez y Fernández (2015) definen al sistema de gestión de seguridad de la información como un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización. Así mismo mencionan que la implementación de un SGSI supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada.

Fundamentalmente se distinguen dos tipos de procesos:

1. Procesos de gestión. Controlan el funcionamiento del propio sistema de gestión y su mejora continua.

2. Procesos de seguridad. Se centran en los aspectos relativos a la propia seguridad de información.

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

### 2.2.5. Oficial de seguridad de la información

El oficial de seguridad de la información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), es la persona encargada de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información. Así como de realizar una correcta gestión de riesgo para la toma de decisiones. (Aguirre, 2014, p.28)

Las responsabilidades de cada oficial de seguridad de la información varían dependiendo de la organización en la que se encuentren, debido a que la protección de la información está limitada por la cultura organizacional. El CISO debe entender que el programa básico de protección de la información se implementará en toda la empresa. Sin embargo, cada unidad de negocios debe tener la libertad de hacer modificaciones para satisfacer sus necesidades específicas — por ejemplo, si una organización es multinacional, será necesario hacer ajustes para cada uno de los países— (Peltier, Peltier y Blackley, 2005).

### 2.2.6. Política de seguridad

La política de seguridad es la información documentada en la que se reflejan, en términos generales, los objetivos de la organización y las principales líneas de acción que permiten proteger la información frente a pérdidas de confidencialidad, integridad y disponibilidad. La definición de esta política debe tener en cuenta los requisitos del negocio, contractuales, legales y estatutarios, los cuales

quedarán reflejados en la misma. Asimismo, este documento debe ser comunicado a todas las partes interesadas del SGSI (Gómez et al., 2015).

Peltier et. al. (2005) considera a la política de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos mencionan que estas cumplen con 2 roles importantes, un rol interno y otro externo.

- **Rol Interno:** Ya que se menciona a cada uno de los miembros de la organización, qué se espera que realicen y cómo se evaluará el trabajo realizado.
- **Rol Externo:** Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

### 2.2.7. Riesgo

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad (INDECOPI, 2007).

Halvorson (2008) explica tres naturalezas del riesgo, estos son: los riesgos estratégicos, tácticos y operacionales.

- Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la información; sin embargo, se encuentran más orientados a los riesgos de las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.
- Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.

- Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para Tipton, Krause y Ozier (2006) existen algunas preguntas clave que los dueños de los activos pueden responder para identificar el potencial daño o pérdida debido a un riesgo, estás son:

1. ¿Qué puede suceder? (¿Cuál es la amenaza?)
2. Si sucede, ¿qué tan malo puede ser? (¿Cuál es el impacto?)
3. ¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)
4. ¿Qué tan ciertas son las respuestas a las tres primeras preguntas? (¿Cuál es el grado de confianza?)

MARGERIT (2012) define el riesgo como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Es decir que el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

### 2.2.8. Análisis y evaluación de riesgos

El análisis de riesgos es “un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización” (MARGERIT, 2012, p.9). Sabiendo lo que podría pasar, hay que tomar decisiones para tratar estos riesgos.

Para Muñoz (Como se citó en López, 2011) el análisis y gestión de riesgos de los sistemas de información es el núcleo de las actuaciones relacionadas con el análisis, la evaluación y la gestión del riesgo. Es así que siguiendo una metodología de gestión de riesgos se puede analizar los riesgos, identificar las amenazas y su impacto, y gestionar el riesgo basado en: (a) elementos (activos, amenazas, vulnerabilidades, riesgos, impactos, salvaguardas), (b) eventos (estáticos, dinámicos organizativos, dinámicos físicos) y (c) procesos (planificación, análisis de riesgos, gestión de riesgos, selección de salvaguardas).

### 2.2.9. Control

Son “medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida” (INDECOPI, 2007, p.13).

Una clasificación generalizada de los controles puede ser:

- “Preventivos: Reducen las vulnerabilidades.
- Detectivos: Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.
- Correctivos: Contrarrestan el impacto de la ocurrencia de una amenaza.
- Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas. [Tupia, 2009]” (Aguirre, 2014, p.30).

### 2.2.10. Serie de normas ISO/IEC 27000

La Seguridad de la Información tiene asignada la serie 27000 dentro de los estándares ISO/IEC, siendo un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Las distintas normas que componen la serie ISO 27000 son:

- **ISO/IEC 27000:** Contiene términos y definiciones empleados en toda la serie 27000.
- **ISO/IEC 27001:** Sistemas de Gestión de la Seguridad de la Información (SGSI). Es el estándar principal de la familia, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información. Es certificable.
- **ISO/IEC 27002:** (antes ISO17799). Guía de mejores prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 14 dominios, 35 objetivos de control y 114 controles. Proporciona recomendaciones de las mejores prácticas en la prevención de la confidencialidad, integridad y disponibilidad. Para ello, la norma se

estructura en dominios que cubren la gestión de la seguridad de la información.

- **ISO/IEC 27003:** Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo con la ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI
- **ISO/IEC 27004:** Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001
- **ISO 27005:** Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2013 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos
- **ISO 27006:** Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información (SGSI).
- **ISO/IEC 27007:** Provee una guía para conducir una auditoria de un SGSI, así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011
- **ISO/IEC TR 27008:** Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.
- **ISO/IEC 27010:** Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.
- **ISO/IEC 27011:** Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.

- **ISO/IEC 27013:** Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.
- **ISO/IEC 27014:** Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.
- **ISO/IEC TR 27015:** Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.
- **ISO/IEC TR 27016:** Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.
- **ISO/IEC 27799:2008:** Brinda una guía para apoyar la implementación de un SGSI en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector (ISO 27000, s.f. a).

### 2.2.11. Normas técnicas peruanas de seguridad de la información

#### *2.2.11.1. Norma técnica peruana NTP–ISO/IEC 27001:2014.*

La norma NTP–ISO/IEC 27001 es una adaptación de la ISO/IEC 27001. La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico, dispone el uso obligatorio de la Norma Técnica Peruana “NTP – ISO/IEC 27001:2014 EDI, Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición.

> Esta Norma Técnica Peruana ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está

influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. (INDECOPI, 2014, p.vii)

**a. Estructura de la NTP-ISO/IEC 27001:2014**

La norma ISO 27001:2013 (en el Perú NTP-ISO/IEC 27001:2014) no sólo establece cambios en el contenido (respecto a la ISO 2001:2005) sino también en la estructura, lo que verá reflejado en otros documentos que forman parte de la familia ISO 27000. La norma ISO 27001:2013 ha sido desarrollada con base al Anexo SL, en la que se proporciona un formato y un conjunto de alineamiento que siguen el desarrollo documental de un sistema de gestión sin que le importe el enfoque empresarial, se alinean bajo la misma estructura todos los documentos que se relacionan con el sistema de gestión de seguridad de la información y así se evitan problemas de integración con otros marcos de referencia (ISOTools Excellence, 2015).

La estructura de la norma queda así:

0. Introducción
1. Objeto y campo de aplicación
2. Referencias Normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación
10. Mejora
11. Anexo A – Lista de controles

Gómez et al. (2015) señalan que cuando una organización quiere cumplir los requisitos de la NTP-ISO/IEC 27001, debe demostrar la efectiva implantación de los apartados 4 al 10, que son los que conforman el cuerpo principal de la norma.

Asimismo, el SGSI debe contar con información documentada en varios niveles (ver Figura 2.1):

- Políticas que proporcionan las líneas generales de actuación en cada caso.
- Información documentada sobre procesos (generalmente denominadas procedimientos), que proporcionan las actividades a ejecutar.
- Información documentada sobre evidencias (anteriormente denominados registros), que permiten demostrar que se han llevado las actividades previstas.

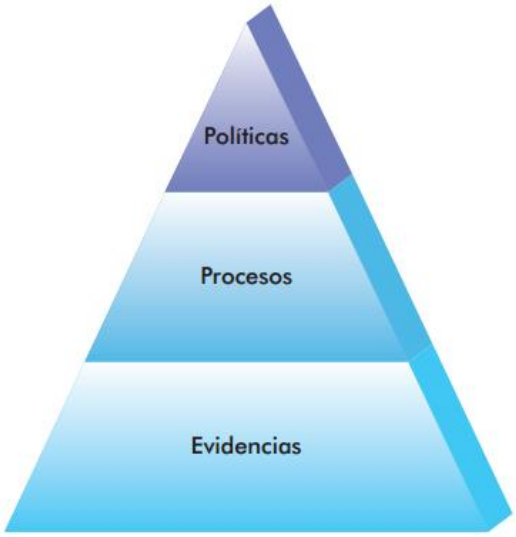


*Figura 2.1*. Niveles de información documentada.

Fuente: Cómo implementar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad, p. 18, Gómez et al. 2015

A continuación, se presenta una breve descripción de los apartados exigidos por la NTP ISO/IEC 27001:2014:

### a.1. Contexto de la organización

En este punto de la NTP-ISO/IEC 27001:2014 es importante conocer la organización y su contexto, de manera que la definición del sistema de gestión tenga en cuenta los propios objetivos del negocio de la organización con los que deberá alinearse la gestión de la seguridad de la información. Este conocimiento implica comprender los aspectos internos y externos de la organización, así como las necesidades y expectativas de las partes interesadas.

En este apartado también se considera la definición del alcance del SGSI, se trata de identificar aquellos procesos sobre los que el SGSI va a actuar, no siendo necesario aplicarlo sobre toda la actividad de la organización. Asimismo, a la hora de definir el alcance se deben tener en cuenta los recursos de los que se dispone, siendo generalmente más práctico limitarlo a aquellos procesos o servicios más importantes para la organización, y en posteriores ciclos de mejora continua, ir incorporando el resto (Gómez et al., 2015). Cabe mencionar que el alcance debe estar disponible como información documentada.

### a.2. Liderazgo

Para poner en marcha un SGSI es importante contar con el liderazgo y compromiso de la dirección, la norma contempla este epígrafe ya que el cambio de cultura que genera el proceso de implementación de un SGSI sería imposible de lograr sin la implicación constante de la dirección. Entre otras cosas, la dirección deberá demostrar su compromiso, aportando los recursos necesarios (tanto económicos como humanos), estableciendo la política y objetivos de seguridad de la información acorde a los objetivos estratégicos de la organización, comunicando la importancia de gestionar efectivamente la seguridad de la información, promoviendo la mejora continua, entre otras actividades (Gómez et al., 2015).

Dentro de este requisito también se contempla el establecimiento de roles, responsabilidades y autoridades organizacionales para asegurar que el SGSI esté conforme a los requisitos de la NTP ISO 27001:2014 y reportar sobre el desempeño del mismo a la alta dirección.

### a.3. Planificación

Teniendo en cuenta el contexto de la organización y las necesidades y expectativas de las partes interesadas, la organización debe establecer acciones para tratar los riesgos y oportunidades; para esto se debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información que:

- Determine los criterios de aceptación de riesgo y la metodología para llevar a cabo la evaluación del riesgo.

- Identifique los riesgos de seguridad de la información, asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información. La identificación de riesgos debe ser lo más exhaustiva posible para poder ser evaluado y tratado, además se debe de identificar también al propietario del riesgo, que deberá aprobar los niveles de riesgo y los planes de tratamiento.
- Analice los riesgos, valorando las consecuencias y probabilidades de materialización de los riesgos identificados en la fase anterior, obteniendo de este modo los niveles de riesgo.
- Evalúe los riesgos de seguridad de la información. Comparando los resultados obtenidos en la anterior fase con los criterios de aceptación de riesgos para determinar las medidas de tratamiento y su prioridad. (Gómez et al., 2015, pp. 21-22)

En este apartado también se debe elaborar un documento denominado Declaración de Aplicabilidad, que contenga los controles necesarios y la justificación de su implementación o exclusión en comparación a los controles definidos en el Anexo A de norma. Además, se debe formular un plan de tratamiento de riesgos de seguridad de la información, que debe ser aprobado por los propietarios del riesgo.

Otro punto a tener en cuenta es el establecimiento de los objetivos de seguridad de información, los cuales deben ser consistente con la política de seguridad de la información, ser medibles (si es práctico), ser comunicados y actualizados.

### a.4. Soporte

En este requisito la NTP-ISO/IEC 27001 la norma contempla:

- La gestión de recursos, para el establecimiento, implementación, mantenimiento y mejora del SGSI.
- La competencia, la organización debe determinar y asegurar la competencia necesaria de todo el personal implicado en el SGSI.
- La concientización de todo del personal de la organización y demás partes interesadas.
- La comunicación. Debe incluir: qué es lo que se debe comunicar, cuándo comunicar, a quién comunicar, quién debe comunicar y los procesos por los que debe efectuarse la comunicación.

- La información documentada. “Establece el proceso de documentar, mantener, controlar y conservar la documentación que corresponde al Sistema de Gestión de Seguridad de la Información” (ISOTools Excellence, 2015).

**a.5. Operación**

Establece todos los requisitos para medir el funcionamiento del sistema de gestión de seguridad de la información. Es así que:

Tras obtener la aprobación, por parte de la dirección, del plan de tratamiento de riesgos y de los procesos definidos en las fases anteriores, es el momento de ponerlos en práctica.

Esta aprobación implica la provisión de los recursos necesarios para llevarlos a cabo y que deberían haberse identificado en el plan de tratamiento de riesgos.

Debe hacerse un seguimiento de las acciones previstas, ajustando aquellos aspectos que se detecten como necesarios y actualizando en su caso los planes de tratamientos de riesgos, procedimientos, etc., siempre bajo la supervisión del responsable de seguridad (Gómez et al., 2015, pp. 27-28).

**a.6. Evaluación**

Este apartado contempla: el monitoreo, medición, análisis y evaluación, del desempeño de la seguridad de la información y la efectividad del SGSI.

La base para poder realizar la identificación y la medición de la eficiencia y el desempeño que realiza el Sistema de Gestión de Seguridad de la Información continúa siendo las auditorías internas y las revisiones del SGSI.

Se tiene que considerar el estado en el que se encuentran los planes de acción para poder atender las no conformidades como es debido, además se establece la necesidad de definir quién y cuándo realiza las

evaluaciones, además de quien tiene que analizar la información que se ha recolectado (ISOTools Excellence, 2015).

**a.7. Mejora**

"El principal elemento del proceso de mejora son las no conformidades identificadas, las cuales tiene que contabilizarse y compararse con las accione correctivas para asegurarse de que no se repitan y que las acciones correctoras que se realicen sean efectivas" (ISOTools Excellence, 2015). Es decir, la organización debe mejorar continuamente su SGSI.

### *2.2.11.2. Norma técnica peruana NTP ISO/IEC 17799:2007*

La norma NTP-ISO/IEC 17799:2007, fue una adaptación de la ISO 17799:2005 (actualmente la ISO 27002). La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico, dispone el uso obligatorio Norma Técnica Peruana NTP ISO/IEC 17799:2007 EDI, Tecnología de la Información.

La ISO 27002 se encuentra en la actualidad en su versión ISO/IEC 27002:2013 y para efectos de esta investigación se usarán los objetivos de control y controles de esta nueva versión, referenciados en el Anexo A de la NTP-ISO/IEC 27001:2014

**a. Objeto y campo de aplicación**

Esta norma contiene 14 capítulos (dominios) en los que se describen los controles de seguridad, es decir, áreas de la seguridad a considerar, con un total de 35 categorías de seguridad (objetivos de control) y con sus correspondientes objetivos y controles asociados a esos objetivos, más un capítulo sobre valoración y tratamiento de riesgos.

Los 14 capítulos (acompañados del número de categorías principales de seguridad incluidos dentro de cada capítulo) son los siguientes:

1. Políticas de seguridad (1)
2. Organización de la seguridad de la información (2)
3. Seguridad relativa a los recursos humanos (3)

4. Gestión de activos (3)
5. Control de acceso (4)
6. Criptografía (1)
7. Seguridad física y del entorno (2)
8. Seguridad de las operaciones (7)
9. Seguridad de las comunicaciones (2)
10. Adquisición, desarrollo y mantenimiento de sistemas de información (3)
11. Relación con proveedores (2)
12. Gestión de incidentes de seguridad de la información (1)
13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio (2)
14. Cumplimiento (2)

> La norma aporta una guía de buenas prácticas para la implantación de controles, pero en ningún caso suponen un requisito y mucho menos se debe considerar la necesidad de aplicar todas y cada una de sus recomendaciones. Es decir, no es necesario cumplir con los 114 controles que propone la norma, sino que se deben utilizar como base para comprobar que no hemos pasado ninguno por alto en nuestra selección. (Gómez et al., 2015, pp. 33-34)

Esta norma no es certificable.

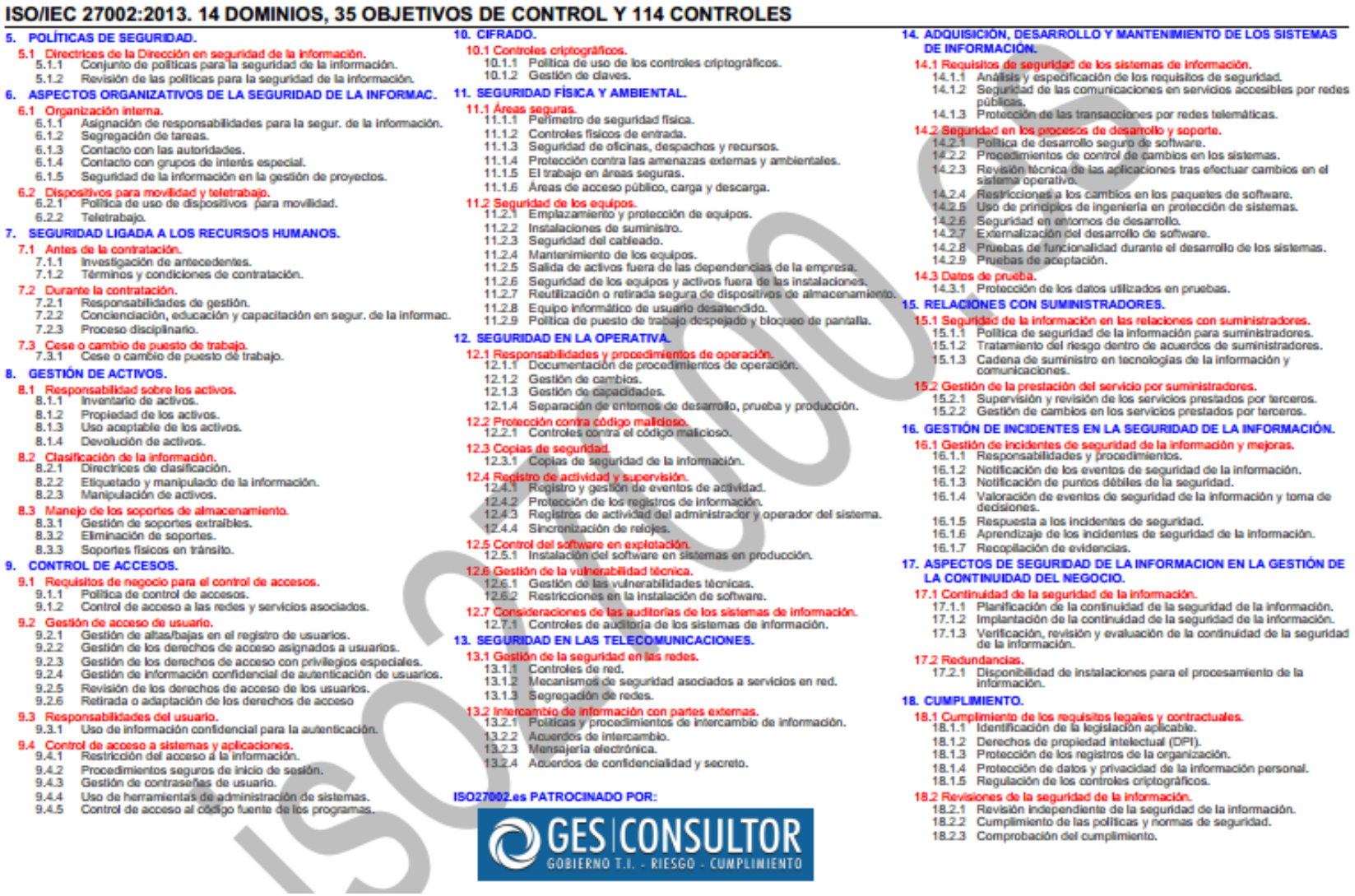


*Figura 2.2.* Controles ISO/IEC 27002:2013

Fuente: ISO 27000

### 2.2.12. Ciclo de mejora continua

La versión 2013 de la norma ISO 27001 no considera el ciclo PDCA (Plan-Do-Check-Act) como marco obligatorio para la gestión de la mejora continua del SGSI, pero en su apartado 10.2 la norma ISO 27001:2013 menciona que la organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información. Es decir, el ciclo PDCA está implícito en la propia estructura de la norma y es importante conocerla.

El modelo PDCA consta de un conjunto de fases, que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzado:

- **Plan**. En esta fase se planifica la implantación de SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos.
- **Do**. En esta fase se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe de disponerse de procedimientos en los que se identifique claramente quién debe hacer qué tareas, asegurando la capacitación necesaria para ello.
- **Check**. En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.
- **Act.** En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase (Gómez et al., 2015).

En la figura 2.3 se muestra la alineación del modelo PDCA en la ISO 27001:2013.

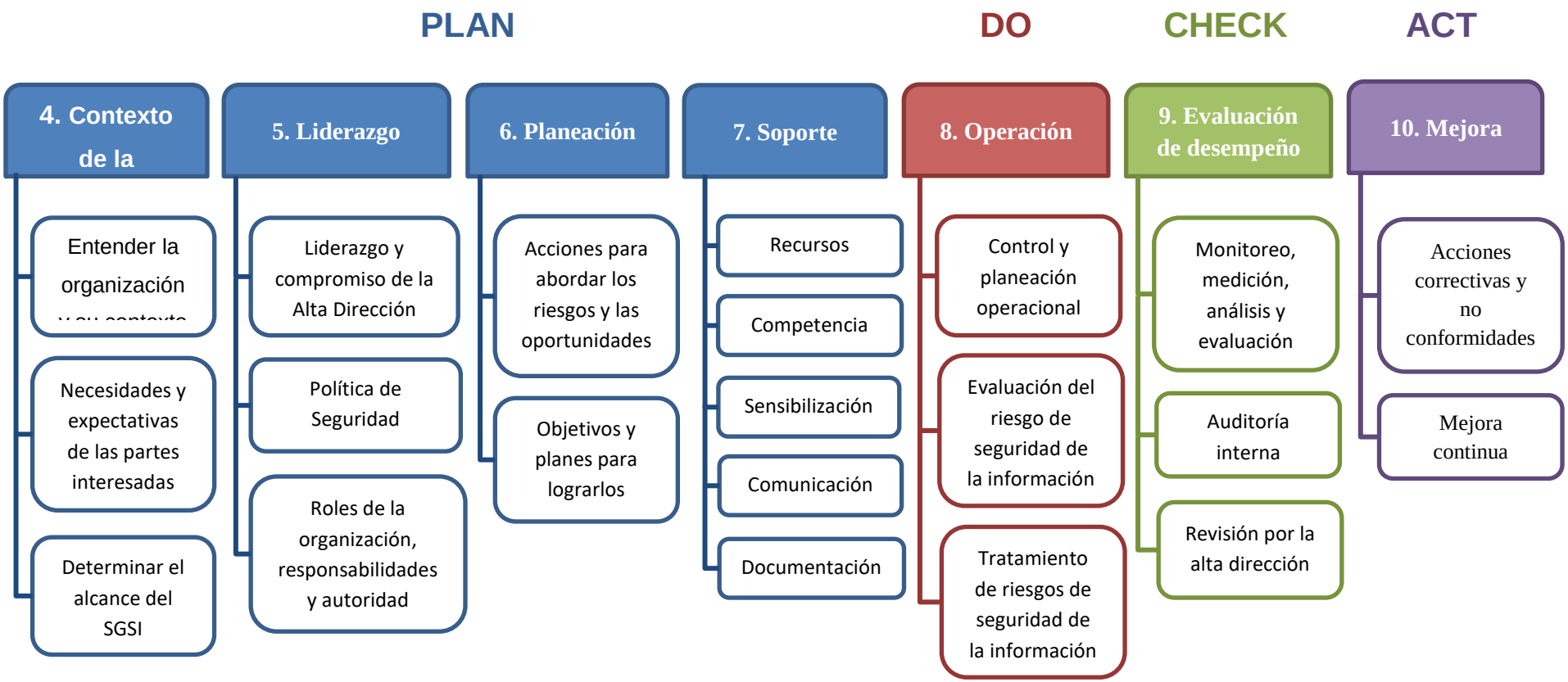


*Figura 2.3.* Ciclo PDCA en ISO/IEC 27001:2013

Fuente: ONGEI, taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013

### 2.2.13. Metodologías de análisis y gestión de riesgos de la información

Algunas de las metodologías mencionadas en la European Union Agency for Network and Information Security (ENISA) son las siguientes (European Union Agency for Network and Information Security, 2016a):

#### a. CRAMM (CCTA Risk Analysis and Management Method)

CRAMM es un método de análisis de riesgos desarrollado por la organización gubernamental británica CCTA (Central Communication and Telecommunication Agency), actual Oficina de Comercio Gubernamental (OGC). CRAMM se encuentra en su quinta versión. Está soportada por una herramienta que lleva su mismo nombre que ayuda en la recogida de datos, así como en el cálculo y procesamiento del informe de gestión del riesgo.

Las primeras versiones de CRAMM (método y herramienta) se basan en las mejores prácticas de las organizaciones del gobierno británico. En la actualidad CRAMM es el método de análisis de riesgo preferido del gobierno del Reino Unido. CRAMM es especialmente apropiado para grandes organizaciones, como organismos gubernamentales y la industria.

La compleja metodología CRAMM cubre todas las fases de la gestión de riesgos, desde el análisis real de los riesgos hasta la propuesta de medidas eficaces para mejorar la seguridad de la información. Permite la creación de documentos de seguridad y planes de contingencia.

#### b. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Fundada en 1995 por ANSSI y regularmente actualizada, el método EBIOS se beneficia de 20 años de experiencia en el campo de la gestión de riesgos. Permite evaluar y abordar los riesgos relacionados con la seguridad informática (SSI). También les permite comunicarse dentro de la organización y con sus socios, formando así una herramienta completa para la gestión de riesgos del SSI.

La ANSSI y EBIOS club desarrolló la versión 2010 del método EBIOS para tener en cuenta la retroalimentación y los cambios normativos y regulatorios.

Este enfoque más simple y claro, contiene ejemplos y consejos. Ofrece la posibilidad de elaborar y supervisar un plan de acción dentro de la seguridad informática.

Se acompaña de una base de conocimientos coherentes con las normas de seguridad estándar, enriquecido con ejemplos prácticos para el desarrollo de escenarios de riesgo relevantes para su organización.

Es modular y compatible con las normas internacionales ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 27001. (ANSSI, 2016)

EBIOS ofrece a los administradores de riesgo un enfoque coherente y de alto nivel. Esto les ayuda a adquirir una visión global y coherente, útil para apoyar la toma de decisiones por parte de los altos directivos en proyectos globales (plan de continuidad de negocio, plan maestro de seguridad, políticas de seguridad), así como en sistemas más específicos (por ejemplo: mensajería electrónica, redes nómadas o en los sitios web). EBIOS aclara el diálogo en temas de seguridad entre el propietario del proyecto y el director del proyecto. De esta manera, contribuye a la comunicación con las partes interesadas pertinentes y se extiende la conciencia en temas de seguridad.

EBIOS cuenta con cinco etapas, que son:

1. Estudio circunstancial - determinar el contexto
2. Requerimientos de seguridad
3. Estudio de riesgo
4. Identificación de los objetivos de seguridad, y
5. Determinación de los requisitos de seguridad (European Union Agency for Network and Information Security, 2016b).

**c. ISAMM**

ISAMM o “Information Security Assessment & Monitoring Method” es un método de apoyo a la gestión de riesgos de un SGSI, con soporte de herramientas. Basado en Telendius ha sido diseñado y continuamente mejorado, cuenta con más de 20 años de experiencia con miles de proyectos de seguridad de la información - y de gestión de riesgos - y decenas de otros métodos y herramientas de gestión de riesgos. Es una metodología de gestión de riesgos de tipo cuantitativo, donde se

expresan los riesgos evaluados a través de su expectativa de pérdida anual (ALE - Annual Loss Expectancy), en unidades monetarias. La pérdida anual esperada o coste anual ALE debe de materializarse en una amenaza o un grupo de amenazas.

Expectativa de pérdida anual (ALE) = [probabilidad] x [impacto promedio]

Esto forma la base para el retorno de la inversión (ROI) y el enfoque basado en las capacidades de justificación económica de ISAMM con respecto al plan de tratamiento de riesgos.

La eficiencia de ISAMM permite la realización de la evaluación de riesgos con un tiempo y esfuerzo mínimo. Con el fin de lograr esto, la mayor parte de nuestra experiencia de seguridad de la información se ha incorporado y puesto a disposición para su reutilización inmediata en cada evaluación. Telindus también ha reducido al mínimo los pasos necesarios para la evaluación mediante el uso de muchos enlaces directos a los controles de la norma ISO/IEC 27002. También se considera el máximo apoyo de la norma ISO/IEC 27001 SGSI como un requisito clave para ISAMM durante su diseño y desarrollo.

La última evolución de la metodología ISAMM introduce un enfoque basado en activos, esto significa que puede ser utilizado para ejecutar las evaluaciones de riesgo en un activo o un conjunto de activos.

Una evaluación de riesgos ISAMM contiene 3 partes principales: el alcance; evaluación (amenazas y el cumplimiento) y el resultado (el cálculo y la presentación de informes) (European Union Agency for Network and Information Security, 2016c).

### d. MARGERIT V.3

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno (Portal de Administración Electrónica, 2016).

> Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (…) Magerit persigue los siguientes objetivos:
>
> Directos:
>
> 1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
> 2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
> 3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control
>
> Indirectos:
>
> 4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. (MARGERIT, 2012, pp. 7–8)

MARGERIT divide la gestión de riesgos en dos subprocesos, estos son:

1. **Análisis de Riesgos:**

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto por probabilidad

La Figura 2.4 recoge los elementos del análisis de riesgos contemplados en MARGERIT.

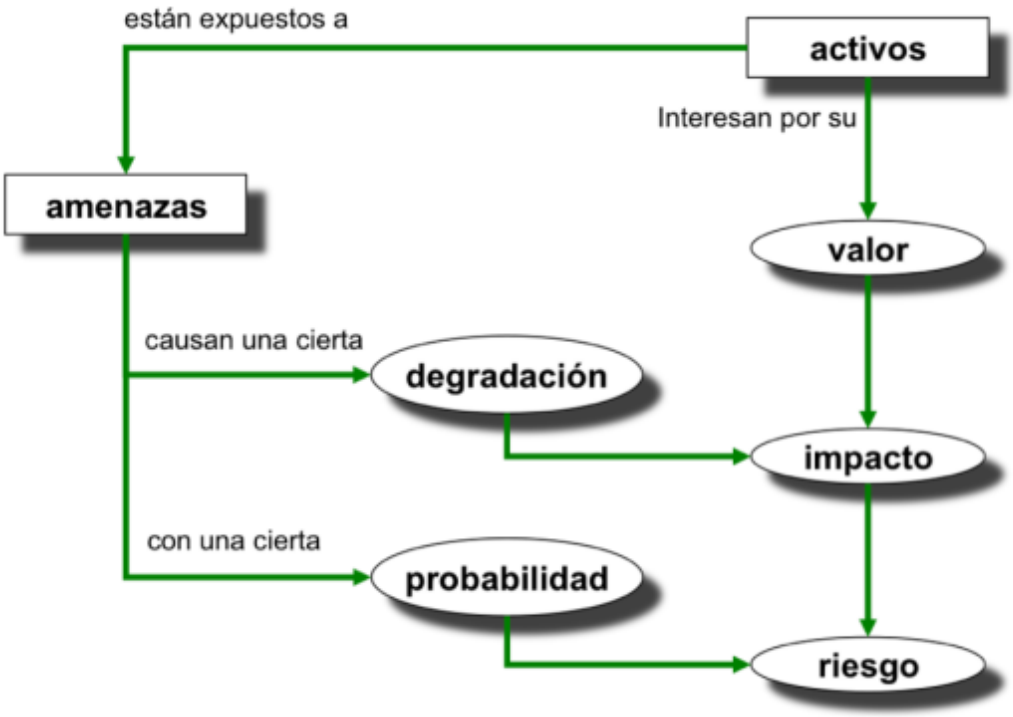


Figura 2.4: Elementos del análisis de riesgos potenciales

Fuente: MARGERIT V.3 – Libro I, p.22

En la Figura 2.5 se muestran las tareas propuestas por MARGERIT para llevar a cabo el análisis de los riesgos.

| MAR – Método de Análisis de Riesgos |
|---|
| MAR.1 – Caracterización de los activos |
| MAR.11 – Identificación de los activos |
| MAR.12 – Dependencias entre activos |
| MAR.13 – Valoración de los activos |
| MAR.2 – Caracterización de las amenazas |
| MAR.21 – Identificación de las amenazas |
| MAR.22 – Valoración de las amenazas |
| MAR.3 – Caracterización de las salvaguardas |
| MAR.31 – Identificación de las salvaguardas pertinentes |
| MAR.32 – Valoración de las salvaguardas |
| MAR.4 – Estimación del estado de riesgo |
| MAR.41 – Estimación del impacto |
| MAR.42 – Estimación del riesgo |

Figura 2.5: Tareas para llevar a cabo el análisis de riesgos

Fuente: MARGERIT V.3 – Libro I, p.36

**2. Tratamiento de riesgos:**

El tratamiento de riesgos permite organizar una defensa concienzuda y prudente, de esta manera la organización puede sobrevivir a los incidentes de seguridad y seguir operando en las mejores condiciones. Pero como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección asume.

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

De esta manera MAGERIT busca no solo concientizar a los responsables del gobierno de TI de la existencia de riesgos, sino que ayuda a descubrir y planificar un tratamiento oportuno para mantener a estos riesgos bajo control (MARGERIT, 2012).

**e. OCTAVE**

OCTAVE es una metodología originaria de la Carnagie Mellon University, Su objetivo es ayudar a que una organización:

1. Desarrolle criterios cualitativos de evaluación de riesgos que describen las tolerancias de riesgo operacional de la organización
2. Identifique los activos que son importantes para la misión de la organización

3. Identifique las vulnerabilidades y las amenazas a los que están expuestos los activos
4. Determine y evalúe las consecuencias potenciales para la organización si se realizan o materializan las amenazas

Desde que se creó en 1999 ha sufrido varios cambios. OCTAVE Allegro es la versión más reciente de OCTAVE y que cuenta con un apoyo activo. Este método se basa en dos versiones más antiguas llamadas OCTAVE original y OCTAVE-S.

OCTAVE Allegro se centra en los activos de información. Los elementos importantes de una organización se identifican y evalúan en función de los activos de información al que están asociados. Este proceso elimina la posible confusión sobre el alcance y reduce la posibilidad de que la recopilación de datos y el análisis de los mismos se lleven a cabo para activos que están mal definidos, fuera del alcance de la evaluación, o que necesitan una mayor descomposición.

OCTAVE Allegro consta de ocho pasos organizados en cuatro fases:

1. Desarrollar criterios de medición de riesgo consistentes con la misión de la organización, los objetivos estratégicos, y los factores críticos de éxito.
2. Crear un perfil que establece límites claros para cada activo de información, identifica sus requisitos de seguridad, e identifica todos sus contenedores.
3. Identificar las amenazas para cada activo de información en el contexto de sus contenedores.
4. Identificar y analizar los riesgos para los activos de información y empezar a desarrollar estrategias de mitigación (Carnegie Mellon University, 2007).

# Capitulo III
# Metodología de la investigación

La metodología adoptada en esta investigación tiene en cuenta el marco de referencia de la NTP ISO/IEC 27001:2014 que especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.

## 3.1. Tipo de investigación

Para McMillan y Schumacher (2005) “La investigación aplicada se centra en un campo de práctica habitual y se preocupa por el desarrollo y la aplicación del conocimiento obtenido en la investigación sobre dicha práctica” (p. 23).

Para Carrasco (2009) La investigación aplicada “se distingue por tener propósitos prácticos inmediatos, bien definidos, es decir se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad” (p. 43).

Por lo antes mencionado, esta investigación es aplicada, porque tiene como propósito diseñar un SGSI dentro de la Municipalidad Provincial de Huamanga, tomando como base los riesgos de seguridad a los que se enfrenta, contribuyendo, con una solución innovadora, a la mejora de la seguridad de la información dentro de dicha institución.

## 3.2. Nivel de la investigación

Para Bernal (2010) las investigaciones descriptivas “muestran, narran, reseñan o identifican hechos, situaciones, rasgos, características de un objeto de estudio o se diseñan productos, modelos, prototipos, guías, etcétera. Pero no se dan explicaciones o razones del porqué de las situaciones, los hechos, los fenómenos, etcétera” (p.113). De acuerdo a este concepto, el nivel de la presente investigación es descriptiva, porque busca identificar y describir las características fundamentales del diseño de un SGSI (teniendo como guía la NTP ISO/IEC 27001) para la Municipalidad Provincial de Huamanga.

## 3.3. Diseño de la investigación

La investigación no experimental se define como la investigación que se realiza sin manipular deliberadamente las variables, es decir no se genera ninguna situación, mas bien lo que se hace es observar situaciones ya existentes y analizarlos.

La investigación no experimental se clasifica en transeccionales y longitudinales. La investigación transeccional (que a su vez se divide en exploratorios, descriptivo y correlacionales–causales) tiene como propósito describir variables y analizar su incidencia e interrelación en un momento dado, mientras que la investigación longitudinal, recolecta datos en diferentes momentos o periodos para hacer inferencias respecto al cambio, sus determinantes y consecuencias (Hernández et al., 2010).

Debido a estas acepciones, el diseño de esta investigación es no experimental – transeccional descriptivo.

## 3.4. Población y muestra

### 3.4.1. Población

La población estuvo conformada por los trabajadores de la Municipalidad Provincial de Huamanga.

### 3.4.2. Muestra

Se tomó un muestreo no probabilístico, con juicio de experto y criterio de saturación, la cual estuvo conformado por los seis trabajadores de la Subgerencia de Sistemas y Tecnología.

## 3.5. Variables e indicadores

### 3.5.1. Definición conceptual de la variable

**X. Diseño de un sistema de gestión de seguridad de la información**

Es un conjunto de procesos que permiten establecer la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

**Indicadores**

**X1. Alcance. -** Es el ámbito de la organización que queda sometido al SGSI (ISO 27000, s.f. b)

**X2. Análisis de Riesgo. -** Es el proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo (ISO 27000, s.f. b)

**X3. Controles de seguridad. -** Son las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. El control es también sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (ISO 27000, s.f. b)

### 3.5.2. Definición operacional de la variable

Según Carrasco Díaz (2006) la operacionalización de las variables es un proceso metodológico que consiste en descomponer o desagregar deductivamente las variables que componen el problema de investigación, partiendo desde lo general a lo específico; es decir, las variables se dividen (si son complejas) en dimensiones, áreas, aspectos, indicadores, índices, subíndices e ítems; pero si son concretas solamente en indicadores, índices e ítems. Asimismo, establece tres criterios metodológicos para realizar la descomposición de las variables: descomposición atendiendo a sus componentes o elementos, descomposición atendiendo a sus roles o funciones y descomposición atendiendo a sus cualidades o características.

En este trabajo de investigación se utiliza, para la definición operacional de la variable de investigación, el criterio de descomposición atendiendo a sus componentes o elementos, debido a que la variable diseño de un sistema de gestión de la seguridad de la información va a ser estudiada en atención a los elementos que la conforman (Ver Tabla 3.1).

## 3.6. Técnicas e instrumentos

Las técnicas e instrumentos utilizados en esta investigación se muestran en la Tabla 3.2.

**Tabla 3.1**

*Operacionalización de la variable diseño de un SGSI*

| VARIABLE | INDICADORES | INDICES | ITEMS |
|---|---|---|---|
| **X. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** | 1. Alcance | 1.1. Aspectos externos e internos relevantes para el SGSI<br>1.2. Requisitos de las partes interesadas relevantes al SGSI | 1. ¿Por qué implementas el SGSI?<br>2. ¿A quiénes le interesa que se implemente el SGSI?<br>3. ¿Qué área o proceso debe ser cubierta por el SGSI? |
| | 2. Análisis de Riesgo | 2.1. Inventario de activos<br>2.2. Identificar los riesgos<br>2.3. Probabilidad e impacto del riesgo<br>2.4. Propietarios del riesgo | 1. ¿Qué activos son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?<br>2. ¿Qué activos de tipo dato/información son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?<br>3. ¿Qué activos de tipo servicio son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?<br>4. ¿Qué activos de tipo software son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?<br>5. ¿Qué activos de tipo hardware son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?<br>6. ¿Qué medios de transporte utiliza la dependencia para transmitir información?<br>7. ¿Qué dispositivos físicos utiliza la dependencia para almacenar información de forma permanente o por largos periodo de tiempo?<br>8. ¿Qué activos sirven de soporte a los sistemas de información?<br>9. ¿En qué lugares se hospedan los SI y comunicaciones?<br>10. ¿Qué actores interactúan con los SI?<br>11. ¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras causando pérdida económica? |

| VARIABLE | INDICADORES | INDICES | ITEMES |
|---|---|---|---|
| | | | 12. ¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control?<br>13. ¿Su divulgación no autorizada puede afectar la imagen de la entidad?<br>14. ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?<br>15. ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?<br>16. ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?<br>17. ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?<br>18. ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control?<br>19. ¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad?<br>20. ¿A qué amenazas están expuestos los activos?<br>21. ¿Cuán perjudicado resultaría el activo?<br>22. ¿Cuál es la probabilidad de que se materialice la amenaza?<br>23. ¿Qué daño causaría sobre el activo la materialización de la amenaza?<br>24. ¿Cuál es nivel de riesgos al que se encuentra expuesto el activo? |
| | 3. Controles de seguridad | 3.1. Criterios de aceptación de riesgos<br>3.2. Políticas de seguridad<br>3.3. Roles y responsabilidades | 1. ¿Qué nivel de riesgo acepta la MPH?<br>2. ¿Qué opciones de tratamiento de riesgos se va a seleccionar?<br>3. ¿Qué medidas de seguridad se van a implantar? |

Nota: Elaboración propia

**Tabla 3. 2**

*Técnicas e instrumentos para la recolección de información*

| Técnica | Instrumento | Instrumento de registro | Detalle |
|---|---|---|---|
| Análisis documental | – Fichas bibliográficas<br>– Referencia | Formato de citas y referencia bibliográfica de esta investigación. | Se utilizó esta técnica para analizar material impreso y digital sobre el tema de investigación. Se usó diferentes fuentes de información, tales como:<br>– tesis, libros, normas de seguridad, documentos de talleres de seguridad de la información, artículos de congresos.<br>– documentación de gestión y del estado de la seguridad de la información en la Municipalidad provincial de huamanga (ROF, MOF, PDI, POI y resultado de auditorías) |
| Observación | Escala de Likert (Ver Tabla 4. 1) | Formato: Anexo A | Ésta técnica fue muy importante porque permitió obtener información sobre el estado inicial de la MPH con respecto a la NTP ISO/IEC 27001:2014 |
| Entrevista | Guía de entrevista (Cuestionarios estructurados y semiestructurados) | Formato: Anexo H | Se realizaron entrevistas a funcionarios y a los trabajadores de la Subgerencia de Sistemas y tecnologías de la MPH, para conocer su opinión sobre el SGSI a diseñar, el impacto que esta investigación tendría dentro del área, la identificación de amenazas y la probabilidad de que estas se materialicen. |
| Encuesta | – Cuestionario autoadministrado<br>– Cuestionario autoadministrado grupal | Formato:<br>Anexo B, E, F.<br>(Tabla 4.7, Tabla 4.9, Tabla 4.14) | Se utilizó esta técnica e instrumento para recabar información sobre el estado de la seguridad de información y la posibilidad de aceptación del SGSI, para identificar y valorar los activos de información Subgerencia de Sistemas y Tecnología. Degradación de los activos de información |
| Internet | Tecnologías de información y comunicaciones (email) | Referencia bibliográfica de esta investigación | El internet es uno de los medios principales, utilizados hoy en día, para recabar información. Se utilizó está técnica para búsqueda de libros y consulta a expertos. |

Nota: Elaboración propia

## 3.7. Herramientas para el tratamiento de datos

Las herramientas que se emplearon para el análisis y tratamiento de los datos, son las siguientes:

**Tabla 3. 3**

*Herramientas para el tratamiento de datos*

| Herramienta | Creador | Descripción |
|---|---|---|
| Microsoft Excel | Microsoft | Herramienta que organiza los datos, numéricos o de texto, en hojas o libros de cálculo. Permite realizar análisis sobre los datos y tomar decisiones. |
| PEST | Liam Fahey y V. K. Narayanan | PEST (iniciales de factores Políticos - legales, Económicos, Socio-culturales y Tecnológicos) analiza los factores externos que pueden afectar el desempeño de cualquier empresa.<br><br>Para efectos de esta investigación se utiliza esta herramienta para analizar los factores externos que pueden afectar a la MPH en el establecimiento e implementación del SGSI. |
| Matriz DAFO | Stanford Research Institute- Albert Humphrey | La matriz DAFO muestra el conjunto de factores DAFO: Debilidades, Amenazas, Oportunidades y Fortalezas. |

Nota: Elaboración propia

## 3.8. Fases del proyecto de investigación

Con el fin de alcanzar los objetivos propuestos en este proyecto de investigación, se establecieron las siguientes fases y actividades:

1. Fase I. Diagnóstico de SGSI
   a. Evaluación el estado inicial de la MPH con respecto a los requisitos de la NTP-ISO/IEC 27001:2014.

b. Estudio de la posibilidad de aceptación de un SGSI y el diagnóstico del estado inicial de la seguridad de información.

2. Fase II. Preparación del SGSI:
   a. Análisis del contexto (externo e interno) de la MPH e identificación de las partes interesadas afectadas por el SGSI.
   b. Definición del alcance del SGSI.
   c. Elaboración de la política y objetivos de seguridad.
   d. Identificación de los requisitos legales
   e. Comité de seguridad
3. Fase III. Planificación del SGSI:
   a. Evaluación de riesgos. Para efectos de esta investigación se adoptó MARGERIT V.3 como metodología de análisis y gestión de riesgos. Las tareas realizadas fueron las siguientes:
      - Se identificaron los activos que dan soporte a los procesos del negocio delimitados en el alcance, de este modo se elaboró un inventario de activos.
      - Se cuantificó el valor de los activos en términos de confidencialidad, integridad y disponibilidad.
      - Se identificaron y valoraron las amenazas
      - Se calculó el impacto de materialización de las amenazas identificadas.
      - Se calculó el riesgo para cada activo.
   b. Identificación de los propietarios del riesgo
   c. Tratamiento de los riesgos
   d. Selección de controles y declaración de aplicabilidad.

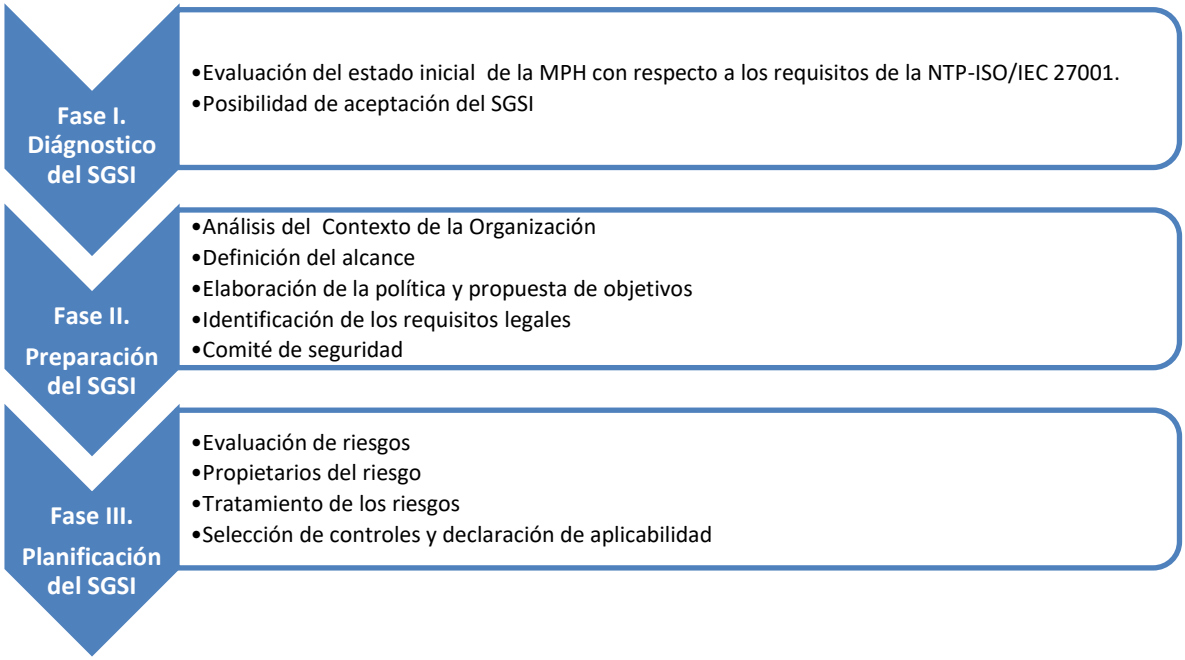


*Figura 3. 1*. Fases para el diseño del SGSI

Fuente: Adaptado de "*Cómo implementar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*", p. 48, Gómez et al. 2015.

La estructura de presentación del Capítulo IV (análisis y resultados de la investigación), de este documento, sigue la estructura propuesta en este ítem.

# Capitulo IV

# Análisis y resultados de la investigación

Este capítulo corresponde a las fases que se definieron en el apartado 3.8 de este documento.

## 4.1 Fase I: Diagnóstico del SGSI

En esta fase se presentan las actividades que se realizaron para conocer la situación de la MPH, frente a la seguridad de la información y el diseño del SGSI.

### 4.1.1 Evaluación del estado inicial de la MPH con respecto a los requisitos de la NTP-ISO/IEC 27001:2014

Para evaluar el estado inicial de la MPH, con respecto a los requisitos de la NTP –ISO/IEC 27001:2014, se ha definido dos maneras de presentar los resultados: una descriptiva y otra cuantificable (Ver Tabla 4.1). Esta técnica se basa en calificar el estado de los requerimientos en función a una escala de Likert aplicando cinco opciones que van de menor a mayor.

**Tabla 4. 1**

*Criterio para evaluar el estado inicial de la MPH con respecto a los requisitos de la NTP ISO/IEC 27001:2014*

| Criterio de Calificación | Valoración |
|---|---|
| **No diseñado:** Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación. | 0% |
| **Parcialmente diseñado:** Las actividades/métodos demuestran que se tiene el requisito definido, pero este no es del todo conforme con el requisito de la NTP ISO/IEC 27001:2014. | 25% |
| **Diseñado:** Los métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, pero sin evidencias de aplicación**.** | 50% |
| **Parcialmente implementado:** Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, pero con pocas evidencias de aplicación. | 75% |
| **Completamente implementado:** Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, y se cuenta con evidencias de aplicación permanentes. | 100% |

Nota: Adaptado de “Propuesta para la implementación del sistema de gestión de calidad basado en la norma ISO 9001:2008 en una empresa del sector construcción” (Tesis), p. 37, Medina Bocanegra. 2013.

Se elaboró la línea base con los capítulos y requerimientos de la norma y se realizó la evaluación de la siguiente manera:

- Se puntuó cada requisito.
- De acuerdo al puntaje obtenido se colocó la evidencia/sugerencia para el cumplimiento de la NTP ISO/IEC 27001:2014.
- Para el porcentaje por capítulo, se sacó el promedio de los requisitos por capítulo.

El resultado que se obtuvo de la evaluación del estado inicial de la MPH respecto a los requisitos de la NTP ISO/IEC 27001:2014 se muestra en forma de tabla. Un extracto de esta evaluación se muestra a continuación (la tabla completa se encuentra en el ANEXO A de este documento):

**Tabla 4. 2**

*Estado inicial de la MPH respecto a la NTP ISO/IEC 27001:2014*

| SECCIÓN | REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? /¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **4** | **CONTEXTO DE LA ORGANIZACIÓN** | **No Diseñado** | **Se sugiere realizar el análisis del contexto de la MPH, para comprender, tanto los aspectos externos como internos, las partes interesadas y requisitos relevantes al SGSI y, elaborara y documentar el alcance del SGSI.** | **6%** |
| **4.1** | **Comprender la Organización y contexto**.<br><br>La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI | Parcialmente diseñado | La MPH posee documentos visibles de su Misión, Visión, Matriz FODA y las Estrategias. Pero no contempla de manera clara ítems de seguridad de la información.<br>Se sugiere establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos. | 25% |
| **4.2** | **Comprender las necesidades y expectativas de las partes interesadas.**<br><br>La organización **debe** determinar las partes interesadas y los requisitos de las mismas. | No Diseñado | **Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información. | 0% |

*Tabla 4.2 Continuación*

| SECCIÓN | REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **4.3** | **Determinar el alcance del SGSI.** | No Diseñado | **Sugerencia.** Determinar el alcance del SGSI teniendo en consideración los aspectos referidos en 4.1, los requisitos de 4.2, documentarlo y ponerlo a disposición de las partes interesadas. | 0% |
| **4.4** | **Sistema de Gestión de Seguridad de la información.**<br><br>La organización **debe** establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta Norma Técnica Peruana | No diseñado | **Sugerencia.** Establecer una plan para la mejora continua del SGSI conforme a la NTP Vigente | 0% |
| **5** | **LIDERAZGO** | **No Diseñado** | **El Titular de la Entidad, debe mostrar liderazgo y compromiso respecto al SGSI. Entonces, debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. Por lo tanto, es necesario establecer: Una Política de Seguridad de la Información, y los Objetivos de Seguridad de la Información acorde al propósito de la organización.** | 1% |
| **5.1** | **Liderazgo y compromiso.**<br><br>La alta dirección **debe** demostrar liderazgo y compromiso respecto al SGSI. | No Diseñado | El titular de la entidad debe mostrar liderazgo y compromiso | 3% |
| **5.2** | **Política.** | No Diseñado | Establecer la Política de Seguridad de la Información acorde al propósito de la MPH, incluir los objetivos de seguridad de la Información (Sección 6.2), mantenerla disponible y comunicada a toda la organización. | 0% |
| **5.3** | **Roles, responsabilidades y autoridades organizacionales.** | No Diseñado | La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. | 0% |
| ⋮ | | | | |
| **PUNTAJE TOTAL DE LA EVALUACIÒN DE REQUISITOS DE LA NTP ISO/IEC 27001:2014** | | | | **5%** |

Nota: Elaboración propia

#### *4.1.1.1. Resultado de la evaluación del estado inicial de la MPH con respecto a los requisitos de la NTP-ISO/IEC 27001:2014*

Según la evaluación realizada, de un total de 100% de los requisitos de la NTP ISO/IEC 27001:2014 que se deben cumplir, la MPH obtuvo un puntaje total de 5%, por lo que se puede determinar que la MPH se encuentra en una etapa básica de cumplimiento de la norma (no diseñado).

El resultado anterior muestra también que la seguridad de la Información dentro de la institución no es gestionada y, que el diseño e implementación del SGSI implicará un mayor esfuerzo, y dependerá del compromiso y disponibilidad del personal de la MPH.

### 4.1.2 Posibilidad de aceptación del SGSI y diagnóstico inicial de la seguridad de la información

La recolección de datos se realizó mediante la encuesta mostrada en el Anexo B de esta investigación. La encuesta consistió en veintiún (21) preguntas dicotómicas para medir actitudes, opiniones y el estado básico de seguridad de información dentro de la Subgerencia de Sistemas y Tecnología. Esto con el fin de corroborar el estado de la seguridad de la información y la posibilidad de aceptación del diseño del SGSI.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los seis trabajadores de la Subgerencia de Sistemas y Tecnología.

Para la pregunta, ¿Sabe Ud. si dentro de la Municipalidad Provincial de Huamanga existe un sistema de gestión de la seguridad de la información? La frecuencia de respuesta fue la siguiente:

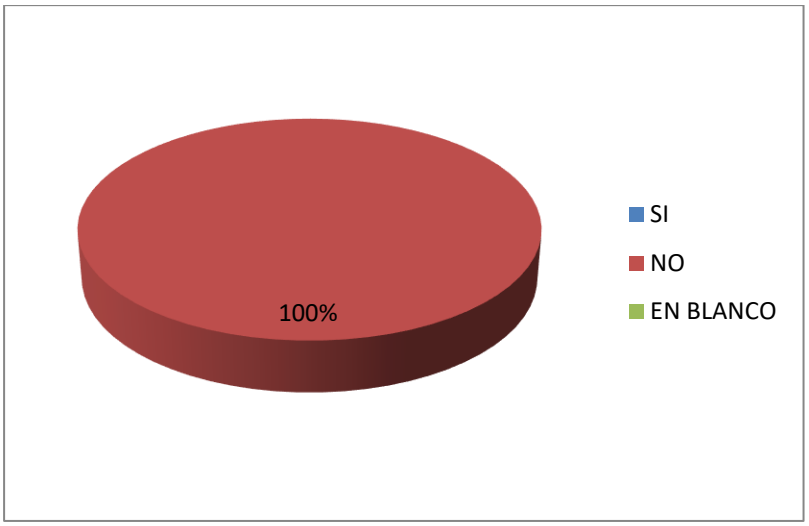


*Figura4. 1.* Frecuencia de respuesta para la pregunta, ¿en la MPH existe un sistema de gestión de la seguridad de la información?

Elaboración propia

**Interpretación**

Del gráfico anterior, se observa que, de los seis trabajadores encuestados, el 100% afirma que no existe un SGSI dentro de la Subgerencia de Sistemas y Tecnología.

**Conclusión:**

La Subgerencia de Sistemas y Tecnología (área responsable de la seguridad de la información dentro de la MPH), requiere con urgencia el diseño e implementación de un SGSI, para levantar las no conformidades, producto de la auditoría presupuestal y financiera practicada a la MPH. Por lo mencionado anteriormente la presente investigación es importante para la Subgerencia de Sistemas y Tecnología.

Para la pregunta, ¿Cree usted que el diseño de un sistema de gestión de la seguridad de la información permitirá mejorar la seguridad de información de su área de trabajo? La frecuencia de respuesta fue la siguiente:

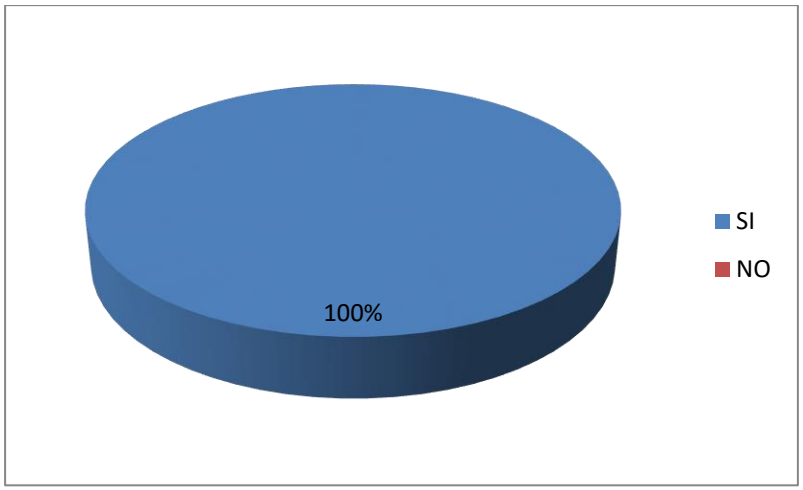


*Figura4. 2.* Frecuencia de respuesta para la pregunta, ¿Cree usted que el diseño de un sistema de gestión de la seguridad de la información permitirá mejorar la seguridad de información de su área de trabajo?

Elaboración propia

**Interpretación:**

En la Figura 4.2, se puede observar que el 100% de los encuestados (seis) están de acuerdo en que el diseño de un SGSI mejorará la seguridad de información de la subgerencia de sistemas y tecnología.

**Conclusión:**

Se puede concluir que todos los trabajadores de la Subgerencia de Sistemas y Tecnología son conscientes del beneficio que traerá el diseño de un sistema de gestión de seguridad de la información.

En la Figura 4.3, se observa la frecuencia de respuesta para la pregunta ¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de este sistema de gestión de la seguridad de la información?

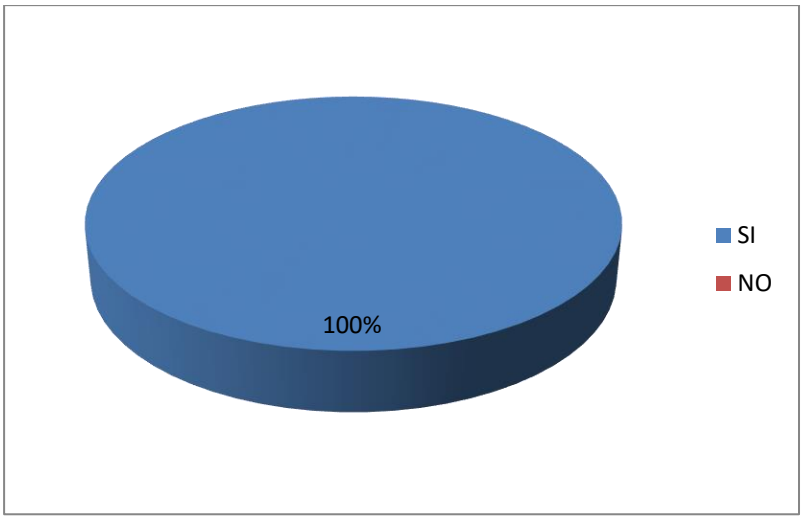


*Figura4. 3.* Frecuencia de respuesta para la pregunta, ¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de este sistema de gestión de la seguridad de la información?

Elaboración propia

**Interpretación:**

Del gráfico anterior, el 100% de los encuestados (seis) cree que con la aplicación de un SGSI se lograrán cambios positivos en la seguridad de la información.

**Conclusión**

Se puede concluir que todos los trabajadores de la Subgerencia de Sistemas y Tecnología son conscientes del beneficio que traerá la implementación del sistema de gestión de seguridad de la información (mejorar y ampliar la calidad tecnológica y de los servicios que prestan).

Para la pregunta, ¿Aprobaría usted la implementación del sistema de gestión de la seguridad de la información en su área de trabajo? La frecuencia de respuesta fue la siguiente:

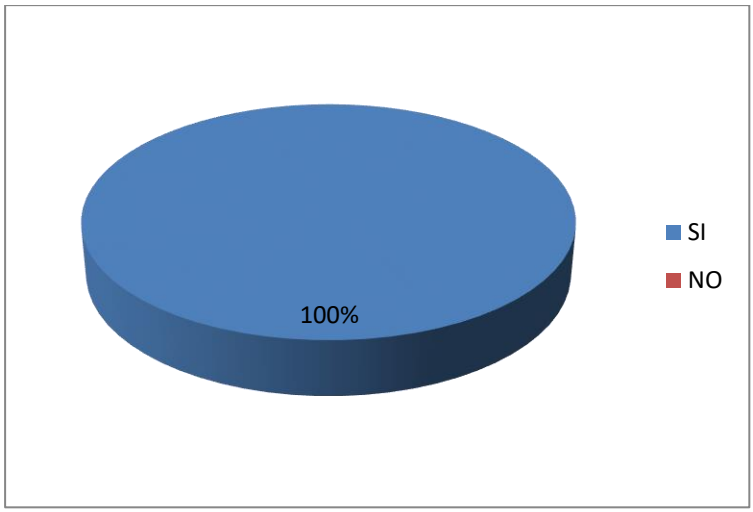


*Figura4. 4.* Frecuencia de respuesta para la pregunta, ¿Aprobaría usted la implementación del sistema de gestión de la seguridad de la información en su área de trabajo?

Elaboración propia

**Interpretación:**

Según la Figura 4.4, el 100% de los encuestados (seis) están dispuestos a aprobar la implementación de un SGSI del SGSI.

Para la pregunta, ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la seguridad de la Información en su área de trabajo? La frecuencia de respuesta fue la siguiente:

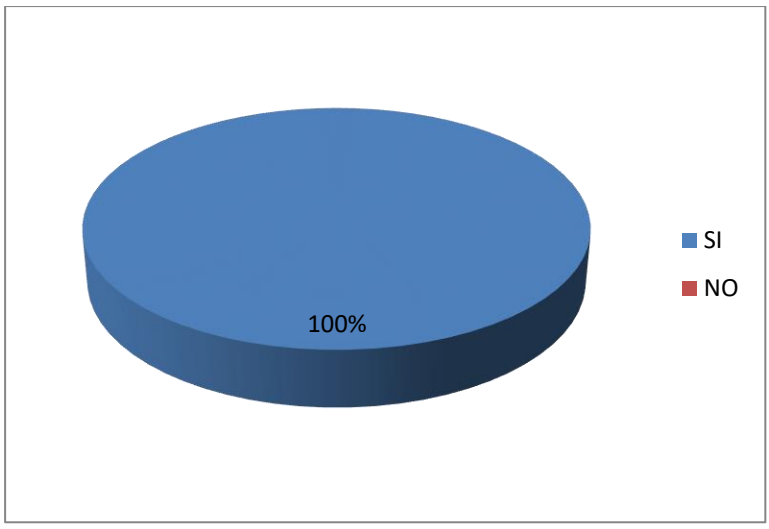


*Figura4. 5.* Frecuencia de respuesta para la pregunta ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la seguridad de la Información en su área de trabajo?

Elaboración propia

**Interpretación:**

Según la Figura 4.5, el 100% de los encuestados (seis) están dispuestos a aprobar programas de sensibilización sobre seguridad de la información en la Subgerencia de sistemas y Tecnología.

Para la pregunta, ¿Estaría usted dispuesto a colaborar para que el diseño e implementación del sistema de gestión de la seguridad de la información se lleve a cabo de su área de trabajo? La frecuencia de respuesta fue la siguiente:

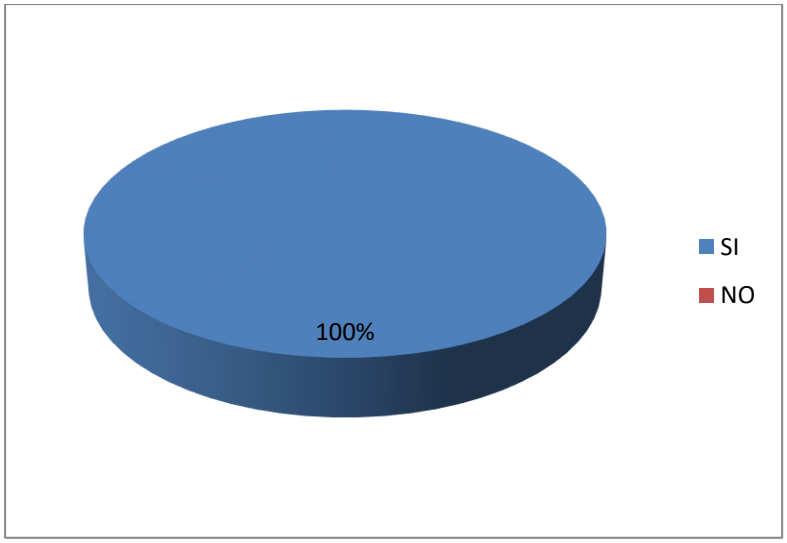


*Figura4. 6.* Frecuencia de respuesta para la pregunta, ¿Estaría usted dispuesto a colaborar para que el diseño e implementación del sistema de gestión de la seguridad de la información se lleve a cabo de su área de trabajo?

Elaboración propia

**Interpretación:**

Según la Figura 4.6, el 100% de los encuestados (seis) están dispuestos a colaborar con el éxito del SGSI.

**Conclusión:**

La aprobación y colaboración del total de los trabajadores (seis) de la Subgerencia de Sistemas y Tecnología, es un factor crítico de éxito importante para la implementación del SGSI, porque reduce los esfuerzos a la hora de implementar el SGSI dentro de la subgerencia, asimismo facilita el desarrollo de programas de capacitación y concientización.

Para la pregunta, ¿Considera Ud. que en su área de trabajo existe información que debe ser protegida? La frecuencia de respuesta fue la siguiente:

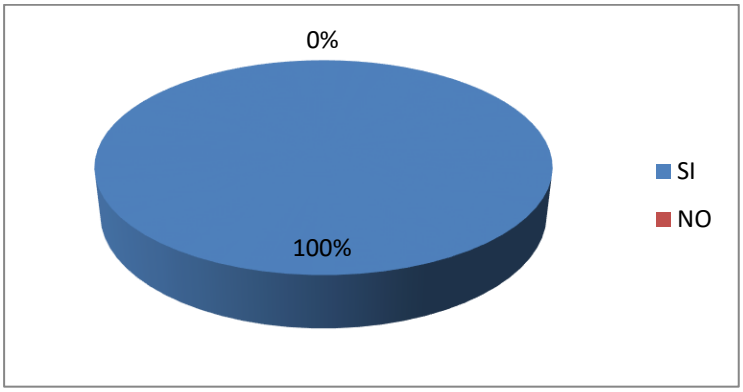


*Figura4. 7.* Frecuencia de respuesta para la pregunta, ¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?

Elaboración propia

**Interpretación:**

De la Figura 4.7, el 100% de los encuestados (seis) considera que dentro de la Subgerencia de Sistemas y Tecnología existe información que debe ser protegida.

**Conclusión:**

Que los trabajadores sean conscientes de la existencia de información que debe ser protegida es importante para el diseño del SGSI.

Para la pregunta, ¿En su área de trabajo se ha categorizado la información de acuerdo al grado de importancia que tienen para la Municipalidad Provincial de Huamanga? La frecuencia de respuesta fue la siguiente:

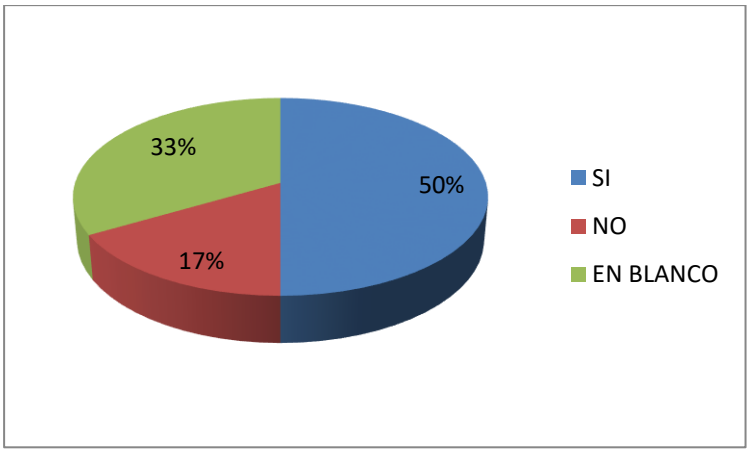


*Figura4. 8.* Frecuencia de respuesta para la pregunta, ¿En su área de trabajo se ha categorizado la información de acuerdo al grado de importancia que tienen para la MPH?

Elaboración propia

**Interpretación:**

En la Figura 4.8, se puede observar que el 50% (3 trabajadores) de los encuestados considera que dentro de la Subgerencia de Sistemas y Tecnología si se ha categorizado la información de acuerdo a su grado de importancia, el 17% (un trabajador) considera que no se ha categorizado la información de acuerdo a su grado de importancia y, el 33% (2 trabajadores) desconoce si la información dentro de la Subgerencia de Sistemas y Tecnología ha sido categorizada o no.

**Conclusión:**

El diseño de un SGSI ayudará a que la Subgerencia de Sistemas y Tecnología categorice adecuadamente su información, mediante la valoración real de los activos de la información, asimismo facilitará la comunicación de esta información.

Para la pregunta, ¿Ha recibido Ud. capacitación sobre seguridad de la información de acuerdo a su función laboral? La frecuencia de respuesta fue la siguiente:

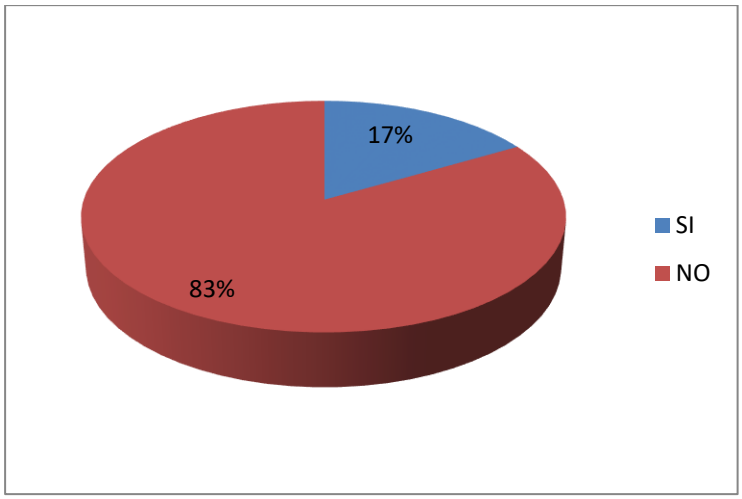


*Figura4. 9.* Frecuencia de respuesta para la pregunta, ¿Ha recibido Ud. capacitación sobre seguridad de la información de acuerdo a su función laboral?

Elaboración propia

**Interpretación:**

En la Figura 4.9, se puede observar que el 17% (un trabajador) de los encuestados afirma haber recibido capacitación sobre seguridad de la información frente a un 83% (5 trabajadores) que no ha recibido capacitación.

**Conclusión:**

El alto porcentaje de trabajadores que no ha recibido capacitación sobre temas de seguridad de información, hace más probable que la información se vea afectada en sus dimensiones de confidencialidad, integridad y disponibilidad.

Para la pregunta, ¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información? La frecuencia de respuesta fue la siguiente:

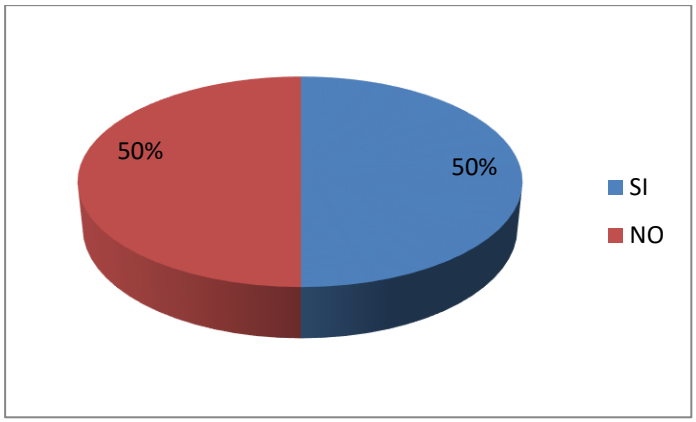


*Figura4. 10.* Frecuencia de respuesta para la pregunta, ¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información?

Elaboración propia

**Interpretación:**

En la Figura 4.10, se observa que 50% (3 trabajadores) de los encuestados afirma que su contrato contempla ítems respecto a la seguridad de la información y el otro 50% considera que su contrato no estipula estos ítems.

Para la pregunta: Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto? La frecuencia de respuesta fue la siguiente:

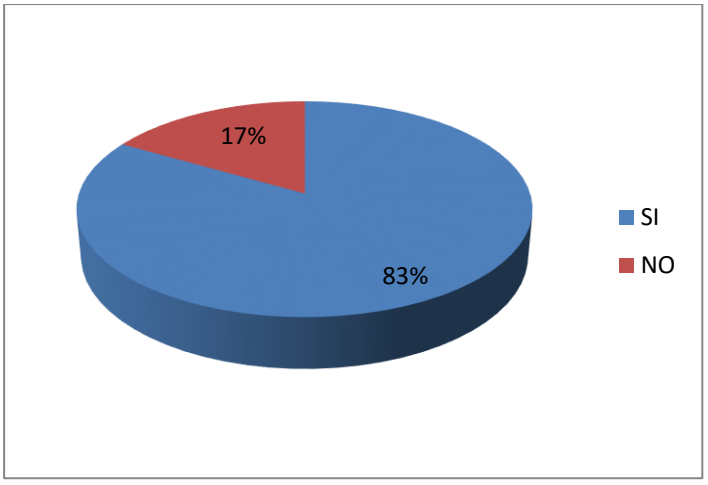


*Figura4. 11.* Frecuencia de respuesta para la pegunta: Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto?

Elaboración propia

**Interpretación:**

En la Figura 4.11, se observa que el 83% (5 trabajadores) de los encuestados afirman que cuando se gestiona un proyecto, sí se tiene en cuenta la seguridad de la información, pero el 17% (un trabajador) está en desacuerdo con esta afirmación.

Para la pregunta, ¿Cuenta Ud. con un computador/laptop para realizar sus funciones? La frecuencia de respuesta fue la siguiente:

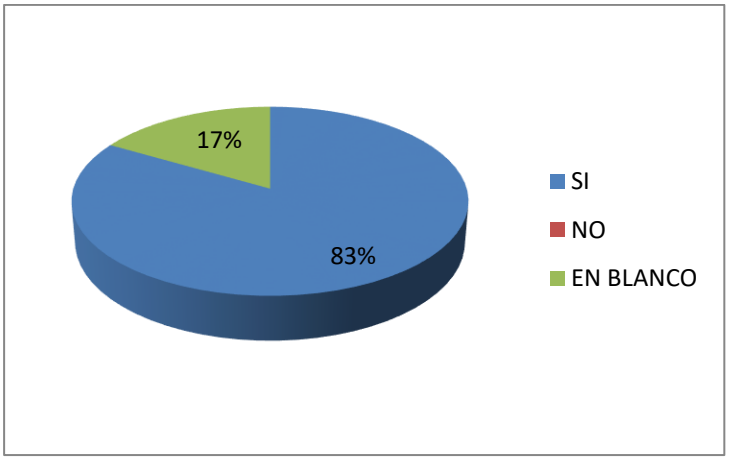


*Figura4. 12.* Frecuencia de respuesta para la pregunta, ¿Cuenta Ud. con un computador/laptop para realizar sus funciones?

Elaboración propia

**Interpretación:**

De la Figura 4.12, del 100% de los encuestados (6 trabajadores), el 83% cuenta con una computadora para realizar sus funciones dentro de la entidad y el 17% no cuenta con una computadora.

**Conclusión:**

El 17% de encuestados que no cuenta con una computadora para llevar a cabo sus funciones es porque se considera que las funciones que realizan no lo ameritan, por ejemplo, en el caso de practicantes de soporte técnico.

Para la pregunta, ¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop? La frecuencia de respuesta fue la siguiente:

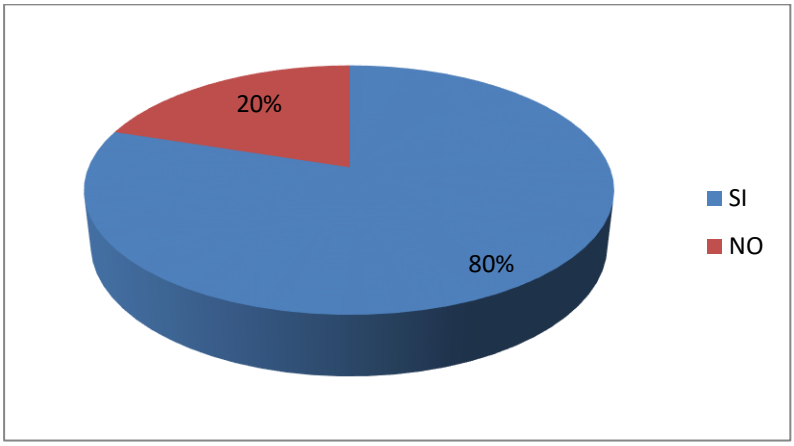


*Figura4. 13.* Frecuencia de respuesta para la pregunta, ¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop?

Elaboración propia

**Interpretación:**

De la Figura 4.13, del 100% (5 trabajadores) de trabajadores que usan un computador o laptop para realizar sus funciones, el 80% cuenta con una clave de acceso para ingresar a su computador/laptop, mientras que el 20% no cuenta con una clave de acceso.

Para la pregunta: Cuando su computador está desatendido ¿Se activa el bloqueo de pantalla con contraseña para proteger la información? La frecuencia de respuesta fue la siguiente:

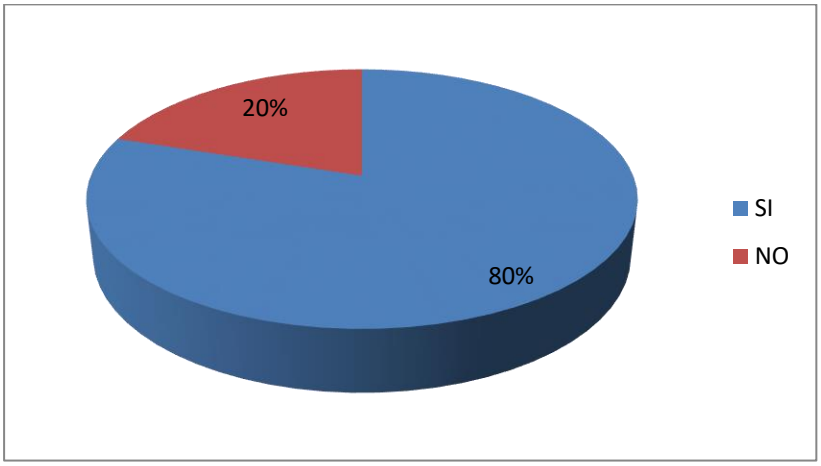


*Figura4. 14.* Frecuencia de respuesta para la pregunta: Cuando su computador está desatendido ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?

Elaboración propia

**Interpretación:**

De la Figura 4.14, del 100% (5 trabajadores) de trabajadores que usan computador o laptop para realizar sus funciones, el 80% afirma que cuando su computador/laptop está desatendido se activa el bloqueo de pantalla mientras que del 20% de trabajadores no se activa el bloqueo de pantalla, cuando su computador está desatendido.

Para la pregunta, ¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, extravío, etc.? La frecuencia de respuesta fue la siguiente:

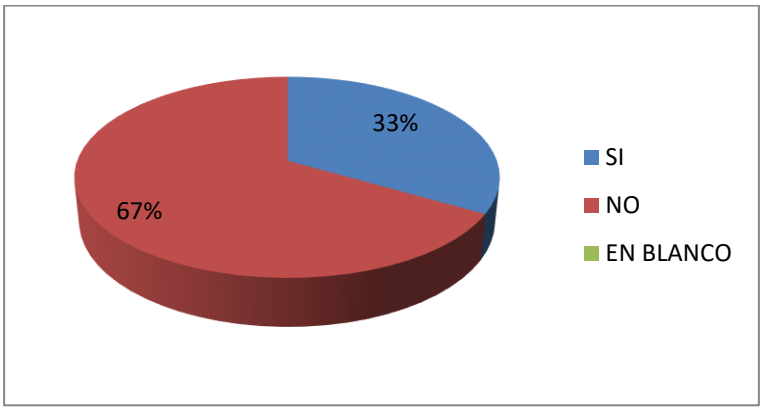


*Figura4. 15.* Frecuencia de respuesta para la pregunta, ¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, extravío, etc.?

Elaboración propia

**Interpretación:**

De la Figura 4.15, del 100% de encuestados (6 trabajadores) el 33% considera haber sido víctima de modificación/pérdida de información, mientras que el 67% considera no haber sufrido ninguna modificación/pérdida de su información.

Para la pregunta, ¿En lo que va del año se ha divulgado información sensible para la Municipalidad Provincial de Huamanga sin su autorización o conocimiento? La frecuencia de respuestas fue la siguiente:

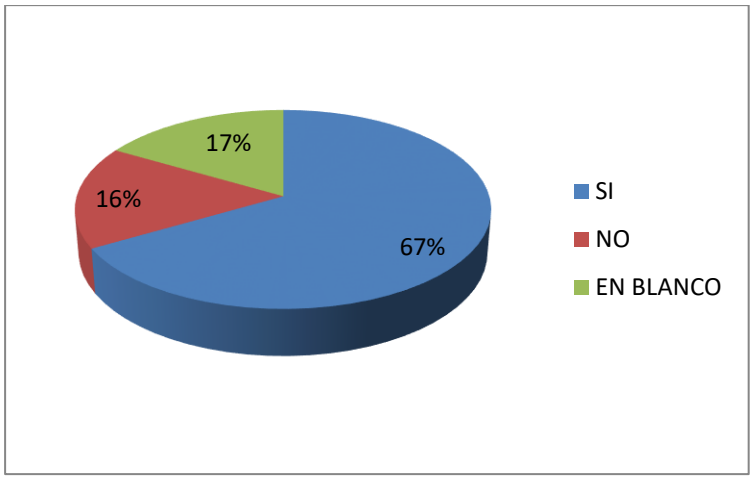


*Figura4. 16.* Frecuencia de respuesta para la pregunta, ¿En lo que va del año se ha divulgado información sensible para la Municipalidad Provincial de Huamanga sin su autorización o conocimiento?

Elaboración propia

**Interpretación:**

De la Figura 4.16, del 100% de los encuestados (6 trabajadores), el 67% afirma que en lo que va del año se ha divulgado información sensible para la Municipalidad Provincial de Huamanga sin su autorización o conocimiento, el 16% considera que no se ha divulgado información sensible de la Municipalidad Provincial de Huamanga y el 17% no sabe no opina.

Para la pregunta, ¿En su área de trabajo se ha realizado evaluación de riesgos relacionados con la información? La frecuencia de respuestas fue la siguiente:

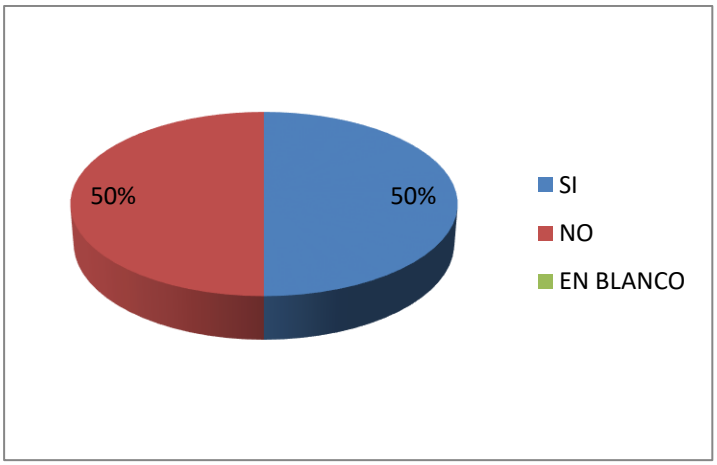


*Figura4. 17.* Frecuencia de respuesta para la pregunta, ¿En su área de trabajo se ha realizado evaluación de riesgos relacionados con la información?

Elaboración propia

**Interpretación:**

En la Figura 4.17, se observa que del 100% de los encuestados (6 trabajadores), el 50% opina que en la Subgerencia de Sistemas y Tecnología no se ha realizado un análisis de riesgos relativo a los sistemas de información, mientras que el otro 50% opina que si se ha realizado un análisis de riesgo de información.

**Conclusión:**

En la Subgerencia de Sistemas y Tecnología no se ha encontrado documentación que evidencie que se ha realizado el análisis y evaluación de riesgos de información, lo cual constituye un elemento importante para el diseño del SGSI.

Para la pregunta, ¿En su área de trabajo se han realizado evaluaciones de vulnerabilidades de la red? La frecuencia de respuestas fue la siguiente:

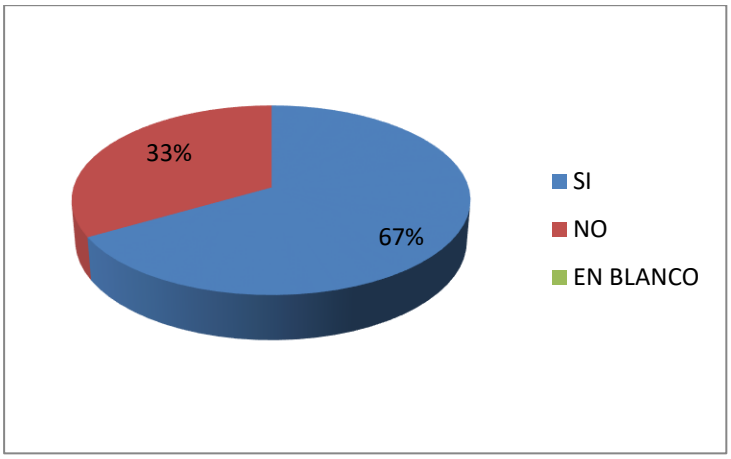


*Figura4. 18.* Frecuencia de respuesta para la pregunta, ¿En su área de trabajo se han realizado evaluaciones de vulnerabilidades de la red?

Elaboración propia

**Interpretación:**

En la Figura 4.18 se observa, que del 100% de los encuestados (6 trabajadores), el 67% opina que en la Subgerencia de Sistemas y Tecnología se ha realizado la evaluación de vulnerabilidades de red, mientras que el 33% opina lo contrario.

**Conclusión:**

A pesar de tener un porcentaje mayor que opina que si se ha realizado la evaluación de vulnerabilidades de red, no se ha encontrado documentación que evidencie esta evaluación y registre las amenazas que afectan a los activos de información, de modo que sigue existiendo debilidad en cuanto a la seguridad de información.

Para la pregunta, ¿Su área de trabajo cuenta con software antivirus actualizado? La frecuencia de respuesta fue la siguiente:

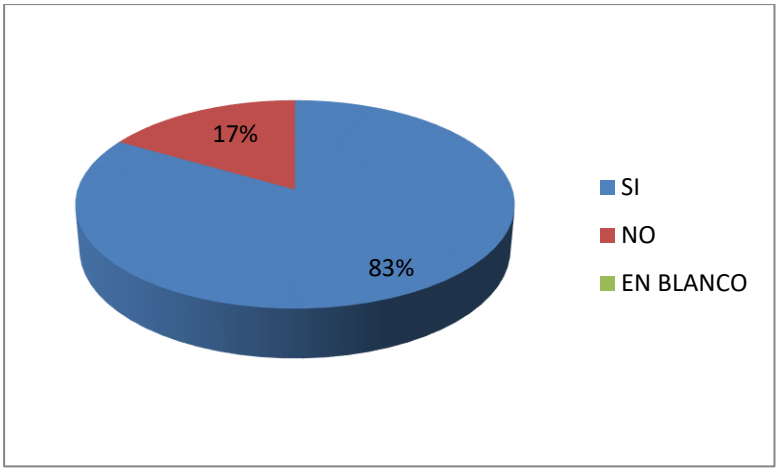


*Figura4. 19.* Frecuencia de respuesta para la pregunta, ¿Su área de trabajo cuenta con software antivirus actualizado?

Elaboración propia

**Interpretación:**

En la Figura 4.19 se puede observar, que del 100% de los encuestados, el 83% opina que en la Subgerencia de Sistemas y Tecnología si cuenta con antivirus actualizado, mientras que el 17% opina lo contrario.

Para la pregunta, ¿Realiza Ud. copias de seguridad para proteger su información? La frecuencia de respuesta fue la siguiente:

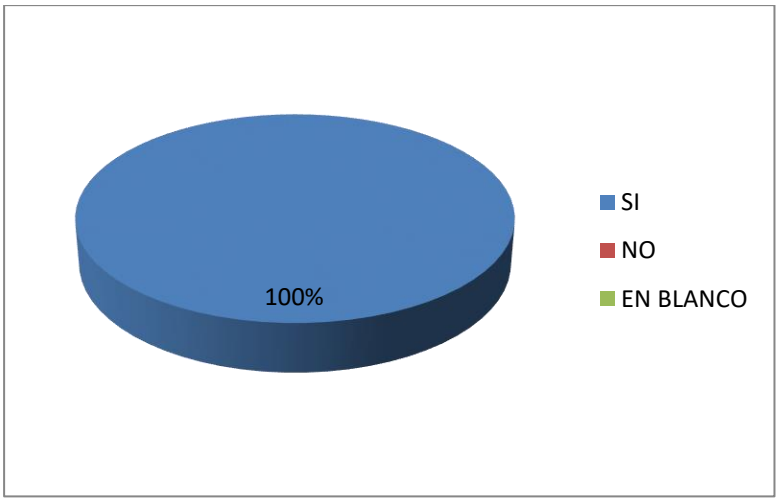


*Figura4. 20.* Frecuencia de respuesta para la pregunta ¿Realiza Ud. copias de seguridad para proteger su información?

Elaboración propia

**Interpretación:**

En la Figura 4.20 se puede observar que, el 100% de los encuestados (6 trabajadores) realiza copias de seguridad para proteger su información.

**Conclusión:**

A pesar de que todos los trabajadores realizan copia de seguridad de su información, en su mayoría estas copias están contenidas en el propio equipo de trabajo, lo cual sigue siendo un riesgo de pérdida de información si al activo que lo contiene le sucediera algo, siendo necesario establecer planes de contingencia.

Para la pregunta, ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionan pérdidas de información? La frecuencia de respuesta fue la siguiente:

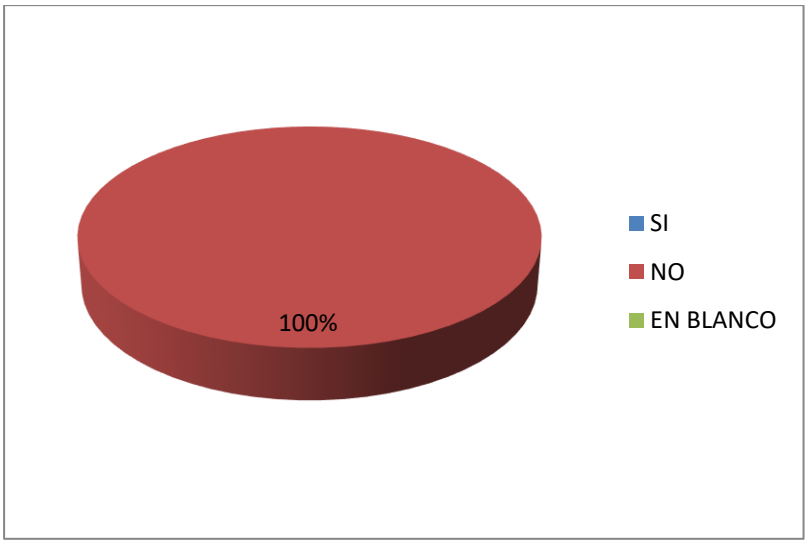


*Figura4. 21.* Frecuencia de respuesta para la pregunta, ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionan pérdidas de información?

Elaboración propia

**Interpretación:**

En la Figura 4.21, se observa que el 100% de los encuestados considera que la Subgerencia de Sistemas y Tecnología es vulnerable a amenazas externas o ambientales que ocasionan pérdidas de información.

**Conclusión:**

El diseño del SGSI permite identificar las amenazas, a las que se encuentra expuesta la Subgerencia de Sistemas y Tecnología, realizar la evaluación de riesgos y establecer los controles necesarios para salvaguardar los activos de información.

## 4.2 Fase II: Preparación del SGSI

Los objetivos de esta fase fueron: definir el alcance del SGSI, elaborar la política y los objetivos de seguridad, identificar los requisitos legales (aplicables a su SGSI) y proponer del comité de seguridad de la MPH. Estos objetivos se consiguieron tras analizar el contexto externo e interno de la MPH y comprender las necesidades y expectativas de las partes interesadas en el SGSI.

### 4.2.1. Contexto de la organización.

La NTP ISO/IEC 27001:2014 menciona en el capítulo 4: Contexto de la organización, la importancia de comprender la organización y su contexto, esto es,

comprender los aspectos internos y externos que son relevantes para el establecimiento del SGSI, asimismo comprender también las necesidades y expectativas de las partes interesadas y determinar el alcance de SGSI.

#### *4.2.1.1. Contexto externo*

En este ítem se analizó los factores externos (relevantes) que afectan a la MPH en el establecimiento e implementación del SGSI. Para ello se utilizó la herramienta de análisis PEST (iniciales de factores Políticos - Legales, Económicos, Socio-culturales y Tecnológicos) mencionada en el ítem 3.7 (herramientas para el tratamiento de datos) de esta investigación.

El resultado del análisis se muestra en la siguiente figura:


*Figura 4. 22.* Contexto externo de la MPH

Fuente: Elaboración propia

La comprensión del contexto externo es importante para asegurarse que los objetivos e inquietudes de las partes externas se tienen en cuenta cuando se desarrollan los criterios de riesgos.

#### *4.2.1.2. Contexto interno*

El SGSI debe alinearse con la cultura, los procesos, la estructura y la estrategia de la organización.

##### *4.2.1.2.1. Naturaleza de la entidad*

La Municipalidad Provincial de Huamanga como órgano de gobierno local provincial tiene personería jurídica de derecho público y plena capacidad para el cumplimiento de sus fines, con autonomía económica y administrativa en asuntos de su competencia, aplicando las leyes y disposiciones que de manera general y de conformidad con la Constitución Política del Perú regulan las actividades y funcionamiento del sector público nacional (Municipalidad Provincial de Huamanga, 2016a).

##### *4.2.1.2.2. Finalidad*

La Municipalidad provincial de Huamanga tiene los siguientes fines:

1. Conducir, promover y fomentar el desarrollo socio-económico integral, sostenible y armónico de la Provincia de Huamanga, considerando los procesos de gestión del riesgo de desastres en forma transversal;
2. Promover el bienestar del ciudadano con la adecuada prestación de los servicios públicos locales que satisfagan sus necesidades vitales de salubridad, vivienda, abastecimiento, seguridad, cultura, recreación, transporte y comunicaciones;
3. Representar política y organizacionalmente a los vecinos en el Gobierno Local, mediante programas de participación comunal y el ejercicio del derecho de petición.
4. Desarrollar programas sociales garantizando el ejercicio pleno de los derechos y la igualdad de oportunidades de sus habitantes;
5. Promover el desarrollo económico local, mediante el impulso y dinamización de la actividad empresarial de la Micro y Pequeña

> Empresa-MYPE, de acuerdo con las normas y políticas regionales y nacionales. (Municipalidad Provincial de Huamanga, 2016a, p. 7)

*4.2.1.2.3. Misión*

La Municipalidad Provincial de Huamanga tiene como misión ser "un gobierno local, promotor del desarrollo integral y sostenible de una Huamanga más humana, segura, ordenada, saludable, turística y productiva, basados en una gestión municipal, con identidad cultural y de participación vecinal que brinda servicios de calidad" (Municipalidad Provincial de Huamanga, 2016b, p. 19).

*4.2.1.2.4. Visión*

La Municipalidad Provincial de Huamanga tiene como visión ser una "municipalidad sólida, moderna, reconocida por la población por ser eficiente, ágil, que cuenta con un equipo humano competitivo, comprometido con el cambio y que practica los valores institucionales" (Municipalidad Provincial de Huamanga, 2016b, p. 17).

*4.2.1.2.5. Líneas estratégicas*

Institucionalmente, la Municipalidad Provincial de Huamanga tiene las siguientes líneas estratégicas:

1. **Competitividad Local;** involucra la situación institucional que favorezca el desarrollo competitivo de la Provincia.
2. **Calidad de Servicio;** hace referencia a los procesos internos y las condiciones de mejora continua, así como la medición de satisfacción de usuarios.
3. **Recursos y Tecnología;** comprende la situación de personal, bienes institucionales, patrimonio, presupuesto, ingresos por toda fuente, implementación de sistemas computarizados, Tecnología de información y comunicaciones, etc.
4. **Gestión Institucional;** incluye el estilo de gestión, la capacidad de liderazgo, la toma de decisiones, el estado de los documentos de gestión, cultura organizacional, entre otros aspectos (Municipalidad Provincial de Huamanga, 2016b).

*4.2.1.2.6. Objetivos estratégicos*

La Municipalidad Provincial de Huamanga tiene los siguientes objetivos estratégicos:

1. Lograr que los usuarios reciban una atención adecuada y sin discriminación.
2. Desarrollar servicios que se adapten y respondan a las necesidades de la población
3. Consolidar el liderazgo de la municipalidad en el desarrollo de la provincia basada en una gestión de procesos y resultados.
4. Modernizar la gestión con tecnologías de información y comunicación con la participación de la población
5. Mejorar la productividad de puestos de trabajo y de los trabajadores.
6. Incrementar los recursos financieros de la municipalidad y utilizarlos con eficiencia y transparencia.
7. Promover el aprovechamiento de oportunidades y emprendimiento empresarial.
8. Contribuir de manera efectiva en el clima de negocios de la provincia.
9. Gestionar la cultura organizacional de manera participativa, motivadora y que promueva la seguridad ciudadana.
10. Desarrollar una infraestructura vial adecuada, articulada y policéntrica.
11. Implementar la gestión ambiental en todos sus programas y proyectos.
12. Desarrollar la gestión municipal de riesgos de desastre. (Municipalidad Provincial de Huamanga, 2016b, pp. 7–8)

Para efectos de esta investigación, se consideró que los objetivos estratégicos con los que debe alinearse el SGSI son los contenidos en los numerales 3, 4 y 12.

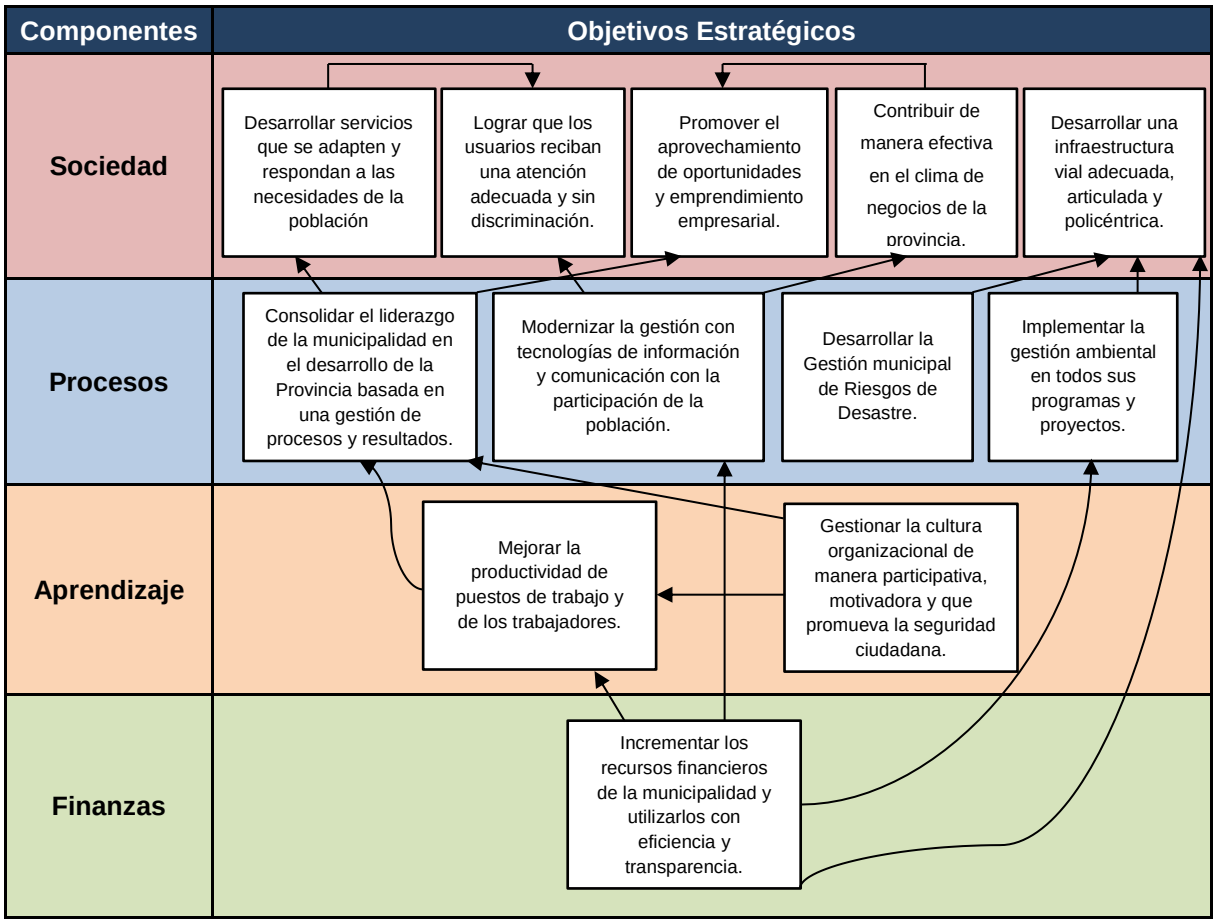


*Figura4. 23.* Mapa estratégico de la MPH

Fuente: PDI-M.P. Huamanga

### *4.2.1.2.7. Estructura orgánica*

En la Figura 4.2 se muestra la estructura orgánica de la Municipalidad Provincial de Huamanga, en este organigrama se ha designado a la Subgerencia de Sistemas y Tecnología (órgano de línea) como responsable de la seguridad de información dentro de la entidad.

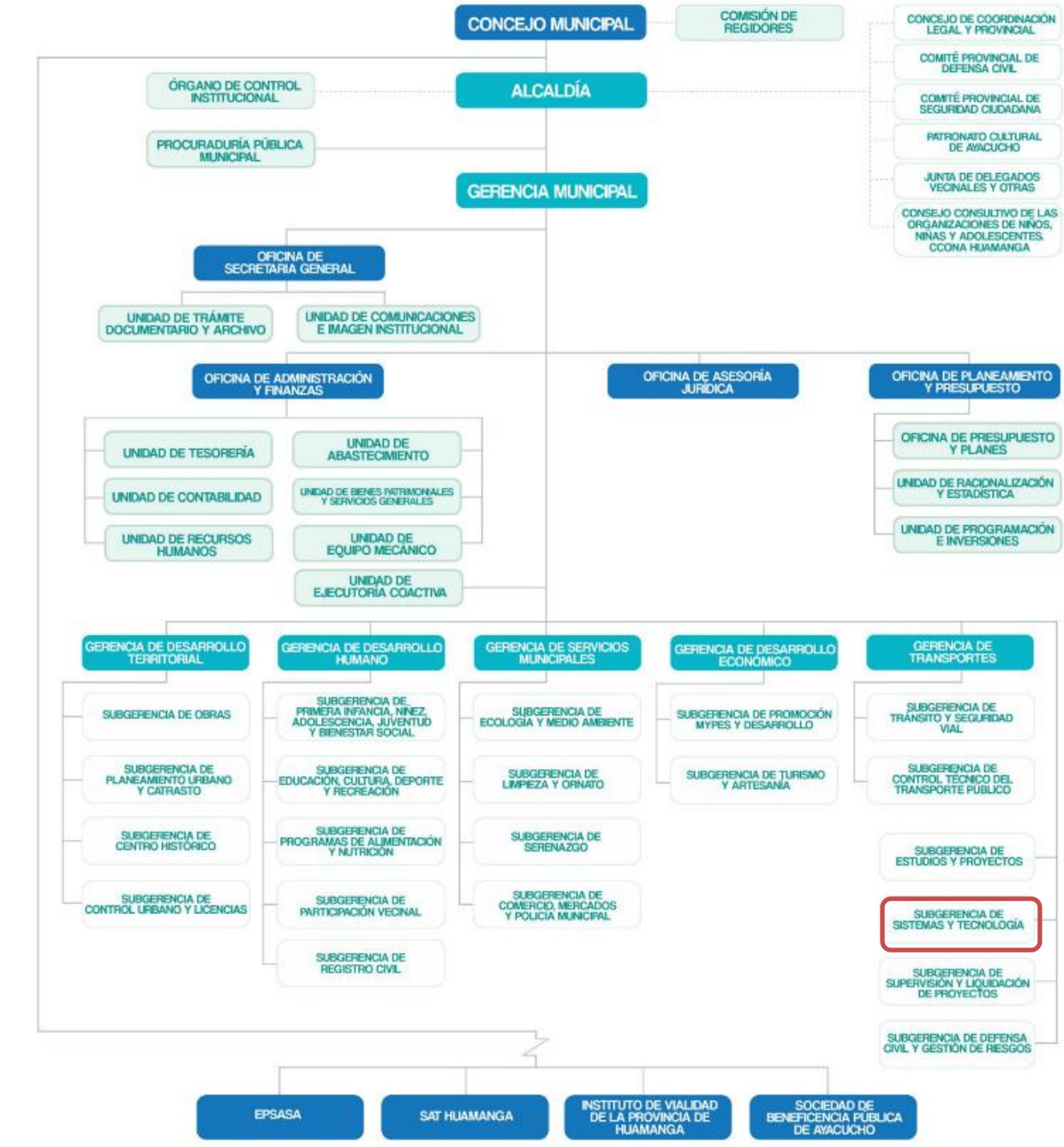


*Figura4. 24.* Organigrama de la Municipalidad Provincial de Huamanga

Fuente: Municipalidad Provincial de Huamanga

*4.2.1.2.8. Mapa de procesos*

Luego de analizar la Municipalidad Provincial de Huamanga y sus diferentes áreas funcionales se procedió a identificar los procesos de la entidad y elaborar el siguiente mapa de procesos:

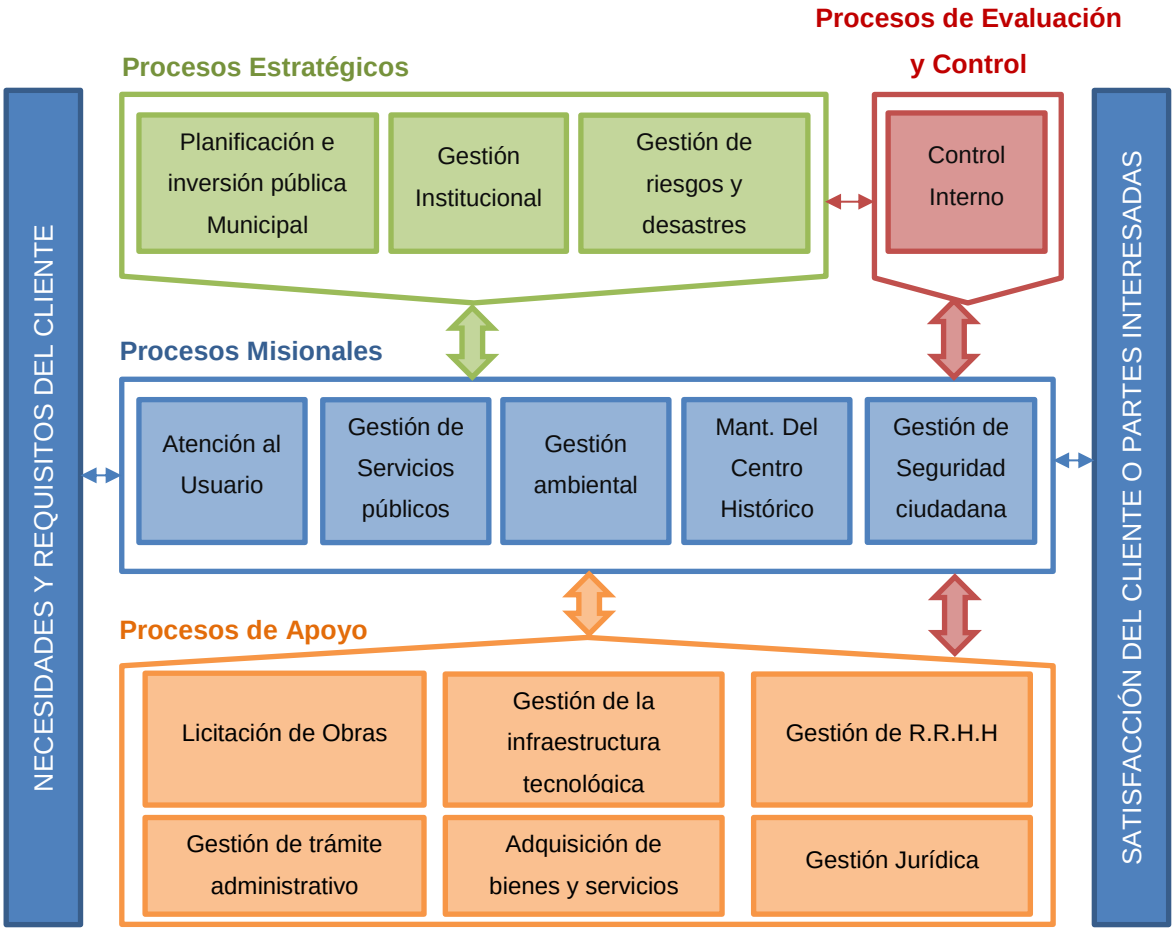


*Figura4. 25.* Mapa de procesos de la MPH

Fuente: Elaboración propia

A continuación, se define el proceso de gestión de infraestructura tecnológica

**a. Proceso gestión de la infraestructura tecnológica**

Tiene como objetivo planear, organizar, dirigir, ejecutar y supervisar el diseño, implementación y mantenimiento de la infraestructura tecnológica de la Entidad, fomentando protocolos de comunicación estandarizada, administrar y proveer los recursos tecnológicos a la entidad, así como garantizar los niveles

adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información, de los datos y de las comunicaciones de la Municipalidad Provincial de Huamanga. Su alcance inicia desde la concepción del Plan operativo informático (POI), su ejecución y adecuada prestación de servicios a los usuarios (internos y externos); estableciendo para este fin planes de contingencia, el monitoreo y la evaluación continua.

El proceso de gestión de la infraestructura tecnológica tiene los siguientes sub procesos:

- Gestión de la infraestructura y plataforma de procesamiento de datos.
- Administrar la operatividad de los sistemas de información, equipos Informáticos y de comunicaciones de la entidad.
- Gestión de soporte técnico
- Gestión de cambios de tecnologías de información
- Gestión de la seguridad de la información
- Gestión de la página web y servicios online
- Gestión del ciclo de vida del desarrollo de software de la entidad
- Gestión de plan de contingencia informática y de comunicaciones
- Administrar el inventario de equipos de cómputo
- Mejora de los sistemas estadísticos de la Municipalidad
- Gestión de proyección social tecnológico para municipalidades distritales y provinciales
- Asesorar a los usuarios internos en sus requerimientos informáticos

El proceso de gestión de infraestructura tecnológica es considerado como uno de los procesos fundamentales para garantizar la integridad, confidencialidad y disponibilidad de la información de la entidad, ya que este proceso administra y soporta los recursos tecnológicos a través de los cuales se gestiona, intercambia y almacena la información de los procesos estratégicos, misionales y de apoyo de la entidad, por lo tanto, es necesario asegurar sus activos de información.

Por lo mencionado anteriormente, es importante diseñar e implementar un adecuado sistema de gestión de seguridad la información y garantizar su mejora continua.

Cabe aclarar en este punto, que para realizar la definición del proceso de gestión de infraestructura tecnológica se mantuvo reuniones con la responsable de la Subgerencia de Sistemas y Tecnología, así mismo se tuvo en cuenta el ROF de la MPH.

*4.2.1.2.9. Aspectos técnicos*

La Municipalidad Provincial de Huamanga dispone, en el local central, de una red de área local (LAN), formada por un total de 190 estaciones de trabajo (aproximadamente), 49 portátiles y 7 servidores (3 servidores de aplicación, 2 servidores de bases de datos, 1 servidor virtual, y un servidor de dominio web).
Cuenta con una página web y correo corporativo gmail para 50 usuarios.
La MPH cuenta con un área de sistemas a nivel de subgerencia.
Tiene un Data center en el que se encuentran además de los servidores, una pequeña centralita telefónica que maneja las comunicaciones y anexos de la MPH.
En los servidores, se centraliza toda la información necesaria para el funcionamiento de los diferentes sistemas de la MPH, además de todos los accesos a la red de la entidad (cuentas de usuarios, etc).
Dispone de un sistema de alimentación ininterrumpida.
Para la salida de los sistemas de información se cuenta con 4 líneas de internet, donde una de ellas es una línea dedicada. Asimismo, cuenta con un firewall para controlar el acceso a la red.
Diariamente se realizan copias de seguridad y se almacenan en un disco duro externo ubicado en el Data Center. Un consolidado de backups se guarda mensualmente en DVDs y se almacenan en un estante con llave.
Dentro de la Subgerencia de Sistemas y Tecnologías se desarrolla software a medida para la Municipalidad Provincial de Huamanga.

Cabe mencionar que la MPH está ejecutando un proyecto de migración del ambiente del Data Center, para este proyecto se han reutilizado algunos recursos materiales como son: el cielo raso, falso piso, entre otros del actual local del Data Center ubicado en el sótano, quedando el cableado expuesto, enmarañado y tendido por el suelo, y todos los activos expuestos a amenazas que afecten sus dimensiones de integridad, disponibilidad y confidencialidad. En el Anexo C se pueden ver algunas fotos del Data Center.

a. Servicios en línea de la MPH

Según información recabada la de página web de la municipalidad Provincial de Huamanga se identificó los siguientes servicios en línea con los que cuenta la entidad:

a.1. Para usuarios externos

1. Consulta de Trámite Documentario: El ciudadano podrá hacer la consulta de su expediente que ingresa por Mesa de Partes en la plataforma de atencion al vecino, saber dónde esta y en qué estado se encuentra.
2. Atención en línea: El ciudadano realizar sus consultas y recibir orientación por parte de un personal de la Plataforma de Atención al vecino mediante un Chat en tiempo real.
3. SAT-H en línea: El ciudadano podrá realizar la consulta a cerca del su Impuesto Predial, Arbitrios Municipales, Impuesto Vehicular, Papeletas, Pagos y Realizar los reclamos al SAT-Huamanga.
4. Consulta de visitas a los funcionarios: El ciudadano podrá realizar la consulta las visitas a los funcionarios de la MPH.
5. Foro Municipal (Yanapakusun): El foro oficial de la MPH en donde un ciudadano podrá resolver las dudas e incidencias que ocurren en la Municipalidad mediante el uso de las Bitácoras.
6. Cursos y Talleres E-Learning (Muniyachay): Entorno de educación que servirá como repositorio de los Cursos, Talleres y Eventos que se llevan en la MPH y cuya información será compartida mediante MUNI-YACHAY la Plataforma Educativa.
7. C-VERDE: El CVerde es un reconocimiento de la municipalidad a los niños, niñas, adolescentes y jóvenes por sus buenas prácticas ambientales.
8. Libro de Reclamaciones: Libro de reclamaciones oficial de la MPH.

a.2. Para Usuarios Internos

1. Calendario de Actividades MPH
2. Sistema de trámite documentario
3. Plataforma de atención en Línea

4. Sistema de información ambiental local (SIAL)
5. Spark-Web
6. Sistemas de Visitas MPH
7. Catastro MPH: Incluye los sistemas de catastro Virtual, Ficha catastral y el sistema SIGALEC

En la Tabla 4.3, se muestra el inventario detallado de los sistemas y aplicativos con los que cuenta la Municipalidad Provincial de Huamanga, esta información fue proporcionada por el personal de la Subgerencia de Sistemas y Tecnología.

#### *4.2.1.3. Matriz DAFO*

Después de analizar de los aspectos internos externos e internos de la Municipalidad Provincial de Huamanga se elaboró la siguiente matriz DAFO:


*Figura4. 26.* Matriz DAFO

Fuente: Elaboración propia

**Tabla 4. 3**

*Inventario de sistemas de información de la MPH*

| Nro | Sistema de Información | Lenguaje de Programaciòn | Base de Datos | F. de Producción | Desarrollo Interno/Externo | Servidor | Documentación |
|---|---|---|---|---|---|---|---|
| **01** | Sistema de Trámite Documentario | Java7 | Postgres | 2016 (aùn en producción) | Desarrollo Interno V1 | SQLServer 2012 | SI (desactualizada) |
| **02** | Atención en Línea | Php5.5 | Mysql5.5 | 2015 | Personalizado | VPS | No |
| **03** | Sistema de control de visitas | PHP5 | Mysql5.5 | 2013 | Externo (ONGEI) | Ubuntu server | No |
| **04** | Foro Municipal (Yanapakusun) | PHP | MySql5.5 | 2016 | Personalizado | VPS | No |
| **05** | Cursos y Talleres E-Learning (Muniyachay) | PHP | MySql5.5 | 2016 | Personalizado | VPS | No |
| **06** | Catastro MPH: Incluye los sistemas de catastro Virtual, Ficha catastral y el sistema SIGALEC | PHP | Postgres | – | Interno | Ubuntu Server | Si (desactualizada) |
| **07** | Libro de Reclamaciones | Java | Postgres | 2013 | Interno | – | Si (desactualizada) |
| **08** | Calendario de Actividades | PHP | Mysql | 2016 | Interno | VPS | No |
| **09** | SIAF | FOXPRO | FOXPRO | 2006 | Externo | | No |
| **10** | Spark-Web | HTML | Flash | 2016 | Externo | VPS | No |
| **11** | SAT-H en línea | .Net | SqlServer | 2015 | Externo | Sevidor externo | No |
| **12** | C-VERDE | - | - | 2016 | Externo | Apache | No |
| **13** | Sistema de información ambiental local (SIAL) | - | - | 2015 | Externo | – | No |

Nota: Elaboración propia

#### *4.2.1.4. Partes interesadas*

Conforme al requisito 4.2 (Comprender las necesidades y expectativas de las partes interesas) de la NTP ISO/IEC 27001:2014. En este apartado se identificaron las partes interesadas externas e internas afectadas por el diseño y posterior implementación del SGSI. Asimismo, se identificaron los requisitos de estas partes interesadas relevantes a la seguridad de la información.

##### *4.2.1.4.1. Partes interesadas externas*

1. Gobierno (ONGEI-PCM)

   La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), es el órgano técnico especializado que depende directamente del despacho de la Presidencia del Consejo de Ministros (PCM). ONGEI, en su calidad de Ente Rector del sistema nacional de informática, se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado. Entre sus actividades permanentes se encuentran las vinculadas a la normatividad informática, la seguridad de la información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y la Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y difusión en temas de gobierno electrónico y la modernización y descentralización del Estado. (Oficina Nacional de Gobierno Electrónico e Informática, 2016)

2. Contraloría General de la República

   La Contraloría General de la República es la máxima autoridad del sistema nacional de control. Supervisa, vigila y verifica la correcta aplicación de las políticas públicas y el uso de los recursos y bienes del Estado. Para realizar con eficiencia sus funciones, cuenta con autonomía administrativa, funcional, económica y financiera. (Contraloría General de la República, s.f.)

3. La comunidad

Corresponde a los individuos y grupos externos que se ven impactados por las actividades que desarrollar la entidad.

4. Proveedores

Personas naturales o Jurídicas que prestan sus servicios a la MPH.

*4.2.1.4.2. Partes interesadas internas*

1. Órganos de Gobierno

Conformado por el Consejo Municipal y Alcaldía. Deben demostrar liderazgo y compromiso con la seguridad de la información, asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización y, garantizando la disponibilidad de los recursos necesarios para su implementación.

2. Órganos de alta Dirección

Conformado por la Gerencia Municipal. Debe demostrar liderazgo y compromiso respecto al sistema de gestión de la seguridad de la información, asegurando que los objetivos que se establecen son compatibles con la planeación estratégica de la organización y estableciendo una política de seguridad de la información.

3. Sub Gerente de Sistemas y Tecnología

Es el responsable entre otros aspectos, de la seguridad de la información y continuidad tecnológica de la Entidad.

4. Responsable de Recursos Humanos

Responsable de la seguridad de la información antes, durante y después de la vinculación de los funcionarios y trabajadores.

5. Trabajadores de la MPH

Responsables de velar por la seguridad de los activos de información de la MPH, cumplir a cabalidad con las normas y políticas de seguridad establecidas en la entidad. Además, tienen la responsabilidad del tratamiento de los datos personales de los titulares vinculados de alguna forma con la Entidad.

En la Tabla 4.4 se muestran los requisitos de las partes interesadas del SGSI.

**Tabla 4. 4**

*Requisitos de las partes interesadas externas e internas*

| | Partes Interesadas | Requisitos |
|---|---|---|
| Externas | Gobierno (ONGEI-PCM) | • Cumplimiento del marco legal y normativo de la seguridad de la información.<br>• Alcanzar el objetivo de la política nacional de gobierno electrónico 2013-2017. |
| | Contraloría General de la república | • Cumplimiento de la normatividad de control interno de las entidades del estado relacionado a las tecnologías de información y comunicaciones: apartado 3.10 de la resolución de Contraloría General Nº 320-2006-CG. |
| | Comunidad | • Seguridad de sus datos sensibles. |
| | Proveedores | • Acuerdos contractuales claros en temas de seguridad de información |
| Internas | Órganos de Gobierno | • Cumplimiento de las leyes y normatividad vigente en temas de seguridad.<br>• Debe demostrar liderazgo y compromiso con la seguridad de la información. |
| | Órganos de Alta Dirección | • Supervisar las actividades y proyectos de la Sub Gerencia de Sistemas y Tecnología en temas de Seguridad de la Información.<br>• Debe demostrar liderazgo y compromiso con la seguridad de la información. |
| | Sub Gerente de Sistemas y Tecnología | • Levantamiento de no conformidades (respecto a la seguridad de información) de la auditoría presupuestal y financiera practicada a la Municipalidad Provincial de Huamanga.<br>• Capacitar a los trabajadores en temas de seguridad de información |
| | Responsable de Recursos Humanos | • Verificar la seguridad de la información antes, durante y después de la vinculación de los funcionarios y trabajadores. |
| | Trabajadores de la MPH | • Conocer las normas y políticas en temas de Seguridad de la información<br>• Velar por los activos de información de la MPH.<br>• Protección de su información personal.<br>• Disponibilidad de los servicios de la MPH.<br>• Capacitación en temas de seguridad de la información |

Nota: Elaboración propia

### 4.2.2. Política de la seguridad de la información

En este apartado, se definió la política de seguridad de la información de la MPH (acorde al requisito 5.2 de la NTP ISO/IEC 27001:2014). La política de seguridad será aprobada por el órgano de Gobierno y revisada anualmente.

Una vez aprobada la política de seguridad, la Municipalidad Provincial de Huamanga comunicará esta política a todos los trabajadores de la entidad y a aquellos proveedores que considere necesario, además estará disponible para ser consultada por las partes interesadas.

La Municipalidad Provincial de Huamanga, en cumplimiento de nuestra misión, visión y objetivo estratégico, y para satisfacer las necesidades de la comunidad, proveedores, y demás partes interesadas, establece la función de seguridad de la información dentro la entidad con el objetivo de:

- Proteger los activos de información de la Municipalidad Provincial de Huamanga.
- Es Política de la Municipalidad asegurar que:
  - La información esté protegida contra pérdidas de disponibilidad, confidencialidad e integridad.
  - Se cumplan los requisitos legales y normas aplicables a la entidad respecto a la seguridad de la Información.
  - Se cumplen con los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.
  - Se gestionen los riesgos de seguridad de la información a través de la aplicación de una metodología, estándares y controles orientados a preservar los activos información de la entidad.
  - Se fortalezca la cultura de seguridad de la información en los trabajadores de la entidad.
  - Se garantice la continuidad de los servicios de la entidad.
  - Cada trabajador es responsable de cumplir esta política y sus procedimientos según aplique a su puesto de trabajo (*).
  - Es política de la Municipalidad Provincial de Huamanga implementar, mantener y realizar un seguimiento del SGSI.

(*) La entidad se reserva el derecho de tomar medidas disciplinarias con el personal que incumpla con lo dispuesto en la presente política, conforme a las disposiciones señaladas en los documentos normativos de la institución, sin perjuicio de las acciones civiles o penales que pudieran corresponder.

*Figura 4. 27.* Política de seguridad

Elaboración propia

### 4.2.3. Alcance de SGSI

El alcance del Sistema de Gestión de Seguridad de la Información de la MPH está incluido dentro del documento que se referencia en el ANEXO D. A continuación, se muestra un extracto del mismo:

> El alcance del sistema de gestión de seguridad de la información aplica sólo para el proceso de GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA, sub proceso de gestión de la seguridad de la información, dentro de los sistemas de información que sustentan los procesos de negocio.
>
> Se tienen en cuenta los activos de información considerados como relevantes dentro del alcance.
>
> El sistema de gestión de seguridad de la información aplica solo para la Sub Gerencia de Sistemas y Tecnología ubicada en la sede principal de la Municipalidad Provincial de Huamanga, Portal Municipal N°44 Ayacucho.

*Figura 4. 28.* Alcance del SGSI de la MPH

Fuente: Elaboración propia

### 4.2.4. Objetivos de seguridad de la información

Los objetivos del sistema de gestión de seguridad de la información se muestran en la siguiente figura:

- Asegurar la confidencialidad de la información de los ciudadanos almacenados en los sistemas de información de la Municipalidad provincial de huamanga.
- Asegurar la confidencialidad, integridad y disponibilidad de la información sensible de la Municipalidad Provincial de Huamanga.
- Maximizar la disponibilidad y calidad de los servicios prestados a los ciudadanos.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación y normatividad vigente en materia de seguridad de la información.
- Reducir los riesgos de seguridad de la información a un nivel aceptable para la Municipalidad.
- Difundir la Política de seguridad a través de cada uno de los responsables de área.
- Evaluar la efectividad del SGSI y llevar a cabo la mejora continua.

*Figura 4. 29.* Objetivos de seguridad de la información.

Fuente: Elaboración propia

### 4.2.5. Requisitos legales

Cumplir con la legislación vigente en Perú es uno de los requisitos que se debe satisfacer para implantar y certificar un sistema de gestión de seguridad de la información. Su cumplimento protege a la entidad de amenazas externas e internas, además permite respetar los derechos de los ciudadanos y proveedores y evitará infracciones involuntarias con sus respectivos costes.

A continuación, se hace mención de algunas leyes y normas relacionadas con seguridad de la información que afectan a la Municipalidad Provincial de Huamanga.

#### *4.2.5.1. Norma de Control Interno de las Entidades del Estado*

Aprobada con Resolución de Contraloría General Nº 320-2006-CG, de fecha 30 de octubre del 2006. Según las NORMAS BÁSICAS PARA LAS ACTIVIDADES DE CONTROL GERENCIAL, en su punto 3.10. Controles para las Tecnologías de Información y Comunicaciones (TIC) se define “La información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas”. Asimismo, la citada norma señala:

Comentario 01.- Los controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad. Los principales controles deben establecerse en:

- Sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico
- Segregación de funciones
- Controles de acceso general, es decir, seguridad física y lógica de los equipos centrales
- Continuidad en el servicio.

Comentario 02.- Para la puesta en funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas:

i. Definición de los recursos
ii. Planificación y organización
iii. Requerimiento y salida de datos o información
iv. Adquisición e implementación
v. Servicios y soporte
vi. Seguimiento y monitoreo.

Comentario 07.- Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia.

Comentario 08.- El programa de planificación y administración de seguridad provee el marco y establece el ciclo continuo de la administración de riesgos para las TIC, desarrollando políticas de seguridad, asignando responsabilidades y realizando el seguimiento de la correcta operación de los controles.

#### *4.2.5.2. Ley N°29733.- Ley de Protección de Datos Personales*

Promulgada el 2011, pero entró en aplicación el 8 de mayo de 2015. La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Esto quiere decir que las empresas y entidades públicas están obligadas a garantizar la protección de los datos con los que cuentan en sus sistemas informáticos evitando que terceros no autorizados accedan a ellos.

#### *4.2.5.3. Ley 30096.- Ley de Delitos Informáticos*

Entró en vigencia el 23 de octubre de 2013. La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

#### *4.2.5.4. Ley N° 30171.- Ley que Modifica la Ley 30096, ley de Delitos Informáticos*

Publicada en el diario Oficial el Peruano en el 10 de marzo del 2014. Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, se modificaron los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos: Acceso ilícito, atentado a la integridad de datos informáticos, atentado a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, abuso de mecanismos y dispositivos informáticos.

#### *4.2.5.5. Resolución Ministerial Nº 004-2016-PCM*

Publicada en el Diario Oficial El Peruano el 8 de enero de 20016. Se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

Esta RM deja sin efecto la Resolución Ministerial Nº 129-2012-PCM.

### 4.2.6. Comité de la seguridad de la información

De acuerdo al requisito 5.3 Roles, responsabilidades y autoridades organizacionales de la NTP ISO/IEC 27001:2014 la alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

Asimismo, la RM Nº 004-2016-PCM en su artículo 5 establece la creación del comité de gestión de seguridad de la información para dar cumplimiento al requisito 5.3 de la NTP ISO/IEC 27001:2014. Este comité de gestión de seguridad de la Información, estará conformado por:

1. El alcalde
2. El gerente municipal
3. El responsable de planificación y presupuesto
4. El sub gerente de sistemas y tecnología;
5. El responsable de la oficina de asesoría jurídica
6. El oficial de seguridad de la información.

A continuación, se describen los roles y responsabilidades propuestos estos roles y responsabilidades así como la necesidad de agregar alguna autoridad más será evaluada por la alta dirección en coordinación con el comité de seguridad de la información.

Cabe mencionar que, según la metodología, este requisito estará sometido a una mejora continua acorde a las necesidades de la MPH.

#### *4.2.6.1. El Alcalde*

- Aprobar la política de seguridad de la información y comunicarla a todos los trabajadores de la entidad.
- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- Promover una cultura de seguridad de la información en la entidad.

#### *4.2.6.2. El Gerente Municipal*

- Proponer al Alcalde y Concejo Municipal la política de seguridad de la información para la entidad.
- Hacer cumplir la política de seguridad de la información dentro de la entidad.
- Revisar la política de seguridad de la información en intervalos planificados o cuando se produzcan cambios significativos en la normatividad de seguridad.
- Controlar el avance de la seguridad de información dentro de la Municipalidad de Huamanga

#### *4.2.6.3. El responsable de la oficina de planificación y presupuestos*

- Gestionar y coordinar los medios necesarios para la implementación, ejecución y mantenimiento del sistema de gestión de seguridad de la información.

#### *4.2.6.4. Sub Gerente de Sistemas y Tecnología*

- Garantizar la disponibilidad y operatividad de los sistemas de información, equipos informáticos y de comunicaciones de la entidad.
- Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- Informar al gerente municipal sobre aspectos relacionados con el SGSI.
- Asegurar la existencia de metodologías para el tratamiento de riesgos y oportunidades, políticas de seguridad de la información, así como la existencia de los documentos exigidos por la NTP ISO/IEC 27001:2014.
- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de infraestructura tecnológica de la entidad.
- Asignar las funciones, roles y responsabilidades de Seguridad, a los trabajadores a su cargo para la operación y administración de la infraestructura tecnológica de la entidad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.
- Aprobar la implementación de los controles y medidas de seguridad

#### *4.2.6.5. El responsable de la oficina de asesoría jurídica*

- Conocer e interpretar las leyes y normatividad vigente relacionada con seguridad de la información y bajo el contexto de la entidad.
- Evaluar el cumplimiento de las leyes y normatividad vigente en temas de seguridad de la información dentro de la entidad.
- Mantener actualizado un archivo de normas legales relacionadas con la seguridad de la información.

#### *4.2.6.6. El Oficial de seguridad de la información.*

- Diseñar y coordinar la implementación de las políticas, normas y procedimientos de seguridad de la información, con la participación activa de las dependencias de la entidad.
- Identificar los riesgos a los que se encuentran expuestos los activos de información de la MPH y gestionar la actualización del mapa de riesgos.
- Definir los controles asociados al sistema de gestión de seguridad de la Información y evaluarlos periódicamente.
- Establecer un programa periódico de revisión de vulnerabilidades y coordinar los respectivos planes de mitigación.
- Desarrollar de forma periódica, charlas de capacitación y concientización en temas de seguridad de información para el personal de la entidad.
- Atender auditorías internas y externas de aspectos asociados a la Seguridad de Información y, facilitar la información sobre documentos de gestión de seguridad y los controles implementados.
- Reportar al subgerente de sistemas y tecnología los incidentes de seguridad de la información, los resultados de las auditorias, la revisión y supervisión del SGSI.
- Asesorar en forma permanente y cercana a las distintas áreas de la institución en temas de seguridad.

### 4.3 Fase III: Planificación del SGSI

En este apartado se llevó a cabo las actividades para tratar los riesgos y asegurar que el diseño del SGSI alcance los objetivos de: evaluar los riesgos de seguridad de la información de la Municipalidad Provincial de Huamanga y elaborar la lista de controles de seguridad para mitigar los riesgos identificados.

### 4.3.1. Evaluación de riesgos

#### *4.3.1.1. El inventario de activos*

De acuerdo a la metodología de análisis y gestión de riesgos adoptada (MARGERIT V.3) se definió la siguiente clasificación de activos:

**Tabla 4. 5**

*Clasificación de activos de información*

| TIPO DE ACTIVO | DESCRIPCIÓN |
|---|---|
| **Dato/Información** | Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. |
| **Servicios** | Los servicios satisfacen la necesidad de los usuarios, contempla servicios prestados por el sistema. |
| **Software/ aplicaciones informáticas** | Se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios |
| **Equipos informáticos** | Son los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. |
| **Redes de Comunicaciones** | Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro. |
| **Soporte de Información** | Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. |
| **Equipamiento Auxiliar** | En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información. |
| **Instalaciones** | En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones. |
| **Personal** | Personas relacionadas con los sistemas de información. |

Nota: MARGERIT V.3 - libro 2

Para identificar los activos de información de la Municipalidad Provincial de Huamanga se utilizó el formato del Anexo E: Cuestionario para identificar activos.

Un extracto de la relación de activos identificados en el proceso gestión de la infraestructura tecnológica se muestra en la Tabla 4.6. El inventario completo se encuentra en el Anexo F de este proyecto de investigación.

**Tabla 4. 6**

*Inventario de activos de información*

| Nombre del activo | Descripción del activo | Tipo de Activo | Ubicación |
|---|---|---|---|
| Datos vitales | Datos que almacenan los diferentes sistemas de información esenciales para el funcionamiento de la MPH | Dato/Información | Data Center |
| Archivos Personales | Documentos personales de los trabajadores de la MPH | Dato/Información | Computadoras Personales |
| Copias de Respaldo | Copias de respaldo de los datos/información que manejan los distintos sistemas de la MPH | Dato/Información | Data Center/PC Administrador |
| Datos de Configuración de los Sistemas de Información | Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes sistemas de información | Dato/Información | Archivo físico (estantería) |
| Datos de Gestión interna | Corresponde a los documentos de la MPH | Dato/Información | Archivo físico (estantería)/ VPS |
| Código fuente de los sistemas de información | Corresponde a los códigos fuente de los distintos sistemas desarrollados en MPH | Dato/Información | Servidores de Versiones (en la nube) |
| Servicios online | Corresponde a los servicios de consulta como por ejemplo: Portal de transparencia, Foro Municipal, consulta de visita a funcionarios. | Servicio | Página Web de la MPH |
| Correo electrónico | Correo electrónico institucional | Servicio | Servidor de correo GMAIL |
| Página Web | Página Web de la entidad | Software/Aplicaciones informática | VPS |
| Sistema de trámite documentario | Sistema para la gestión de trámite externo e interno, utilizado por la unidad de trámite documentario y archivos | Software/Aplicaciones informática | Servidor de aplicaciones Windows |
| SIAF | Sistema que manejan la oficina de administración y Finanzas y Planeamiento y Presupuesto | Software/Aplicaciones informática | Servidor SIAF |
| Sistema Gestor de Base de Datos | Sistema de gestión y administración de las bases de datos de la entidad | Software/Aplicaciones informática | PC de los administradores |
| Aplicaciones Comerciales | Office, sistemas operativos, antivirus, entre otros | Software/Aplicaciones informática | Computadoras Personales |
| Servidores de aplicaciones de Producción | Servidores de producción que soportan las aplicaciones y sistemas de información | Equipos informáticos | Data Center de la Municipalidad |
| Servidores de Base de datos | Servidores de producción que soportan las aplicaciones y sistemas de información | Equipos informáticos | Data Center de la Municipalidad |
| Computador del Funcionario | Computadores que utilizan los funcionarios de la entidad | Equipos informáticos | SG de Sistemas y Tecnología |

| Nombre del activo | Descripción del activo | Tipo de Activo | Ubicación |
|---|---|---|---|
| Computadores administradores de SI | Computadores que utilizan los administradores de las plataformas, los desarrolladores | Equipos informáticos | SG de Sistemas y Tecnología |
| Internet | Red de comunicación contratado a terceros | Redes de Comunicaciones | Red inalámbrica |
| Red local | Red de comunicaciones cableada | Redes de Comunicaciones | Red local |
| Disco duro externo | Disco duro externo | Soportes de Información | Data center |
| Soportes no electrónicos | Dispositivos físicos de almacenamiento no electrónico como material impreso | Soportes de Información | Archivo físico o estantería |

Nota: Elaboración propia

#### *4.3.1.2. Valoración de activos*

Para valorar los activos de información se consideró tres aspectos: el económico, el legal y la imagen, que pueden afectar a los activos en sus dimensiones de confidencialidad, integridad y disponibilidad.

El criterio que se siguió para valorar los activos de información se muestra en la Tabla 4.7.

***Tabla 4. 7***

*Criterio para la valoración de activos*

| ASPECTOS | DESCRIPCIÓN | CRITERIO DE CALIFICACIÓN | VALORACIÓN |
|---|---|---|---|
| **Económico (E)** | Pérdidas económicas para la Municipalidad | Pérdidas económicas excepcionalmente elevadas | 5 |
| | | Causa de pérdidas económicas elevadas | 4 |
| | | Causa de graves pérdidas económicas | 3 |
| | | Causa de pérdidas financieras o merma de ingresos | 2 |
| | | Supondría pérdidas económicas mínimas | 1 |
| **Legal (L)** | Incumplimiento de leyes y normas | Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación | 5 |
| | | Probablemente cause un incumplimiento grave de una ley o regulación | 4 |
| | | Probablemente sea causa de incumplimiento de una ley o regulación | 3 |
| | | Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación | 2 |
| | | Pudiera causar el incumplimiento leve o técnico de una ley o regulación | 1 |
| **Imagen (IMG)** | Afecta a la imagen de la Municipalidad | Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones | 5 |
| | | Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones | 4 |
| | | Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones | 3 |
| | | Probablemente afecte negativamente a las relaciones internas de la organización | 2 |
| | | Pudiera causar una pérdida menor de la confianza dentro de la Organización | 1 |

Nota: Adaptado de *"Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso"*, p. 85, Guzmán Silva. 2015.

Asimismo, se estableció preguntas para determinar la criticidad del activo de información. Estas preguntas se muestran en siguiente tabla:

**Tabla 4. 8**

*Preguntas para determinar la criticidad del activo de información*

| Parámetro | Aspecto | Pregunta |
|---|---|---|
| **Confidencialidad** | Económico | ¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras causando pérdida económica? |
| | Legal | ¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control? |
| | Imagen | ¿Su divulgación no autorizada puede afectar la imagen de la entidad? |
| **Integridad** | Económico | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad? |
| | Legal | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control? |
| | Imagen | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad? |
| **Disponibilidad** | Económico | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad? |
| | Legal | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control? |
| | Imagen | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad? |

Nota: Adaptado de *"Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso"*, p. 86, Guzmán Silva. 2015.

Por último, para determinar el nivel de criticidad del activo valorado, se usó el criterio establecido en la Tabla 4.9. De esta manera se determinó la importancia de los activos de información dentro del proceso: gestión de la infraestructura tecnológica.

**Tabla 4. 9**

*Nivel de criticidad de los activos de información*

| CRITERIO DE EVALUACIÓN | VALOR | NIVEL |
|---|---|---|
| El activo de información compromete en un nivel alto la integridad y/o confidencialidad y/o disponibilidad de la información de la MPH. | 3<VF<=5 | Alto |
| El activo de información compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información de la MPH. | VF=3 | Medio |
| El activo de información compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la MPH. | 0<VF<3 | Bajo |

Nota: Adaptado de *"Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso"*, p. 86, Guzmán Silva. 2015.

El Anexo G, de esta investigación, muestra el cuestionario que se usó para valorar los activos del proceso: gestión de la infraestructura tecnológica.

En la Tabla 4.10, se muestra un extracto del resultado de la valoración de activos su nivel de criticad.

**Tabla 4. 10**

*Valoración de activos de información y nivel de criticidad*

| N° | NOMBRE DEL ACTIVO | CONFIDENCIALIDAD | | | INTEGRIDAD | | | DISPONIBILIDAD | | | VFC | VFI | VFD | VF | NIVEL DE CRITICIDAD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | E | L | IMG | E | L | IMG | E | L | IMG | | | | | |
| 1 | Copias de Respaldo | 4 | 5 | 3 | 5 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | ALTO |
| 2 | Datos de Configuración de los Sistemas de Información | 2 | 1 | 1 | 2 | 2 | 3 | 3 | 3 | 1 | 2 | 3 | 3 | 3 | MEDIO |
| 3 | Datos de Gestión interna | 4 | 4 | 3 | 3 | 3 | 3 | 4 | 3 | 3 | 4 | 3 | 4 | 4 | ALTO |
| 4 | Credenciales (contraseñas) | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | ALTO |
| 5 | Datos de control de acceso | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | ALTO |
| 6 | Log de los sistemas de información | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | MEDIO |
| 7 | Código fuente de los sistemas de información | 5 | 5 | 4 | 5 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | ALTO |
| 8 | Código ejecutable | 3 | 3 | 3 | 1 | 1 | 2 | 2 | 3 | 3 | 3 | 2 | 3 | 3 | MEDIO |
| 9 | Correo electrónico | 3 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | MEDIO |
| 10 | Gestión de privilegios | 5 | 5 | 5 | 4 | 4 | 5 | 2 | 3 | 4 | 5 | 5 | 4 | 5 | ALTO |
| 11 | Base de Datos | 2 | 3 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | ALTO |
| 12 | Página Web | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 3 | 5 | 3 | 3 | 5 | 5 | ALTO |
| 13 | Sistema de trámite documentario | 1 | 4 | 3 | 4 | 3 | 2 | 5 | 3 | 3 | 4 | 4 | 5 | 5 | ALTO |
| 14 | Sistema de Registro de visitas | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 1 | 1 | 3 | 3 | MEDIO |
| 15 | SIAF | 4 | 4 | 4 | 5 | 4 | 3 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | ALTO |
| 16 | Sistema de Catastro virtual y ficha catastral | 1 | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 2 | 3 | 3 | 2 | 3 | MEDIO |
| 17 | Aplicaciones Comerciales | 2 | 2 | 1 | 1 | 1 | 1 | 5 | 5 | 5 | 2 | 1 | 5 | 5 | ALTO |
| 18 | Gestor de máquinas virtuales | 2 | 1 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | MEDIO |
| 19 | Scripts de backup | 1 | 2 | 2 | 2 | 1 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 3 | MEDIO |
| 20 | Servidores de aplicaciones de Producción | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 5 | ALTO |
| 21 | Servidor de Base de Datos | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | ALTO |
| 22 | Servidor de Pruebas | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 3 | MEDIO |
| 23 | Servidor de Desarrollo | 1 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | MEDIO |
| 24 | Computador del Funcionario | 2 | 3 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | ALTO |
| 25 | Computadores administradores de SI | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | ALTO |
| 26 | Computadores de escritorio usuarios | 1 | 3 | 1 | 1 | 2 | 3 | 1 | 3 | 3 | 3 | 3 | 3 | 3 | MEDIO |
| 27 | Impresoras | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 2 | 2 | 1 | 1 | 3 | 3 | MEDIO |
| 28 | Firewall | 4 | 4 | 3 | 4 | 3 | 3 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | ALTO |
| 29 | Soporte de la red | 1 | 1 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | MEDIO |
| 30 | Centralita telefónica | 3 | 3 | 3 | 1 | 1 | 1 | 2 | 2 | 3 | 3 | 1 | 3 | 3 | MEDIO |
| 31 | Red inalámbrica | 2 | 2 | 2 | 2 | 1 | 2 | 3 | 2 | 3 | 2 | 2 | 3 | 3 | MEDIO |
| 32 | Red local | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 2 | 3 | 1 | 1 | 3 | 3 | MEDIO |
| 33 | Internet | 1 | 1 | 1 | 1 | 1 | 1 | 4 | 3 | 4 | 1 | 1 | 4 | 4 | ALTO |

Nota: Elaboración Propia. E=Económico, L=Legal, IMG=Imagen, VFC=Valor final de confiabilidad, VFI=Valor final de integridad, VFD=Valor final de disponibilidad, VF=Valor final del activo de información.

De la Tabla 4.10:

- El valor de la columna VFC (valor final de confiabilidad), corresponde al máximo valor de los aspectos: económico, legal e imagen, que afectan a la seguridad del activo en su dimensión de confiabilidad. Este mismo criterio se siguió para obtener los valores de VFI (valor final de integridad) y VFD (valor final de disponibilidad) cada uno dentro de la dimensión que le corresponde.
- El valor de VF (valor final del activo de información), es el máximo valor de VFC, VFI y VFC.
- El nivel de criticidad del activo se obtiene de acuerdo a la Tabla 4.9.

Terminada la valoración de los activos de información, se seleccionó aquellos activos con nivel de criticidad alto y medio, para luego agruparlos en los activos que lo contienen. El resultado de esta actividad se muestra en la Tabla 4.11.

**Tabla 4. 11**

*Activos por contenedor*

| ACTIVO DE INFORMACION | CONTENEDOR |
|---|---|
| Servidores de aplicaciones de Producción (EQ) alto | Data Center (INSTALACION) alto |
| Servidor de Base de Datos (HW) alto | |
| Firewall (HW) alto | |
| Disco duro externo (SOP_INF) alto | |
| Servidor de Pruebas (HW) medio | |
| Servidor de Desarrollo (HW) (servidor de versiones) | |
| Soporte de la red (HW) medio | |
| Centralita telefónica (HW) medio | |
| Sistema de aire acondicionado (AUX) medio | |
| Copias de Respaldo (D) alto | Servidores/disco duro externo/PC administrador |
| Datos de control de acceso (D) alto | Servidor de Base de Datos / usuario interno |
| Base de Datos (S) alto | Servidores de Base de datos |
| Página Web (SW) alto | VPS servidor proveedor |
| Sistema de trámite documentario (SW) | Servidor de aplicaciones Windows |
| SIAF (SW) alto | Servidor de aplicaciones SIAF |
| Discos Virtuales (SOP_INF) medio | Servidor Virtual |
| Código ejecutable (D) medio | Servidor de desarrollo |
| Correo electrónico (S) medio | Servidor de correo electrónico proveedor |
| Sistema de Registro de visitas (SW) medio | Servidor de aplicaciones Linux |

*Tabla 4. 11 Continuación*

| ACTIVO DE INFORMACION | CONTENEDOR |
|---|---|
| Sistema de Catastro virtual y ficha catastral (SW) | Servidor de aplicaciones catastro |
| Credenciales (contraseñas) (D) | PC administrador |
| Gestor de máquinas virtuales (SW) | PC administrador |
| Scripts de backup (SW) medio | PC administrador |
| Código fuente de los sistemas de información (D) | PC desarrolladores/Servidor de versiones (nube) |
| Gestión de privilegios (S) | Recursos tecnológicos y aplicaciones |
| Aplicaciones Comerciales (SW) | Computadores Personales |
| Computador del funcionario (HW) | Local Subgerencia |
| Computadores administradores de SI (HW) | Local Subgerencia |
| Personal de soporte técnico (P) | Local Subgerencia |
| Administradores de las plataformas (P) | Local Subgerencia |
| Desarrolladores/Programadores (P) | Local Subgerencia |
| Computadores de escritorio usuarios (HW) | Local Subgerencia |
| Impresoras (HW) | Local Subgerencia |
| Proveedores (P) | Externo |
| Datos de Gestión interna (D) | Estantería |
| Dispositivos de almacenamiento externo (SOP_INF) | |
| Datos de Configuración de los Sistemas de Información (D) | |
| Material impreso (SOP_INF) | |
| Log de los sistemas de información (D) | Log de Eventos servidores |
| ADSL (COM) | Red LAN |
| Red local (COM) | |
| Internet | Data center, Local MPH |
| Sistema de alimentación ininterrumpida (AUX) | Data Center/Local subgerencia |
| Usuarios Internos (P) | Oficinas MPH |

Nota: Elaboración propia

De acuerdo a lo anterior, los siguientes fueron los contenedores y/o activos de información que se seleccionaron para el proceso de valoración de riesgos.

1. Data Center
2. Local de la Subgerencia
3. Copias de respaldo
4. Servidor de aplicaciones
5. Servidor de Bases de Datos
6. Bases de Datos
7. Firewall/Soportes de la red
8. Disco duro externo
9. Datos de control de acceso al sistema
10. Página Web
11. Servidor Virtual
12. Credenciales
13. Código Fuente

14. Computadores Personales
15. Datos de Gestión
16. LAN
17. Correo electrónico
18. Estantería
19. SIAF
20. Sistema de trámite documentario
21. Script de backup
22. Administradores de las plataformas
23. Usuarios internos

#### *4.3.1.3. Identificación y valoración de amenazas*

Es esta etapa, para identificar las amenazas que afectan a los activos de información, se elaboró una lista de amenazas, de acuerdo al catálogo de amenazas contemplado en MARGERIT V.3 (ver Anexo H).

Luego, junto con el personal de sistemas y tecnología de la MPH, se procedió a identificar aquellas amenazas que afectan a los activos valorados en el ítem anterior y se determinó la probabilidad de ocurrencia de estas amenazas.

Para determinar la probabilidad de que estas amenazas se materialicen se estableció el criterio mostrado en la Tabla 4.12.

**Tabla 4. 12**

*Probabilidad de materialización de amenazas*

| PROBABILIDAD DE QUE SE MATERIALICE LA AMENAZA | | |
|---|---|---|
| **CRITERIO** | **VALOR** | **PUNTUACIÓN** |
| Más de 2 años | Prácticamente Imposible | 1 |
| Anual | Poco Probable | 2 |
| Trimestral | Posible | 3 |
| Mensual | Probable | 4 |
| A diario | Muy probable | 5 |

Nota: Elaboración Propia

A continuación, se muestra en la Tabla 4.13, la relación de amenazas identificadas, la dimensión de seguridad en que se ve afectado el activo [1] y, la probabilidad de materialización de las amenazas. El Anexo I de este documento, contiene la tabla general de identificación de amenazas, riesgos y consecuencias.

**Tabla 4. 13**

*Identificación de amenazas*

| CÓDIGO | AMENAZA | DIMENSIONES AFECTADAS | | | PROBABILIDAD DE OCURRENCIA |
|---|---|---|---|---|---|
| | | C | I | D | |
| 1 | Fuego | | | 1 | 1 |
| 2 | Tormenta eléctrica, rayos | | | 1 | 3 |
| 3 | Error de Usuario | 2 | 1 | 3 | 4 |
| 4 | Errores del administrador | 3 | 2 | 1 | 2 |
| 5 | Errores de configuración | | 1 | | 2 |
| 6 | Alteración accidental de la información | | 1 | | 2 |
| 7 | Eliminación accidental de Información | | | 1 | 4 |
| 8 | Fugas de Información | 1 | | | 4 |
| 9 | Vulnerabilidades de los programas (software) | 3 | 1 | 2 | 3 |
| 10 | Errores de mantenimiento/actualización de programas (software) | | 1 | 2 | 3 |
| 11 | Errores de mantenimiento/actualización de equipos (hardware) | | | 1 | 4 |
| 12 | Indisponibilidad del personal por enfermedad | | | 1 | 3 |
| 13 | Manipulación de los registros de Actividad (log) | | 1 | | 1 |
| 14 | Suplantación de la identidad del usuario | 1 | 3 | 2 | 2 |
| 15 | Abuso de privilegios de acceso | 1 | 2 | 3 | 4 |
| 16 | Difusión de software dañino | 3 | 2 | 1 | 4 |
| 17 | Acceso no autorizado | 1 | 2 | | 1 |
| 18 | Destrucción deliberada de Información | | | 1 | 1 |
| 19 | Manipulación de programas | 1 | 2 | 3 | 2 |
| 20 | Caída del sistema por agotamiento de recursos | | | 1 | 3 |
| 21 | Robo de Equipos | 2 | | 1 | 2 |
| 22 | Indisponibilidad del personal por huelga | | | 1 | 2 |
| 23 | Ejecución de ingeniería social | 1 | 2 | 3 | 2 |
| 24 | Corte del suministro eléctrico | | | 1 | 4 |
| 25 | Condiciones inadecuadas de temperatura o humedad | | | 1 | 3 |
| 26 | Degradación de los soportes de almacenamiento de la información | | | 1 | 2 |
| 27 | Instalación de software no autorizado | 1 | 2 | | 4 |
| 28 | Inestabilidad de la línea de internet | | | 1 | 4 |

Nota: Elaboración propia. C=Confidencialidad, I=integridad, D=disponibilidad.

[1] Las amenazas pueden afectar a los activos de información en uno, dos, o sus tres dimensiones de seguridad. Para efectos de esta investigación, se muestra la(s) dimensión(es) de seguridad afectada en orden de relevancia, donde 1 es muy relevante, 2 medianamente relevante y 3 poco relevante.

Como no todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir, se clasificó las amenazas por activo de información.

Finalmente, se valoró la degradación[2] de cada activo de acuerdo al criterio de la Tabla 4.14. El resultado final de esta valoración se muestra la Tabla 4.15.

**Tabla 4. 14**

*Criterio para valorar la degradación del activo*

| CRITERIO | VALOR |
|---|---|
| Sin degradación (SD) | 1 |
| Degradación baja (B) | 2 |
| Degradación media (M) | 3 |
| Degradación alta (A) | 4 |

Nota: Elaboración Propia

[2] Cuan perjudicado resultaría el activo

**Tabla 4. 15**

*Degradación de los activos: Data Center y SIAF*

| DATA CENTER | | | | |
|---|---|---|---|---|
| **Amenazas** | **Probabilidad** | **Degradación Confidencialidad** | **Degradación Integridad** | **Degradación Disponibilidad** |
| Fuego | 1 | 1 | 1 | 4 |
| tormenta eléctrica, rayos | 3 | 1 | 1 | 4 |
| Errores del administrador | 2 | 1 | 2 | 4 |
| Suplantación de la identidad del usuario | 2 | 4 | 2 | 3 |
| Abuso de privilegios de acceso | 4 | 3 | 3 | 1 |
| Acceso no autorizado | 1 | 4 | 2 | 1 |
| Robo de Equipos | 2 | 2 | 1 | 4 |
| Corte del suministro eléctrico | 4 | 1 | 4 | 4 |
| Condiciones inadecuadas de temperatura o humedad | 3 | 1 | 4 | 4 |
| **SIAF** | | | | |
| **Amenazas** | **Probabilidad** | **Degradación Confidencialidad** | **Degradación Integridad** | **Degradación Disponibilidad** |
| Error de Usuario | 4 | 3 | 3 | 1 |
| Errores del administrador | 2 | 1 | 2 | 4 |
| Errores de configuración | 2 | 1 | 4 | 1 |
| Errores de mantenimiento/actualización de programas (software) | 3 | 1 | 3 | 1 |
| Indisponibilidad del personal por enfermedad | 3 | 1 | 1 | 3 |
| Suplantación de la identidad del usuario | 2 | 4 | 1 | 3 |
| Abuso de privilegios de acceso | 4 | 4 | 2 | 1 |
| Acceso no autorizado | 1 | 4 | 3 | 1 |
| Caída del sistema por agotamiento de recursos | 3 | 1 | 1 | 4 |
| Corte del suministro eléctrico | 4 | 1 | 1 | 4 |

Nota: Elaboración Propia

#### *4.3.1.4. Cálculo del impacto*

En este ítem, se calculó el impacto, que viene dado en función del valor del activo y la degradación que producirá la amenaza en caso de materializarse. Para ello se estableció el siguiente criterio:

**Tabla 4. 16**

*Criterio para calcular el impacto*

| DEGRADACIÓN DE LA AMENAZA | VALOR DEL ACTIVO | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 1 (Sin degradación) | 1 | 1 | 1 | 1 | 1 |
| 2 (Degradación baja) | 1 | 2 | 2 | 3 | 4 |
| 3 (degradación media) | 1 | 2 | 3 | 4 | 4 |
| 4 (degradación alta) | 1 | 3 | 4 | 4 | 5 |

Nota: Elaboración propia

**Tabla 4. 17**

*Valor del Impacto*

| VALOR | DESCRIPCIÓN |
|---|---|
| 1 | Insignificante |
| 2 | Menor |
| 3 | Medio |
| 4 | Crítico |
| 5 | Catastrófico |

Nota: Elaboración propia

Conviene aclarar, que esta valoración se calculó sin considerar las posibles medidas de seguridad que actualmente se estén aplicando. De esta manera se trata de calcular el máximo riesgo para cada uno de los activos.

En la Tabla 4. 20 se muestra el resultado del impacto para los activos Data Center y SIAF.

### *4.3.1.5. Cálculo del riesgo*

El cálculo del riesgo está en función del impacto que se producirá sobre el activo en caso de materializarse y de la probabilidad de materialización.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo. Para la presente investigación se elaboró la siguiente matriz de evaluación de riesgos:

**Tabla 4. 18**

*Matriz de evaluación de riesgos*

| IMPACTO | | MATRIZ DE EVALUACIÓN DE RIESGOS | | | | |
|---|---|---|---|---|---|---|
| Catastrófico | 5 | 15 | 19 | 22 | 24 | 25 |
| Crítico | 4 | 10 | 14 | 18 | 21 | 23 |
| Medio | 3 | 6 | 9 | 13 | 17 | 20 |
| Menor | 2 | 3 | 5 | 8 | 12 | 16 |
| Insignificante | 1 | 1 | 2 | 4 | 7 | 11 |
| | | 1 | 2 | 3 | 4 | 5 |
| | | Prácticamente imposible | Poco probable | Posible | Probable | Muy Probable |
| | | PROBABILIDAD (DE LA AMENAZA) = FUTURO | | | | |

Nota: Elaboración Propia

En la matriz anterior se puede distinguir tres niveles de riesgo: alto, medio y bajo. Estos niéveles fueron asignado de acuerdo al siguiente criterio

**Tabla 4. 19**

*Niveles de riesgos*

| CRITERIO | NIVEL |
|---|---|
| 17<Nivel de riesgo<=25 | Alto |
| 8<Nivel de riesgo<=17 | Medio |
| 0<Nivel de riesgo<=8 | Bajo |

Nota: Elaboración propia

Usando la matriz de evaluación de riesgos, se valoró el riesgo inherente a las amenazas asociadas (clasificadas por activos).

En la Tabla 4. 20 se muestra el resultado de la valoración de riesgo para los activos Data Center y SIAF.

Finalmente se identificó los activos con mayores riesgos y, las amenazas que causan esos riesgos. En el Figura 4.30 se puede observar la cantidad de riesgos altos, medios y bajos y, el total de riesgos por activo.

**Tabla 4. 20**

*Impacto y riesgo para el Data Center y SIAF*

| DATA CENTER | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Amenazas | Probabilidad | Degradación | | | Impacto | | | Estimación del Riesgo | | | |
| | | Confidencialidad | Integridad | Disponibilidad | Confidencialidad | Integridad | Disponibilidad | Confidencialidad | Integridad | Disponibilidad | |
| Fuego | 1 | 1 | 1 | 4 | Insignificante | Insignificante | Catastrófico | Bajo | Bajo | Medio | |
| tormenta eléctrica, rayos | 3 | 1 | 1 | 4 | Insignificante | Insignificante | Catastrófico | Bajo | Bajo | **Alto** | |
| Errores del administrador | 2 | 1 | 2 | 4 | Insignificante | Crítico | Catastrófico | Bajo | Medio | **Alto** | |
| Suplantación de la identidad del usuario | 2 | 4 | 2 | 1 | Catastrófico | Crítico | Insignificante | **Alto** | Medio | Bajo | |
| Abuso de privilegios de acceso | 4 | 3 | 3 | 1 | Crítico | Crítico | Insignificante | **Alto** | **Alto** | Bajo | |
| Acceso no autorizado | 1 | 4 | 2 | 1 | Catastrófico | Crítico | Insignificante | Medio | Medio | Bajo | |
| Robo de Equipos | 2 | 2 | 1 | 1 | Crítico | Insignificante | Insignificante | Medio | Bajo | Bajo | |
| Corte del suministro eléctrico | 4 | 1 | 1 | 1 | Insignificante | Insignificante | Catastrófico | Bajo | Bajo | Alto | |
| Condiciones inadecuadas de temperatura o humedad | 3 | 1 | 1 | 1 | Insignificante | Insignificante | Catastrófico | Bajo | Bajo | Alto | |
| **SIAF** | | | | | | | | | | | |
| Error de Usuario | 4 | 3 | 3 | 1 | Crítico | Crítico | Insignificante | **Alto** | **Alto** | Bajo | |
| Errores del administrador | 2 | 1 | 2 | 4 | Insignificante | Crítico | Catastrófico | Bajo | Medio | **Alto** | |
| Errores de configuración | 2 | 1 | 4 | 1 | Insignificante | Catastrófico | Insignificante | Bajo | **Alto** | Bajo | |
| Errores de mantenimiento/actualización de programas (software) | 3 | 1 | 3 | 1 | Insignificante | Crítico | Insignificante | Bajo | **Alto** | Bajo | |
| Indisponibilidad del personal por enfermedad | 3 | 1 | 1 | 3 | Insignificante | Insignificante | Crítico | Bajo | Bajo | **Alto** | |
| Suplantación de la identidad del usuario | 2 | 4 | 1 | 3 | Crítico | Insignificante | Crítico | Medio | Bajo | Medio | |
| Abuso de privilegios de acceso | 4 | 4 | 2 | 1 | Crítico | Crítico | Insignificante | **Alto** | **Alto** | Bajo | |
| Acceso no autorizado | 1 | 4 | 3 | 1 | Crítico | Crítico | Insignificante | Medio | Medio | Bajo | |
| Caída del sistema por agotamiento de recursos | 3 | 1 | 1 | 4 | Insignificante | Insignificante | Catastrófico | Bajo | Bajo | **Alto** | |
| Corte del suministro eléctrico | 4 | 1 | 1 | 4 | Insignificante | Insignificante | Catastrófico | Bajo | Bajo | **Alto** | |

Nota: Elaboración Propia

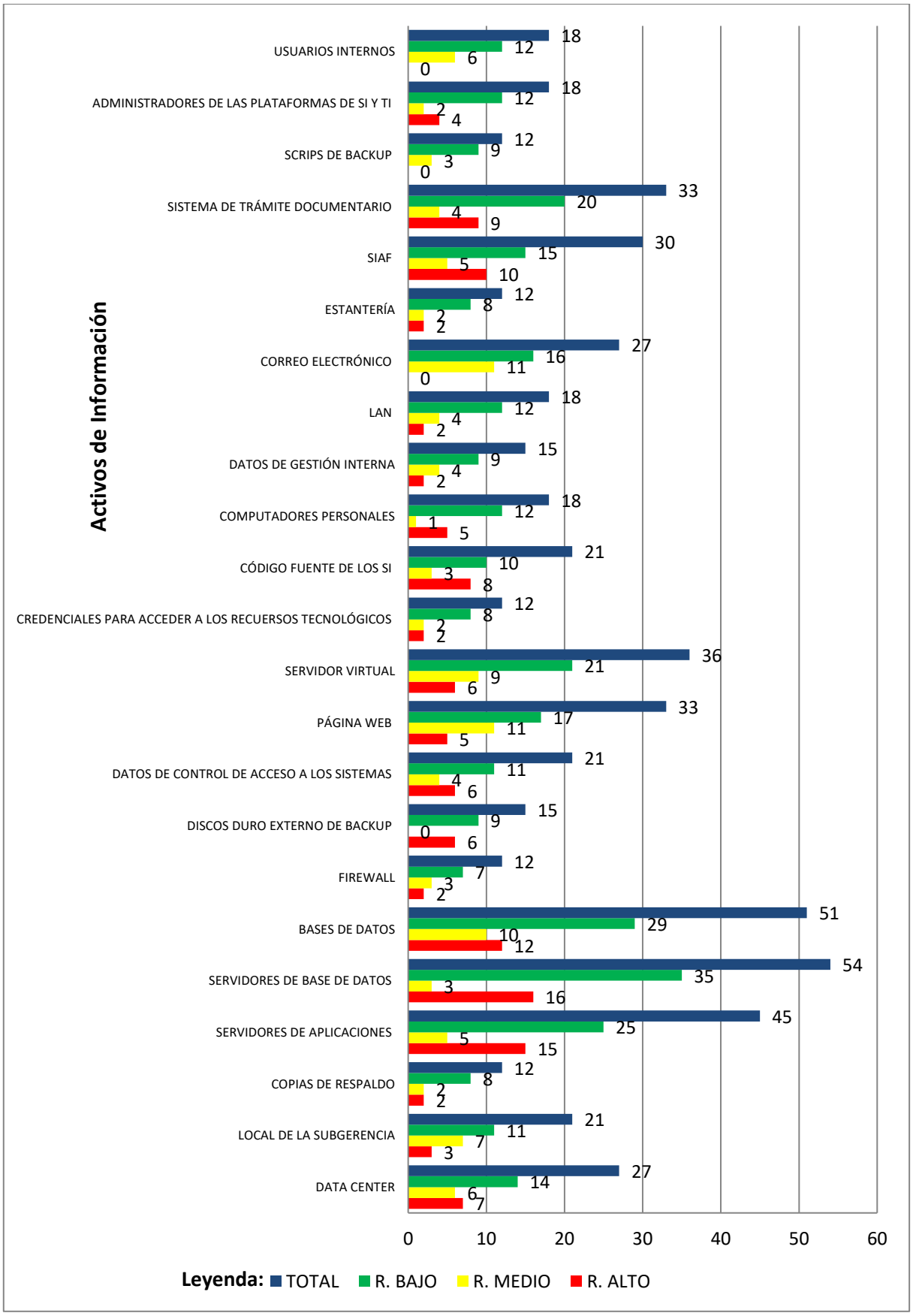


*Figura4. 30.* Riesgos por activo

Elaboración propia

En el gráfico anterior, se puede observar que el activo servidor de base de datos está expuesto a una mayor cantidad de riesgos. A continuación, se muestran las amenazas que ocasionan estos riesgos.

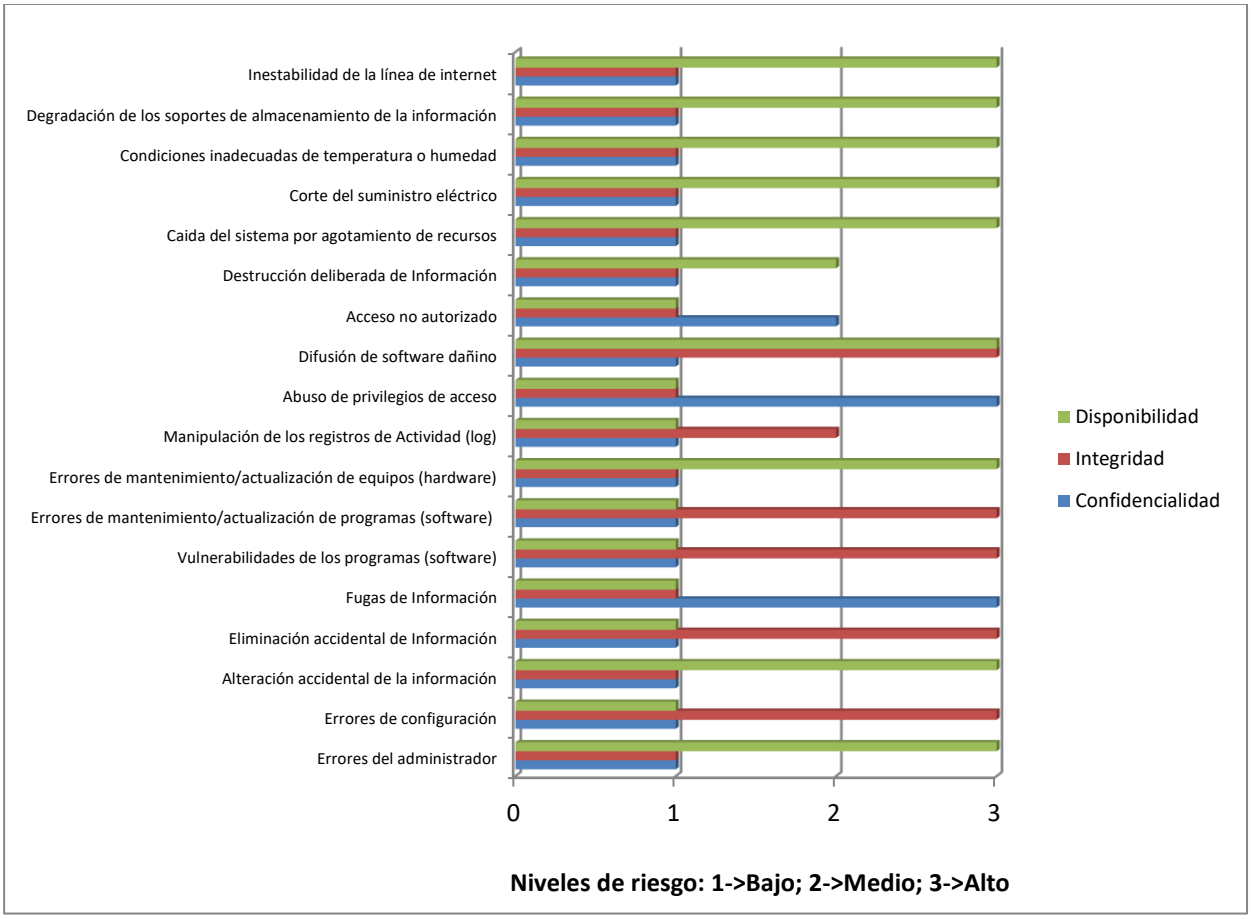


*Figura 4. 31.* Amenazas y niveles de riesgo para el activo servidor de Base de Datos

Fuente: Elaboración propia

### 4.3.2. Propietarios del riesgo

En esta etapa, se identificó al propietario del riesgo, éste es el responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgos (para reducir los riesgos a un nivel aceptable).

Para este proyecto de investigación, se determinó que el único propietario del riesgo es la sub gerencia de Sistemas y Tecnología de la Municipalidad Provincial de Huamanga.

### 4.3.3. Tratamiento de los riesgos

De acuerdo a la naturaleza del riesgo, las opciones para tratarlos pueden ser: eliminar, transferir, mitigar o asumir el riesgo.

**Tabla 4. 21**

*Jerarquía de controles*

| TRATAMIENTO | DESCRIPCIÓN |
|---|---|
| Eliminar | Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un activo, proceso o del área del negocio que es fuente de riesgo. |
| Transferir | El riesgo fuera del apetito del riesgo se comparte con una o varias partes, pueden ser agentes externos. |
| Mitigar | Reducir el riesgo cuando se encuentra fuera del apetito del riesgo, se puede cambiar la probabilidad de ocurrencia o cambiar las consecuencias. |
| Asumir | En este escenario se decide aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó. |

Nota: Adaptado de "*Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013",* p.50, Justino Salinas. 2015.

En el presente trabajo de investigación, dados los valores y niveles de riesgos obtenidos, se estableció como máximo riesgo asumible los riesgos de nivel bajo; para todos los riesgos que tienen niveles medio y alto se aplicarán controles, que ayuden a reducir el riesgo producido por las amenazas a un nivel aceptable, en las dimensiones afectadas.

Se priorizará el tratamiento de los riesgos de nivel alto, a estos es necesario aplicarles de manera urgente todas las medidas de seguridad posibles. Asimismo, cabe mencionar que los riesgos de nivel bajo serán monitoreados para evitar que su impacto y probabilidad crezcan con el tiempo.

### 4.3.4. Determinar los controles y declaración de aplicabilidad

En este apartado, se determinó, en función de las amenazas identificadas, los controles que ayudarán a reducir los riesgos a un nivel aceptable. En la Tabla 4.22 se muestran los controles para reducir los riesgos del servidor de base de datos. El Anexo J contiene controles para reducir los riesgos de los otros activos.

**Tabla 4. 22**

*Controles para el tratamiento de riesgos del servidor de base de datos.*

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Estimación del Riesgo | | | Jerarquía de Control | Control alineado a la NTP ISO/IEC 27001:2014 | Control Específico | Responsable |
| | | | | | | Confidencialidad | Integridad | Disponibilidad | | | | |
| Servidores de Bases de Datos | 5 | 5 | 5 | Errores del administrador | No existe un plan/manual de las BDs que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios, desmotivación | Bajo | Bajo | **Alto** | Mitigar | A.8.2 Clasificación de la información<br>A.12.4.3 Registros del administrador y del operador | Manual de sistemas y requerimientos técnicos.<br>Elaboración de un procedimiento formal de control de cambios.<br>Elaboración de un procedimiento formal de manejo de servidores<br>Capacitación en temas de seguridad. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Errores de configuración | Inexistencia de plan de configuración y manejo de log | Bajo | **Alto** | Bajo | Mitigar | A.12.4.3 Registros del administrador y del operador.<br>A.12.4.1 Registro de eventos. | Elaboración del manual de configuración de servidores.<br>Actualización de log de eventos. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Alteración accidental de la información | Inexistencia de normas de seguridad, mala configuración de roles y permisos. | Bajo | Bajo | **Alto** | Mitigar | A.8.2 Clasificación de la información<br>A.12.4.3 Registros del administrador y del operador.<br>A.12.4.1 Registro de eventos. | Control de versiones del software.<br>Procedimiento formal de control de cambios.<br>Verificación de roles y permisos. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Eliminación accidental de Información | Inexistencia de normas de seguridad y plan de contingencia. | Bajo | **Alto** | Bajo | Mitigar | A.8.2 Clasificación de la información<br>A.12.4.3 Registros del administrador y del operador.<br>A.12.4.1 Registro de eventos. | Control de versiones del software.<br>Procedimiento formal de control de cambios.<br>Verificación de roles y permisos. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Fugas de Información | Inadecuada administración de seguridad, contraseñas no seguras, inexistencia de los de eventos de seguridad. | **Alto** | Bajo | Bajo | Mitigar | A. 12.4.3 Registros del administrador y del operador<br>A.7.2.3 Proceso disciplinario. | Establecimiento de métodos de cifrado y backup.<br>Gestión de Permisos.<br>Procedimientos disciplinarios establecidos en los contratos. | Oficial de seguridad/ Administrador de Servidores de BD |

*Tabla 4.22 Continuación.*

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Nombre del Activo** | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Amenaza** | **Vulnerabilidad** | **Estimación del Riesgo** | | | Jerarquía de Control | Control alineado a la NTP ISO/IEC 27001:2014 | Control Específico | Responsable |
| | | | | Vulnerabilidades de los programas (software) | Falta de licencia, inexistencia de monitorización de software/versiones. | Bajo | **Alto** | Bajo | Mitigar | A.14.2.4 Restricción sobre cambios a los paquetes software. A.16.6.1 Gestión de vulnerabilidades técnicas. | Adquisición de licencia de programas y/o evaluación del uso de software libre. Gestión de vulnerabilidades | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Errores de mantenimiento/actualización de programas (software) | Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica. | Bajo | **Alto** | Bajo | Mitigar | A.16.6.1 Gestión de vulnerabilidades técnicas | Elaboración de un plan de mantenimiento y actualización de software. Elaboración de un plan de contingencia. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Errores de mantenimiento/actualización de equipos (hardware) | Inexistencia de plan de mantenimiento y vigilancia tecnológica, falta de equipos de contingencia, ausencia de un sistema de continuidad del negocio. | Bajo | Bajo | **Alto** | Mitigar | A.11.2.4 Mantenimiento de equipos A.16.6.1 Gestión de vulnerabilidades técnicas | Elaboración de un Plan de contingencia – Equipos de contingencia. Plan de mantenimiento de hardware | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Manipulación de los registros de Actividad (log) | Inexistencia de auditorías a las cuentas de usuario, inexistencia de mecanismos de cifrado. | Bajo | Medio | Bajo | Mitigar | A.12.4.2 Protección de información de registros. | Establecer controles para evitar accesos no autorizados la información de los registros. Mecanismos de cifrado. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Abuso de privilegios de acceso | Falta de políticas de acceso y auditorías internas. (cuentas de usuario sin auditar) | **Alto** | Bajo | Bajo | Mitigar | A.7.2.3 Proceso disciplinario A.9.4.1 Restricción de acceso a la información. | Elaboración de políticas de acceso. Diseñar esquemas de seguridad basado en roles y permisos Diseñar un esquema de privilegios sobre el fileserver | Oficial de seguridad/ Administrador de Servidores de BD/ Jefe de RR.HH |
| | | | | Difusión de software dañino | falta de monitoreo del estado y reglas del firewall y antivirus, inadecuada asignación de roles y permisos, no existe políticas de seguridad. | Bajo | **Alto** | **Alto** | Mitigar | A.12.2.2 Controles contra códigos maliciosos. A.16.6.2 Restricción sobre la instalación de software | Plataforma de seguridad perimetral. Control de la red. Control de instalación de software. Actualización de antivirus (monitorización) | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Acceso no autorizado | Falta de monitoreo del estado y reglas del firewall, | Medio | Bajo | Bajo | Mitigar | A.14.2.8 Pruebas de seguridad del | Diseñar esquemas de seguridad basado en roles y | Oficial de seguridad/ Administrador de |

*Tabla 4.22 Continuación.*

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | antivirus, configuración incorrecta de las cuentas de usuario. | | | | | sistema. | permisos<br>Diseñar un esquema de privilegios sobre el fileserver.<br>Plataforma de seguridad perimetral. | Servidores de BD |
| | | | | Destrucción deliberada de Información | Administradores de plataformas descontentos, inexistencia de un sistema de continuidad del negocio, falta de seguridad en los soportes de red. | Bajo | Bajo | Medio | Mitigar | A.7.2.3 Proceso disciplinario | Establecimiento de métodos de cifrado y backup.<br>Procedimientos disciplinarios establecidos en los contratos. | Oficial de seguridad/ Administrador de Servidores de BD/ Jefe de RR.HH |
| | | | | Caida del sistema por agotamiento de recursos | No existe un monitoreo de consumo de recursos hardware de los sistemas, falta de mantenimiento de equipos. | Bajo | Bajo | Alto | Mitigar | A.11.2.3 Seguridad del cableado.<br>A.13.1.3 Segregación en redes. | Plataforma de seguridad perimetral.<br>Elaboración de un Plan de contingencia – monitoreo preventivo de consumo de recursos Hardware de los sistemas. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Corte del suministro eléctrico | Susceptibilidad a las variaciones de tensión. | Bajo | Bajo | Alto | Mitigar | A.11.2.2 Servicios de suministro | Contar con sistema de alimentación ininterrumpida.<br>Mantenimiento de sistema de alimentación ininterrumpida. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Condiciones inadecuadas de temperatura o humedad | Susceptibilidad a humedad, recalentamiento, polvo y suciedad | Bajo | Bajo | Alto | Mitigar | A.11.2.1 Emplazamiento y protección de los equipos.<br>A.11.2.4 Mantenimiento de equipos | Ubicación adecuada de equipos según estándares internacionales.<br>Plan de mantenimiento de equipos. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Degradación de los soportes de almacenamiento de la información | Equipos/dispositivos susceptibles a cambios de temperatura y humedad, falta de esquemas de reemplazo. | Bajo | Bajo | Alto | Mitigar | A.11.2.4 Mantenimiento de equipos | Plan de mantenimiento de soportes de información.<br>Inventario de activos y monitoreo del funcionamiento y tiempo de vida. | Oficial de seguridad/ Administrador de Servidores de BD |
| | | | | Inestabilidad de la línea de internet | Un solo proveedor de servicios de comunicaciones, gestión inadecuada de la red. | Bajo | Bajo | Alto | Mitigar | A.13.1.2 Seguridad de servicios de red. | Plan de contingencia- Uso de varias líneas dedicadas y redundancia de servicios con diversos proveedores del servicio. – balanceo de carga.<br>Acuerdos de nivel de servicio con el(los) proveedor(es) de comunicaciones | Oficial de seguridad/ Administrador de Servidores de BD |

Nota: Elaboración propia.

Finalmente se elaboró la declaración de aplicabilidad según lo contemplado en el requisito 6.1.3 ítem d) de la NTP ISO/IEC 27001:2014, esta declaración de aplicabilidad incluye todos los controles necesarios identificados, así como la justificación de la inclusión o exclusión de los controles del Anexo A.

Este documento puede ser revisado en el Anexo K del presente proyecto de investigación. La declaración de aplicabilidad contempla la siguiente información:

- ✓ Sección: Contiene el identificador de sección de los controles propuestos por la en el Anexo A de la NTP ISO/IEC 27001:2014.
- ✓ Objetivo: Es el objetivo de control.
- ✓ Control: Es el nombre del control propuesto por la norma para lograr el objetivo de control y este hace referencia a un tema específico al que un riesgo puede estar relacionado.
- ✓ Estado: Menciona el estado del control dentro de la MPH, es decir si está aplicado, se va a aplicar o no.
- ✓ Justificación: La justificación de la aplicabilidad o no aplicabilidad del control en mención.

# Capítulo V
# Conclusiones y recomendaciones

## 5.1 Conclusiones

a. Se determinó como características esenciales del diseño del SGSI para la Municipalidad Provincial de Huamanga, el compromiso y apoyo de la alta dirección, el conocimiento de la organización, la adecuada identificación del alcance del SGSI, la evaluación de riesgos y la mejora continua.

b. Luego de analizar las áreas funcionales de la Municipalidad Provincial de Huamanga, se identificó como alcance del SGSI el proceso de gestión de infraestructura tecnológica, siendo responsable de este proceso la Subgerencia de Sistemas y Tecnología.

c. El análisis y gestión de riesgos es la columna vertebral de un sistema de gestión de seguridad de la información, porque permitió cuantificar el riesgo. Es decir, es un indicador estadístico que mide la incertidumbre. En este trabajo de investigación la evaluación de riesgos, adoptando MARGERIT V.3 como metodología de análisis y gestión de riesgos, permitió identificar y valorar los activos, identificar y valorar las amenazas, calcular el impacto e identificar los riesgos a los que se encuentra expuesta la Municipalidad Provincial de Huamanga. Asimismo, el uso de MARGERIT permitió contar con la documentación (sobre evaluación de riesgos) exigida por la NTP ISO/IEC 27001:2014.

d. Teniendo en cuenta los riesgos identificados, se elaboró los controles de seguridad para mitigar los riesgos altos y medios (Ver Tabla 4.22). Asimismo, los controles de seguridad de la ISO 27002, permiten establecer métricas, que ayuden a medir la eficacia y eficiencia del SGSI una vez implementados.

## 5.2 Recomendaciones

a. Los procedimientos utilizados en esta investigación pueden ser usados para diseñar los SGSI de otras municipalidades.

b. Se recomienda, a los responsables del área de TI de las entidades públicas, adoptar los lineamientos propuestos por la NTP ISO/IEC 27001:2014, por tener carácter de obligatoriedad.

c. Evaluando las necesidades de la entidad. Se recomienda complementar este trabajo de investigación, con el establecimiento de políticas, directivas y la adopción de buenas prácticas como ITIL V.3 y COBIT.

d. Durante el desarrollo de este trabajo de investigación, se observó la necesidad que tiene la MPH, de implementar un SGSI y contar con los documentos de gestión referentes a la seguridad de la información. Se recomienda contratar los servicios de una consultora que le guíe en la implementación exitosa de la norma.

e. Dentro de la organización existe un personal que hace las veces de oficial de seguridad de la información, pero a su vez está encargado de otras funciones y tareas, se recomienda a la Sub Gerente de Sistemas y Tecnología segregar y definir claramente las funciones y responsabilidades del oficial de seguridad de la información.

f. Como gran parte de la seguridad depende de las personas, se recomienda generar conciencia de seguridad de información en los funcionarios y trabajadores de la entidad, mediante capacitaciones y charlas informativas.

g. Es necesario que la Municipalidad Provincial de Huamanga asigne presupuesto para la implantación del SGSI (establecimiento de controles, capacitaciones, mantenimiento, mejora continua).

## Referencias bibliográficas


Aguirre Mollehuanca, D. A. (2014). *Diseño de un sistema de gestión de seguridad de información para Servicios Postales del PERÚ S.A* (Tesis de grado). Pontificia Universidad Católica del Perú, Lima, Perú.

ANSSI. (2016). *EBIOS – Expression des besoins et identification des objectifs de sécurité.* Recuperado de: http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

Barragán P., Góngora Z. y Martínez C. (2011). *Implementación de Políticas de Seguridad Informática para la Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002* (Tesis de grado). Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador.

Bernal Torres, C. A. (2010). *Metodología de la Investigación* (Tercera ed.). Colombia: Pearson Educación

Carnegie Mellon University. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Recuperado de: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Carrasco Díaz, S. (2006). *Metodología de la Investigación Científica*. Lima, Perú: Editorial San Marcos.

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración*. Mexico: McGraw-Hill Interamericana.

Contraloría General de la República. (s.f.). *La contraloría.* Recuperado de: http://www.contraloria.gob.pe/wps/portal/portalcgrnew/siteweb/contraloria/queeslacontraloria/!ut/p/b1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOLdXf29TZwNjAz8_QNNDDzNjUKNDB2DDEyDDYEKIoEKDHAARwNC-r30o9Jz8pOAVoXrR-FTbOZsDFWAxzI_j_zcVP2C3IjK4IB0RQDPz7Xy/dl4/d5/L2dBISEvZ0FBIS9nQSEh/

European Union Agency for Network and Information Security (ENISA). (2016a). *Inventory of Risk Management / Risk Assessment Methods.* Recuperado de: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

European Union Agency for Network and Information Security (ENISA). (2016b). *EBIOS.* Recuperado de: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html

European Union Agency for Network and Information Security (ENISA). (2016c). *ISAMM.* Recuperado de: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isamm.html

Ferrell, O. C., y Geoffrey, H. (2004). *Introducción a los Negocios en un Mundo Cambiante*. Cuarta Edición. México: McGRAW-HILL Interamericana Editores.

Fitzgerald, T. (2007). Information Security Governance. En H. Tipton, & M. Krause (Ed.), *Information Security Management Handbook* (15-34). USA: Auerbach Publications.

Gómez Fernández, L. Y Fernández Rivero, P.P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* Primera edición. Madrid, España: AENOR.

Guzmán Silva, C. A. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Financiera de Segundo Piso* (Trabajo de Grado). Institución Universitaria Politécnico Grancolombiano. Colombia.

Halvorson, N. (2008). *Information Risk Management: A Process Approach to Risk Diagnosis and Treatment. Information Security Management Handbook*. Sexta edición. Volumen 2. USA: Auerbach Publications

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, M. (2014). *Metodología de la Investigación* (Sexta ed.). México: McGRAW-HILL Interamericana Editores.

INDECOPI. (2007). *Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI (ISO 27002:2005). Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información*. Segunda edición. Lima, Perú.

INDECOPI. (2014). *Norma Técnica Peruana "NTP-ISO/ IEC 27001:2014. Tecnología de la Información*. *Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requisitos.* Segunda edición. Lima, Perú.

Instituto de Estudios Peruanos - IEP - (2016). *Municipalidades en el Perú.* Recuperado de https://municipioaldia.com/municipalidades-del-peru/#2-section

ISO 27000 (s.f. a). *ISO 27000.es. El Portal de ISO 27001 en Español*. Recuperado de: http://www.iso27000.es/iso27000.html

ISO 27000 (s.f. b). *ISO 27000.es. El Portal de ISO 27001 en Español*. Recuperado de: http://www.iso27000.es/glosario.html#section10p

ISOTools Excellence (18, 08, 2015). *La norma ISO 27001:2013 ¿Cuál es su estructura?* [Entrada en Blog]. Recuperado de http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

Justino Salinas, Z. I. (2015). *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013* (Tesis de grado). Pontificia Universidad Católica del Perú, Lima, Perú.

Laudon, K. C., & Laudon, J. P. (2012). *Sistemas de información gerencial* (Duodécima ed.). México D.F.: Pearson Educación.

López M., A. A. (2011). *Diseño de un plan de gestión de seguridad de la información. Caso: dirección de informática de la alcaldía del municipio jiménez del estado lara* (Trabajo de maestría). Universidad Centroccidental Lisandro Alvarado, Barquisimetro, Venezuela.

MARGERIT (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método*. Madrid: Ministerio de Hacienda y Administración Pública

Mcmillan, J. Y Schumacher, S. (2005). *Investigación Educativa*. Madrid, España: Pearson Educación.

Municipalidad Provincial de Huamanga. (2016a). *munihuamanga*. Reglamento de Organización y Funciones (ROF). Recuperado de: http://www.munihuamanga.gob.pe/downloads/Reglamentos/ROF-2016.pdf.

Municipalidad Provincial de Huamanga. (2016b). *munihuamanga*. Plan de Desrrollo Institucional. Recuperado de: http://www.munihuamanga.gob.pe/index.php/transparencia/normas-legales/675-plan-de-desarrollo-institucional.

Oficina Nacional de Gobierno Electrónico e Informática – ONGEI. (2016). *Sistema Nacional de Informática*. Recuperado de http://www.ongei.gob.pe/quienes/ongei_quienes.asp?pk_id_entidad=1878&opciones=S

Pallas Mega, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico* (Tesis de Maestría). Instituto de Computación. Facultad de Ingeniería Universidad de la República. Montevideo, Uruguay.

Peltier, T. R., Peltier, J. y Blackley, J. (2005). *Information Security Fundamentals*. USA: Auerbach Publications. Recuperado de: https://binhthanhdang.files.wordpress.com/2010/08/information-security-fundamentals-ebook-een.pdf

Peso Navarro, E. y Ramos Gonzalez, M. A. (2004). *El Documento de Seguridad: Análisis técnico y jurídico. Modelo*. Madrid España: Diaz de Santos. Recuperado de: https://books.google.com.pe/books?id=4I2Cdi_8wgcC&printsec=frontcover&hl=es#v=onepage&q&f=false

Ponemon Institute (2016). *Flipping the Economics of Attacks.* Recuperado el 2016 de: http://www.ponemon.org/news-2/70

Presidencia de Consejo de Ministros – PCM (2016). *Dispositivos legales. Resoluciones ministeriales.* Recuperado el 2016 de: http://www.pcm.gob.pe/wp-content/uploads/2016/01/RM_N_04-2016-PCM.pdf

Real Academia Española (RAE). (2014). *Diccionario de lengua española* (Vigesimotercera ed.). Recuperado de http://dle.rae.es/?id=XTrgHXd

Sandoval Vargas, C. A. (2014). *Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una Empresa* (Tesis de Maestría). Universidad Católica de Santiago de Guayaquil, Guayaquil, Ecuador.

Suárez Padilla, G. J. (2013). *Estudio de la Seguridad de la Información aplicado a Recursos Humanos, Adquisiciones y Cómputo para empresas del Sector Pesquero* (Tesis de grado). Universidad de Guayaquil, Guayaquil, Ecuador.

Tipton, H. F., Krause, M. y Ozier, W. (2006). Risk Analysis and Assessment. En Tipton, H. F. y Krause, M. (Ed.), *Information Security Management Handbook* (Fifth Edition ed., Vol. 3, p. 1053). Recuperado de: https://books.google.com.pe/books?id=mBDNBQAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

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

## Glosario de términos

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

**Alcance:** Ámbito de la organización que queda sometido al SGSI.

**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**Control:** Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. El control es también usado como sinónimo de salvaguardia o contramedida

**Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

**Degradar:** Reducir o desgastar las cualidades inherentes a algo.

**Impacto:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

**Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**Plan de tratamiento de Riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

**Probabilidad:** Frecuencia con que ocurre una amenaza.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad.

**Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo.

**Vulnerabilidad:** Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

**Incidencia:** Una incidencia es toda interrupción o reducción de la calidad no planificada del servicio.

# Anexo A

# Evaluación completa del estado inicial de la MPH respecto a la NTP ISO/IEC 27001:2014

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? / ¿QUÉ SE TENDRÍA QUE HACER?) | VALORACIÓN |
|---|---|---|---|---|
| **4** | **CONTEXTO DE LA ORGANIZACIÓN** | **No Diseñado** | **Se sugiere realizar el análisis del contexto de la MPH, para comprender, tanto los aspectos externos como internos, las partes interesadas y requisitos relevantes al SGSI y, elaborara y documentar el alcance del SGSI.** | **6%** |
| **4.1** | **Comprender la Organización y contexto**.<br><br>La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI | Parcialmente diseñado | La MPH posee documentos visibles de su Misión, Visión, Matriz FODA y las Estrategias. Pero no contempla de manera clara ítems de seguridad de la información.<br>Se sugiere establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos. | 25% |
| **4.2** | **Comprender las necesidades y expectativas de las partes interesadas.**<br><br>La organización **debe** determinar las partes interesadas y los requisitos de las mismas. | No Diseñado | **Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información. | 0% |
| | a) las partes interesadas relevantes al SGSI. | No Diseñado | **Sugerencia:** Determinar las partes interesadas para el SGSI | 0% |
| | b) los requisitos de estas partes interesadas relevantes a la seguridad de la información. | No Diseñado | **Sugerencia:** Determinar los requisitos relevantes a la seguridad de la información | 0% |
| **4.3** | **Determinar el alcance del SGSI.** | **No Diseñado** | **Sugerencia.** Determinar el alcance del SGSI teniendo en consideración los aspectos referidos en 4.1, los requisitos de 4.2, documentarlo y ponerlo a disposición de las partes interesadas. | 0% |
| | La organización **debe** determinar los límites y la aplicabilidad del SGSI para establecer su alcance. | No Diseñado | **Sugerencia:** Determinar el alcance del SGSI | 0% |
| | Cuando se determina este alcance la organización **debe** considerar: | | | 0% |
| | a) Los aspectos externos e internos referidos en 4.1 | No diseñado | **Sugerencia:** Tener en cuenta los aspectos internos y externos relevantes a la seguridad de información para determinar el alcance. | 0% |
| | b) Los requisitos referidos en 4.2 | No diseñado | **Sugerencia:** Al determinar el alcance tener en cuenta los requisitos de las partes interesadas. | 0% |
| | c) Las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones. | No diseñado | **Sugerencia:** Tener en cuenta las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones. | 0% |

| | | | | |
|---|---|---|---|---|
| | El alcance **debe** estar disponible como información documentada. | No diseñado | **Sugerencia:** Una vez determinado el alcance del SGSI, hay que documentarlo y colocarlo en lugar en un lugar accesible a las partes interesadas | 0% |
| **4.4** | **Sistema de Gestión de Seguridad de la información.**<br><br>La organización **debe** establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta Norma Técnica Peruana | No diseñado | Sugerencia. Establecer una plan para la mejora continua del SGSI conforme a la NTP Vigente | 0% |
| **5** | **LIDERAZGO** | **No Diseñado** | **El Titular de la Entidad, debe mostrar liderazgo y compromiso respecto al SGSI. Entonces, debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. Por lo tanto, es necesario establecer: Una Política de Seguridad de la Información, y los Objetivos de Seguridad de la Información acorde al propósito de la organización.** | 1% |
| **5.1** | **Liderazgo y compromiso.**<br><br>La alta dirección **debe** demostrar liderazgo y compromiso respecto al SGSI. | No Diseñado | El titular de la entidad debe mostrar liderazgo y compromiso | 3% |
| | a) asegurando que la política de la seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización; | No Diseñado | Establecer una política de seguridad de la información que sea compatible con la dirección estratégica de la organización. | 0% |
| | b) asegurando la integración de los requisitos del SGSI en los procesos de la organización; | No Diseñado | Asegurar la integración del SGSI en los procesos de la organización. | 0% |
| | c) asegurando que los recursos necesarios para el SGSI estén disponibles; | No Diseñado | La alta dirección debe asegurar los recursos necesarios para la implementación del SGSI, esto es disponer de un presupuesta para gestionar el proyecto del SGSI | 0% |
| | d) comunicando la importancia de una efectiva gestión de seguridad de la información y en concordancia con los requisitos del SGSI; | No Diseñado | La alta dirección debe comunicar la importancia de una efectiva gestión de la seguridad de la información | 0% |
| | e) asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s); | No Diseñado | | 0% |
| | f) dirigiendo y apoyando a las personas para que contribuyan con la efectividad del SGSI; | Parcialmente diseñado | | 25% |
| | g) promoviendo la mejora continua; | No Diseñado | | 0% |
| | h) apoyando a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica en sus áreas de responsabilidad. | No Diseñado | | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **5.2** | **Política.** | No Diseñado | Establecer la Política de Seguridad de la Información acorde al propósito de la organización, incluir los objetivos de seguridad de la Información (Sección 6.2), mantenerla disponible y comunicada a toda la organización. | 0% |
| | La alta dirección **debe** establecer una política de seguridad de la información que: | | | 0% |
| | a) es apropiada al propósito de la organización; | No Diseñado | | 0% |
| | b) incluye objetivos de seguridad de la información (según 6.2) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información; | No Diseñado | | 0% |
| | c) incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; | No Diseñado | | 0% |
| | d) incluye un compromiso de mejora continua del SGSI. | No Diseñado | | 0% |
| | La política de seguridad **debe:** | No Diseñado | | 0% |
| | a) estar disponible como información documentada, | No Diseñado | Documentar la política de seguridad de la información | 0% |
| | b) estar comunicada dentro de la organización; | No Diseñado | Establecer medios para comunicar la política de la seguridad de la información (Correo electrónico, intranet, carpeta compartida, etc.) | 0% |
| | c) estar disponible a las partes interesadas, según sea apropiado | No Diseñado | Establecer medios para mantener disponible la política de seguridad de la información a las partes interesadas. | 0% |
| **5.3** | **Roles, responsabilidades y autoridades organizacionales.** | No Diseñado | La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. | 0% |
| | La alta dirección **debe** asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas. | No Diseñado | | 0% |
| | La alta dirección **debe** asignar la responsabilidad y la autoridad para: | No Diseñado | | 0% |
| | a) asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de esta Norma Técnica Peruana; | No Diseñado | Designar un responsable auditor que compruebe que el SGSI está conforme al NTP vigente. | 0% |
| | b) reportar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección. | No Diseñado | Asignar un responsable que reporte a la alta dirección sobre el desempeño del SGSI. | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **6** | **PLANIFICACIÓN** | **No Diseñado** | **Adoptar, planificar y documentar el procedimiento de valoración y tratamiento de riesgos de la seguridad de la información.**<br>**Establecer y documentar los objetivos de seguridad de la información conforme a los propósitos de la organización y elaborar un plan para lograr estos objetivos de seguridad de la información.** | **0%** |
| **6.1** | **Acciones para tratar los riesgos y oportunidades** | No Diseñado | Adoptar, planificar y documentar el procedimiento la valoración y tratamiento de riesgos de la seguridad de la información. | 0% |
| **6.1.1** | **Generalidades** | No Diseñado | Al planificar el SGSI tener en cuenta la sección 4.1, 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para asegurar que el SGSI logré los resultados esperados, prevenir o reducir efectos indeseados y lograr una mejora continua.<br>Elaborar un plan de acción para el tratamiento de riesgos y oportunidades y su integración e implementación en el SGSI, asimismo considerar indicadores para evaluar la efectividad de las acciones adoptadas. | 0% |
| | Cuando se planifica para el SGSI, la organización **debe** considerar los asuntos referidos en el numeral 4.1 y los requisitos referidos en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para: | No Diseñado | Al planificar el SGSI tener en cuenta la sección 4.1, 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para asegurar que el SGSI logré los resultados esperados, prevenir o reducir efectos indeseados y lograr una mejora continua. | 0% |
| | a) asegurar que el sistema de gestión de seguridad de la información pueda lograr su(s) resultado(s) esperado(s); | No Diseñado | | 0% |
| | b) prevenir, o reducir, efectos indeseados; | No Diseñado | | 0% |
| | c) lograr la mejora continua. | No Diseñado | | 0% |
| | La organización **debe** planificar: | No Diseñado | Elaborar un plan de acción para el tratamiento de riesgos y oportunidades y su integración e implementación en el SGSI, asimismo considerar indicadores para evaluar la efectividad de las acciones adoptadas. | 0% |
| | d) acciones que traten estos riesgos y oportunidades; | No Diseñado | Planificar acciones que traten estos riesgos y oportunidades | 0% |
| | e) como integrar e implementar estas acciones en los procesos del SGSI; y evaluar la efectividad de estas acciones. | No Diseñado | Planificar la integración e implementación de las acciones para la gestión del riesgo. | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **6.1.2** | **Valoración del riesgo de seguridad de la información** | No Diseñado | Establecer y documentar el procedimiento de valoración de Riesgos de Seguridad de la Información. | 0% |
| | La organización **debe** definir y aplicar un proceso de valoración del riesgo de seguridad de la información que: | No Diseñado | Establecer un procedimiento para la valoración del riesgo de seguridad de la información. | 0% |
| | a) establezca y mantenga criterios de riesgo de seguridad de la información que incluyan; 1) los criterios de aceptación de los riesgos; y 2) los criterios para realizar valoraciones de riesgo de seguridad de la información; | No Diseñado | Definir y aplicar un procedimiento que establezca y mantenga criterios de aceptación y valoración de riesgos de seguridad de la información | 0% |
| | b) asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables; | No Diseñado | Definir y aplicar un procedimiento que asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables. | 0% |
| | c) identifique los riesgos de seguridad de la información 1) aplicando el proceso de valoración de riesgos de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad para la información dentro del alcance del SGSI; 2) identificando a los propietarios de riesgos | No Diseñado | Establecer un procedimiento, o adoptar una metodología de Gestión de Riesgos de Seguridad de la Información. | 0% |
| | d) analice los riesgos de seguridad de la información: 1) valorando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse; 2) valorando la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y 3) determinando los niveles de riesgo; | No Diseñado | Determinar los niveles de riesgo teniendo en cuenta el impacto y probabilidad del riesgo de acuerdo al procedimiento adoptado | 0% |
| | e) evalúe los riesgos de seguridad de la información: 1) comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2 a); y 2) priorizando los riesgos analizados para el tratamiento de riesgos. | No Diseñado | Evaluar los riesgos de acuerdo con los criterios de riesgos establecidos en 6.1.2 a), priorizar estos riesgos para su tratamiento | 0% |
| | La organización **debe** retener información documentada sobre el proceso de valoración de riesgos de seguridad de la información. | No Diseñado | Documentar el procedimiento de valoración de riesgos de seguridad de la información. | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **6.1.3** | **Tratamiento de Riesgos de Seguridad de la Información** | No Diseñado | Planificar y documentar el procedimiento para el tratamiento de Riesgos de Seguridad de la Información | 0% |
| | La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para: | No Diseñado | Definir y aplicar un procedimiento para el tratamiento de riesgos de seguridad de la información. | 0% |
| | a) seleccionar opciones de tratamiento de riesgos de seguridad de la información apropiadas, tomando en cuenta los resultados de la valoración de riesgos; | No Diseñado | Tener en cuenta los resultados de la valoración de riesgos al seleccionar las opciones de tratamiento de riesgos de seguridad de la información. | 0% |
| | b) determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información; | No Diseñado | Determinar los controles necesarios para el tratamiento de riesgos de seguridad de la información | 0% |
| | c) Comparar los controles determinados en 6.1.3 b) con aquellos del Anexo A y verificar que no se ha omitido ningún control necesario; | No Diseñado | Comparar los controles adoptados para el tratamiento de riesgos de seguridad de la información con los controles proporcionados en el anexo A de la NTP para evitar omitir algún control. | 0% |
| | d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (véase 6.1.3 b) y c)) y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A; | No Diseñado | Elaborar la Declaración de Aplicabilidad con los controles a implementar y/o justificaciones de omisión de algunos controles del Anexo A. | 0% |
| | e) formular un plan de tratamiento de riesgos de seguridad de la información; | No Diseñado | Elaborar un plan de tratamiento de riesgos de seguridad de la información. | 0% |
| | f) obtener la aprobación, por parte de los propietarios de riesgos, del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la seguridad de la información. | No Diseñado | Reunirse con los propietarios de los riesgos y obtener la aprobación del plan de tratamiento de riesgos y aceptación de los riesgos residuales de la seguridad de la información | 0% |
| | La organización **debe** retener información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información. | No Diseñado | Documentar el procedimiento de tratamiento de riesgos de seguridad de la información. | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| 6.2 | **Objetivos de seguridad de la información y planificación para conseguirlos** | No Diseñado | Establecer los objetivos de seguridad de la información alineados a los objetivos estratégicos de la organización y elaborara un plan para lograr estos objetivos de seguridad. | 0% |
| | La organización **debe** establecer objetivos de seguridad de la información a niveles y funciones relevantes. | No Diseñado | Establecer los objetivos de seguridad de la información alineados a los objetivos estratégicos de la organización. | 0% |
| | Los objetivos de seguridad de la información **deben**: | No Diseñado | Elaborar los objetivos de seguridad de la información, estos objetivos deben ser consistentes con la política de la seguridad de la información, ser medibles, conforme a los requisitos de seguridad de la información y la gestión de riesgos. Asimismo, deben ser comunicados y actualizados. | 0% |
| | a) ser consistentes con la política de seguridad de la información; | No Diseñado | | 0% |
| | b) ser medibles (si es práctico); | No Diseñado | | 0% |
| | c) tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos; | No Diseñado | | 0% |
| | d) ser comunicados; | No Diseñado | | 0% |
| | e) ser actualizados según sea apropiado. | No Diseñado | | 0% |
| | La organización **debe** retener información documentada sobre los objetivos de seguridad de la información. | No Diseñado | Documentar los objetivos de la seguridad de la información. | 0% |
| | Cuando planifique cómo lograr sus objetivos de seguridad de la información, la organización **debe** determinar: | No Diseñado | Dentro del proyecto de implementación del SGSI contemplar los pasos a realizar, los recursos necesarios, los responsables, tiempo final y métodos o procedimientos para evaluar los resultados. | 0% |
| | f) qué se hará; | No Diseñado | | 0% |
| | g) qué recursos serán requeridos; | No Diseñado | | 0% |
| | h) quién será responsable; | No Diseñado | | 0% |
| | i) cuándo se culminará; | No Diseñado | | 0% |
| | j) cómo los resultados serán evaluados. | No Diseñado | | 0% |
| 7 | **SOPORTE** | No Diseñado | | 7% |
| 7.1 | **Recursos**<br><br>La organización **debe** determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. | No Diseñado | Asignar presupuesto para la implementación, mantenimiento y mejora continua del SGSI. | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| 7.2 | **Competencia**<br><br>La organización **<u>debe</u>:** | No Diseñado | Determinar las competencias del personal a su cargo para un correcto desempeño del SGSI, cuando sea necesario tomar acciones para adquirir las competencias necesarias sobre la seguridad de la información, documentar las competencias como evidencia. | 0% |
| | a) Determinar la competencia necesaria de la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información; | No Diseñado | | 0% |
| | b) Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados; | No Diseñado | | 0% |
| | c) Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas; y | No Diseñado | | 0% |
| | d) Retener información documentada apropiada como evidencia de competencia. | No Diseñado | | 0% |
| 7.3 | **Concientización**<br><br>Las personas que trabajan bajo el control de la organización **<u>deben</u>** ser conscientes de la política de seguridad, su contribución a la efectividad del SGSI y las implicancias de no tener la conformidad de los requisitos del SGSI. | No Diseñado | Concientizar al personal que trabaja en la organización sobre la importancia de la seguridad de la información, la política de seguridad y el papel crucial que cumple cada uno de ellos en el correcto desempeño de SGSI, asimismo concientizarlos sobre las consecuencias de no cumplir con los requisitos del SGSI. | 8% |
| | a) la política de seguridad de información; | No Diseñado | Elaborar la política de seguridad de la información | 0% |
| | b) su contribución a la efectividad del SGSI, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; | Parcialmente diseñado | De la reunión con el responsable de la Subgerencia de Sistemas y Tecnología se han evidenciado cursos y talleres a los que ha asistido el personal del área, pero no existe documentos de charlas o capacitaciones para el resto del personal de la MPH. | 25% |
| | c) las implicancias de no tener conformidad con los requisitos del SGSI. | No Diseñado | Implementar la NTP ISO:IEC 27001 por cumplimiento legal | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| 7.4 | **Comunicación**<br><br>La organización **debe** determinar la necesidad de comunicaciones internas y externas<br>relevantes al sistema de gestión de seguridad de la información incluyendo: | Parcialmente diseñado | Según la entrevista al jefe de la Subgerencia de Sistemas y Tecnología existe comunicación externa con la ONGEI sobre la seguridad de la información, existe un responsable dentro del área para responder anualmente la ENRIAP (Encuesta Nacional de Recursos Informáticos en la Administración Pública); dentro de esta encuesta existe un ítem de seguridad de la información y el medio por donde se responde es a través de la web. Se recomienda documentar los procedimientos de comunicación para tenerlos como evidencia e incluir en el mismo la comunicación interna. | 25% |
| | a) qué comunicar; | Parcialmente diseñado | | 25% |
| | b) cuándo comunicar; | Parcialmente diseñado | | 25% |
| | c) a quién comunicar; | Parcialmente diseñado | | 25% |
| | d) quién debe comunicar; | Parcialmente diseñado | | 25% |
| | e) los procesos por los cuales la comunicación debe ser efectuada. | Parcialmente diseñado | | 25% |
| 7.5 | **Información documentada** | No Diseñado | Existe documentación de origen externo (NTP, Resoluciones, etc.) identificados pero que aún se han sido analizados completamente para empezar la planificación y posterior implementación del SGSI en la MPH.<br>Se sugiere empezar a elaborar la documentación necesaria exigida por la NTP vigente para lograr la efectividad del SGSI asimismo determinar los procedimientos de creación, actualización y control de la documentación. | 3% |
| 7.5.1 | **Generalidades**<br><br>El sistema de gestión de seguridad de la información de la organización **debe** incluir: | No Diseñado | Se sugiere empezar a elaborar la documentación necesaria exigida por la NTP vigente para lograr la efectividad del SGSI. | 0% |
| | a) información documentada requerida por esta Norma Técnica Peruana; | No Diseñado | | 0% |
| | b) información documentada determinada por la organización como necesaria para la efectividad del SGSI. | No Diseñado | | 0% |
| 7.5.2 | **Creación y actualización**<br><br>Cuando se crea y actualiza información documentada, la organización **debe** asegurar: | No Diseñado | Asegurar la creación de los documentos necesarios exigidos por la NTP vigente (NTP ISO/IEC 27001:2014), determinar las herramientas y formatos de los documentos, así como los medios y procedimientos para su aprobación, revisión y actualización. | 0% |
| | a) identificación y descripción apropiados (por ejemplo, un título, fecha, autor, o número de referencia); | No Diseñado | | 0% |
| | b) formato (por ejemplo el lenguaje, versión de software, gráficos) y medios (por ejemplo papel, electrónico) apropiados; | No Diseñado | | 0% |
| | c) revisión y aprobación apropiadas para su conveniencia y adecuación. | No Diseñado | | 0% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **7.5.3** | **Información documentada** | No Diseñado | Existe documentación de origen externo (NTP, Resoluciones, etc.) identificados pero que aún se han sido analizados completamente para empezar la planificación y posterior implementación del SGSI en la MPH. | 8% |
| | La información documentada requerida por el sistema de gestión de seguridad de la información y por esta Norma Técnica Peruana se **debe** controlar para asegurar que esté disponible y protegida. | No Diseñado | Controlar que la documentación necesaria exigida por la NTP esté disponible y protegida adecuadamente en su confidencialidad, integridad y disponibilidad. | 0% |
| | a) que esté disponible y sea conveniente para su uso donde y cuando sea necesaria; | No Diseñado | | 0% |
| | b) que esté protegida adecuadamente (por ejemplo de pérdida de confidencialidad, uso impropio, o pérdida de integridad). | No Diseñado | | 0% |
| | Para el control de la información documentada, la organización **debe** realizar las siguientes actividades, según sea aplicable: | No Diseñado | Establecer procedimientos de control para la información documentada, esto es distribución, acceso, uso, almacenamiento, preservación, control de cambios, retención y disposición. | 0% |
| | c) distribución, acceso, recuperación y uso; | No Diseñado | | 0% |
| | d) almacenamiento y preservación, incluyendo la preservación de legibilidad; | No Diseñado | | 0% |
| | e) control de cambios (por ejemplo control de versiones); | No Diseñado | | 0% |
| | f) retención y disposición. | No Diseñado | | 0% |
| | La información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, **debe** ser identificada según sea apropiado y controlarse. | Parcialmente diseñado | Existe documentación de origen externo (NTP, Resoluciones, etc.) identificados pero que aún se han sido analizados completamente para empezar la planificación y posterior implementación del SGSI en la MPH. | 25% |
| **8** | **OPERACIÓN** | No Diseñado | | 0% |
| **8.1** | **Planificación y control operacional** | No Diseñado | 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. | 0% |
| | La organización **debe** planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1. La organización **debe** también implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2. | No Diseñado | Planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1. Asimismo implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2. | 0% |

| | | | | |
|---|---|---|---|---|
| | La organización **debe** mantener información documentada en la medida necesaria para estar segura de que los procesos se han llevado a cabo tal como fueron planificados. | No Diseñado | Mantener información documentada para estar segura de que los procesos se han llevado a cabo tal como fueron planificados. | 0% |
| | La organización **debe** controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario. | No Diseñado | Controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuar para mitigar cualquier efecto adverso según sea necesario. | 0% |
| | La organización **debe** asegurar que los procesos tercerizados son determinados y controlados. | No Diseñado | Asegurar que los procesos tercerizados son determinados y controlados. | 0% |
| **8.2** | **Evaluación de riesgos de seguridad de la información** | No Diseñado | Planificar los intervalos de tiempo en los que se llevarán a cabo las evaluaciones de riesgos de seguridad de la información, documentar los resultados de éstas evaluaciones. | 0% |
| | La organización **debe** realizar evaluaciones de riesgos de seguridad de la información en intervalos planificados o cuando cambios significativos se propongan u ocurran, tomando en cuenta los criterios establecidos en 6.1.2 a). | No Diseñado | Planificar los intervalos de tiempo en los que se llevarán a cabo las evaluaciones de riesgos de seguridad de la información acorde a los criterios establecidos en 6.1.2 a). | 0% |
| | La organización **debe** retener información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información. | No Diseñado | Disponer de información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información. | 0% |
| **9** | **EVALUACIÓN DEL DESEMPEÑO** | No Diseñado | Implementar el SGSI y elaborar un plan para evaluar periódicamente su funcionamiento y garantizar que el sistema se mantiene eficaz a lo largo del tiempo. Asimismo documentar dichas evaluaciones. | 21% |
| **9.1** | **Monitoreo, medición, análisis y evaluación** | No Diseñado | Establecer procedimientos para realizar el monitoreo, medición, análisis y evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. Documentar los resultados del monitoreo, medición, análisis y evaluación del SGSI. | 0% |
| | La organización **debe** evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. | No Diseñado | Evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. | 0% |
| | La organización **debe** determinar: | No Diseñado | Determinar qué necesita ser monitoreado y medido, los métodos para el monitoreo, medición, análisis y evaluación, cuándo debe realizarle el monitoreo y medición, cuándo deben ser analizados y evaluados los resultados de monitoreo y medición y quién es el responsable de monitorear y medir, analizar y evaluar los resultados. | 0% |
| | a) qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información; | No Diseñado | | 0% |
| | b) los métodos para monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos; | No Diseñado | | 0% |
| | c) cuándo el monitoreo y medición debe ser realizado; | No Diseñado | | 0% |

| | | | | |
|---|---|---|---|---|
| | d) quién debe monitorear y medir; | No Diseñado | | 0% |
| | e) cuándo los resultados del monitoreo y medición deben ser analizados y evaluados; | No Diseñado | | |
| | f) quién debe analizar y evaluar estos resultados. | No Diseñado | | 0% |
| | La organización **debe** retener información documentada apropiada como evidencia del monitoreo y los resultados de la medición. | No Diseñado | Retener información documentada apropiada como evidencia del monitoreo y los resultados de la medición. | 0% |
| **9.2** | **Auditoría interna** | Parcialmente diseñado | Existen documentos del resultado de la auditoría realizado por el órgano de control interno en el que se contempla la no conformidad con el ítem de seguridad de la información.<br>Se recomienda planificar la frecuencia de las auditorías internas y levantar la no conformidad de la auditoría interna para el cumplimento legal. | 39% |
| | La organización **debe** conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información: | Parcialmente diseñado | | 38% |
| | a) está en conformidad con 1) los requisitos de la propia organización para su sistema de gestión de seguridad de la información; y 2) los requisitos de esta Norma Técnica Peruana; | Diseñado | | 50% |
| | b) está efectivamente implementado y mantenido. | Parcialmente diseñado | | 25% |
| | La organización **debe**: | Parcialmente diseñado | | 40% |
| | c) planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos e informes de planificación. Los programas de auditoría deben tomar en consideración la importancia de los procesos concernientes y los resultados de auditorías previas; | No Diseñado | | 0% |
| | d) definir los criterios y el alcance de cada auditoría; | Diseñado | | 50% |
| | e) seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría; | Diseñado | | 50% |
| | f) asegurar que los resultados de las auditorías se reporten a los gerentes relevantes; | Diseñado | | 50% |
| | g) retener información documentada como evidencia del (de los) programa(s) de auditoría y los resultados de la auditoría. | Diseñado | | 50% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **9.3** | **Revisión por la gerencia** | Parcialmente diseñado | Existe documentación (resultado de auditoría y memorandos a la subgerencia de Sistemas y Tecnología) que dan a conocer el estado actual de la organización respecto al SGSI (no implementado) y la orden de implementación de las funciones de seguridad. Pero éstos documentos no están del todo conforme con los requisitos de la NTP. | 25% |
| | La alta dirección **debe** revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua. | Parcialmente diseñado | Los documentos de auditoría interna han sido dados a conocer a la alta gerencia, pero la revisión y otros documentos no están conformes a la NTP. | 25% |
| | La revisión por la gerencia **debe** incluir consideraciones de: | No Diseñado | Las revisiones por parte de la gerencia deben incluir el estado de las acciones con relación a las revisiones anteriores, cambios externos e internos, retroalimentación sobre el desempeño de la seguridad de la información. Retroalimentación de las partes interesadas, resultados de la evaluación y estado del plan de tratamiento de riesgos y oportunidades de mejora continua. | 0% |
| | a) el estado de las acciones con relación a las revisiones anteriores por parte de la gerencia; | No Diseñado | | 0% |
| | b) cambios en asuntos externos e internos que son relevantes al sistema de gestión de seguridad de la información; | No Diseñado | | 0% |
| | c) retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en: 1) no conformidades y acciones correctivas; 2) resultados del monitoreo y medición; 3) resultados de auditoría; y 4) cumplimiento de los objetivos de seguridad de la información; | No Diseñado | | 0% |
| | d) retroalimentación de partes interesadas; | No Diseñado | | 0% |
| | e) resultados de la evaluación de riesgo y estado del plan de tratamiento de riesgos; | No Diseñado | | 0% |
| | f) oportunidades para la mejora continua. | No Diseñado | | 0% |
| | Los productos de la revisión por la gerencia **deben** incluir decisiones relacionadas a oportunidades de mejora continua y cualquier necesidad de cambios al sistema de gestión de seguridad de la información. | Diseñado | Existen memorandos a la subgerencia de sistemas para levantar la no conformidad y ordenar la implementación del SGSI. | 50% |
| | La organización **debe** retener información documentada como evidencia de los resultados de revisiones por parte de la gerencia. | Parcialmente diseñado | Existen documentos que evidencian los resultados de la revisión (memorandos) pero no están acorde a la NTP.<br>Se recomienda considerar en los items establecidos en la NTP. | 25% |

| SECCIÓN | REQUERIMIENTO DE LA ISO/IEC 27001:2013 | ESTADO | EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE?/¿QUÉ SE TENDRÍA QUE HACER? | VALORACIÓN |
|---|---|---|---|---|
| **10** | **MEJORAS** | No Diseñado | Implantar el SGSI y elaborar un plan de mejora continua para actualizar el SGSI de acuerdo a los cambios y novedades de la organización, las tecnologías, las amenazas, etc., tratando de mantener los riesgos controlados en todo momento. | 0% |
| **10.1** | **No conformidades y acción correctiva** | No Diseñado | | 0% |
| | Cuando ocurre una no conformidad, la organización **debe**: | No Diseñado | | 0% |
| | a) reaccionar a la no conformidad y, según sea aplicable:<br>1) tomar acción para controlarla y corregirla; y<br>2) ocuparse de las consecuencias; | No Diseñado | | 0% |
| | b) evaluar la necesidad de la acción para eliminar las causas de la no conformidad con el fin de que no recurra u ocurra en otro lugar de las siguientes maneras:<br>1) revisando la no conformidad;<br>2) determinando las causas de la no conformidad; 3) determinando si existen no conformidades similares o si podrían ocurrir potencialmente; | No Diseñado | | 0% |
| | c) implementar cualquier acción necesaria; | No Diseñado | | 0% |
| | d) revisar la efectividad de cualquier acción correctiva tomada; | No Diseñado | | 0% |
| | e) hacer cambios al sistema de gestión de seguridad de la información, si fuera necesario. | No Diseñado | | 0% |
| | Las acciones correctivas **deben** ser apropiadas a los efectos de las no conformidades encontradas. | No Diseñado | | 0% |
| | La organización **debe** retener información documentada como evidencia de: | No Diseñado | | 0% |
| | f) la naturaleza de las no conformidades y cualquier acción subsiguiente tomada; | No Diseñado | | 0% |
| | g) los resultados de cualquier acción correctiva. | No Diseñado | | 0% |
| **10.2** | **Mejora Continua**<br><br>La organización **debe** mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información. | No Diseñado | | 0% |
| **PUNTAJE TOTAL DE LA EVALUACIÒN DE REQUISITOS DE LA NTP ISO/IEC 27001:2014** | | | | 5% |

## Anexo B

## Cuestionario sobre la posibilidad de aceptación del SGSI y diagnóstico inicial de la seguridad de la información

1. ¿Sabe Ud. si dentro de la Municipalidad Provincial de Huamanga existe un sistema de gestión de la seguridad de la información?

   Sí☐ No☐

2. ¿Cree usted que el diseño de un sistema de gestión de la seguridad de la información de la Información permitirá mejorar la seguridad de información de su área de trabajo?

   Sí☐ No☐

3. ¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de este sistema de gestión de la seguridad de la información?

   Sí☐ No☐

4. ¿Aprobaría usted la implementación del sistema de gestión de la seguridad de la información en su área de trabajo?

   Sí☐ No☐

5. En su área de trabajo, ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la seguridad de la Información?

   Sí☐ No☐

6. ¿Estaría usted dispuesto a colaborar para que el diseño e implementación del sistema de gestión de la seguridad de la información se lleve a cabo en su área de trabajo?

   Sí☐ No☐

7. ¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?

   Sí☐ No☐

8. ¿En su área de trabajo se ha categorizado la información de acuerdo al grado de importancia que tienen para la Municipalidad Provincial de Huamanga?

   Sí☐ No☐

9. ¿Ha recibido Ud. capacitación sobre seguridad de la información de acuerdo a su función laboral?

   Sí☐ No☐

10. ¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información?

    Sí☐ No☐

11. Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto?

    Sí☐ No☐

12. ¿Cuenta Ud. con un computador/laptop para realizar sus funciones? (Si la respuesta es **No** pasar a la pregunta 15)

    Sí☐ No☐

13. ¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop?

    Sí☐ No☐

14. Cuando su computador está desatendido ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?

    Sí☐ No☐

15. ¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, tras papeleo, etc.?

    Sí☐ No☐

16. ¿En lo que va del año se ha divulgado información sensible para la Municipalidad Provincial de Huamanga sin su autorización o conocimiento?

    Sí☐ No☐

17. ¿En su área de trabajo se han realizado evaluación de riesgos relacionados con la información?

    Sí☐ No☐

18. ¿En su área de trabajo se han realizado una evaluación de vulnerabilidades de la red?

    Sí☐ No☐

19. ¿Su área de trabajo cuenta con software antivirus actualizado?

    Sí☐ No☐

20. ¿Realiza Ud. copias de seguridad para proteger su información?

    Sí☐ No☐

21. ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionen pérdidas de información?

    Sí☐ No☐

## Anexo C

## Imágenes del Data Center de la Municipalidad Provincial de Huamanga

*Figura C. 1.* Servidores, Racks y Switch de la MPH

Fuente: Elaboración propia

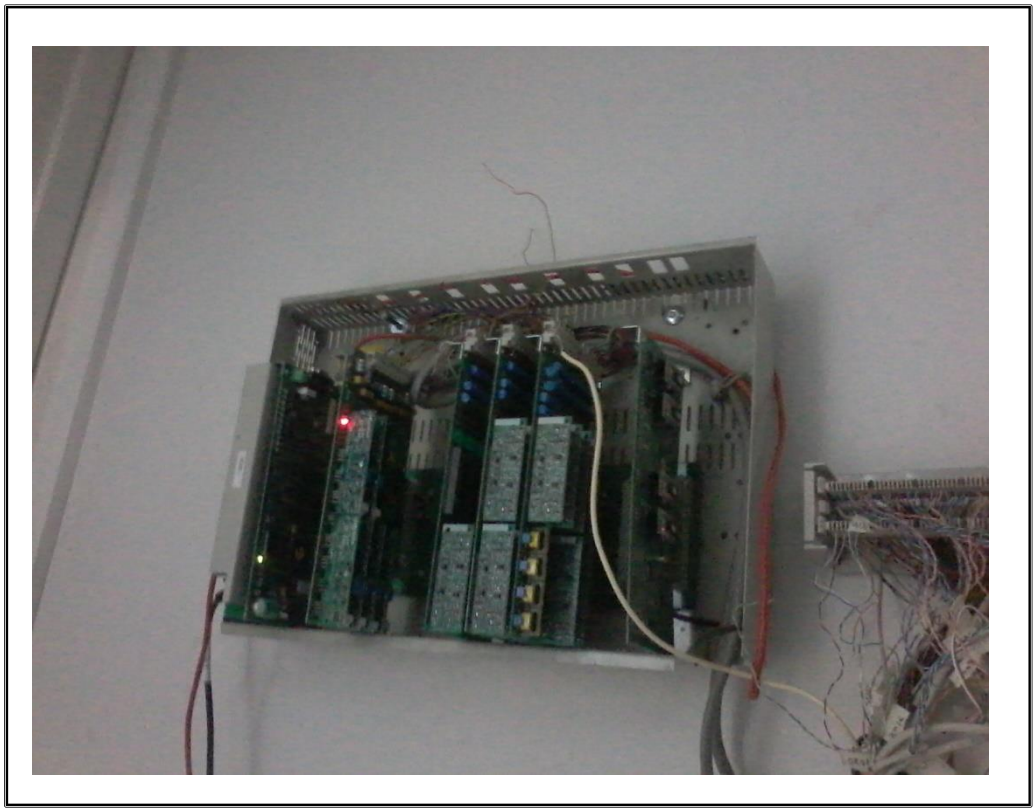

*Figura C. 2.* Anexos telefónicos de la MPH

Fuente: Elaboración propia


*Figura C. 3.* Firewall de la MPH

Fuente: Elaboración propia


*Figura C. 4.* UPS

Fuente: Elaboración propia

*Figura C. 5.* Router de la MPH

Fuente: Elaboración propia

## Anexo D

## Alcance del sistema de gestión de seguridad de la información

### 1. Propósito, alcance y usuarios

El propósito de este documento es definir claramente cuáles son los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de la Municipalidad Provincial de Huamanga y es aplicable a toda la documentación perteneciente al SGSI.

Los únicos usuarios autorizados a este documento son los miembros del comité de seguridad de la información y el personal autorizado de la Sub Gerencia de Sistemas y Tecnología de la Municipalidad Provincial de Huamanga.

### 2. Alcance del SGSI

El alcance del sistema de gestión de seguridad de la información aplica sólo para el proceso de GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA, sub proceso de gestión de la seguridad de la información, dentro de los sistemas de información que sustentan los procesos de negocio.

Se consideran los activos de información considerados como relevantes dentro del alcance.

El sistema de gestión de seguridad de la información aplica solo para la Sub Gerencia de Sistemas y Tecnología ubicada en sede principal de la Municipalidad Provincial de Huamanga, Portal Municipal N°44 Ayacucho.

## Anexo E

## Cuestionario para identificar activos

**Dependencia:**

_____

**Instrucciones:** En cada tabla marque (X) los activos con los que cuenta la dependencia

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO ACTIVOS ESENCIALES** |
|---|
| ¿Qué activos son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? |
| Marque (X) los activos con los que cuenta la dependencia<br>( ) Datos de interés para la administración pública<br>( ) Datos vitales (esencial para el funcionamiento de la organización)<br>( ) Datos de carácter personal (información concerniente al personal)<br>( ) Datos clasificados (aquellos sometidos a normatividad específica de la organización y que determina su control de acceso y distribución)<br>( ) Servicios |
| Nota: Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO DATO/INFORMACIÓN** |
|---|
| ¿Qué activos de tipo dato/información son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? |
| Marque (X) los activos con los que cuenta la dependencia<br>( ) Ficheros o bases de datos<br>( ) Copias de respaldo<br>( ) Datos de configuración de los sistemas de información<br>( ) Datos de gestión interna<br>( ) Credenciales (Ejem. contraseñas)<br>( ) Datos de validación de credenciales<br>( ) Datos de control de acceso<br>( ) Registro de actividad o log de los sistemas de información<br>( ) Código fuente de los sistemas de información<br>( ) Código ejecutable de los sistemas de información<br>( ) Datos de prueba para la implementación de los sistemas de información |
| Nota: Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. |

| TABLA DE RELACIÓN DE ACTIVOS DE TIPO SERVICIO |
|---|
| ¿Qué activos de tipo servicio son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? |
| Marque (X) los activos con los que cuenta la dependencia<br>( ) Anónimo (sin requerir identificación del usuario)<br>( ) Al público en general (sin relación contractual)<br>( ) A usuarios externos (bajo una relación contractual)<br>( ) Interno (a usuarios de la propia organización)<br>( ) Internet<br>( ) Intranet<br>( ) Acceso remoto a cuenta local<br>( ) Correo Electrónico<br>( ) Almacenamiento de ficheros (File Server)<br>( ) Transferencia de ficheros (FTP)<br>( ) Intercambio electrónico de datos (EDI)<br>( ) Servicios de directorio<br>( ) Gestión de Identidades (Servicios que permiten altas y bajas de usuarios de los sistemas)<br>( ) Gestión de privilegios<br>( ) PKI - infraestructura de clave pública (Servicios asociados a sistemas de criptografía de clave pública – Gestión de certificados) |
| Nota: Esta sección contempla servicios prestados por el sistema. |

| TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOFTWARE/APLICACIONES INFORMÁTICAS |
|---|
| ¿Qué activos de tipo software son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? |
| Marque (X) los activos con los que cuenta la dependencia<br>( ) Software de desarrollo propio<br>( ) Software de desarrollo a medida (subcontratado)<br>( ) Página Web<br>( ) Intranet<br>( ) Servidor de presentación<br>( ) Servidor de aplicaciones<br>( ) ERP<br>( ) Cliente de correo electrónico<br>( ) Servidor de correo electrónico<br>( ) Servidor de ficheros<br>( ) sistema de gestión de bases de datos<br>( ) monitor transaccional<br>( ) ofimática<br>( ) anti virus |

| |
|---|
| (  ) sistema operativo<br>(  ) gestor de máquinas virtuales<br>(  ) Servidor de Terminales<br>(  ) Sistema de backup<br>(  ) Otros._____ |
| Nota: Esta sección contempla servicios prestados por el sistema. |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO EQUIPOS INFORMÁTICOS** |
|---|
| ¿Qué activos de tipo hardware son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? |
| Marque (X) los activos con los que cuenta la dependencia<br>(  ) Grandes equipos<br>(  ) Equipos medios<br>(  ) Informática personal<br>(  ) Informática móvil<br>(  ) Equipo virtual<br>(  ) Equipamiento de respaldo<br>(  ) Medios de impresión (impresoras y servidores de impresión)<br>(  ) Escáneres<br>(  ) Dispositivos Criptográficos<br>(  ) Dispositivos de frontera<br>(  ) Módems<br>(  ) Concentradores (Hub)<br>(  ) Conmutadores (Swicth)<br>(  ) Encaminadores (Router)<br>(  ) Pasarelas (bridge)<br>(  ) Cortafuegos (Firewall)<br>(  ) Punto de acceso inalámbrico<br>(  ) Centralita telefónica<br>(  ) Teléfono IP<br>(  ) Otros._____ |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO REDES DE COMUNICACIONES** |
|---|
| ¿Qué medios de transporte utiliza la dependencia para transmitir información? |
| Marque (X) los activos con los que cuenta la dependencia<br>(  ) red telefónica<br>(  ) rdsi (red digital)<br>(  ) X25 (red de datos)<br>(  ) ADSL<br>(  ) punto a punto |

| |
|---|
| (  ) Comunicaciones radio<br>(  ) red inalámbrica<br>(  ) telefonía móvil<br>(  ) por satélite<br>(  ) red local<br>(  ) red metropolitana<br>(  ) Internet |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOPORTE DE INFORMACIÓN** |
|---|
| ¿Qué dispositivos físicos utiliza la dependencia para almacenar información de forma permanente o por largos periodo de tiempo? |
| Marque (X) los activos con los que cuenta la dependencia<br>(  ) discos<br>(  ) discos virtuales<br>(  ) almacenamiento en red<br>(  ) disquetes<br>(  ) cederrón (CD-ROM)<br>(  ) memorias USB<br>(  ) DVD<br>(  ) cinta magnética<br>(  ) tarjetas de memoria<br>(  ) tarjetas inteligentes<br>(  ) material impreso<br>(  ) cinta de papel<br>(  ) microfilm<br>(  ) tarjetas perforadas<br>(  ) Otros._____ |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO EQUIPAMIENTO AUXILIAR** |
|---|
| Marque (X) los activos con los que cuenta la dependencia<br>(  ) fuentes de alimentación<br>(  ) sistemas de alimentación ininterrumpida<br>(  ) generadores eléctricos<br>(  ) equipos de climatización<br>(  ) cable eléctrico<br>(  ) fibra óptica<br>(  ) suministros esenciales<br>(  ) equipos de destrucción de soportes de información<br>(  ) mobiliario: armarios, etc |

| |
|---|
| (  ) cajas fuertes |
| (  ) Otros._____ |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO INSTALACIONES** |
|---|
| Marque (X) los activos con los que cuenta la dependencia |
| (  ) recinto |
| (  ) edificio |
| (  ) cuarto |
| (  ) plataformas móviles |
| (  ) Vehículo terrestre: coche, camión, etc. |
| (  ) Vehículo aéreo: avión, etc. |
| (  ) Vehículo marítimo: buque, lancha, etc. |
| (  ) contenedores |
| (  ) canalización |
| (  ) instalaciones de respaldo |
| (  ) Otros._____ |

| **TABLA DE RELACIÓN DE ACTIVOS DE TIPO PERSONAL** |
|---|
| Marque (X) los activos con los que cuenta la dependencia |
| (  ) usuarios externos |
| (  ) usuarios internos |
| (  ) operadores |
| (  ) administradores de sistemas |
| (  ) administradores de comunicaciones |
| (  ) administradores de BBDD |
| (  ) administradores de seguridad |
| (  ) desarrolladores / programadores |
| (  ) subcontratas |
| (  ) proveedores |

## Anexo F

## Inventario de activos del proceso gestión de la infraestructura tecnológica

| N° | Nombre del activo | Descripción del activo | Tipo de Activo | Ubicación |
|---|---|---|---|---|
| 1 | Datos vitales | Datos que almacenan los diferentes sistemas de información esenciales para el funcionamiento de la MPH | Dato/Información | Data Center |
| 2 | Archivos Personales | Documentos personales de los trabajadores de la MPH | Dato/Información | Computadoras Personales |
| 3 | Copias de Respaldo | Copias de respaldo de la datos/información que manejan los distintos sistemas de la MPH | Dato/Información | Data Center/PC Administrador |
| 4 | Datos de Configuración de los Sistemas de Información | Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes sistemas de información | Dato/Información | Archivo físico (estantería) |
| 5 | Datos de Gestión interna | Corresponde a los documentos de la MPH | Dato/Información | Archivo físico (estantería)/VPS |
| 6 | Credenciales (contraseñas) | Usuario y Contraseña que utilizan los usuarios para ingresar a los recursos tecnológicos. | Dato/Información | Excel (Administradores) |
| 7 | Datos de control de acceso | Corresponde a los datos de los usuarios internos que utilizan los sistemas de información y/o aplicaciones | Dato/Información | Base de Datos/Usuario Interno |
| 8 | Log de los sistemas de información | Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones. | Dato/Información | Servidores |
| 9 | Código fuente de los sistemas de información | Corresponde a los códigos fuente de los distintos sistemas desarrollados en MPH | Dato/Información | Servidores de Versiones (en la nube) |
| 10 | Código ejecutable | Corresponde a los códigos ejecutables de los diferentes sistemas de información | Dato/Información | Servidor de desarrollo/Disco de backup) |
| 11 | Servicios online | Corresponde a los servicios de consulta como por ejemplo: Portal de transparencia, Foro Municipal, consulta de visita a funcionarios. | Servicio | Página Web de la MPH |
| 12 | Correo electrónico | Correo electrónico institucional | Servicio | Servidor de correo electrónico GMAIL corporativo |
| 13 | Gestión de privilegios | Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones. | Servicio | Sistemas de información |
| 14 | Base de Datos | Bases de datos de los diferentes sistemas que almacenan la información de la entidad | Servicio | Servidores de base de Datos |

| N° | Nombre del activo | Descripción del activo | Tipo de Activo | Ubicación |
|---|---|---|---|---|
| 15 | Página Web | Página Web de la entidad | Software/Aplicaciones informática | VPS |
| 16 | Sistema de trámite documentario | Sistema para la gestión de trámite externo e interno, utilizado por la unidad de trámite documentario y archivos | Software/Aplicaciones informática | Servidor de aplicaciones Windows |
| 17 | Aplicación de atención en línea | Sistema de orientación en tiempo real (mediante de un chat) sobre los servicios que ofrece la MPH | Software/Aplicaciones informática | Servidor VPS |
| 18 | Sistema de Registro de visitas | Sistema de registro de visitas que los usuarios hacen a la MPH | Software/Aplicaciones informática | Servidor de aplicaciones Linux |
| 19 | Muniyachay | Repositorio de cursos que se dictan en la MPH | Software/Aplicaciones informática | Servidor VPS |
| 20 | Calendario de actividades | Registro de las actividades que se realizan en la MPH | Software/Aplicaciones informática | Servidor VPS |
| 21 | SIAF | Sistema que manejan las dependencias de la oficina de administración | Software/Aplicaciones informática | Servidor SIAF |
| 22 | SIAL | Sistema que maneja la información ambiental local de Huamanga | Software/Aplicaciones informática | Servidor de Ministerio de ambiente |
| 23 | Sistema de Catastro virtual y ficha catastral | Sistemas que usa la Sub Gerencia de Planeamiento Urbano y Catastro | Software/Aplicaciones informática | Servidor de aplicación catastro/servidor de BD Catastro |
| 24 | SIGALEC | Aplicativo de la Subgerencia de Control Urbano y Licencias | Software/Aplicaciones informática | Servidor de aplicación catastro/servidor de BD Catastro |
| 25 | Sistema Gestor de Base de Datos | Sistema de gestión y administración de las bases de datos de la entidad | Software/Aplicaciones informática | PC de los administradores |
| 26 | Aplicaciones Comerciales | Office, sistemas operativos, antivirus, entre otros | Software/Aplicaciones informática | Computadoras Personales |
| 27 | Gestor de máquinas virtuales | Aplicativo que gestiona las máquinas virtuales | Software/Aplicaciones informática | PC Administradores |
| 28 | Scripts de backup | Scripts para sacar backup | Software/Aplicaciones informática | PC Administradores |
| 29 | Aplicativos de Desarrollo | Aplicativos que se usan para el desarrollo de software interno | Software/Aplicaciones informática | PC de administradores |
| 30 | Servidores de aplicaciones de Producción | Servidores de producción que soportan las aplicaciones y sistemas de información | Equipos informáticos | Data Center de la Municipalidad |
| 31 | Servidores de Base de datos | Servidores de producción que soportan los motores e instancias de bases de datos | Equipos informáticos | Data Center de la Municipalidad |
| 32 | Servidores de prueba | Servidor en que se realizan las pruebas de los sistemas de información. | Equipos informáticos | Data Center de la Municipalidad |
| 33 | Servidor de desarrollo | Servidor de desarrollo | Equipos informáticos | |
| 34 | Computador del Funcionario | Computadores que utilizan los funcionarios de la entidad | Equipos informáticos | Sub Gerencia de Sistemas y Tecnología |

| N° | Nombre del activo | Descripción del activo | Tipo de Activo | Ubicación |
|---|---|---|---|---|
| 35 | Computadores administradores de SI | Computadores que utilizan los administradores de las plataformas, los desarrolladores | Equipos informáticos | Sub Gerencia de Sistemas y Tecnología |
| 36 | Computadores de escritorio usuarios | Computadores asignados a los colaboradores de la Subgerencia de Sistemas y Tecnología | Equipos informáticos | Sub Gerencia de Sistemas y Tecnología |
| 37 | Impresoras | Impresoras de la subgerencia | Equipos informáticos | Sub Gerencia de Sistemas y Tecnología |
| 38 | Escáner | Escáner de la subgerencia | Equipos informáticos | Sub Gerencia de Sistemas y Tecnología |
| 39 | Firewall | Equipos informáticos destinados a proteger la seguridad perimetral de la entidad | Equipos informáticos | Data center |
| 40 | Soporte de la red | Equipamiento necesario para transmitir datos: routers, módems, switch, punto de acceso inalámbrico | Equipos informáticos | Data center |
| 41 | Centralita telefónica | Red de comunicación analógica | Redes de Comunicaciones | Data center |
| 42 | ADSL | Infraestructura utilizada para la conectividad | Redes de Comunicaciones | Data center |
| 43 | Red inalámbrica | Red de comunicación inalámbrica | Redes de Comunicaciones | Oficinas de la MPH |
| 44 | Red local | Red de comunicaciones cableada | Redes de Comunicaciones | Red local |
| 45 | Internet | Red de redes | Redes de Comunicaciones | Internet |
| 46 | Discos Virtuales | Dispositivo de almacenamiento virtual | Soportes de Información | Servidor virtualizado |
| 47 | Disco duro externo | Disco duro externo | Soportes de Información | Data center |
| 48 | Dispositivos de almacenamiento externo | CDs, DVDs, etc. | Soportes de Información | Archivo físico o estante |
| 49 | Soportes no electrónicos | Dispositivos físicos de almacenamiento no electrónico como material impreso | Soportes de Información | Archivo físico o estante |
| 50 | Sistema de alimentación ininterrumpida | UPS | Equipamiento auxiliar | oficinas |
| 51 | Sistema de aire acondicionado | Sistema de aire acondicionado | Equipamiento auxiliar | Data Center |
| 52 | Gabinetes | Armarios de soporte a los sistemas de información | Equipamiento auxiliar | Data center |
| 53 | Data Center | Centro Principal de procesamiento donde reside la infraestructura para soporta la operación del negocio | Instalaciones | Local central de la MPH |
| 54 | Área de personal | Instalación donde están ubicados los colaboradores de la Subgerencia | Instalaciones | Local central de la MPH |
| 55 | Usuarios Externos | Usuarios externos a la MPH y que usan los servicios a través de la Página Web | Personal | Usuarios Externos |

| N° | Nombre del activo | Descripción del activo | Tipo de Activo | Ubicación |
|---|---|---|---|---|
| 56 | Usuarios Internos | Personal propio de la MPH | Personal | Oficinas de la MPH |
| 57 | Administradores de las plataformas | Corresponde a los administradores de los diferentes Sistemas, comunicaciones, BBDD, Seguridad | Personal | Subgerencia de Sistemas y Tecnologías |
| 58 | Desarrolladores/Programadores | Personal encargado de producir los sistemas de información | Personal | Subgerencia de Sistemas y Tecnologías |
| 59 | Personal de soporte técnico | Personal encargado del soporte técnico de la Municipalidad | Personal | Subgerencia de Sistemas y Tecnologías |
| 60 | Proveedores | Proveedores de tecnología y comunicaciones | Personal | Externo |

Nota: Elaboración propia

# Anexo G

## Cuestionario para la valorar los activos de información

| | | Confidencialidad | | | Integridad | | | Disponibilidad | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | ¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras, causando pérdida económica? | ¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control? | ¿Su divulgación no autorizada puede afectar la imagen de la entidad? | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad? | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control? | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad? | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad? | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control? | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad? |
| **N°** | **Nombre del activo** | **Económico** | **Legal** | **Imagen** | **Económico** | **Legal** | **Imagen** | **Económico** | **Legal** | **Imagen** |
| 1 | Datos vitales | | | | | | | | | |
| 2 | Archivos Personales | | | | | | | | | |
| 3 | Copias de Respaldo | | | | | | | | | |
| 4 | Datos de Configuración de los Sistemas de Información | | | | | | | | | |
| 5 | Datos de Gestión interna | | | | | | | | | |
| 6 | Credenciales (contraseñas) | | | | | | | | | |
| 7 | Datos de control de acceso | | | | | | | | | |
| 8 | Log de los sistemas de información | | | | | | | | | |
| 9 | Código fuente de los sistemas de información | | | | | | | | | |
| 10 | Código ejecutable | | | | | | | | | |
| . . . | | | | | | | | | | |
| 60 | Proveedores | | | | | | | | | |

# Anexo H

## Cuestionario para identificar amenazas y establecer probabilidad de materialización

| Amenaza | Marca (X) | Probabilidad de ocurrencia |
|---|---|---|
| Fuego | | |
| Tormenta eléctrica, rayo | | |
| Error de Usuario | | |
| Errores del administrador | | |
| Errores de configuración | | |
| Alteración accidental de la información | | |
| Destrucción de Información | | |
| Fugas de Información | | |
| Vulnerabilidades de los programas (software) | | |
| Errores de mantenimiento / actualización de programas (software) | | |
| Errores de mantenimiento / actualización de equipos (hardware) | | |
| Caída del sistema por agotamiento de recursos (interrupción en los servicios) | | |
| Indisponibilidad del personal | | |
| Manipulación de los registros de Actividad (log) | | |
| Manipulación de la configuración | | |
| Suplantación de la identidad del usuario | | |
| Abuso de privilegios de acceso | | |
| Difusión de software dañino | | |
| Acceso no autorizado | | |
| Modificación deliberada de la información | | |
| Destrucción deliberada de Información | | |
| Divulgación de la Información | | |
| Manipulación de programas | | |
| Manipulación de los equipos | | |
| Denegación del servicio | | |
| Robo de Equipos | | |
| Indisponibilidad deliberada del personal | | |
| Extorsión | | |
| Ejecución de ingeniería social | | |
| Corte del suministro eléctrico | | |
| Condiciones inadecuadas de temperatura o humedad | | |
| Degradación de los soportes de almacenamiento de la información | | |
| Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones | | |
| Hacking no ético | | |
| Instalación de software no autorizado | | |
| Otro:_____ | | |

# Anexo I

## Tabla de descripción de amenazas, riesgos y consecuencias.

| AMENAZAS | | | | | | | RIESGOS | |
|---|---|---|---|---|---|---|---|---|
| CÓDIGO | AMENAZA | DESCRIPCIÓN | TIPOS DE ACTIVOS AFECTADOS | DIMENSIONES | | | RIESGO | CONSECUENCIA |
| | | | | C | I | D | | |
| 1 | Fuego | Incendios: posibilidad de que el fuego acabe con recursos del sistema. | Equipos informáticos, soportes de información, equipamiento auxiliar, instalaciones | | | 1 | Incendio | pérdida de los activos de información (activos no disponibles) |
| 2 | Tormenta eléctrica, rayos | Incidentes que se producen sin intervención humana | Equipos informáticos, soportes de información, equipamiento auxiliar, instalaciones | | | 1 | Apagón | No disponibilidad de la infraestructura tecnológica |
| 3 | Error de Usuario | Equivocaciones de las personas cuando usan los servicios, datos, etc. | Datos/información, servicios, aplicaciones (software), soportes de información | 2 | 1 | 3 | Equivocaciones de los usuarios | No disponibilidad, de los datos/información, soportes de información , etc. |
| 4 | Errores del administrador | Equivocaciones de personas con responsabilidades de instalación y operación de los sistemas de información | Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones, soportes de información | 3 | 2 | 1 | Equivocaciones de los administradores | Mal funcionamiento de los servicios/SI |
| 5 | Errores de configuración | Introducción de datos de configuración erróneos. | Datos de configuración | | 1 | | Introducción de datos de configuración erróneos. | Pérdida de la integridad de los datos |
| 6 | Alteración accidental de la información | Alteración accidental de la información.<br>Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. | Datos/información, servicios, aplicaciones (SW) comunicaciones (tránsito), soportes de información, instalaciones | | 1 | | Alteración de los datos | Pérdida de la disponibilidad |
| 7 | Eliminación accidental de Información | Pérdida accidental de información.<br>Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. | Datos/información, servicios, aplicaciones (SW), comunicaciones (tránsito), soportes de información, instalaciones | | | 1 | Eliminación de la Información | Pérdida total de información. |
| 8 | Fugas de Información | Revelación por indiscreción.<br>Incontinencia verbal, medios electrónicos, soporte papel, etc. | Datos/información, servicios, aplicaciones (SW), comunicaciones (tránsito), soportes de información, instalaciones, personal (revelación) | 1 | | | Mal uso de la información | Pérdida de la confidencialidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 9 | Vulnerabilidades de los programas (software) | Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. | Aplicaciones (software) | 3 | 1 | 2 | Defectos en el código | Pérdida de la integridad de los datos o la capacidad de operar de los sistemas y/o aplicaciones. |
| 10 | Errores de mantenimiento/actualización de programas (software) | Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. | Aplicaciones (software) | | 1 | 2 | Defectos en los procedimientos o controles de actualización del código. | Pérdida de la disponibilidad de los sistemas y/o aplicaciones. |
| 11 | Errores de mantenimiento/actualización de equipos (hardware) | Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. | Equipos informáticos, soportes electrónicos, equipamiento auxiliar | | | 1 | Defectos en los procedimientos o controles de actualización de los equipos. | Mal funcionamiento de los equipos |
| 12 | Indisponibilidad del personal por enfermedad | Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público. | Personal interno | | | 1 | Insatisfacción de los clientes | No se atiendan los servicios adecuadamente |
| 13 | Manipulación de los registros de Actividad (log) | Manipulación intencionada de los registros de actividad | Registros de actividad | | 1 | | Disminuye su valor como evidencia | Pérdida de la integridad del log |
| 14 | Suplantación de la identidad del usuario | Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. | Datos/información, servicios, aplicaciones (software), redes de comunicaciones | 1 | 3 | 2 | Mal uso intencionado de la infraestructura tecnológica | Modificación de la información |
| 15 | Abuso de privilegios de acceso | Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. | Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones | 1 | 2 | 3 | Abuso de privilegios para realizar tareas que no son de su competencia. | Modificación a los accesos o información |
| 16 | Difusión de software dañino | Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | Aplicaciones (software) | 3 | 2 | 1 | Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | Pérdida de dato/información |
| 17 | Acceso no autorizado | El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. | Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones, soportes de información, equipamiento auxiliar, | 1 | 2 | | Ataque a los recursos del sistema | Hackeo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | instalaciones | | | | | |
| 18 | Destrucción deliberada de Información | Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. | Datos/información, servicios (acceso), aplicaciones (SW), soportes de información, instalaciones | | | 1 | Eliminación intencional de información | Información no disponible |
| 19 | Manipulación de programas | Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. | Aplicaciones (software) | 1 | 2 | 3 | Alteración intencionada del funcionamiento de los programas. | Mal funcionamiento de los programas |
| 20 | Caída del sistema por agotamiento de recursos | la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. | Servicios, equipos informáticos, redes de comunicaciones | | | 1 | No disponibilidad de los sistemas | Insatisfacción de los clientes, llamadas de atención, sanciones graves, pérdida de imagen |
| 21 | Robo de Equipos | La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. | Equipos informáticos, soportes de información, equipamiento auxiliar | 2 | | 1 | Carencia de un medio para prestar los servicios, es decir una indisponibilidad. | pérdida económica, Insatisfacción de los clientes, llamadas de atención, sanciones graves, pérdida de imagen |
| 22 | Indisponibilidad del personal por huelga | Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, etc. | Personal interno | | | 1 | Cierre de la entidad por falta de personal, mayor carga laboral. | Insatisfacción de los clientes, no prestación de los servicios |
| 23 | Ejecución de ingeniería social | Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. | Personal interno | 1 | 2 | 3 | Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. | Robo de información |
| 24 | Corte del suministro eléctrico | Cese de la alimentación de potencia | Equipos informáticos, soportes de información, equipamiento auxiliar | | | 1 | Malogren los equipos, pérdida de la información | Dejen de funcionar los servicios, insatisfacción del cliente |
| 25 | Condiciones inadecuadas de temperatura o humedad | Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc. | Equipos informáticos, soportes de información, equipamiento auxiliar | | | 1 | Malogren los equipos | No disponibilidad de los equipo y servicios prestados a través de ellos |
| 26 | Degradación de los soportes de almacenamiento de la información | Degradación como consecuencia del paso del tiempo | Soportes de información | | | 1 | Pérdida de información | No disponibilidad de la información |
| 27 | Instalación de software no autorizado | Instalación de software no autorizado por parte del personal interno. | Aplicaciones (software) | 1 | 2 | | Infectar/malograr el sistema | sanciones por uso de software no autorizado y sin licencia, funcionamiento incorrecto |
| 28 | Inestabilidad de la línea de internet | Fallo en el servicio prestado por un tercero | Servicios | | | 1 | No disponibilidad de los servicios | Insatisfacción de los clientes |

# Anexo J

## Controles para el tratamiento de riesgos

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| Data Center | 5 | 5 | 5 | Fuego | Extintores vencidos. Falta de capacitación en uso de extintores, ausencia de un sistema de continuidad del negocio, falta de mecanismos de respaldo de información. | Incendio | Bajo | Bajo | Medio | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Uso de estándar para el diseño de un Data Center Compra de extintores y capacitación al personal. Instalación de detectores de humo. Plan de contingencia. | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | Tormenta eléctrica, rayos | Ausencia de un sistema de continuidad de negocio. | Apagón | Bajo | Bajo | **Alto** | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Uso de estándar para el diseño de un Data Center Pozo a tierra, pararrayos. UPS para dispositivos críticos. Mantenimiento de grupos electrógenos. | Jefe de la Subgerencia de Sistemas y Tecnología. |
| | | | | Errores del administrador | Falta de capacitación. Mala segregación de funciones, desmotivación del personal. | Equivocaciones de los administradores | Bajo | Medio | **Alto** | Mitigar | A.11.1.2 Controles de ingreso físico. A.11.1.5 Trabajo en áreas seguras. | Elaborar un plan de seguridad. Capacitaciones en temas de seguridad. Verificación de funciones. | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | Suplantación de la identidad del usuario | Usuarios confiados, no hay un registro de quién entra y qué hace en el Data Center. | Mal uso intencionado de la infraestructura tecnológica | **Alto** | Medio | Bajo | Mitigar | A.9.3.1 Uso de información de autentificación secreta. A.11.1.2 Controles de ingreso físico. | Buenas prácticas en el uso de información de autentificación secreta. Implementar control de acceso restringido y controlar las tareas que se realizan dentro del Data Center. | Jefe de la Subgerencia de Sistemas y Tecnología Oficial de seguridad |
| | | | | Abuso de privilegios de acceso | Mala segregación de funciones, administradores descontentos. | Abuso de los privilegios para realizar tareas que no son de su competencia. | **Alto** | **Alto** | Bajo | Mitigar | A.7.2.3 Proceso disciplinario A.11.1.2 Controles de ingreso físico. | Correcta segregación de funciones. Términos y condiciones de contrato claros en temas de seguridad. | Jefe de Recursos Humanos |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Acceso no autorizado | Usuarios confiados, no hay un registro de quién entra y qué hace en el Data Center. | Ataque a los recursos del sistema | Medio | Medio | Bajo | Mitigar | A.11.1.2 Controles de ingreso físico. A.11.1.3 Asegurar oficinas, áreas e instalaciones. | Instalación de cámaras de video vigilancia. Implementación de un control de acceso seguro (biométrico, etc.) | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | Robo de Equipos | No hay un registro de quién entra y qué hace en el Data Center, no existe inventario de activos, ausencia o inadecuada plataforma de vigilancia, | Carencia de un medio para prestar los servicios, es decir una indisponibilidad. | Medio | Bajo | Bajo | Mitigar | A.11.1.3 Asegurar oficinas, áreas e instalaciones. | Instalación de cámaras de video vigilancia. Inventario de activos de información del Data Center. | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | Corte del suministro eléctrico | Falta de algunos UPS. | Malogren los equipos, pérdida de la información | Bajo | Bajo | **Alto** | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Adquisición de equipos alimentación ininterrumpida para equipos críticos del Data Center. Mantenimiento de equipos de alimentación ininterrumpida. Acuerdos de niveles de servicio con Electrocentro. | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | Condiciones inadecuadas de temperatura o humedad | No se monitoriza las condiciones de temperatura y humedad | Malogren los equipos | Bajo | Bajo | **Alto** | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Monitoreo constante de temperatura del Data Center | Administrador del Data Center |
| Local de la Sub Gerencia | 4 | 4 | 4 | Fuego | Extintores vencidos. Falta de capacitación en uso de extintores | Incendio | Bajo | Bajo | Medio | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Compra de extintores y capacitación al personal. | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | tormenta eléctrica, rayos | Falta de Pozo a tierra y sistema eléctrico estable | Apagón | Bajo | Bajo | **Alto** | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Implementación de Pozo a tierra. Adquisición de equipos alimentación ininterrumpida | Jefe de la Subgerencia de Sistemas y Tecnología |
| | | | | Suplantación de la identidad del usuario | Usuarios confiados. Inexistencia de reg. de quienes entran a la SG. | Mal uso intencionado de la infraestructura tecnológica | Medio | Medio | Medio | Mitigar | A.11.1.2 Controles de ingreso físico. | Sistema de gestión de visitas | Portería/Secretaría de la subgerencia |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Acceso no autorizado | Inadecuado control de seguridad. | Ataque a los recursos del sistema | Medio | Bajo | Bajo | Mitigar | A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles de ingreso físico. | Establecer controles para indicar las áreas accesibles por los visitantes, implementar control de acceso restringido y controlar el acceso (Sistema de gestión de visitas). | Jefe de la Subgerencia de Sistemas y Tecnología/Oficial de seguridad. |
| | | | | Robo de Equipos | No existe inventario de activos. Vigilancia en la Subgerencia, inadecuada plataforma de vigilancia. | Carencia de un medio para prestar los servicios, es decir una indisponibilidad. | Medio | Bajo | Medio | Mitigar | A.11.1.3 Asegurar oficinas, áreas e instalaciones. A.11.2.5 Remoción de activos | Establecer controles de acceso restringido. Inventario de activos. Controles de remoción de activos. | Jefe de la Subgerencia de Sistemas y Tecnología/Oficial de seguridad. |
| | | | | Corte del suministro eléctrico | Falta de algunos UPS, inestabilidad del sistema eléctrico. | Malogren los equipos, pérdida de la información | Bajo | Bajo | **Alto** | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Adquisición de equipos alimentación ininterrumpida. Mantenimiento equipos alimentación ininterrumpida. Acuerdos de niveles de servicio con Electrocentro. | Jefe de la Subgerencia de Sistemas y Tecnología/Oficial de seguridad. |
| | | | | Condiciones inadecuadas de temperatura o humedad | inadecuada ubicación de equipos y ventilación del local | Malogren los equipos | Bajo | Bajo | **Alto** | Mitigar | A.11.1.4 Protección contra amenazas externas y ambientales. | Establecer controles de seguridad y salud en las oficinas. | Jefe de la Subgerencia de Sistemas y Tecnología/Oficial de seguridad. Jefe de recursos Humanos |
| Copias de respaldo | 5 | 5 | 5 | Errores del administrador | Falta de plan de gestión de sistemas y políticas de respaldo y un adecuado estudio de sistemas críticos, entrenamiento insuficiente en temas de seguridad. | Equivocaciones de los administradores | Bajo | Bajo | **Alto** | Mitigar | A.8.2 Clasificación de la información A.12.3.1 Respaldo de la información | Clasificación de la información, etiquetado y manejo. Establecer políticas de respaldo. Establecer un plan o cronograma de prueba de backups Almacenamiento de backups fuera del Data Center. | Oficial de seguridad/ Administrador de BD |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Errores de configuración | No existe un manual del administrador | Introducción de datos de configuración erróneos. | Bajo | Medio | Bajo | Mitigar | A.12.3.1 Respaldo de la información A.12.4.3 Registros del administrador y del operador | Elaboración de un manual de administrador. Revisar log de eventos. | Oficial de seguridad/ Administrador de BD |
| | | | | Fugas de Información | Poca fidelización trabajadores, no existe un registro de acceso y manejo de backup | Mal uso de la información | **Alto** | Bajo | Bajo | Mitigar | A.12.3.1 Respaldo de la información A. 12.4.3 Registros del administrador y del operador | Establecimiento de métodos de cifrado. Prevención de la exposición de backups. Almacenamiento en lugares seguros y control de acceso a backups. | Oficial de seguridad/ Administrador de BD |
| | | | | Destrucción deliberada de Información | Poca fidelización trabajadores, no existe un registro de acceso y manejo de backup, falta de un plan de contingencia, Ausencia de un sistema de continuidad del negocio. | Eliminación intencional de información | Bajo | Bajo | Medio | Mitigar | A.12.3.1 Respaldo de la información A.12.4.1 Registro de eventos. | Almacenamiento en lugares seguros y control de acceso a backups. Revisar log de eventos. Elaboración del plan de contingencia. | Oficial de seguridad/ Administrador de BD |
| Servidores de Aplicación | 4 | 4 | 5 | Errores del administrador | No existe un plan/manual de los sistemas que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios, desmotivación | Equivocaciones de los administradores | Bajo | Medio | **Alto** | Mitigar | A.8.2 Clasificación de la información A.12.4.3 Registros del administrador y del operador | Manual de sistemas y requerimientos técnicos. Elaboración de un procedimiento formal de control de cambios. Elaboración de un procedimiento formal de manejo de servidores Capacitación en temas de seguridad. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Errores de configuración | Inexistencia de plan de configuración y manejo de log | Introducción de datos de configuración erróneos. | Bajo | Medio | Bajo | Mitigar | A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos. | Elaboración del manual de configuración de servidores. Actualización de log de eventos. | Oficial de seguridad/ Administrador de Servidores de aplicación |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Alteración accidental de la información | Inexistencia de normas de seguridad. | Alteración de los datos | Bajo | Bajo | **Alto** | Mitigar | A.8.2 Clasificación de la información A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos. | Control de versiones del software. Procedimiento formal de control de cambios. Verificación de roles y permisos. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Eliminación accidental de Información | Inexistencia de normas de seguridad y plan de contingencia. | Eliminación de la Información | Bajo | **Alto** | Bajo | Mitigar | A.8.2 Clasificación de la información A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos. | Control de versiones del software. Procedimiento formal de control de cambios. Verificación de roles y permisos. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Vulnerabilidades de los programas (software) | Falta de licencia | Defectos en el código | Bajo | **Alto** | **Alto** | Mitigar | A.14.2.4 Restricción sobre cambios a los paquetes software. A.16.6.1 Gestión de vulnerabilidades técnicas. | Adquisición de licencia de programas y/o evaluación del uso de software libre. Gestión de vulnerabilidades | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Errores de mantenimiento/actualización de programas (software) | Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica. | Defectos en los procedimientos o controles de actualización del código. | Bajo | **Alto** | Bajo | Mitigar | A.16.6.1 Gestión de vulnerabilidades técnicas | Elaboración de un plan de mantenimiento y actualización de software. Elaboración de un plan de contingencia. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Errores de mantenimiento/actualización de equipos (hardware) | Inexistencia de plan de mantenimiento y vigilancia tecnológica, falta de equipos de contingencia, ausencia de un sistema de continuidad del negocio. | Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. | Bajo | Bajo | **Alto** | Mitigar | A.11.2.4 Mantenimiento de equipos A.16.6.1 Gestión de vulnerabilidades técnicas | Elaboración de un Plan de contingencia – Equipos de contingencia. Plan de mantenimiento de hardware | Oficial de seguridad/ Administrador de Servidores de aplicación |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Abuso de privilegios de acceso | Falta de políticas de acceso y auditorías internas. (cuentas de usuario sin auditar) | Abuso del privilegios para realizar tareas que no son de su competencia. | Alto | Alto | Alto | Mitigar | A.7.2.3 Proceso disciplinario<br>A.9.4.1 Restricción de acceso a la información. | Elaboración de políticas de acceso.<br>Diseñar esquemas de seguridad basado en roles y permisos<br>Diseñar un esquema de privilegios sobre el fileserver | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Difusión de software dañino | falta de monitoreo del estado y reglas del firewall y antivirus, inadecuada asignación de roles y permisos, no existe políticas de seguridad. | Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | Bajo | Medio | Alto | Mitigar | A.12.2.2 Controles contra códigos maliciosos.<br>A.16.6.2 Restricción sobre la instalación de software | Plataforma de seguridad perimetral.<br>Control de la red.<br>Control de instalación de software.<br>Actualización de antivirus (monitorización) | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Acceso no autorizado | Falta de monitoreo del estado y reglas del firewall, antivirus, configuración incorrecta de las cuentas de usuario. | Ataque a los recursos del sistema | Medio | Bajo | Bajo | Mitigar | A.14.2.8 Pruebas de seguridad del sistema. | Diseñar esquemas de seguridad basado en roles y permisos<br>Diseñar un esquema de privilegios sobre el fileserver.<br>Plataforma de seguridad perimetral. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Caida del sistema por agotamiento de recursos | No existe un monitoreo de consumo de recursos hardware de los sistemas, falta de mantenimiento de equipos. | No disponibilidad de los sistemas | Bajo | Bajo | Alto | Mitigar | A.11.2.3 Seguridad del cableado.<br>A.13.1.3 Segregación en redes. | Plataforma de seguridad perimetral.<br>Elaboración de un Plan de contingencia – monitoreo preventivo de consumo de recursos Hardware de los sistemas. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Corte del suministro eléctrico | Susceptibilidad a las variaciones de tensión. | Malogren los equipos, pérdida de la información | Bajo | Bajo | Alto | Mitigar | A.11.2.2 Servicios de suministro | Contar con sistema de alimentación ininterrumpida.<br>Mantenimiento de sistema de alimentación ininterrumpida. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Condiciones inadecuadas de temperatura o humedad | Susceptibilidad a humedad, recalentamiento, polvo y suciedad | Malogren los equipos | Bajo | Bajo | Alto | Mitigar | A.11.2.1 Emplazamiento y protección de los equipos.<br>A.11.2.4 Mto. Eq | Ubicación adecuada de equipos según estándares internacionales.<br>Plan de mantenimiento de equipos. | Oficial de seguridad/ Administrador de Servidores de aplicación |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Degradación de los soportes de almacenamiento de la información | Equipos/dispositivos Susceptibilidad a cambios de temperatura y humedad, falta de esquemas de reemplazo. | Pérdida de información | Bajo | Bajo | Medio | Mitigar | A.11.2.4 Mantenimiento de equipos | Plan de mantenimiento de soportes de información. Inventario de activos y monitoreo del funcionamiento y tiempo de vida. | Oficial de seguridad/ Administrador de Servidores de aplicación |
| | | | | Inestabilidad de la línea de internet | Un solo proveedor de servicios de comunicaciones, gestión inadecuada de la red. | No disponibilidad de los servicios | Bajo | Bajo | **Alto** | Mitigar/ Transferir | A.13.1.2 Seguridad de servicios de red. | Plan de contingencia- Uso de varias líneas dedicadas y redundancia de servicios con diversos proveedores del servicio. – balanceo de carga. Acuerdos de nivel de servicio con el(los) provedor(es) de comunicaciones | Oficial de seguridad/ Administrador de Servidores de aplicación/ Proveedor de comunicaciones |
| Bases de Datos | 4 | 4 | 4 | Error de Usuario | Mala configuración de perfiles, falta de capacitación, inexistencia de procedimientos de control de cambios. | Equivocaciones de los usuarios | Bajo | **Alto** | Bajo | Mitigar | A.9.4.1 Restricción de acceso a la información A.7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información. | Prevención del abuso de derechos excesivos: identificaciòn y eliminación de derechos excesivos, implementar controles a nivel consulta. Perfilado dinámico (Dynamic Profiling) de SecureSphere: gestión de los permisos de los usuarios y control automatizado de acceso a nivel de consulta. Capacitación en temas de seguridad. | Oficial de seguridad/ Administrador de BD |
| | | | | Errores del administrador | No existe un plan/manual de los sistemas que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios, desmotivación | Equivocaciones de los administradores | Bajo | Medio | Medio | Mitigar | A.12.1.2 Gestión del cambio | Elaboración de un plan de seguridad. Elaboración de procedimientos de control de cambios. Capacitación en temas de seguridad, segregación adecuada de funciones.. | Oficial de seguridad/ Administrador de BD |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Errores de configuración | Inexistencia de plan de configuración y falta de capacitación, desconocimiento de medidas de seguridad. | Introducción de datos de configuración erróneos. | Bajo | Medio | Bajo | Mitigar | A.12.1.1 Procedimientos operativos documentados. | Elaboración de un manual del administrador, capacitaciones. | Oficial de seguridad/ Administrador de BD |
| | | | | Alteración accidental de la información | Poco conocimiento en temas de seguridad, mala definición de permisos y accesos, inexistencia de un plan de respaldo, ausencia de procedimientos de control de cambios. | Alteración de los datos | Bajo | Bajo | Medio | Mitigar | A.9.4.1 Restricción de acceso a la información A.12.1.2 Gestión del cambio | Elaboración de un plan de backup. Procedimientos de control de cambios. Gestión de permisos | Oficial de seguridad/ Administrador de BD |
| | | | | Eliminación accidental de Información | Poco conocimiento en temas de seguridad, mala definición de permisos y accesos, inexistencia de un plan de respaldo, ausencia de procedimientos de control de cambios. | Eliminación de la Información | Bajo | **Alto** | Bajo | Mitigar | A.12.3.1 Respaldo de la información. | Elaboración de un plan de backup. Procedimientos de control de cambios. Gestión de permisos | Oficial de seguridad/ Administrador de BD |
| | | | | Fugas de Información | Abuso de privilegios, inexistencia de mecanismo de control de acceso. | Mal uso de la información | **Alto** | Bajo | Bajo | Mitigar | A.7.2.3 Proceso disciplinario. A.13.1.2 Seguridad de servicios de red. A.14.1.3 Protección de transacciones en servicios de aplicación. | Gestión de permisos. Penalidades en los contratos. Prevención de los ataques de protocolo de comunicación de BD. Identificación de tablas con información confidencial. Cifrado de datos | Oficial de seguridad/ Administrador de BD/ Jefe de RR.HH |
| | | | | Vulnerabilidades de los programas (software) | Falta de licencia, inexistencia de monitorización de software/versiones. | Defectos en el código | Bajo | **Alto** | Bajo | Mitigar | A.14.1.1 Análisis y especificación de requisitos de seguridad de la información. | Evaluación y parcheo de vulnerabilidades. | Oficial de seguridad/ Administrador de BD |
| | | | | Errores de mantenimiento/actualización de programas (software) | Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica. | Defectos en los procedimientos o controles de actualización del código. | Bajo | **Alto** | **Alto** | Mitigar | A.14.2.3 Revisión técnica de aplicaciones después de cambios a la PO | Compra de licencia y/o evaluación de uso de software libre. Plan de mantenimiento y vigilancia tecnológica. | Oficial de seguridad/ Administrador de BD |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Errores de mantenimiento/actualización de equipos (hardware) | Inexistencia de plan de mantenimiento y vigilancia tecnológica, falta de equipos de contingencia, ausencia de un sistema de continuidad del negocio. | Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. | Bajo | Bajo | **Alto** | Mitigar | A.11.2.4 Mantenimiento de equipos. | Plan de mantenimiento y vigilancia tecnológica. Plan de contingencia y equipos de contingencia. | Oficial de seguridad/ Administrador de BD |
| | | | | Manipulación de los registros de Actividad (log) | Trazas de auditoría ineficientes | Disminuye su valor como evidencia | Bajo | Medio | Bajo | Mitigar | A.12.4.2 Protección de información de registros. | Prevención de auditorías deficientes | Oficial de seguridad/ Administrador de BD |
| | | | | Suplantación de la identidad del usuario | Falta capacitación del personal en temas de seguridad. | Mal uso intencionado de la infraestructura tecnológica | Medio | Bajo | Medio | Mitigar | A.9.3.1 Uso de información de autentificación secreta. | Capacitaciones en temas de seguridad (Phising, scam, etc) | Oficial de seguridad/ Administrador de BD |
| | | | | Abuso de privilegios de acceso | Mala configuración de permisos de acceso, inexistencia de documento que autorice los permisos para un usuario, mala segregación de roles, inexistencia de mecanismo de control de acceso. | Abuso del privilegios para realizar tareas que no son de su competencia. | **Alto** | Medio | Bajo | Mitigar | A.7.2.3 Proceso disciplinario A.9.4.1 Restricción de acceso a la información. | Prevención del abuso de derechos excesivos: identificación y eliminación de derechos excesivos, implementar controles a nivel consulta. Perfilado dinámico (Dynamic Profiling) de SecureSphere: gestión de los permisos de los usuarios y control automatizado de acceso a nivel de consulta. | Oficial de seguridad/ Administrador de BD |
| | | | | Difusión de software dañino | Vulnerabilidades del sistema, antivirus desactualizado, instalación de software pirata. | Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | Bajo | **Alto** | **Alto** | Mitigar | A.12.2.2 Controles contra códigos maliciosos. A.12.5.1 Instalación de software en sistemas operacionales | Identificación y evaluación de vulnerabilidades del sistema. Prevención contra instalación de software no autorizado. Monitorear el estado del antivirus y reglas del firewall. | Oficial de seguridad/ Administrador de BD |

| Activo y valoración | | | | Amenaza, vulnerabilidad y riesgo | | | Análisis y evaluación del riesgo | | | Tratamiento del riesgo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Estimación del Riesgo | | | | | | |
| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Amenaza | Vulnerabilidad | Riesgo | Confidencialidad | Integridad | Disponibilidad | Jerarquía de Control | Control alineado a la norma | Control Específico | Responsable |
| | | | | Acceso no autorizado | Desconocimiento en temas de seguridad, vulnerabilidades del sistema, vulnerabilidades de protocolos de comunicación de BD | Ataque a los recursos del sistema | Medio | Bajo | Bajo | Mitigar | A.14.2.8 Pruebas de seguridad del sistema. | Integración del IPS y el perfilado dinámico.<br>Prevención de SQL injection.<br>Verificación de Firewall.<br>Prevención de los ataques de protocolo de comunicación de BD. | Oficial de seguridad/ Administrador de BD |
| | | | | Destrucción deliberada de Información | Abuso de privilegios de acceso, sabotaje del personal interno, falta de compromiso, vulnerabilidades del sistema. | Eliminación intencional de información | Bajo | Bajo | Medio | Mitigar | A.7.2.3 Proceso disciplinario.<br>A.13.1.2 Seguridad de servicios de red.<br>A.14.1.3 Protección de transacciones en servicios de aplicación. | Prevención de la elevación de privilegios: IPS y control de acceso a nivel consulta.<br>Integración del IPS y el perfilado dinámico.<br>Prevención de SQL injection | Oficial de seguridad/ Administrador de BD |
| | | | | Caida del sistema por agotamiento de recursos | No existe un monitoreo de consumo de recursos, desconocimiento en temas de seguridad, antivirus no brinda la protección adecuada. | No disponibilidad de los sistemas | Bajo | Bajo | **Alto** | Mitigar | A.11.2.3 Seguridad del cableado.<br>A.13.1.3 Segregación en redes. | Prevención de la denegación de servicios.<br>Prevención de los ataques de protocolo de comunicación de BD. | Oficial de seguridad/ Administrador de BD |
| | | | | Inestabilidad de la línea de internet | Un solo proveedor de servicios de comunicaciones, gestión inadecuada de la red. | No dosponibilidad de los servicios | Bajo | Bajo | **Alto** | Mitigar | A.13.1.2 Seguridad de servicios de red. | Plan de contingencia- Uso de varias líneas dedicadas y redundancia de servicios con diversos proveedores del servicio. – balanceo de carga.<br>Acuerdos de nivel de servicio con el(los) proveedor(es) de comunicaciones | Oficial de seguridad/ Administrador de BD |

# Anexo K

## Declaración de aplicabilidad

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.5** | **Políticas de seguridad de la información** | | | |
| **A.5.1** | Proporcionar directrices de gestión de seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones | 5.1.1 Políticas para la seguridad de la Información | Aplicar | Exigido por la NTP ISO/IEC 27001:2014 |
| | | 5.1.2 Revisión de las políticas para la seguridad de la información | Aplicar | Exigido por la NTP ISO/IEC 27001:2015 |
| **A.6** | **Organización de la seguridad de la información** | | | |
| **A.6.1** | Organización interna | 6.1.1 Roles y responsabilidades en seguridad de la información | Aplicar | Exigido por la NTP ISO/IEC 27001:2015 |
| | | 6.1.2 Segregación de funciones | Aplicar | Se deben segregar las funciones para la realización de actividades, para evitar usos indebidos y el impacto de los incidentes de seguridad. Documentar |
| | | 6.1.3 Contacto con autoridades | Aplicado | Se mantiene comunicación con la ONGEI que es la entidad encargada de verificar el estado de seguridad en las entidades del estado, con PeCERT. Es necesario mantener contacto con foros especializados, revistas de interés. |
| | | 6.1.4 Contacto con grupos especiales de interés | Aplicar | Será necesario mantener contacto con foros especializados, revistas, etc. en temas de seguridad para estar alertas a la aparición de nuevas amenazas |
| | | 6.1.5 Seguridad de información en la gestión de proyectos | Aplicar | Será necesario identificar riesgos derivados de los proyectos |
| **A.6.2** | Dispositivos móviles y teletrabajo: Asegurar la seguridad del teletrabajo y el uso de dispositivos móviles | 6.2.1 Política de dispositivos móviles | No aplicar | No se usan dispositivos móviles para el tratamiento y almacenamiento de información. |
| | | 6.2.2 Teletrabajo | No aplicar | No se realiza teletrabajo en la entidad. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.7** | **Seguridad de los recursos humanos** | | | |
| **A.7.1** | Antes del empleo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera | 7.1.1 Investigación de antecedentes | Aplicado | Se controla la selección del personal y se solicitan referencias. |
| | | 7.1.2 Términos y condiciones del empleo | Aplicado | Están establecidos en el contrato. Aunque se recomienda revisar para asegurar que no se excluyen responsabilidades de seguridad de la información relevantes. |
| **A.7.2** | Durante el empleo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información. | 7.2.1 Responsabilidades de la gerencia | Aplicar | Es necesario documentar y comunicar las responsabilidades antes de capacitar al personal para que cumpla con las políticas de seguridad. |
| | | 7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información | Aplicar | Según el análisis de riesgos, una amenaza habitual es la falta de formación en materia de seguridad. |
| | | 7.2.3 Proceso disciplinario | Aplicar | En la comunicación de responsabilidades y políticas se informará de las consecuencias de su incumplimiento. |
| **A.7.3** | Terminación y cambio de empleo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo. | 7.3.1 Responsabilidades ante la finalización o cambio de empleo | Aplicar | Es necesario definir y contemplar en los contratos las responsabilidades ante la finalización del empleo, especialmente en relación a la confidencialidad de la información. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.8** | **Gestión de activos** | | | |
| **A.8.1** | Responsabilidad sobre los activos: Identificar los activos de la organización y definir responsabilidades de protección apropiadas. | 8.1.1 Inventario de activos | Aplicar | Necesario para llevar a cabo el proceso de evaluación de riesgos según la metodología adoptada. |
| | | 8.1.2 Propiedad de los activos | Aplicar | Es necesario identificar a los responsables de la seguridad de los activos. |
| | | 8.1.3 Uso aceptable de los activos | Aplicar | Se marcarán pautas de utilización de los activos. |
| | | 8.1.1 Retorno de activos | Aplicado | Cuando el contrato del empleado termina, éste devuelve todos los activos que poseía. |
| **A.8.2** | Clasificación de la información: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización. | 8.2.1 Clasificación de la información | Aplicar | Es necesario identificar la información acorde a los requisitos legales, valor, criticidad dentro de la Subgerencia para aplicar medidas adecuadas. |
| | | 8.2.2 Etiquetado de la información | Aplicar | Necesario para que los usuarios de la información identifiquen las protecciones a aplicar. |
| | | 8.2.3 Manejo de activos | Aplicar | Para adoptar medidas de seguridad en función a la clasificación establecida. |
| **A.8.3** | Manejo de los medios: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios. | 8.3.1 Gestión de medios removibles | Aplicar | Necesario dada la proliferación de soportes USB. |
| | | 8.3.2 Disposición de medios | Aplicar | Es necesario poner a disposición los medios de manera segura cuando ya no se requieran, sobre todo en los backups, formalizar el procedimiento. |
| | | 8.3.3 Transferencia de medios físicos | No aplicar | No se extraerían soportes con información relevante fuera de la oficina. |
| **A.9** | **Control de acceso** | | | |
| **A.9.1** | Requisitos de la empresa para el control de acceso: Limitar el acceso a la información y a las instalaciones de procesamiento de la información. | 9.1.1 Política de control de acceso | Aplicado | Los usuarios cuentan con la información pertinente respecto a los permisos de acceso que poseen. |
| | | 9.1.2 Acceso a redes y servicios de red | Aplicado | Se controla el acceso a los servicios de red en función de la necesidad de uso. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.9.2** | Gestión de acceso de usuario: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios. | 9.2.1 Registro y baja de usuarios | Aplicar | El movimiento de alta y baja de usuarios en los sistemas haría indispensable este control. Contar con documentos formales autorizado por el jefe del proceso sobre la creación o baja de usuario. |
| | | 9.2.2 Aprovisionamiento de acceso a usuario | Aplicado | Se conceden o retiran los permisos, en función de las necesidades de acceso de los usuarios. Se debe contar con un procedimiento o sistema que permita retirar todos los permisos de todos los sistemas para un determinado usuario. |
| | | 9.2.3 Gestión de derechos de acceso privilegiados | Aplicar | Es necesario restringir y controlar la asignación y uso de acceso privilegiado. |
| | | 9.2.4 Gestión de información de autentificación secreta de usuarios | Aplicar | Dado el resultado del análisis de riesgo, se cree conveniente aplicar este tipo de control. Es decir establecer un proceso de gestión controlado para la asignación de información confidencial de autenticación. |
| | | 9.2.5 Revisión de los derechos de acceso de usuarios. | Aplicar | Realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los usuarios manteniendo los registros de las revisiones y hallazgos. |
| | | 9.2.6 Remoción o ajuste de derechos de acceso | Aplicado | Se hace bajo petición del responsable directo del usuario. |
| **A.9.3** | Responsabilidades de los usuarios: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación | 9.3.1 Uso de información de autentificación secreta | Aplicar | Buenas prácticas de seguridad sería necesario para proteger el acceso a la información. |
| **A.9.4** | Control de acceso a sistemas y aplicaciones: Prevenir el acceso no autorizado a los sistemas y aplicaciones | 9.4.1 Restricción de acceso a la información | Aplicado | Los usuarios acceden únicamente a la información que requieren para desarrollar su trabajo. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| | | 9.4.2 Procedimientos de ingreso seguro | Aplicado | Se requiere usuario y contraseña para el acceso a sistemas y aplicaciones. |
| | | 9.4.3 Sistema de gestión de contraseñas | Aplicar | Se reforzará la gestión de contraseñas implantada actualmente al identificarse riesgos en este sentido. |
| | | 9.4.4 Uso de programas utilitarios privilegiados | Aplicar | Controlar el uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas para evitar incidentes de seguridad. |
| | | 9.4.5 Control de acceso de código fuente de los programas | Aplicar | Se reforzará el control de acceso al código fuente dado los riesgos identificados. |
| **A.10** | **Criptografía** | | | |
| **A.10.1** | Controles criptográficos: Asegurar el uso apropiado y efectivo de la criptografía para proteger la información | 10.1.1 Política sobre el uso de controles criptográficos | Aplicar | Establecer políticas para determinar el uso de técnicas criptográficas que ayuden a proteger la información de la organización. |
| | | 10.1.2 Gestión de claves | No Aplicar | No se gestionan claves criptográficas en la entidad. |
| **A.11** | **Seguridad física y ambiental** | | | |
| **A.11.1** | Áreas seguras: impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización | 11.1.1 Perímetro de seguridad física | Aplicar | Exigido por la NTP ISO/IEC 27001:2014 |
| | | 11.1.2 Controles de ingreso físico | Aplicar | Establecer controles para indicar las áreas accesibles por los visitantes, implementar control de acceso restringido y controlar el acceso. |
| | | 11.1.3 Asegurar oficinas, áreas e instalaciones | Aplicado | En circunstancias aconsejables los equipos e información de encuentran aislados. |
| | | 11.1.4 Protección contra amenazas externas y ambientales | Aplicado | Se cuenta con lo básico para hacer frente a amenazas ambientales externas y ambientales (equipo contra incendios, otros) |
| | | 11.1.5 Trabajo en áreas seguras | Aplicado | Los servidores se encuentran en una zona segura aislada, pero se debe mejorar este control supervisando lo que se realiza en el Data center. |
| | | 11.1.6 Áreas de despacho y carga | Aplicado | Se establece una zona en recepción para carga y descarga. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.11.2** | Equipos: Prevenir la pérdida, daño, robo o compromiso de activos o interrupción de las operaciones de la organización | 11.2.1 Emplazamiento y protección de los equipos | Aplicado | Los equipos están en áreas controladas por personal autorizado. |
| | | 11.2.2 Servicios de suministro | Aplicado | Se dispone de un sistema de alimentación ininterrumpida. |
| | | 11.2.3 Seguridad del cableado | Aplicado | La instalación del cableado es segura. |
| | | 11.2.4 Mantenimiento de equipos | Aplicado | Existe personal de soporte técnico que da mantenimiento a los equipos. Mejorar el control manteniendo registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo |
| | | 11.2.5 Remoción de activos | No aplicar | No salen equipos con información sensible de la entidad. |
| | | 11.2.6 Seguridad de equipos y activos fuera de las instalaciones | Aplicar | Controlar el uso de los equipos que se prestan y supervisar el estado de salida y retorno. |
| | | 11.2.7 Disposición y reutilización segura de equipos | Aplicado | Los equipos descartados se formatean e instalan de nuevo cuando se ponen de nuevo en servicio. Mejorar el control analizando la información confidencial que maneja el equipo y decidir si es necesario aplicar otra técnica que haga imposible recuperar esa información. |
| | | 11.2.8 Equipos de usuarios desatendidos | Aplicado | Los equipos cuenta con una clave de protección en caso estén desatendidos. Mejorar el control para el equipo de secretaría. |
| | | 11.2.9 Política de escritorio limpio y pantalla limpia | Aplicar | Se evitará así filtraciones de información indeseadas. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.12** | **Seguridad de las operaciones** | | | |
| **A.12.1** | Procedimientos y responsabilidades operativas: asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras. | 12.1.1 Procedimientos operativos documentados | Aplicar | Será necesario documentar algunos de los procedimientos de seguridad, especialmente los de requisito más técnico (copias de seguridad, mantenimiento del equipo, manejo de medios, manejo del correo y seguridad, recuperación del sistema) |
| | | 12.1.2 Gestión del cambio | Aplicar | Los cambios se realizaran de manera controlada. |
| | | 12.1.3 Gestión de la capacidad | Aplicado | Se ha implementado por ejemplo una línea dedicada para los sistemas más críticos. |
| | | 12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones | Aplicado | Los entornos de desarrollo, prueba y operación están separados para reducir los riesgos de acceso no-autorizado o cambios en los sistemas operacionales. |
| **A.12.2** | Protección contra códigos maliciosos | 12.2.1 Controles contra códigos maliciosos | Aplicado | Se dispone de antivirus aunque es necesario complementar este control con capacitación y concienciación de los usuarios. |
| **A.12.3** | Respaldo: Proteger contra la pérdida de datos | 12.3.1 Respaldo de la información | Aplicado | Se realizan copias de seguridad diarias. Mejorar este control estableciendo periodos de prueba de recuperación de backup, almacenamiento fuera de daños y desastres del local principal. |
| **A.12.4** | Registros y monitoreos: Registrar eventos y generar evidencias | 12.4.1 Registro de eventos | Aplicar | El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información. |
| | | 12.4.2 Protección de información de registros | Aplicar | Es necesario proteger contra posibles alteraciones y accesos no autorizados la información de los registros. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| | | 12.4.3 Registro del administrador y del operador | Aplicar | Necesario para revisar y proteger los registros asociados a las actividades del administrador y del operador del sistema. |
| | | 12.4.4 Sincronización del reloj | Aplicado | Para evitar fallas en las comunicaciones y asegurar la integridad de registro de eventos. |
| **A.12.5** | Control de software operacional: Asegurar la integridad de los sistemas operacionales | 12.5.1 Instalación de software en sistemas operacionales | Aplicado | Se realizan instalaciones con el conocimiento de la Subgerencia de Sistemas y Tecnología y con personal autorizado. |
| **A.12.6** | Gestión de vulnerabilidad técnica: Prevenir la explotación de vulnerabilidades técnicas | 16.6.1 Gestión de vulnerabilidades técnicas | Aplicado | Se instalan las actualizaciones de seguridad en los puestos de los usuarios y los servidores. |
| | | 16.6.2 Restricción sobre la instalación de software | Aplicar | Restringir los permisos de instalación a los usuarios. |
| **A.12.7** | Consideraciones para la auditoría de sistemas de información: Minimizar el impacto de las actividades de auditoría en sistemas operacionales | 12.7.1 Controles de auditoría de sistemas de información | Aplicar | Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio. |
| **A.13** | **Seguridad de las comunicaciones** | | | |
| **A.13.1** | Gestión de seguridad de la red | 13.1.1 Controles en la red | Aplicado | Se dispone de un firewall. |
| | | 13.1.2 Seguridad de servicios de red | Aplicar | Verificar los acuerdos de nivel de servicio con el proveedor y que estén estipulados en el contrato |
| | | 13.1.3 Segregación en redes | Aplicado | Las redes se encuentran separadas para prevenir accesos no autorizados. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| **A.13.2** | Transferencia de información: Mantener la seguridad de la información transferida dentro de una organización y cualquier entidad externa | 13.2.1 Políticas y procedimientos de transferencia de la información | Aplicado | Se realizan configuraciones para proteger la transferencia de información por las redes. |
| | | 13.2.2 Acuerdo sobre transferencia de información | Aplicado | Se firman acuerdos de intercambio con los proveedores. |
| | | 13.2.3 Mensajes electrónicos | Aplicado | Los sistemas antivirus, el firewall disponen de medidas de protección. |
| | | 13.2.4 Acuerdos de confidencialidad o no divulgación | Aplicado | Los contratos con proveedores y personal incluyen acuerdos de confidencialidad. |
| **A.14** | **Adquisición, desarrollo y mantenimiento de sistemas** | | | |
| **A.14.1** | Requisitos de seguridad de los SI: Garantizar que la seguridad de información es una parte integral de los SI a través del ciclo de vida completo. Esto también incluye los requisitos para SI que proporcionen servicios sobre redes públicas | 14.1.1 Análisis y especificación de requisitos de seguridad de la información | Aplicar | Se exigirá a los analistas programadores y documentar el establecimiento de medidas de seguridad en el desarrollo de software. |
| | | 14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas | Aplicar | Utilizar sistema de cifrado para la información, exigir al proveedor donde se aloja la PW acuerdos de seguridad. Nivel de confianza de la dirección. |
| | | 14.1.3 Protección de transacciones en servicios de aplicación | Aplicar | Realizar informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos test de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas para prevenir ataques web. |
| **A.14.2** | Seguridad en los procesos de desarrollo y soporte: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información | 14.2.1 Política de desarrollo seguro | Aplicar | Se establecerá una política para contemplar los requisitos de seguridad al desarrollar SI. |
| | | 14.2.2 Procedimiento de control de cambio del sistema | Aplicar | Cada cambio debe ser controlado y documentado. |
| | | 14.2.3 Revisión técnica de aplicaciones después de cambios a la plataforma operativa | Aplicado | Se realizan pruebas al realizar cambios para comprobar que funcionen correctamente. Verificar también funciones de seguridad. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| | | 14.2.4 Restricciones sobre cambios a los paquetes de software | No aplicar | No se realizan cambios en los paquetes de software de terceros. |
| | | 14.2.5 Principios de ingeniería de sistemas seguros | Aplicar | Se deberá establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información. |
| | | 14.2.6 Ambiente de desarrollo seguro | Aplicar | Proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema. |
| | | 14.2.7 Desarrollo contratado externamente | No aplicar | No se contrata desarrollo externo |
| | | 14.2.8 Pruebas de seguridad del sistema | Aplicar | Realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo. |
| | | 14.2.9 Pruebas de aceptación del sistema | Aplicado | Se comprueba el cumplimiento de los requisitos especificados |
| **A.14.3** | Datos de prueba: Asegurar la protección de datos utilizados para las pruebas | 14.3.1 Protección de datos de prueba | Aplicar | Seleccionar cuidadosamente, proteger y controlar los datos de prueba. Tener autorización de uso de datos reales. |
| **A.15** | **Relaciones con proveedores** | | | |
| **A.15.1** | Seguridad de la información en las relaciones con los proveedores: Asegurar protección a los activos de la organización que son accesibles por los proveedores. | 15.1.1 Política de seguridad de la información para las relaciones con los proveedores | No aplicar | Se considera que el coste de implementación de este control superaría el beneficio que se obtendría. |
| | | 15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores | Aplicado | En los contratos con los proveedores se incluyen acuerdos de confidencialidad. Verificar otros temas relacionados a la seguridad. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| | | 15.1.3 Cadena de suministro de tecnología de información y comunicaciones | Aplicar | Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones. |
| **A.15.2** | Gestión de entrega de servicios del proveedor | 15.2.1 Monitoreo y revisión de servicios de los proveedores | Aplicar | Monitorear y revisar la prestación de servicios de tercero para saber si ¿Lo que se recibe vale lo que se paga por ello? |
| | | 15.2.2 Gestión de cambios a los servicios de proveedores | Aplicado | Se firman nuevos contratos con los proveedores ante un cambio en las condiciones, revisar implicaciones en temas de seguridad. |
| **A.16** | **Gestión de incidentes de seguridad de la información** | | | |
| **A.16.1** | Gestión de incidentes de seguridad de la información y mejoras: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades | 16.1.1 Responsabilidades y procedimientos | Aplicar | Necesario para implicar al personal en la gestión de incidencias. |
| | | 16.1.2 Reporte de eventos de seguridad de la información | Aplicar | La organización debe generar un procedimiento para gestionar adecuadamente cada uno de los eventos de seguridad de la información reportados por el personal o detectados por cada uno de los controles implementados, además se debe realizar charlas de capacitación con el personal para explicarles cuáles son sus roles y responsabilidades dentro del sistema de gestión. |
| | | 16.1.3 Reporte de debilidades de seguridad de la información | Aplicar | La organización debe capacitar adecuadamente a todo el personal de la organización para que sea capaz de detectar debilidades en el sistema de gestión de seguridad de información y puedan reportarlas adecuadamente, asimismo, se debe recalcar las sanciones que podrían recibir si es que deciden probar las debilidades encontradas |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| | | 16.1.4 Evaluación y decisión sobre eventos de seguridad de la información. | Aplicar | Es necesario identificar a una persona responsable de evaluar las incidencias y determine las acciones que se deben tomar. |
| | | 16.1.5 Respuestas a incidentes de seguridad de la información | Aplicar | Para solucionar las incidencias y documentarlos. |
| | | 16.1.6 Aprendizaje de los incidentes de seguridad de la información | Aplicar | Tener para esto un registro de incidencias y revisarlas periódicamente para prevenir incidencias. |
| | | 16.1.7 Recolección de evidencias | Aplicar | Mantener un registro de incidencias y de las operaciones realizadas. |
| **A.17** | **Aspectos de seguridad de la información en la gestión de continuidad del negocio** | | | |
| **A.17.1** | Continuidad de seguridad de la información: La seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio. | 17.1.1 Planificación de continuidad de seguridad de la información | Aplicar | Necesario para identificar puntos débiles en cuanto a la continuidad de las operaciones. |
| | | 17.1.2 Implementación de continuidad de seguridad de la información | Aplicar | Necesario para garantizar la continuidad de los servicios. |
| | | 17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información | Aplicar | Necesario para verificar la adecuación a los planes y de mejora continua. |
| **A.17.2** | Redundancias: Asegurar la disponibilidad de las instalaciones y procesamiento de la información | 17.2.1 Instalaciones de procesamiento de la información | No aplicar | Por el momento se considera que no es necesario debido a que el coste supera los beneficios obtenidos. |
| **A.18** | **Cumplimiento** | | | |
| **A.18.1** | Cumplimiento con requisitos legales y contractuales: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad. | 18.1.1 Identificación de requisitos contractuales y de legislación aplicables | Aplicar | Se debe identificar las leyes aplicables a la organización |
| | | 18.1.2 Derechos de propiedad intelectual | Aplicado | Se contempla como propiedad de la MPH los desarrollos realizados en la entidad. Disponer de los derechos de propiedad de software originales. |

| Sección | Objetivo | Control | Estado | Justificación |
|---|---|---|---|---|
| | | 18.1.3 Protección de registros | Aplicar | Se deben proteger los registros mediante medidas de seguridad física y lógica. Se debe establecer guías y procedimiento que especifiquen por cuanto tiempo la organización está dispuesta a almacenar la información. |
| | | 18.1.4 Privacidad y protección de datos personales | Aplicar | Se debe establecer un procedimiento para el adecuado manejo de la información personal almacenada dentro de la organización, en conformidad con la ley de protección de datos personales. |
| | | 18.1.5 Regulación de controles criptográficos | Aplicar | A nivel nacional existe una directiva que indica que la información sensible debe ser encriptado para asegurar su integridad y confidencialidad, esta directiva es la 007-95-INEI-SJI. |
| **A.18.2** | Revisiones de seguridad de la información: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos. | 18.2.1 Revisión independiente de la seguridad de la información | Aplicar | Se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información, planificar las revisiones. |
| | | 18.2.2 Cumplimiento de políticas y normas de seguridad | Aplicar | En las auditorias se verificará el cumplimiento de políticas, procedimientos y normas. |
| | | 18.2.3 Revisión del cumplimiento técnico | Aplicar | Establecer un plan de revisión de los SI y verificar si cumplen con las políticas y normas de seguridad dispuesta por la organización. |