**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS**

**ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN**

**TESIS DE GRADO**

# DISEÑO DE UN PLAN DE GESTIÓN DE LA SEGURIDAD Y DE LA INFORMACIÓN PARA EL SISTEMA DE INTRANET DE LA PREFECTURA DE ESMERALDAS, BASADO EN ESTÁNDARES INTERNACIONALES.

**LÍNEA DE INVESTIGACIÓN**

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN**

**AUTOR:**

ALEXANDER GEOVANNY ARROYO ARROYO

**ASESOR:**

MGT. KLEBER LEONARDO VERA TORTORELLA

**ESMERALDAS, OCTUBRE DEL 2019**

## TRIBUNAL DE GRADUACIÓN

Trabajo de tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de Grado de la PUCESE previo a la obtención del título de INGENIERO DE SISTEMAS Y COMPUTACIÓN.

……..

Mgt. Kleber Vera

**Tutor de Tesis**

……..……..

Mgt. Susana Patiño

**Lector 1**

…….

Mgt. Xavier Quiñonez Ku

**Lector 2**

……..…….…….

Mgt. Xavier Quiñonez Ku

**Director de la Escuela de Sistemas y Computación**

……..

Mgt. Kleber Vera Tortorella

**Secretario General PUCESE**

**Fecha:**

## AUTORÍA

Yo, **ALEXANDER GEOVANNY ARROYO ARROYO** portador de la cédula de identidad **0804363513** declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de "Ingeniero de Sistemas y Computación" son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

……..…….....

Alexander Geovanny Arroyo Arroyo

C.I. 080436351-3

## CERTIFICACIÓN

Mgt. Kleber Vera docente investigador de la PUCESE, certifica que:

La investigación realizada por **ALEXANDER GEOVANNY ARROYO ARROYO** bajo el título **"DISEÑO DE UN PLAN DE GESTIÓN DE LA SEGURIDAD Y DE LA INFORMACIÓN PARA EL SISTEMA DE INTRANET DE LA PREFECTURA DE ESMERALDAS, BASADOS EN ESTÁNDARES INTERNACIONALES"** reúne los requisitos de calidad, originalidad y presentación, además de haber sido incorporadas al documento final, las sugerencias dadas; en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, octubre del 2019.

**Mgt. Kleber Vera.**

**ASESOR**

# DEDICATORIA

A Dios por darme salud, sabiduría e inteligencia en todo lo largo de mi vida.

A mi **madre Marisol Arroyo** y mi **reina Jordana Arroyo** por ser el alma de mi alma y fuerza de mi fuerza.

A mi **chiquita Digna**, **mi abuelita** querida, siempre ha estado pendiente de cada paso que doy y con su amor he llegado a aprender cosas fundamentales de la vida, a mis tías **Mariluz, Maribel y Maritza,** por el apoyo y por ser el fruto del reconocimiento vital que nos ofrecen las personas que nos aman de verdad.

A mis hermanos **Danfer y Darkiel**, así mismo mis primos **Joel, Anthony, Jorshua, Nayeli, Niurka y Anahis** porque me enseñaron que uno debe ser ejemplo del otro.

A mi **novia Nelly Arleth**, porque ha luchado conmigo en las buenas y malas.

No ha sido sencillo el camino hasta ahora, pero gracias a sus aportes, su amor y su inmensa bondad lo he logrado**.**

## AGRADECIMIENTO

Deseo expresar mi agradecimiento a **Dios** por permitirme el privilegio de vivir.

A mi madre **Marisol Arroyo** por apoyarme en cada decisión, gracias a la vida porque cada día me demuestra lo hermoso que es y lo justo que puede llegar a ser, cuando se forja una meta para poder lograrlo.

A mi asesor **Kleber Vera** por la dedicación y apoyo brindado a este trabajo en conjunto; por las sugerencias, ideas, rigor que ha facilitado a las mismas.

A todos los **docentes** y **directores de la carrera** por la confianza ofrecida desde que llegue, por el apoyo personal y humano, por su amabilidad para facilitarme su orientación, tiempo, ideas y atención a mis consultas.

## RESUMEN

El presente proyecto de investigación tiene como finalidad proponer el diseño de un plan de gestión de seguridad de la información dentro del sistema de intranet de la prefectura de esmeraldas, mediante estándares internacionales como la ISO 27001, siendo así la información el activo más importante.

La ISO 27001, da una serie de requisitos para una perfecta elaboración de un sistema de gestión de seguridad de la información, definiendo cada uno de sus cláusulas, objetivos de control, políticas de seguridad y una seria de controles que más se ajusten a las necesidades al momento que persista una eventualidad en el sistema de intranet.

La puesta en práctica de esta investigación se abordó con una vía de investigación, para verificar y evidenciar las falencias que tienen los activos involucrados al sistema de intranet, y tomando decisiones acertadas para la solución de problemáticas que se presentan. Los instrumentos fueron aplicados, al equipo que conforman el departamento de tecnologías en cada uno de sus procesos, se localizaron datos cualitativos en entrevistas con los dueños de los activos, los cuales fueron presentados en cuadros definiendo sus procesos, dueño del activo, amenazas, vulnerabilidades y evaluación de riesgos; cuyos datos confirman la buena práctica de la ISO 27001. Por lo tanto, el departamento se encuentra sumergido a posibles ataques y que deben de implementar estos requisitos.

Este proyecto termina su ejecución con un tratamiento, evaluación de los riegos y un plan de gestión de seguridad de la información aplicado netamente al sistema de intranet y que debe ser incluido a los activos asociados al mismo.

**Palabras claves:** seguridad de la información, SGSI, sistema de intranet, ISO 27001.

## ABSTRACT

The purpose of this research project is to propose the design of an information security management plan within the intranet system of the esmeraldas prefecture, using international standards such as ISO 27001, making information the most important asset.

The ISO 27001, gives us a series of requirements for a perfect development of an information security management system, defining each of its clauses, control objectives,

security politics and a series of controls that best fit the needs at the time that persists an eventuality in the intranet system.

The implementation of this research was approached with a way of investigation, to verify and evidence the flaws that have the assets involved in the intranet system, and making wise decisions for the solution of problems that arise. Once the instruments that make up the technology department were executed in each of its processes, qualitative data were located in interviews with the owners of the assets, which were presented in tables defining their processes, owner of the asset, threats, vulnerabilities and risk assessment; whose data confirm the good practice of ISO 27001. Therefore, the department is submerged in possible attacks and must implement these requirements.

This project ends its execution with a treatment, risk assessment and an information security management plan clearly applied to the intranet system and which must be included in the assets associated with it.

**Keywords:** security of the information, information security management system, intranet system, international organization for standardization 27001**.**

# INDICE GENERAL

# Índice de Ilustraciones

# Índice de Tablas

# INTRODUCCIÓN

## Presentación del tema de investigación

Existen muchas herramientas que se han implementado con la finalidad de prevenir y reducir los riesgos de manera asociada con el manejo de la información y el uso de tecnologías que van a la par con la administración de la seguridad de dicha información. No obstante, que aquellas herramientas no logran ser totalmente efectivas dentro de la gestión de la seguridad de la información, y por lo tanto está sujeto a cambios en sus propósitos, si no se controla de forma eficiente un elemento importante, como lo es el recurso humano.

En la seguridad de la información se mezclan muchos aspectos tales como combinación de herramientas, estrategias y técnicas de seguridad, y factores humanos para la detección de fugas de información, ataques de hackers maliciosos; por lo consecuente hay que tratar de apartar las vulnerabilidades y amenazas que atenten a la seguridad de la información.

Los Sistemas de Gestión de Seguridad de la Información son descritos por la ISO/IEC 27001, definido por un conjunto de políticas o reglas para la correcta administración de la Información, dentro de las empresas u organizaciones, incluyendo objetivos de control, controles y cláusulas según el anexo a, preservando la confidencialidad, integridad y disponibilidad, de la información mediante la administración de gestión de riesgo.

El departamento de tecnologías de la información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas es una entidad integrada bajo la necesidad de brindar servicios tecnológicos eficientes como implementación y manejo de infraestructura tecnológica, redes, desarrollo de aplicaciones y servicios de capacitación tecnológica al sistema de intranet.

Teniendo el conocimiento de que el departamento de TIC es el encargado de manejar de forma ordenada la infraestructura tecnológica y los sistemas de información, se hace acreedor y responsable de las obligaciones en el manejo de la seguridad de los activos de información del sistema de intranet del área de recursos humanos de la institución, es por esta razón que las falencias por la falta de controles oportunos, y de un plan de tratamiento de riesgo para su gestión se convierte en un factor crítico en contra del cumplimiento de los objetivos que tienen como institución, por lo tanto se debería de tener un plan

plenamente efectivo y con controles que minimicen los riesgos, amenazas, vulnerabilidades y las consecuencias en caso de efectuarse alguna de ellas.

## Planteamiento del problema

El sistema de intranet del Gobierno autónomo descentralizado de la provincia de Esmeraldas no cuenta con controles adecuados en seguridad de la información, ni con un plan de tratamiento de riesgo para la gestión de seguridad de la información, tampoco con un diseño de plan de seguridad de la información.

Hay muchos factores que intensifican la inseguridad del sistema de intranet los cuales son, pocas políticas de seguridad, falta de controles, mucha perdida de información, ausencia de documentación en manuales de funciones, procedimientos y políticas de seguridad, falta de planes de capacitación, falta de continuidad en los planes de crecimiento y carencia de un diseño de sistema integral de seguridad de la información.

Existen muchas eventualidades en el sistema de intranet en donde la información puede estar sujeta a pérdidas, debido a que no se manejan los procesos de contrato de acceso al personal de manera automatizada y con políticas de seguridad. No obstante, estos procesos están expuesto a riesgos y amenazas, ya que la red de ordenadores del área de recursos humanos no cuenta con un respaldo en los protocolos de comunicación y sumado a eso se manejan IPs públicas.

Especificando que al no contar el sistema de intranet con un diseño de un plan de gestión de la seguridad de la información y de un tratamiento de riesgo se puede decir que se han retrasado de manera muy agravante los objetivos organizacionales que tiene la institución y esto implica niveles muy bajos e ineficientes en la labor interina del departamento; una vez detectada la necesidad que tiene el sistema de intranet y con la intención de mejorar sus procesos de los servicios que brinda, se plantea implementar el proyecto del tema:

**“DISEÑO DE UN PLAN DE GESTIÓN DE LA SEGURIDAD Y DE LA INFORMACIÓN PARA EL SISTEMA DE INTRANET DE LA PREFECTURA DE ESMERALDAS, BASADO EN ESTÁNDARES INTERNACIONALES.”**

## Justificación

Dentro de las organizaciones públicas o privadas en la planificación estratégica que estén ligadas a optimizar los procesos de seguridad de la información, se lo proyecta con el objetivo de proteger el activo más importante que es la información.

La presente investigación aportará con la aplicación de enfoques teóricos y prácticos en lo relacionado a la gestión de la seguridad de la información, aplicando una ruta de referencia que son las normas de seguridad de la familia ISO/IEC 27000.

La puesta en práctica de este proyecto beneficiará de manera objetiva al funcionamiento del sistema de intranet del Gobierno autónomo descentralizado de la provincia de Esmeraldas, para que haya una buena prevención el personal estará presto a asumir cambios a la buena manera de acceder a la información y seguir controles rigurosos para que no haya fallas en la administración de los datos que deseen procesar.

El sistema de intranet del GADPE saldrá beneficiado con la propuesta y a su vez de la aplicación de las políticas de seguridad, del plan de tratamiento de riesgos y del diseño del plan de gestión de la información; estas políticas podrán proporcionar un nivel de seguridad muy alto, sin fallas sujetas a fugas de información.

En la elaboración del análisis de riesgo, el diseño del plan de seguridad de la gestión de la información del sistema de intranet del área de recursos humanos obtendrá un alto reconocimiento en comparación con otras organizaciones al tener información segura, en la parte práctica, esta investigación constituirá una oportunidad importante para la organización, tendrán una precisión sobre los problemas que se presentan al momento de acceder a la información y corregirlos sin causar fugas de la misma.

# OBJETIVOS

## General

Diseñar un plan de gestión de la seguridad y de la información para el sistema de intranet de la prefectura de Esmeraldas, basado en estándares internacionales.

## Específicos

- Describir el sistema de la intranet, evidenciando su infraestructura y procesos implementados en cuanto a la seguridad de la información.
- Determinar los niveles de riesgos y amenazas de seguridad de la información de la intranet del GADPE.
- Proponer un plan de la seguridad de la información en el sistema de intranet del GADPE basados en estándares internacionales.

# CAPÍTULO I: MARCO TEÓRICO

La gestión de seguridad de la información es uno de los pilares fundamentales en las organizaciones, pudiendo así tener un control más ordenado y seguro de la información que se maneja en las diferentes áreas de toda organización. Utilizar estándares internacionales es una de los puntos a favor para el buen manejo de la información, teniendo una gama de herramientas que aportan al crecimiento y objetivos institucionales.

Por otro lado, al realizar un diseño de gestión de seguridad de la información con normativas internacionales, la alta dirección debe de aprobarlo y manifestarlo a las personas involucradas para así, ingrese al presupuesto anual de la organización.

## 1.1. Bases Teórico - Científico

### Conceptos básicos de seguridad de información

La seguridad hoy en día es uno de los pilares fundamentales de cualquier empresa, ya que este mundo está cada día más conectado y expuesto a ataques, saboteos y filtraciones de información; en donde se debe tener cuidado y aplicar los procesos pertinentes para que este no sea atacado. En este espacio se va a abordar definiciones básicas generales en cuanto a seguridad se refiere [1].

### Seguridad de la información

Es importante no confundir el termino seguridad informática, con seguridad de la información ya que este primero engloba de forma general al segundo y por lo tanto la seguridad de la información se ocupa de la información de forma escrita, oral, impresa, electrónica, electromagnética entre otras; y también en cualquier momento de su ciclo de vida ya sea de creación, mantenimiento, distribución y uso, y almacenamiento, archivo y destrucción para protegerla de cualquier amenaza que pueda ocurrir [1].

La seguridad de la información de una u otra manera puede afectar a toda la organización, ya que toda trabaja con información constantemente debería tener una gestión coordinada muy transparente, lo cual debe incluir una planificación y gestión, no puede ser de forma improvisada, se debería de tenerla en primer plano como el resto de los procesos del negocio [1].

## Gestión de Seguridad de la Información

La seguridad de la información es un proceso que la organización debe manejarlo de forma debida con recursos pertinentes, ya sean personales o económicos; asignando bien sus funciones, para que sea eficiente y quede plasmada de forma segura [1].

La gestión de la seguridad de la información tiende a recibir un gran número de actividades, en la ilustración 1 muestra cada una de estas actividades que son de tipo organizativo o técnico y en ocasiones, también jurídico. Dependiendo del despliegue de la seguridad de la información, será necesario priorizar estas actividades [1].

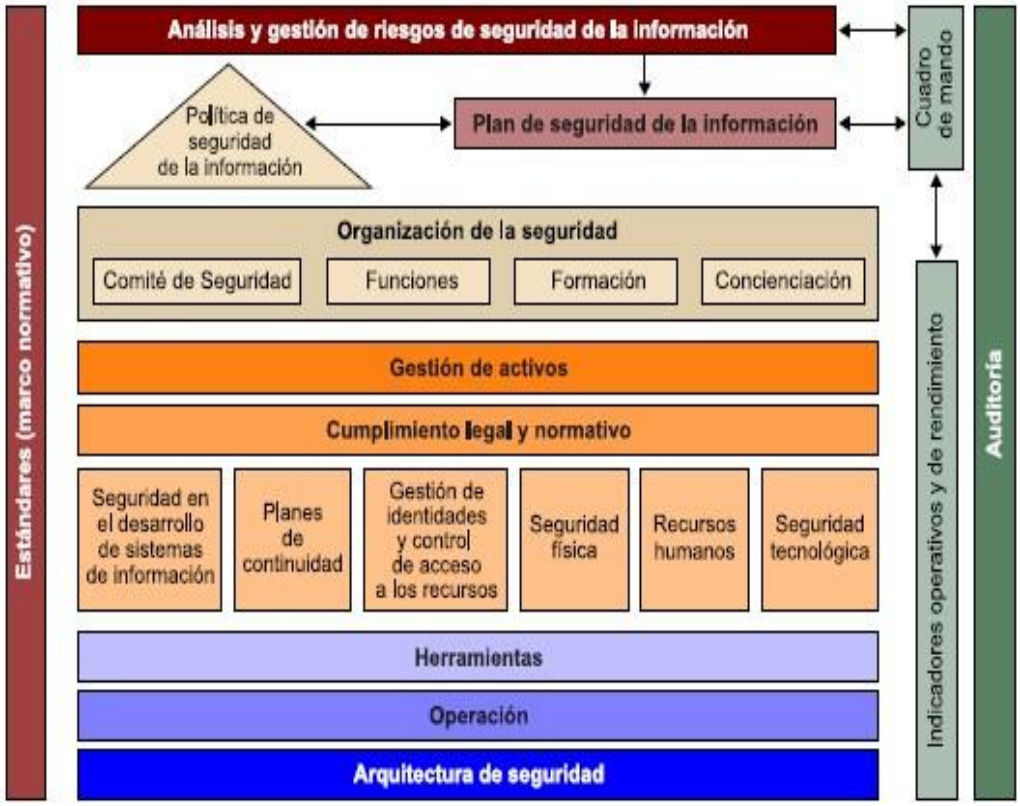



Ilustración 1 El proceso de la gestión de la seguridad de información [1].

### Amenazas

Para la detección de las amenazas es importante saber identificarlas ya que presentan un potencial muy alto en dañar los activos de cualquier empresa, por lo tanto, se debe reconocer las principales. En esta se va establecer un listado de aquellas que puedan de una u otra manera afectar a los activos de la información, algunas pueden ser producto de fenómenos físicos que ocurran en la tierra, como incendios, terremotos, inundaciones, mientras que otras pueden ser el producto de algún mal manejo de los encargados [2].

En la siguiente tabla se presentarán las diferentes posibles amenazas que afecten según el tipo de activo y las dimensiones de seguridad [2]:

Tabla 1 Listado de Amenazas *[2]*.

| **Amenazas** |
|---|
| Incendios de causa normal |
| Inundaciones de causa natural |
| Terremotos |
| Incendios generados de forma accidental o mal intencionada |
| Inundaciones por fuga de agua |
| Derrumbes |
| Explosiones |
| Sobrecargas y fluctuación eléctricas |
| Polvo y suciedad |
| Averías de origen físico o lógico |
| Fallo den el servicio de comunicaciones |
| Degradación de los soportes de almacenamiento de información |

### 1.1.1. Análisis de riesgo

El análisis de riesgo corresponde a la primera fase que una empresa debería de realizar para mejorar su seguridad. Un análisis de riesgos corresponde, desde el punto de vista de la seguridad, al proceso de identificación de éstos, determinando su magnitud e identificando las áreas que requieren medidas de protección [3].

Un análisis de riesgos equivale a realizar una fotografía de una organización, desde el punto de vista de la seguridad, que muestre los aspectos con una mayor probabilidad que podrían provocar un incidente de seguridad [3].

Cabe destacar que un proceso de análisis de riesgos da como resultado una información y no una medida de seguridad como tal; es decir, el proceso en sí no va a evitar que la organización sufra incidentes de seguridad, sino que permitirá identificar los peligros a los que se encuentra expuesta. Eso quiere decir que, si tenemos perfectamente identificados los peligros, le será más fácil a la organización protegerse de aquellas situaciones que representan un mayor riesgo [3].

De hecho, un análisis de riesgos va permitir responder a las tres grandes preguntas sobre la seguridad de la información en una organización para, con posterioridad, poder realizar un análisis y estar en disposición de tomar decisiones basándose en situaciones concretas. Las tres preguntas son las siguientes [3]:

- **¿Qué hay que proteger?** Se identifican los elementos que la organización, debe tratar de asegurar.

- **¿De qué o de quién nos tenemos que proteger, y por qué?** Se identifican los peligros que pueden afectar a la organización y el motivo por el que podría producirse una incidencia.

- **¿Cómo nos queremos proteger?** Después de un análisis exhaustivo, se opta por la mejor protección para que los peligros no lleguen a materializarse.

En la ilustración 2 se muestra cómo se deben efectuar los pasos para la correcta elaboración del análisis de seguridad de la información, su planificación y monitorización como eje de verificación de su situación actual.


Ilustración 2 Ciclo de vida correcto de la seguridad de la información *[3]*.

## Justificación y estudio de análisis de riesgo

Se sabe que un análisis de riesgos debería ser la primera y principal tarea que una organización ha de realizar cuando se plantea mejorar en cualquier aspecto la seguridad de la información [3].

Los motivos por los que se debe realizar un análisis de riesgos son los siguientes [3]:

- Permite identificar los diferentes riesgos a los que se encuentra expuesta la organización desde el punto de vista de la seguridad y que podrían afectar al desarrollo de las diferentes actividades de negocio de la organización.

- Permite a la organización realizar una selección de medidas de seguridad que se deben implantar en ella, mucho más ajustada a las necesidades de esta.

- Permite realizar y elaborar los planes de contingencias de una organización. Esto quiere decir que un análisis de riesgo presentará las situaciones que pueden provocar un incidente de seguridad y que, a su vez, no pueden ser reducidos a través de la implantación de las medidas de seguridad. Ha de servir, por tanto, como base para la elaboración de los planes de contingencias.

- Las organizaciones que tengan previsto implantar las diferentes normativas de seguridad (ISO 27001) y crear un SGSI, con la intención de conseguir certificarlo, deberán poseer un análisis de riesgos, que será el auténtico punto de partida de todo el proceso de certificación.

## Metodologías de análisis de riesgo

En la actualizad hay diversas metodologías de análisis de riesgo, todas estas presentan resultados similares si se aplican de una manera correcta a las mismas organizaciones.
Las diferencias entre una y otra es la forma en que presentan los resultados [3].

### ▯ Magerit

Esta metodología puede ser aplicada a cualquier organización, independientemente de que se encuentre en el Estado español o en otro país. Al mismo tiempo, esta metodología ha desarrollado una herramienta que ayuda a su aplicación.

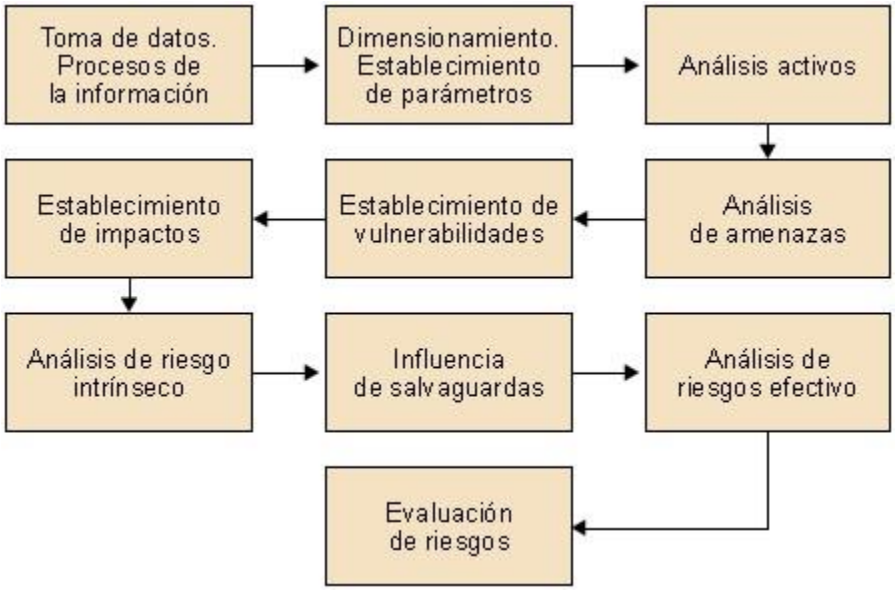



Ilustración 3 Fases de Magerit [3]**.**

La metodología MAGERIT tiene como gran virtud que los resultados que se ofrecen están expresados económicamente. Esto tiene como ventaja que es fácilmente defendible ante la dirección, puesto que es ésta la que tiene que aceptar y asumir los riesgos a los que se encuentra expuesta la organización y la que tiene que gastar unos recursos determinados para reducir dichos riesgos [3].

Por el contrario, su principal inconveniente es que tratar los activos sobre la base de su valoración económica hace que el método sea más costoso, ya que realizar la estimación económica de determinados activos es laborioso [3].

### ▯ Nist

Esta metodología resulta mucho más sencilla que MAGERIT en cuanto a su aplicación, debido a que no es necesario hacer un estudio tan pormenorizado de cada activo para asignarle una valoración. Además, también es más sencillo asignar tanto la probabilidad como el impacto [3].

Sin embargo, esta metodología no permite designar claramente los riesgos reales a los que se encuentra expuesta la organización, puesto que únicamente indica tres niveles de riesgos: no clasifica, dentro de los que son considerados altos, cuál es más alto o cuál supone un mayor riesgo [3].

Una forma de aprovechar esta metodología podría ser utilizándola en grandes alcances para identificar con claridad los riesgos más altos a gran escala que posee la organización. Después se utilizaría una segunda metodología (MAGERIT o CRAMM) para analizar con más detalle los riesgos propios de estos activos que han sido identificados como aquellos que tienen los riesgos más elevados [3].

### Cramm

Esta metodología es de origen británico, y su característica principal es el uso de valoraciones numéricas para el cálculo de los riesgos a los que se encuentra expuesta una organización [3].

Los valores que se requieren para aplicar CRAMM son los siguientes [3]:

- **Valoraciones de los activos.** Entendidas como el valor que tiene ese activo dentro del alcance que se está estudiando.
- **Estimación de las probabilidades**. Entendida como la probabilidad de que una amenaza, aprovechando una vulnerabilidad, dañe un determinado activo.
- **Estimación de los impactos.** Entendida como las consecuencias que tendría para la organización el hecho de que una amenaza aprovechara una vulnerabilidad para dañar a un activo.

### Octave

Esta metodología es de origen británico, al igual que CRAMM, pero tiene un modo de representar los riesgos a los que se encuentra expuesta una organización totalmente diferente a las anteriores [3].

OCTAVE requiere entrar en un proceso iterativo de revisión para tratar de obtener una reducción de todos los riesgos a los que se encuentra expuesta una organización [3].

La metodología acaba traduciéndose en la construcción de un árbol de riesgos en el que queda marcado cuál es el camino más crítico ante el que la organización tiene que actuar

primero. Una vez que se consigue reducir este riesgo, será necesario que se repita el estudio para volver a encontrar el siguiente camino crítico, y así sucesivamente hasta reducir todos esos riesgos. El resultado acaba siendo el siguiente [3]:

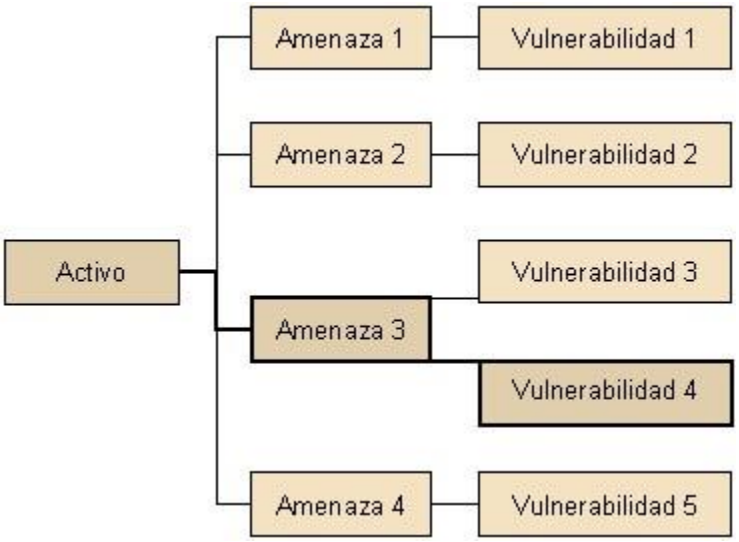



Ilustración 4 Resultados de Octave [3]**.**

Esta metodología tiene como aspecto positivo lo necesario de centrarse en analizar todas las situaciones de riesgos. En cambio, tiene como gran inconveniente que se debe completar un ciclo de revisión del análisis para acabar de identificar todos los riesgos que en cada ocasión son los más críticos [3].

Tabla 2 Metodologías para la gestión de riesgo [4].

| **Análisis de las metodologías para la gestión de riesgo** | |
|---|---|
| **Magerit** | Puede ser efectiva pero para la producción de la organización como tal, es muy costosa [4]. |
| **Nist** | La valoración que se realiza no es económica sino cualitativas, en donde se establecen probabilidades e impactos de cada uno de los activos para su facilidad [4]. |

| | |
|---|---|
| **Cramm** | Esta utiliza valoraciones numéricas para el cálculo de los riesgos, a los que se encuentra expuesta una organización. Donde se hace una valoración de los activos, estimación de las probabilidades y estimación de los impactos [4]. |
| **Octave** | Esta es muy diferente a las anteriores, ya que estable un árbol de riesgo en lo que queda marcado cual es el camino más crítico y que la organiza ción debe tratar como prioridad. Una vez que ya se haya reducido el riesgo se debe hacer nuevamente el estudio para establecer el siguiente camino crítico [4]. |

## Criterios de evaluación de los riesgos

Para realizar este paso se debe de previamente haber identificado las amenazas, para ahora si ver el nivel de riesgo existente, para poder tomar medidas pertinentes que ayuden a proteger los activos de la información, para la realización del mismo se debe de determinar la probabilidad y el nivel de impacto que pueda ocasionar. La probabilidad de ocurrencias se determina mediante interrogantes: ¿ya ha sucedido antes?, ¿sucede muy seguido?, y ¿podrá suceder más adelante? La valoración se determinará en la siguiente tabla [2]:

Tabla 3 Criterios para el cálculo de la probabilidad de ocurrencia [2].

| **Nivel** | **Probabilidad** |
|---|---|
| 1 | Muy Baja |
| 2 | Baja |
| 3 | Moderada |
| 4 | Alta |
| 5 | Muy Alta |

En el nivel de impacto se determinará cuál es su nivel que tiene la materialización de la amenaza, teniendo en cuenta los controles que ya existen, se tomará como criterio en qué medida repercute en las operaciones de la organización. Para la valoración se planteara la siguiente tabla [2]:

Tabla 4 Criterios para el caculo de impacto [2].

| **Nivel** | **Impacto** |
|---|---|
| 1 | Insignificante |
| 2 | Menor |
| 4 | Moderado |
| 6 | Mayor |
| 8 | Catastrófico |

Para solución de la evaluación de riesgo se obtiene multiplicando la probabilidad y el nivel de impacto previamente definidos, esto permitirá localizar el riesgo con una matriz inherente de calor [2].

## Tratamiento de Riesgo

Se debe de identificar quienes son los responsables del tratamiento de los riesgos y evaluar los tipos de tratamientos más apropiados. Para evidenciar esta se debe tratar el riesgo de cuatro maneras, dejando a decisión de la organización el tipo de tratamiento que va a escoger. En la siguiente tabla se explicará los criterios [2].

Tabla 5 Tratamiento de Riesgo [2].

| **Tratamiento** | **Descripción** |
|---|---|
| Mitigar | Implementar controles de seguridad de la información a fin de reducir el riesgo a niveles aceptables. Se utiliza cuando al implementar controles trae beneficios mayores a la inversión de su implementación. |

| | |
|---|---|
| Aceptar | Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas. Se utiliza cuando el costo de implementar controles, en términos económicos, superan el impacto del riesgo que se desea reducir, o cuando el impacto del riesgo es mínimo. |
| Transferir | Transferir el impacto del riesgo a terceros, empresas aseguradoras o proveedoras de servicio. Se utiliza cuando no se puede reducir la probabilidad de ocurrencia del riesgo, pero su impacto es inminente. |
| Evitar | Eliminar la fuente que genera la amenaza. Se utiliza cuando el nivel de riesgo es Alto, la actividad del proceso o sistema que lo genera no es de gran impacto en términos de negocio para la institución, de modo que puede ser retirada funcionalmente. |

| Valores | Nivel de riego | Descripción del riesgo y acciones necesarias |
|---|---|---|
| 8 | ALTO | Requiere fuertes medidas correctivas. Planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de alta dirección |
| 6-7 | MEDIO ALTO | Requiere vigilancia de alta dirección con planes de tratamiento implementados y reportados a los gerentes de UTB |
| 4-5 | MEDIO | Se requieren acciones correctivas controladas por grupos de manejo de incidentes en período de tiempo razonable |
| 2-3 | MEDIO BAJO | Riego aceptable-Administrado por los grupos de incidentes bajo procedimientos normales de control |
| 0-1 | BAJO | El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo |

Ilustración 5 Informe Tratamiento de Riesgo [5].

### 1.1.2. Estándares de seguridad de la información

En la actualidad existen muchos estándares de seguridad de la información con un alto reconocimiento a nivel internacional, que se puede aplicar a cualquier tipo de organización, independientemente del tipo de actividad o tamaño. Estos estándares son guías de referencia y hojas de rutas para la gestión de la seguridad de la información [1].

Los estándares surgen a través del desarrollo de descripciones detalladas de características particulares de un producto o servicio por parte de expertos de empresas e instituciones científicas. Representan un consenso sobre características tales como calidad, seguridad y confiabilidad que deberían seguir siendo aplicables por un período prolongado de tiempo y, por lo tanto, están documentadas y publicadas. El objetivo del desarrollo de estándares es apoyar tanto a las personas como a las empresas a la hora de adquirir productos y servicios. Los proveedores de productos y servicios pueden mejorar su reputación al certificar su cumplimiento de las normas.

## Normas de la familia ISO 27000

La norma ISO 27000 se emitió en 2009 para proporcionar una visión general de la familia de normas ISO 27 K y una base conceptual común; 46 términos básicos de seguridad de la información se definen y diferencian en la sección "Términos y condiciones". El significado de la seguridad de la información y el compromiso sistemático con los aspectos de seguridad se deriva del riesgo para las empresas cuyos procesos empresariales dependen cada vez más del procesamiento de la información y cuyas infraestructuras de TI complejas e interconectadas son vulnerables a fallas e interrupciones [6].

En la fase de planificación para un SGSI se definirán los requisitos para la protección de la información y los sistemas de información, se identificarán y evaluarán los riesgos, y se desarrollarán procedimientos y medidas adecuados para reducir los riesgos. Estos procedimientos y medidas se ejecutaron durante la implementación y las operaciones. Los informes generados a través del monitoreo continuo de las operaciones se utilizarán para derivar mejoras y para su desarrollo del SGSI [7].

## ISO 27001

Este estándar se basa en la especificación de requisitos de sistemas de gestión de seguridad de la información, es decir en la norma certificable [1].

La norma ISO 27001 se publicó en 2005 con el título, en 42 páginas, describe los requisitos que debe cumplir un SGSI para obtener la certificación. Como marco, el estándar está dirigido a empresas de todos los sectores y de todos los tamaños. Las medidas concretas para el cumplimiento de los requisitos no están estipuladas en la norma, sino que deben desarrollarse e implementarse en una base específica de la empresa. Los requisitos de certificación de ISO 27001 se dilucidan mediante la elaboración de términos y conceptos y se complementan con una guía de implementación dentro de ISO 27002 [7].

Los requisitos, que se aplicarán a la documentación del SGSI, se describen en la norma a través de la estipulación de contenido esencial, documentos necesarios, así como especificaciones y estructuras de supervisión para la gestión de documentos, tales como:

- Procesos de cambios y aprobaciones

- Control de versiones
- Reglas para los derechos de acceso y protección de acceso
- Especificaciones para los sistemas de archivo [7].

La mejora y el posterior desarrollo del sistema de gestión de seguridad de la información se implementarán de forma continua, en la política de seguridad, el registro y la evaluación de las operaciones, los resultados de las pruebas y los resultados de las medidas de mejora. Además, la mejora y el desarrollo adicional deben avanzar a través de auditorías internas periódicas. La adecuada implementación de la política de seguridad, así como su idoneidad y exhaustividad, deben garantizarse mediante revisiones anuales de la administración [7].

La siguiente tabla tendrá una presentación sobre el control de objetivos según la ISO 27001, en donde expone de manera general los dominios que establecen esta norma y sus objetivos de cada uno de ellos:

Tabla 6 ISO 27001 Objetivos de Control [7].

| Dominio | Objetivos de Control |
|---|---|
| **En el domino de Políticas de Seguridad** | Se basa en la gestión y realiza soporte en todos los equipos de la organización y establece algunas leyes |
| **Organización de la seguridad de la información** | • Aparte de la gestión y soporte propios de la seguridad, regula todo esto y los clasifica en requisitos y leyes con más importancia.<br>• Mantener la seguridad de las instalaciones de procesamiento de información e información de la organización a las que acceden, procesan, comunican o administran partes externas. |

| | |
|---|---|
| **Gestión de activos** | Para lograr y mantener una protección adecuada de los activos de la organización.<br><br>Para asegurar que la información reciba un nivel apropiado de protección. |
| **Seguridad de los recursos humanos** | Para garantizar que los empleados, contratistas y usuarios de terceros entiendan sus responsabilidades, y sean adecuados para los roles para los que son considerados, y para reducir el riesgo de robo, fraude o mal uso de las instalaciones.<br><br>Para garantizar que los empleados, contratistas y usuarios externos salgan de una organización o cambien de empleo de manera ordenada. |
| **Seguridad física y ambiental** | Para prevenir acceso físico no autorizado, daño en donde interactúen las posibles conexiones donde de la organización.<br><br>Para que no ocurra cualquier tipo de eventualidad en cuenta a sustracción en los activos y la interrupción de las actividades de la organización. |
| **Comunicaciones y gestión de operaciones** | Para garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. |

| | |
|---|---|
| | - Implementar y mantener el nivel adecuado de seguridad de la información y entrega de servicios en línea con los acuerdos de prestación de servicios de terceros.<br>- Para minimizar el riesgo de fallas en los sistemas.<br>- Para proteger la integridad del software y la información.<br>- Mantener la integridad y disponibilidad de las instalaciones de procesamiento de información e información.<br>- Para evitar la divulgación no autorizada, la modificación, eliminación o destrucción de activos, y la interrupción de actividades comerciales.<br>- Para garantizar la seguridad de los servicios de comercio electrónico y su uso seguro.<br>- Para detectar actividades de procesamiento de información no autorizadas. |
| **Control de acceso** | - Para controlar el acceso a la información.<br>- Para que haya una buena administración en la entrada de los clientes cuando el administrador se lo autorice y cuando no haya autorización. |

| | |
|---|---|
| | - Para evitar el acceso no autorizado de los usuarios, el compromiso o el robo de información y también cuando se procesan datos.<br>- Para evitar la denegación en los accesos a servicios en red.<br>- Para evitar el acceso no autorizado a los sistemas operativos.<br>- Para garantizar la seguridad de la información cuando se utilizan las instalaciones de informática móvil. |
| **Adquisición, desarrollo y mantenimiento de sistemas de información** | - Para garantizar que la seguridad sea una parte integral de los sistemas de información.<br>- Para evitar errores, pérdidas, modificaciones no autorizadas o uso incorrecto de la información en las aplicaciones.<br>- Para proteger la confidencialidad, integridad de la información por medios criptográficos.<br>- Para garantizar la seguridad de los archivos del sistema.<br>- Para mantener la seguridad del software y la información del sistema de aplicación.<br>- Para reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas. |

| | |
|---|---|
| **Gestión de incidentes de seguridad de información** | Para garantizar que no se aplique una situación que haga efecto de daño a los sistemas de gestión de seguridad de la información. |
| **Plan de continuidad del negocio** | Dentro de las actividades que realiza la organización debe de tratar de minimizar los procesos críticos y contar con un plan de contingencia para proteger la información de un catástrofe física o humana. |
| **Conformidad** | Para evitar infracciones de cualquier ley, obligaciones legales, reglamentarias o contractuales, y de cualquier requisito de seguridad.<br><br>Para garantizar el cumplimiento de los sistemas con las políticas y estándares de seguridad de la organización.<br><br>Maximizar la efectividad de y minimizar la interferencia hacia / desde el proceso de auditoría de los sistemas de información. |

## ISO 27002

Este estándar se centra en el código de buenas prácticas, los requisitos codificados en ISO 27001 se amplían y explican en ISO 27002 en forma de una guía. El manual se publicó por primera vez en el año 2000 en ese momento con la designación "ISO 17799". En 2007 esto fue revisado y alineado con la familia de normas 27 K y la designación fue cambiada a ISO 27002. Con el desarrollo de las prácticas comunes ISO 27002 a menudo también conocidas como mejores prácticas, se ofrecieron como procedimientos y métodos

probados en la práctica, que podrían adaptarse a los requisitos específicos dentro de las empresas [7].

La seguridad de la información debe estar anclada en la organización de la empresa para que las medidas de seguridad de la información se puedan promover y establecer de manera eficiente. Por lo tanto, se deben definir las funciones y responsabilidades y, en particular, las obligaciones para mantener la confidencialidad y las reglas para las comunicaciones con terceros (clientes, proveedores, autoridades, etc.). Todos los activos tangibles e intangibles que deben protegerse mediante las medidas de seguridad de la información deben identificarse y clasificarse para establecer responsabilidades específicas y reglas de manejo [7].

Los riesgos de seguridad también son causados por las vulnerabilidades de los sistemas de TI; más de la mitad de todos los ataques son iniciados por personal interno; sin embargo, una gran proporción también se iniciará mediante acciones conjuntas del personal interno y externo [7].

Debido a que el personal interno puede usar el conocimiento interno (sobre procesos internos, hábitos, puntos débiles, relaciones sociales, etc.) para los ataques, se debe considerar que tienen un mayor potencial de éxito y daño [7].

Los riesgos correspondientes se deben tener en cuenta con medidas de personal como el reclutamiento y la asignación. Por lo tanto, por ejemplo, los derechos de acceso para un usuario deben restringirse en la medida necesaria para llevar a cabo el trabajo al que está asignado el usuario. Con los cambios en las responsabilidades, deberes o trabajos, los derechos de acceso deben adaptarse en consecuencia y si el personal es despedido, los derechos de acceso deben revocarse rápidamente [7].

En la siguiente tabla 7 se va a explicar detalladamente cada una de la familia de estándares.

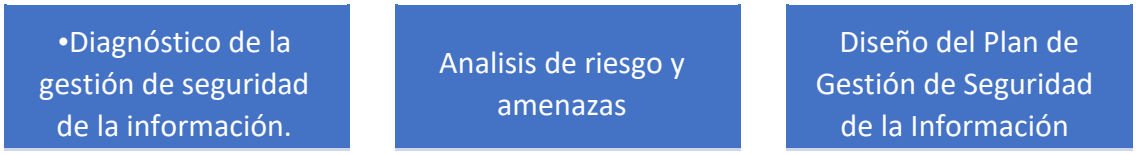
Tabla 7 Familia de Estándares

| Norma | Descripción |
|---|---|
| **ISO/IEC 27000** | Introducción y vocabulario. |
| **ISO/IEC 27001** | Requerimientos para sistemas de gestión de seguridad de la información. |

| | |
|---|---|
| **ISO/IEC 27002** | Código de buenas prácticas para sistemas de gestión de seguridad. |
| **ISO/IEC 27003** | Guía de implementación. |
| **ISO/IEC 27004** | Métricas y mediciones. |
| **ISO/IEC 27005** | Gestión de riesgo de seguridad de la información. |
| **ISO/IEC 27006** | Requerimientos para organizaciones que proveen auditorias y certificaciones. |
| **ISO/IEC 27007** | Directrices de auditoria para SGSI. |
| **ISO/IEC 27008** | Directrices de auditoria para controles del SGSI. |
| **ISO/IEC 27010** | Directrices de seguridad para las comunicaciones entre organizaciones. |
| **ISO/IEC 27011** | Directrices de seguridad para organizaciones de telecomunicaciones. |
| **ISO/IEC 27013** | Directrices para la integración de ISO 27001 e ISO 20000-1. |
| **ISO/IEC 27014** | Gobierno de la seguridad de información. |
| **ISO/IEC 27015** | Directrices para servicios financieros. |
| **ISO/IEC 27016** | Economía organizacional. |

### 1.1.3. Diseño del plan de gestión de la seguridad de la información

Se debe tener en cuenta que para la elaboración de este diseño se debe establecer las fases, los cuales poseen una serie de actividades para poder alcanzar los objetivos específicos que se deriva del objetivo general de esta investigación.



| | | |
|---|---|---|
| • Verifica los niveles críticos que existen en la organización y verificación de la situacion actual del departamento, mediante la iso de la familia 27000. | • Dar valores a los riesgos y amenazas, localizándolos para establecer planes de tratamiento.<br>• Establecer la política de seguridad para su perfecta gestión. | • Se recopila toda la información acerca del diagnóstico de la gestión de la seguridad y del análisis de riesgo y amenazas para describir un mapa organizativo de cada una de las claúsulas de la ISO 27001. |

Ilustración 6 Etapas de Diseño del Plan

Para que se efectué de manera ordenada el diseño del plan, se presentará las fases a seguir mediante un mapa de conceptos realizada por el autor.

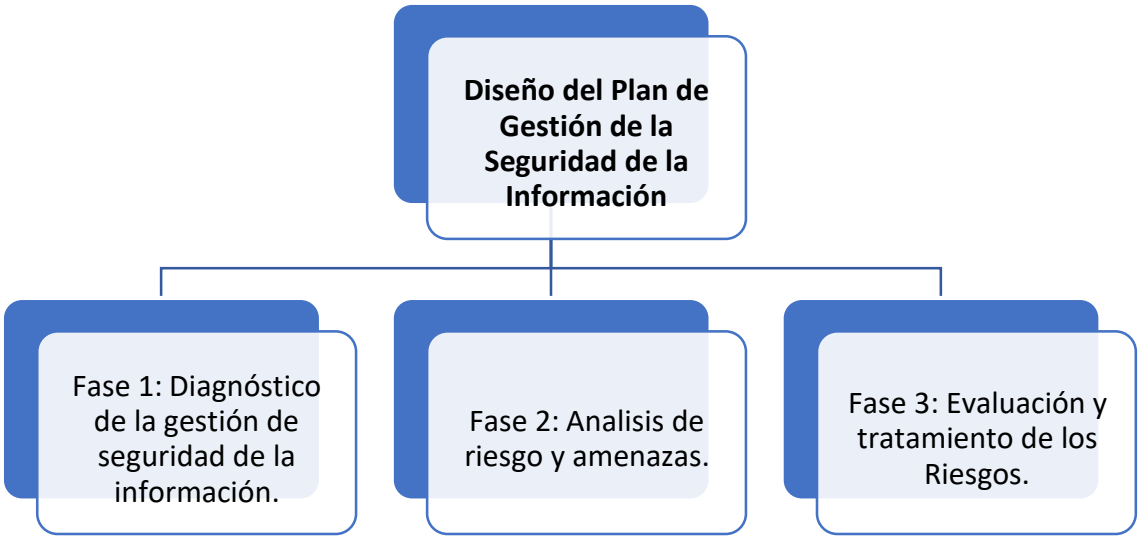



Ilustración 7 Fases para el Diseño del Plan

## 1.2. Antecedentes

Dentro de los objetivos que tiene toda organización para bien de su crecimiento, persisten altas incidencias, esto conlleva a tomar recaudos pertinentes como medidas de protección y buen afianzamiento de la información. Todo esto, ha seguido a pasos agigantados en las últimas épocas.

En estudios previos se enfocan en la importancia que adoptan las normas ISO/IEC 27001 y ISO/IEC 27002 en el diseño de un sistema de gestión de seguridad de la información como una estrategia de mejora. Las normas o estándares internacionales según ese estudio adoptan un modelo sólido y con una aceptación alta para los principios y lineamientos que gobiernan desde la evaluación, diseño hasta llegar a la implementación de la seguridad de la información en cualquier organización [2].

Partiendo desde la literatura consultada, algunos estudios revelan que la mala administración y el fracaso de las intranets en organizaciones como problemática más complicada de resolver, es porque no cuentan con adecuados sistemas de seguridad de la información que en ellas se soporta y mucho menos para fomentar la gestión del conocimiento a todo el personal [8].

Según el estudio de vulnerabilidades en las empresas, estas están expuestas a ataques internos y externos que pueden ocasionar pérdidas grandes de información y afectar económicamente a las mismas, desde allí mantener la seguridad de los sistemas de información, puesto a las consecuencias, que pueden poner en riesgo la integridad de la información [9].

En los estudios realizados como enfoque sobre la prevención y protección del activo que más influyente en una organización (la información) viene a ser el mismo en la mayoría de los casos, la diferencia entre muchas organizaciones es que están determinadas por los activos de la organización y sus falencias o necesidades de controles para su protección, en ningún caso es idéntica en cuanto a los riesgos, amanezcas y vulnerabilidades que pueda persistir en la información, pero con un único objetivo que es la preservación de la confidencialidad, integridad y disponibilidad de este activo de mucha importancia.

La presente investigación tiene una intención al igual a los otros estudios que se han mencionado, la moderación de riesgos, amenazas y vulnerabilidades que está expuesta la información en sistema de intranet del Gobierno Autónomo y Descentralizado de la Provincia de Esmeraldas garantizando la confidencialidad, integridad, disponibilidad y accesibilidad de la misma.

## 1.3. Marco Legal

Cualquier tipo de organización, institución u empresa que requiera la implementación de un sistema de gestión de la seguridad de la información, controles de riesgos o un diseño

de un plan de seguridad de la información deberá estar apegado en lo que dice la ley y cumplirla a cabalidad para el desarrollo de sus actividades.

La norma ISO/IEC 27001 fue preparada por preparada por el comité técnico conjunto ISO/IEC JTC 1 Tecnología de la Información, subcomité SC con 27 técnicas de seguridad descritas por abogados para proporcionar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información, de acuerdo al reglamento interior de CEN/CENELEC[10], están obligados a adoptar esta norma europea los organismos de normalización de los siguientes países: Alemania, Antigua República Yugoslava de Macedonia, Austria, Bélgica, Bulgaria entre otros; y también los 12 países de Sudamérica[10].

Como punto fundamental en cuanto a las leyes específicas del control de la información partimos de la "LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA" que estipulan los derechos que tiene la ciudadanía a acceder a cualquier fuente de información definida como pública para ejercer la participación democrática respecto a la rendición de cuentas a los que está expuesto cada empleado público, esta ley contiene un conjunto de artículos definidos que establecen dichos derechos y sus límites.

En LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS establece las formas de interacción económica en la red, de esta se va a establecer las más relevantes para la presente investigación.

**Art. 9.-Protección de datos. –**

Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

**Art. 20.-Certificado de firma electrónica. -**

Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

**Artículo 190.-Apropiación fraudulenta por medios electrónicos.**

La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones.

**Artículo 229.-Revelación ilegal de base de datos.**

La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas.

**Artículo 232.-Ataque a la integridad de sistemas informáticos**

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de in formación, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen.

# CAPÍTULO II: MATERIALES Y MÉTODOS

## 2. METODOLOGÍA

### 2.1. Tipo de Diseño

En la presente investigación se utilizó el tipo de diseño experimental y es de tipo cuasi experimental ya que se puede tener un diseño de plan de seguridad de la información con políticas de seguridad, pero este no va ser totalmente efectivo en el control de pérdidas de la información, pero si se tendrá un mayor control posible.

### 2.2. Área de Estudio

El Gobierno Autónomo Descentralizado de la provincia de Esmeraldas se encuentra en las calles 10 de agosto entre Bolívar y Pedro Vicente Maldonado, diagonal al parque central como se lo denomina 20 de marzo. Está en todo el centro de la ciudad de Esmeraldas y desde mencionada dirección brinda su labor a toda la ciudadanía esmeraldeña.

El Gobierno Autónomo Descentralizado de la ciudad de Esmeraldas posee muchas áreas que están divididas y cada una con un objetivo. Entre dichos departamentos se encuentra la dirección de Tecnologías de la información y la comunicación, está encargada de 4 áreas dentro de la institución: redes y comunicaciones, desarrollo e integración de aplicaciones, soporte e infraestructura tecnológica y proyectos, y servicios web en cada una de estas áreas hay un responsable o jefe de área y un ayudante, constituyéndose así que cada área es responsabilidad de dos personas y todas son responsabilidad del jefe del departamento. En esta área es donde se realizó el levantamiento de información, analizando el sistema de intranet.

### 2.3. Recolección de Datos

Para la recolección de los datos el primer paso fue tener una entrevista con el jefe del departamento de TI, esto con el propósito de realizar un levantamiento de información entorno al objetivo que tiene la empresa para con la sociedad, entender cuáles son los procesos del negocio, identificando lo más crítico. Después se dio paso a realizar la verificación del sistema, cómo se encuentra su situación actual; luego el análisis de riesgo y ver cuál de estos están expuesto en el departamento, para ahora sí, definir el campo

crítico. Se realizó un análisis técnico, con evidencias visualizando cada uno de los activos y comparando que la información detallada por el encargado tenga un grado de verdad.

## 2.4. Tipo de Investigación

La presente investigación tiene un tipo de investigación cualitativa ya que se basa en entrevistas con respuestas concretas y partir de ahí para ver cómo se comportan sus variables y poder llegar a una solución.

## 2.5. Métodos y Técnicas

El método y técnica es inductivo ya que permitió analizar y observar la situación en la que se encuentra el departamento y luego se seleccionó las herramientas necesarias para solucionar el problema planteado.

Se utilizó una técnica de entrevista estructurada a los directivos, administrativos y miembros del departamento, con el objetivo de tener información relevante y de suma importancia acerca del funcionamiento y las actividades que realiza.

## 2.6. Población y Muestra

En la población y muestras de estudio (técnicas de muestreo) se conformó por 10 personas, estas corresponden a todo el personal del departamento y sus áreas: redes y comunicaciones, desarrollo e integración de aplicaciones, soporte e infraestructura tecnológica, proyectos y servicios web.

# CAPÍTULO III: RESULTADOS

## ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

### ENTREVISTA DIRIGIDA AL ANALISTA DE SISTEMAS DE TIC (ANEXO 1)

**Presentación de la situación actual del sistema de intranet y los activos que le conforman, en la prefectura de Esmeraldas.**

La siguiente entrevista se la realizó al desarrollador de aplicaciones que es el indicado en verificar, implementar y ejecutar la seguridad de la información que debe existir en el sistema de intranet, dicha entrevista se manejó con preguntas claves y puntuales (Anexo 1) más, sin embargo, se utilizó una verificación y corroboración de la información que nos impartió el entrevistado, evidenciando cada una de estas.

**Situación actual de la organización.**

La situación en la que se encuentra el sistema de intranet de la prefectura de esmeraldas, con sus activos que lo involucran es totalmente eficiente y se integra a las necesidades de sus usuarios, de hecho, existen políticas de seguridad, los usuarios están totalmente capacitados cuando se actualiza alguna nueva versión del sistema. Lo que sí preocupa es que estas capacitaciones no se las realiza periódicamente como establece en la ISO 27001 a intervalos planificados, sí existe una funcionalidad llamada “ayuda”, donde se actualiza los módulos informativos (sí se agrega alguna función).

Cabe recalcar que en el sistema de intranet no ha existido ningún ataque malicioso, solo existieron ataques a la base de datos interna, pero se bloqueó de manera automática sin provocar pérdida de información.

En cuanto a los activos que involucran el sistema de intranet, os encontramos con los siguientes:

La seguridad física de los equipos informáticos, estos están netamente identificados por nombres y claves para su autenticación en el momento de acceder, cabe recalcar que algunos equipos no cuentan inscritos dentro del dominio de la organización y esto puede provocar que terceros ingresen de manera deliberada; adicional a esto, los antivirus no están correctamente instalados y provoca que algún troyano acceda la información con facilidad. Estos equipos no cuentan con una seguridad de activos, en donde cada usuario tenga un perfil que no pueda cambiar propiedades en el sistema operativo (cambiar la

hora, el fondo de escritorio, formatear el sistema operativo, instalar cualquier tipo de programa etc.)

Dentro del control de los activos, los equipos si cuentan con un sistema que registra las incidencias de cuando ocurre algún daño de un ordenador especificando el tipo, parte del computador, característica, medidas a tomar; este es llamado helpdeks lo administra la encargada de la mesa de servicios.

Otro de los activos que involucran al sistema de intranet, es la data center tiene una seguridad física, lógica y perimetral muy buena, cualquier persona no puede ingresar ya que posee un sistema biométrico y se encuentra en un espacio seguro, estos equipos cuentas con refrigeración las 24 horas del día, aparte tienen sensores de humedad, humo, y temperatura que dan aviso a cualquier alerta. El sistema de intranet posee dos servidores dentro del data center, uno dedicado a la base de datos y el otro a realización de aplicaciones web, en un futuro se tiene pensado implementar otro para livianas cargas, por el momento no es tan necesario. Este activo sí permite que haya continuidad a los servicios informáticos, solo ingresan el personal autorizado, tiene un buen ambiente, se encuentra climatizado bajo los entandares de temperaturas fijas, el UPS permite garantizar que si hay algún apagón los equipos puedan funcionar con normalidad en un tiempo adecuado hasta tomar otra medida como encender la planta generadora de energía

Cabe recalcar que cada uno de los roles dentro del departamento están totalmente organizados, si existe algún fallo en cualquier parte de los activos hay algún encargado para reparar de manera rápida el fallo presentado, con esto no se presentará fallos no localizados que dentro de la ISO 27001 debe de estar planificado.

**Infraestructura y procesos.**

La infraestructura tecnológica que posee el sistema de intranet en lo relacionado a la seguridad de la información es totalmente administrada por el desarrollador de programas, pese a ese hecho se realizó la entrevista correspondiente para verificar que esta cuenta con normativas y seguridad pertinente para su perfecto funcionamiento.

Con la entrevista realizada al desarrollador de aplicaciones del área de tecnologías de la prefectura, se recabó la siguiente información en cuanto a los procesos que maneja el departamento en lo relacionado a la seguridad de la información. Cada funcionario debe tener un nombre de usuario y clave de ingreso para poder acceder y que es de

conocimiento únicamente de él, están totalmente encriptadas las claves; si existe alguna pérdida de datos, el usuario solicita al administrador resetear con una contraseña temporal que debe ser cambiada inmediatamente. La información personal es debidamente protegida y ninguna otra persona debe tener acceso, ningún usuario tiene acceso a información de otros departamentos, esta se encuentra totalmente protegida con seguridad de candados administrados dentro de los servidores de base de datos.

El desarrollador de aplicaciones no tiene implementado los controles y cláusulas de la familia ISO 27000 y tampoco tiene conocimiento del mismo, esto puede ocurrir que no existe la seguridad de la información de manera completa; lo que se utiliza son los objetivos de control que existen dentro de COBIT.

Cada una de las tareas en cuanto a los procesos que maneja el departamento son las siguientes: gestión de redes y comunicación, soporte técnico, gestión de la seguridad de la información, administración de data center y desarrollo de aplicaciones.

**Demostrar que partes de los activos involucrados en el sistema de intranet, están sujetos a amenazas, riesgos y vulnerabilidades.**

**Activos**

En esta sección se presentará, la identificación de cada uno de los activos que se involucran dentro del sistema de intranet de la prefectura, especificando su categoría ya sea específica y general, conforme a lo señalado en la tabla 7.

Tabla 8 Activos involucrados al sistema de intranet y seguridad de la información. (Fuente: Elaboración propia del autor.)

| N° | Activos | Categoría Específica | Propietario |
|---|---|---|---|
| **A001** | DATA CENTER LIEBERT | Ambiente Externo | Infraestructura |
| **A002** | Servidor Panasonic | Equipo Fijo | Infraestructura |
| **A003** | Servidor Tipo IBM | Equipo Fijo | Infraestructura |
| **A004** | Servidor “9” HP Prolian DL 160 G6 | Equipo Fijo | Infraestructura |
| **A005** | Servidor “10” HP Prolian DL 360 p G6 | Equipo Fijo | Infraestructura |
| **A006** | Servidor “11” Prolian DL 360 p G8 | Equipo Fijo | Infraestructura |
| **A007** | Servidor “8” Prolian DL 380 E G8 | Equipo Fijo | Infraestructura |

| | | | |
|---|---|---|---|
| **A008** | Servidor “36” HP Prolian ML 110 | Equipo Fijo | Infraestructura |
| | | | |
| **A009** | Ordenador Personal Lenovo | Equipo Fijo | Infraestructura |
| **A010** | Sistema operativo Windows 7 | Sistema Operativo | Infraestructura |
| **A011** | Computadora portátil COMPAQ | Equipo Fijo | Infraestructura |
| **A012** | UPS | Equipo Fijo | Infraestructura |
| **A013** | Swich | Equipo Fijo | Infraestructura |
| **A014** | Sistema de cámara video vigilancia | Equipo Fijo | Infraestructura |
| **A015** | Alarma de incendio | Equipo Fijo | Infraestructura |
| **A016** | Sistema de enfriamiento | Equipo Fijo | Infraestructura |
| **A017** | Microtik | Equipo Fijo | Infraestructura |
| **A018** | KVM – 440 D-Link | Equipo Fijo | Infraestructura |
| **A019** | Sistema eléctrico | Equipo Fijo | Infraestructura |
| **A020** | Respaldo de Base de Datos | Copia de respaldo | Desarrollo de Software |
| **A021** | Copia Respaldo del Data Center | Copia de respaldo | Infraestructura |
| **A022** | Registro de Actividades de Base de Datos | Copia de respaldo | Infraestructura |
| **A023** | Respaldo de Configuración de Mikrotik | Copia de respaldo | Infraestructura |
| **A024** | Respaldo de Máquina Virtual Cabild | Copia de respaldo | Infraestructura |
| **A025** | Respaldo de Máquina Virtual Centos 7-Servicios | Copia de respaldo | Infraestructura |
| **A026** | Respaldo de Máquina Virtual Elastix | Copia de respaldo | Infraestructura |
| **A027** | Respaldo de Máquina Virtual Ipcop-Proxy | Copia de respaldo | Infraestructura |
| **A028** | Respaldo de Máquina Virtual Windows 7 Cloud | Copia de respaldo | Infraestructura |
| **A029** | Respaldo de Máquina Virtual Storage Manager (localhost) | Copia de respaldo | Infraestructura |
| **A030** | Respaldo de Máquina Virtual Cabildo-Principal | Copia de respaldo | Infraestructura |
| **A031** | Respaldo de Máquina Virtual SisRiesgo | Copia de respaldo | Infraestructura |

| | | | |
|---|---|---|---|
| **A032** | Respaldo de Máquina Virtual FreeNas | Copia de respaldo | Infraestructura |
| **A033** | Respaldo de Máquina Virtual Pruebas-Cabildo-Técnicos | Copia de respaldo | Infraestructura |
| **A034** | Respaldo de Máquina Virtual Serverantivirus | Copia de respaldo | Infraestructura |
| **A035** | Respaldo de Máquina Virtual 2003 SERVER | Copia de respaldo | Infraestructura |
| **A036** | Respaldo de Máquina Virtual servidor.ime.org | Copia de respaldo | Infraestructura |
| **A037** | Respaldo de Máquina Virtual SIGCES | Copia de respaldo | Infraestructura |
| **A038** | Usuario – Administrador Jefe de infraestructura | Usuario | Jefe de TI |
| **A039** | Usuario – Administrador Jefe de desarrollo | Personal de operación | Infraestructura |
| **A040** | Usuario – Equipo de mantenimiento | Usuario | Jefa de desarrollo |
| **A041** | Ordenador personal Jefe de TI | Equipo fijo | Jefe de Infraestructura |
| **A042** | Ordenador personal Jefe de Infraestructura | Equipo fijo | Jefe de TI |
| **A043** | Ordenador personal jefe de desarrollo | Equipo fijo | Infraestructura |
| **A044** | Ordenador personal de mantenimiento | Equipo fijo | Jefa de desarrollo |
| **A045** | Reporte Trafico de Red | Copia de Reporte | Infraestructura |
| **A046** | Ordenador Apple | Equipo fijo | Infraestructura |
| **A047** | Ordenador Portátil Toshiba | Equipo fijo | Infraestructura |
| **A048** | Ordenador Aditk | Equipo fijo | Infraestructura |
| **A049** | Ordenador Altek | Equipo fijo | Infraestructura |
| **A050** | Sistema de Contabilidad Olimpo | Virtualización | Analista de Sistema |
| **A051** | Sistema de Automatización de Temperatura | Virtualización | Analista de Sistema |
| **A052** | Backup | Virtualización | Analista de Sistema |
| **A053** | Liberty Data Center | Ambiente Interno | Infraestructura |
| **A054** | Red de Datos | Virtualización | Infraestructura |

| | | | |
|---|---|---|---|
| **A055** | Diccionario de Datos | Sistemas | Analista de Sistema |
| **A056** | Esquema de Datos | Proceso de Sistemas | Analista de Sistema |
| **A057** | Programa Roles de Pago | Proceso de Sistemas | Analista de Sistema |
| **A058** | Código Fuente Sistema de Intranet | Proceso de Sistemas | Analista de Sistema |
| | | | |
| **A050** | Información Respaldada | Proceso de Sistemas | Analista de Sistema |
| **A060** | Sistemas de Procesos Programadas | Proceso de Sistemas | Analista de Sistema |

**Tasación de los activos**

En la siguiente tabla se presentará detalladamente cada uno de los activos involucrados al sistema de intranet con su respetiva valoración en cuanto a su situación, definiendo parámetros teles como: confidencialidad (C), integridad (I), disponibilidad (D) y un promedio (P); exponiendo así mismo su valoración de bajo (1), medio (2) y alto (3).

Tabla 9 Tasación de los Activos

**Tasación de activos**

| N° | Activos | Categoría Específica | Propietario | Nivel de Impacto (1 – 3) | | | |
|---|---|---|---|---|---|---|---|
| | | | | C | I | D | P |
| **A001** | Data center Liebert | Ambiente Externo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A002** | Servidor Panasonic | Equipo Fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A003** | Servidor Tipo IBM BLADE | Equipo Fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A004** | Sensores de temperatura | Equipo Fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A005** | Servidor “10” HP Prolian DL 360 p G6 | Equipo Fijo | Infraestructura | 3 | 2 | 2 | **2,33** |
| **A006** | Sensores de calor | Equipo Fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A007** | Servidor “6” Prolian DL 380 E G8 | Equipo Fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A008** | Servidor “36” HP Prolian ML 110 | Equipo Fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A009** | Ordenador Personal Lenovo | Equipo Fijo | Infraestructura | 3 | 1 | 3 | 2,33 |
| **A010** | Sistema operativo Windows 7 | Sistema Operativo | Infraestructura | 1 | 2 | 2 | 1,67 |
| **A011** | Computadora portátil COMPAQ | Equipo Fijo | Infraestructura | 2 | 2 | 2 | 2 |
| **A012** | UPS | Equipo Fijo | Infraestructura | 3 | 2 | 3 | 2,67 |
| **A013** | Swich | Equipo Fijo | Infraestructura | 3 | 3 | 3 | 3 |
| **A014** | Sistema de cámara video vigilancia | Equipo Fijo | Infraestructura | 3 | 3 | 3 | 3 |
| **A015** | Alarma de incendio | Equipo Fijo | Infraestructura | 3 | 3 | 3 | 3 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A016** | Sistema de enfriamiento | Equipo Fijo | Infraestructura | 3 | 3 | 3 | 3 |
| **A017** | Microtik | Equipo Fijo | Infraestructura | 3 | 3 | 2 | 2,67 |
| **A018** | KVM – 440 D-Link | Equipo Fijo | Infraestructura | 3 | 3 | 2 | 2,67 |
| **A019** | Sistema eléctrico | Equipo Fijo | Infraestructura | 2 | 2 | 3 | 2,33 |
| **A020** | Liberty Data Center | Ambiente Interno | Infraestructura | 3 | 3 | 3 | 3 |
| **A021** | Copia Respaldo del Data Center | Copia de respaldo | Infraestructura | 3 | 2 | 3 | 2,67 |
| **A022** | Registro de Actividades de Base de Datos | Copia de respaldo | Infraestructura | 3 | 2 | 3 | 2,67 |
| **A023** | Respaldo de Configuración de Mikrotik | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A024** | Respaldo de Máquina Virtual Cabild | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A025** | Respaldo de Máquina Virtual Centos 7-Servicios | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A026** | Respaldo de Máquina Virtual Elastix | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A027** | Respaldo de Máquina Virtual Ipcop-Proxy | Copia de respaldo | Infraestructura | 3 | 1 | 3 | 2,33 |
| **A028** | Respaldo de Máquina Virtual Windows 7 Cloud | Copia de respaldo | Infraestructura | 3 | 1 | 3 | 2,33 |
| **A029** | Respaldo de Máquina Virtual Storage Manager (localhost) | Copia de respaldo | Infraestructura | 3 | 2 | 3 | 2,67 |
| **A030** | Respaldo de Máquina Virtual Cabildo-Principal | Copia de respaldo | Infraestructura | 3 | 3 | 3 | 3 |
| **A031** | Respaldo de Máquina Virtual SisRiesgo | Copia de respaldo | Infraestructura | 3 | 3 | 3 | 3 |
| **A032** | Respaldo de Máquina Virtual FreeNas | Copia de respaldo | Infraestructura | 3 | 2 | 3 | 2,67 |
| **A033** | Respaldo de Máquina Virtual Pruebas-CabildoTécnicos | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A034** | Respaldo de Máquina Virtual Server-antivirus | Copia de respaldo | Infraestructura | 3 | 2 | 1 | 2 |
| **A035** | Respaldo de Máquina Virtual 2003 SERVER | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A036** | Respaldo de Máquina Virtual servidor.ime.org | Copia de respaldo | Infraestructura | 3 | 2 | 2 | 2,33 |
| | | | | | | | 2,33 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A037** | Respaldo de Máquina Virtual SIGCES | Copia de respaldo | Infraestructura | 3 | 2 | 2 | |
| **A038** | Usuario – Administrador Jefe de infraestructura | Usuario | Jefe de TI | 3 | 2 | 3 | 2,67 |
| **A039** | Usuario – Administrador Jefe de desarrollo | Personal de operación | Infraestructura | 3 | 3 | 3 | 3 |
| **A040** | Usuario – Equipo de mantenimiento | Usuario | Jefa de desarrollo | 3 | 3 | 2 | 2,67 |
| **A041** | Ordenador personal Jefe de TI | Equipo fijo | Jefe de Infraestructura | 3 | 3 | 2 | 2,67 |
| **A042** | Ordenador personal Jefe de Infraestructura | Equipo fijo | Jefe de TI | 3 | 2 | 2 | 2,33 |
| **A043** | Ordenador personal jefe de desarrollo | Equipo fijo | Infraestructura | 3 | 2 | 3 | 2,67 |
| **A044** | Ordenador personal de mantenimiento | Equipo fijo | Jefa de desarrollo | 3 | 2 | 2 | 2,33 |
| **A045** | Respaldo de Base de Datos | Copia de Respaldo | Desarrollo de Software | 3 | 2 | 2 | 2,33 |
| **A046** | Ordenador Apple | Equipo fijo | Infraestructura | 3 | 3 | 2 | 2,67 |
| **A047** | Ordenador Portátil Toshiba | Equipo fijo | Infraestructura | 3 | 3 | 2 | 2,67 |
| **A048** | Ordenador Aditk | Equipo fijo | Infraestructura | 3 | 3 | 2 | 2,67 |
| **A049** | Ordenador Altek | Equipo fijo | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A050** | Sistema de Contabilidad Olimpo | Virtualización | Analista de Sistema | 3 | 1 | 2 | 2 |
| **A051** | Sistema de Automatización de Temperatura | Virtualización | Analista de Sistema | 3 | 3 | 2 | 2,67 |
| **A052** | Backup | Virtualización | Analista de Sistema | 3 | 2 | 2 | 2,33 |
| **A053** | Reporte Trafico de Red | Copia de Reporte | Infraestructura | 3 | 2 | 2 | 2,33 |
| **A054** | Red de Datos | Virtualización | Infraestructura | 3 | 3 | 2 | 2,67 |
| **A055** | Diccionario de Datos | Sistemas | Analista de Sistema | 2 | 2 | 1 | 1,67 |
| **A056** | Esquema de Datos | Proceso de Sistemas | Analista de Sistema | 2 | 3 | 1 | 2 |
| **A057** | Programa Roles de Pago | Proceso de Sistemas | Analista de Sistema | 3 | 3 | 2 | 2,67 |
| **A058** | Código Fuente Sistema de Intranet | Proceso de Sistemas | Analista de Sistema | 3 | 2 | 1 | 2 |
| | | | | | | | 2,67 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A059** | Información Respaldada | Proceso de Sistemas | Analista de Sistema | 3 | 3 | 2 | |
| **A060** | Sistemas de Procesos Programadas | Proceso de Sistemas | Analista de Sistema | 3 | 3 | 2 | 2,67 |

**Amenazas y vulnerabilidades**

En conformidad a las siguientes tablas, se presentarán las amenazas(AM) y vulnerabilidades(V) de cada uno de los procesos más precios con sus respectivos activos involucrados en el sistema de intranet.

Tabla 10 Listado de Amenazas y Vulnerabilidades del Data Center

| **Proceso:** | | **Administración de Data Center** | | | | | |
|---|---|---|---|---|---|---|---|
| **Responsable:** | | **Administrador de Redes** | | | | | |
| **Activo** | | **Categoría General** | **Categoría Especifica** | **Amenaza** | | **Vulnerabilidad** | |
| **A001** | Data center Liebert | Sitio | Ambiente Interno | **AM001** | Terremoto | **V001** | Susceptible a desastres naturales |
| **A002** | Servidor Panasonic | Hardware | Equipo Fijo | **AM002** | Errores de mantenimiento | **V002** | Mantenimiento inadecuado |
| | | | | **AM003** | Interrupción de suministro eléctrico | **V003** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM004** | Puertos USB habilitados | **V004** | Sustracción de información |
| | | | | **AM005** | Fallas de equipos | **V005** | Uso de equipamiento obsoleto |
| **A003** | Servidor Tipo IBM BLADE | Hardware | Equipo Fijo | **AM006** | Errores de mantenimiento | **V006** | Mantenimiento inadecuado |
| | | | | **AM007** | Interrupción de suministro eléctrico | **V007** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| **A004** | | Hardware | Equipo | **AM008** | Errores de mantenimiento | **V008** | Mantenimiento inadecuado |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Sensores de temperatura | | Fijo | **AM009** | Interrupción de suministro eléctrico | **V009** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM010** | Falla de sensor | **V010** | Uso de equipamiento obsoleto |
| **A005** | | Hardware | | **AM011** | Errores de mantenimiento | **V011** | Mantenimiento inadecuado |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Servidor “10” HP Prolian DL 360 p G6 | | Equipo Fijo | **AM012** | Interrupción de suministro eléctrico | **V012** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM013** | Puertos USB habilitados | **V013** | Sustracción de información |
| | | | | **AM014** | Falla de equipos | **V014** | Uso de equipamiento obsoleto |
| **A006** | Sensores de calor | Hardware | Equipo Fijo | **AM015** | Errores de mantenimiento | **V015** | Mantenimiento inadecuado |
| | | | | **AM016** | Interrupción de suministro eléctrico | **V016** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM017** | Falla de sensor | **V017** | Uso de equipamiento obsoleto |
| **A007** | Servidor “6” Prolian DL 380 E G8 | Hardware | Equipo Fijo | **AM018** | Errores de mantenimiento | **V018** | Mantenimiento inadecuado |
| | | | | **AM019** | Interrupción de suministro eléctrico | **V019** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM020** | Puertos USB habilitados | **V020** | Sustracción de información |
| | | | | **AM021** | Fallas en equipos | **V021** | Uso de equipamiento obsoleto |
| **A008** | | Hardware | Equipo | **AM022** | Errores de mantenimiento | **V022** | Mantenimiento inadecuado |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Servidor “36” HP Prolan ML 110 | | Fijo | **AM023** | Interrupción de suministro eléctrico | **V023** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM024** | Puertos USB habilitados | **V024** | Sustracción de información |
| | | | | **AM025** | Fallas en equipos | **V025** | Uso de equipamiento obsoleto |
| **A009** | Ordenador Personal Lenovo | Hardware | Equipo Fijo | **AM026** | Falla en equipos | **V026** | Uso continuo e inadecuado de equipos |
| | | | | **AM027** | Deterioro de soportes | **V027** | Mantenimiento insuficiente |
| | | | | **AM028** | Puertos USB habilitados | **V028** | Sustracción de información |
| **A010** | Sistema operativo Windows 7 | Software | Sistema Operativo | **AM029** | Uso no autorizado de software | **V029** | Sistema desprotegido mediante acceso no autorizado |
| | | | | **AM030** | Sustracción de información | **V030** | Nivel de confidencialidad no definido con claridad |
| **A011** | Computadora portátil COMPAQ | Personal | Usuario | **AM031** | Intercepción de información. | **V031** | Conexión de red pública sin conexión. |
| | | | | **AM032** | Contrato de confidencialidad | **V032** | Salvaguardas los intereses institucionales de toda la información que custodian |
| **A012** | UPS | Hardware | Equipo Fijo | **AM033** | Intercepción de información | **V033** | Las copias de seguridad no se disponen en lugar fuera de la Institución |
| | | | | **AM034** | Robo | **V034** | Equipamiento móvil proclive para robar |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A013** | Swich | Hardware | Equipo Fijo | **AM035** | Interrupción de servicio eléctrico | **V035** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM036** | Falla de equipos | **V036** | Uso de equipamiento obsoleto |
| **A014** | Sistema de cámara video vigilancia | Hardware | Equipo Fijo | **AM037** | Interrupción de servicio eléctrico | **V037** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM038** | Deterioro de soportes | **V038** | Mantenimiento insuficiente |
| **A015** | Alarma de incendio | Hardware | Equipo Fijo | **AM039** | Interrupción de servicio eléctrico | **V039** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM040** | Falla de equipos | **V040** | Uso de equipamiento obsoleto |
| **A016** | Sistema de enfriamiento | Hardware | Equipo Fijo | **AM041** | Interrupción de servicio eléctrico | **V041** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM042** | Falla de equipos | **V042** | Uso de equipamiento obsoleto |
| | | | | **AM043** | Error de mantenimiento | **V043** | Mantenimiento inadecuado |
| **A017** | Mikrotik | Hardware | Equipo Fijo | **AM044** | Interrupción de servicio eléctrico | **V044** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM045** | Fallas de los vínculos de comunicación | **V045** | Inadecuada gestión de redes |
| | | | | **AM046** | Falla de equipos | **V046** | Uso de equipamiento obsoleto |
| **A018** | KVM – 440 DLink | Hardware | Equipo Fijo | **AM047** | Interrupción de servicio eléctrico | **V047** | Susceptibilidad del equipamiento a alteraciones en el voltaje |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | **AM048** | Falla de equipos | **V048** | Uso de equipamiento obsoleto |
| **A019** | Sistema eléctrico | Hardware | Equipo Fijo | **AM049** | Interrupción de servicio eléctrico | **V049** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | | | **AM050** | Deterioro de soportes | **V050** | Mantenimiento insuficiente |
| | | | | **AM051** | Errores de mantenimiento | **V051** | Mantenimiento inadecuado |
| **A020** | Liberty Data Center | Ambiente Interno | Infraestructura | **AM052** | Errores de mantenimiento | **V052** | Mantenimiento inadecuado |
| | | | | **AM053** | Interrupción de suministro eléctrico | **V053** | Susceptibilidad del equipamiento a alteraciones en el voltaje |

En la tabla 10 se presentará las amenazas(AM) y vulnerabilidades(V) con respecto a los activos de seguridad de la información que se encuentran involucrados en el sistema de intranet.

Tabla 11 Listado de Amenazas y Vulnerabilidades de Seguridad de la Información

| **Proceso:** | | **Seguridad de la Información** | | | | | |
|---|---|---|---|---|---|---|---|
| **Responsable:** | | **Analista de Sistema** | | | | | |
| **Activo** | | **Categoría General** | **Categoría Especifica** | **Amenaza** | | **Vulnerabilidad** | |
| **A021** | Copia Respaldo del Data Center | Copia de respaldo | Infraestructura | **AM054** | Intercepción de Información | **V054** | Falta de control en datos de entrada y salidas |
| | | | | **AM055** | Modificación accidental de datos del sistema de información | **V055** | Sesiones activas después del horario laboral |
| **A022** | Registro de Actividades de | Copia de respaldo | Infraestructura | **AM056** | Acceso no autorizado al sistema de información | **V056** | Contraseñas inseguras |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Base de Datos | | | **AM057** | Daños ocasionados durante pruebas de intrusión | **V057** | Sesiones activas después del horario laboral |
| **A023** | Respaldo de Configuración de Mikrotik | Copia de respaldo | Infraestructura | **AM058** | Modificación accidental de datos del sistema de información | **V058** | Sesiones activas después del horario laboral |
| **A024** | Respaldo de Máquina Virtual Cabild | Copia de respaldo | Infraestructura | **AM059** | Acceso físico no autorizado | **V059** | Sistemas desprotegidos ante acceso no autorizado |
| | | | | **AM060** | Código Malicioso | **V060** | Protección desactualizada contra códigos malicioso |
| **A025** | Respaldo de Máquina Virtual Centos 7-Servicios | Copia de respaldo | Infraestructura | **AM061** | Instalación no autorizada de software | **V061** | Falta de inventario de licencias instaladas |
| **A026** | Respaldo de Máquina Virtual Elastix | Copia de respaldo | Infraestructura | **AM062** | Destrucción de registros | **V062** | Inadecuada gestión de redes |
| | | | | **AM063** | Interceptación de información | **V063** | Ubicación susceptible a perdidas |
| **A027** | Respaldo de Máquina Virtual Ipcop-Proxy | Copia de respaldo | Infraestructura | **AM064** | Errores de aplicaciones | **V064** | Inadecuada capacitación |
| **A028** | Respaldo de Máquina Virtual Windows 7 Cloud | Copia de respaldo | Infraestructura | **AM065** | Interceptación de información | **V065** | Mantenimiento inadecuado |
| **A029** | Respaldo de Máquina Virtual Storage Manager (localhost) | Copia de respaldo | Infraestructura | **AM066** | Interceptación de información | **V066** | Poderes de gran alcance |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A030** | Respaldo de Máquina Virtual Cabildo-Principal | Copia de respaldo | Infraestructura | **AM067** | Interceptación de información | **V067** | Ubicación susceptible a perdidas |
| **A031** | Respaldo de Máquina Virtual SisRiesgo | Copia de respaldo | Infraestructura | **AM068** | Destrucción de registros | **V068** | Inadecuada gestión de redes |
| **A032** | Respaldo de Máquina Virtual FreeNas | Copia de respaldo | Infraestructura | **AM069** | Incumplimiento de leyes | **V069** | Poderes de gran alcance |
| **A033** | Respaldo de Máquina Virtual Pruebas-Cabildo-Técnicos | Copia de respaldo | Infraestructura | **AM070** | Sustracción de información | **V070** | Acceso no autorizado a instalaciones |
| **A034** | Respaldo de Máquina Virtual Server-antivirus | Copia de respaldo | Infraestructura | **AM071** | Interceptación de información | **V071** | Ubicación susceptible a perdidas |
| **A035** | Respaldo de Máquina Virtual 2003 SERVER | Copia de respaldo | Infraestructura | **AM072** | Sustracción de información | **V072** | Acceso no autorizado a instalaciones |
| **A036** | Respaldo de Máquina Virtual servidor.ime.org | Copia de respaldo | Infraestructura | **AM073** | Fuga o revelación de información | **V073** | Solo una copia de la información |
| **A037** | Respaldo de Máquina Virtual SIGCES | Copia de respaldo | Infraestructura | **AM074** | Fuga o revelación de información | **V074** | Solo una copia de la información |
| **A041** | Ordenador personal Jefe de TI | Equipo fijo | Jefe de Infraestructura | **AM075** | Interceptación de información | **V075** | Información disponible para personas no autorizada |
| | | | | **AM076** | Contagio de virus | **V076** | Falta de antivirus con licencia |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A042** | Ordenador personal Jefe de Infraestructura | Equipo fijo | Jefe de TI | **AM077** | Falsificación de registros | **V077** | Inadecuados derechos de usuario |
| | | | | **AM078** | Contagio de virus | **V078** | Falta de antivirus con licencia |
| | | | | **AM079** | Sustracción de información | **V079** | Puertos USB habilitados |
| **A043** | Ordenador personal jefe de desarrollo | Equipo fijo | Infraestructura | **AM080** | Contagio de virus | **V080** | Falta de antivirus con licencia |
| | | | | **AM081** | Interceptación de información | **V081** | Información disponible para personas no autorizada |
| **A044** | Ordenador personal de mantenimiento | Equipo fijo | Jefe de desarrollo | **AM082** | Contagio de virus | **V082** | Falta de antivirus con licencia |
| | | | | **AM083** | Instalación no autorizada de software | **V083** | Falta de inventario de licencias instaladas |
| **A045** | Respaldo de Base de Datos | Copia de Respaldo | Desarrollo de Software | **AM084** | Sustracción de información | **V084** | Puertos USB habilitados |
| | | | | **AM085** | Contagio de virus | **V085** | Falta de antivirus con licencia |

En la tabla 11 se presentará las amenazas(AM) y vulnerabilidades(V) correspondiente al proceso de soporte técnico, involucrados de manera más crítica en el sistema de intranet.

Tabla 12 Listado de Amenazas y Vulnerabilidades de Soporte Técnico y Redes

| **Proceso:** | **Soporte Técnico y Redes** |
|---|---|

| **Responsable:** | | **Infraestructura Tecnológica** | | | | | |
|---|---|---|---|---|---|---|---|
| **Activo** | | **Categoría General** | **Categoría Especifica** | **Amenaza** | | **Vulnerabilidad** | |
| **A046** | Ordenador Apple | Equipo fijo | Infraestructura | **AM086** | Modificación accidental de datos del sistema de información | **V086** | Sesiones activas después del horario laboral |
| **A047** | Ordenador Portátil Toshiba | Equipo fijo | Infraestructura | **AM087** | Sustracción de información | **V087** | Puertos USB habilitados |
| | | | | **AM088** | Modificación accidental de datos del sistema de información | **V088** | Sesiones activas después del horario laboral |
| **A048** | Ordenador Aditk | Equipo fijo | Infraestructura | **AM089** | Daños provocados por actividades de tercero | **V089** | Eliminación de Registros y datos de funcionamiento de la información |
| **A049** | Ordenador Altek | Equipo fijo | Infraestructura | **AM090** | Errores de mantenimiento | **V090** | Inadecuado control de cambios |
| **A050** | Sistema de Contabilidad Olimpo | Virtualización | Analista de Sistema | **AM091** | Robo | **V091** | Inadecuada gestión del empleador |
| **A051** | Sistema de Automatización de Temperatura | Virtualización | Analista de Sistema | **AM092** | Modificación accidental de datos del sistema de información | **V092** | Sesiones activas después del horario laboral |
| **A052** | Backup | Virtualización | Analista de Sistema | **AM093** | Intercepción de información | **V093** | Ubicación susceptible a perdidas |
| **A053** | Reporte Trafico de Red | Copia de Reporte | Infraestructura | **AM094** | Sustracción de información | **V094** | Nivel de confidencialidad no definido con claridad |
| **A054** | Red de Datos | Virtualización | Infraestructura | **AM095** | Fuga o revelación de información | **V095** | Falta de control en datos de entrada y salida |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A055** | Diccionario de Datos | Sistemas | Infraestructura | **AM096** | Fuga o revelación de información | **V096** | Falta de control en datos de entrada y salida |
| **A056** | Esquema de Datos | Proceso de Sistemas | Analista de Sistema | **AM097** | Fuga o revelación de información | **V097** | Falta de control en datos de entrada y salida |
| **A057** | Programa Roles de Pago | Proceso de Sistemas | Analista de Sistema | **AM098** | Modificación accidental de datos del sistema de información | **V098** | Sesiones activas después del horario laboral |
| **A058** | Código Fuente Sistema de Intranet | Proceso de Sistemas | Analista de Sistema | **AM099** | Mala utilización de la aplicación | **V099** | Mala redacción del manual |
| | | | | **AM100** | Plagio | **V100** | Falta de control de desarrollo |
| **A059** | Información Respaldada | Proceso de Sistemas | Analista de Sistema | **AM101** | Perdida de servicios | **V101** | Solo una copia de la información |
| **A060** | Sistemas de Procesos Programadas | Proceso de Sistemas | Analista de Sistema | **AM102** | Otros desastres (causados por el hombre) | **V102** | Falta de separación de entornos de prueba y operativos |

**Riesgos**

La intención de mostrar un análisis de riesgo es para verificar que probabilidad tiene de efectuarse un evento y el impacto que llegase a materializar las amenazas, para ello se va a definir niveles del 1 al 5 que corresponde a bajo (1 - 3) representado por el color verde, medio (2 - 4) representado por el color amarillo, alto (3 – 5) representado por el color rojo. En los criterios de evaluación se considera como apetito del riesgo aquellos que obtengan como resultado 9, los demás se los considera no aceptables, de los cuales hay que implementar un control.

Tabla 13 Evaluación y cálculo de los riesgos del Data Center

| **Proceso:** | | **Administración de Data Center** | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Responsable:** | | **Administrador de Redes** | | | | | | |
| **Activo** | | **Probabilidad de la amenaza explote la vulnerabilidad** | **Impacto de materializarse la amenaza** | **Riesgo del Activo** | **Amenaza** | | **Vulnerabilidad** | |
| **A001** | Data center Liebert | 4 | 3 | 12=Medio | **AM001** | Terremoto | **V001** | Susceptible a desastres naturales |
| **A002** | Servidor Panasonic | 1 | 3 | 3=Bajo | **AM002** | Errores de mantenimiento | **V002** | Mantenimiento inadecuado |
| | | 3 | 2 | 6=Medio | **AM003** | Interrupción de suministro eléctrico | **V003** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 3 | 9=Medio | **AM004** | Puertos USB habilitados | **V004** | Sustracción de información |
| | | 3 | 2 | 6=Medio | **AM005** | Fallas de equipos | **V005** | Uso de equipamiento obsoleto |
| **A003** | Servidor Tipo IBM BLADE | 2 | 2 | 4=Bajo | **AM006** | Errores de mantenimiento | **V006** | Mantenimiento inadecuado |
| | | 3 | 2 | 6=Medio | **AM007** | Interrupción de suministro eléctrico | **V007** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| **A004** | | 3 | 3 | 9=Medio | **AM008** | Errores de mantenimiento | **V008** | Mantenimiento inadecuado |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Sensores de temperatura | 3 | 2 | 6=Medio | **AM009** | Interrupción de suministro eléctrico | **V009** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 2 | 2 | 4=Bajo | **AM010** | Falla de sensor | **V010** | Uso de equipamiento obsoleto |
| **A005** | Servidor "10" HP Prolian DL 360 p G6 | 3 | 2 | 6=Medio | **AM011** | Errores de mantenimiento | **V011** | Mantenimiento inadecuado |
| | | 3 | 3 | 9=Medio | **AM012** | Interrupción de suministro eléctrico | **V012** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 2 | 6=Medio | **AM013** | Puertos USB habilitados | **V013** | Sustracción de información |
| | | 2 | 2 | 4=Bajo | **AM014** | Falla de equipos | **V014** | Uso de equipamiento obsoleto |
| **A006** | Sensores de calor | 3 | 2 | 6=Medio | **AM015** | Errores de mantenimiento | **V015** | Mantenimiento inadecuado |
| | | 3 | 3 | 9=Medio | **AM016** | Interrupción de suministro eléctrico | **V016** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 5 | 2 | 10=Medio | **AM017** | Falla de sensor | **V017** | Uso de equipamiento obsoleto |
| **A007** | Servidor "6" Prolian DL 380 E G8 | 2 | 1 | 2=Bajo | **AM018** | Errores de mantenimiento | **V018** | Mantenimiento inadecuado |
| | | 3 | 2 | 6=Medio | **AM019** | Interrupción de suministro eléctrico | **V019** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 3 | 9=Medio | **AM020** | Puertos USB habilitados | **V020** | Sustracción de información |
| | | 3 | 2 | 6=Medio | **AM021** | Fallas en equipos | **V021** | Uso de equipamiento obsoleto |
| **A008** | | 2 | 2 | 4=Bajo | **AM022** | Errores de mantenimiento | **V022** | Mantenimiento inadecuado |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Servidor “36” HP Prolan ML 110 | 3 | 2 | 6=Medio | **AM023** | Interrupción de suministro eléctrico | **V023** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 3 | 9=Medio | **AM024** | Puertos USB habilitados | **V024** | Sustracción de información |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 3 | 2 | 6=Medio | **AM025** | Fallas en equipos | **V025** | Uso de equipamiento obsoleto |
| **A009** | Ordenador Personal Lenovo | 2 | 2 | 4=Bajo | **AM026** | Falla en equipos | **V026** | Uso continuo e inadecuado de equipos |
| | | 1 | 2 | 2=Bajo | **AM027** | Deterioro de soportes | **V027** | Mantenimiento insuficiente |
| | | 1 | 3 | 3=Bajo | **AM028** | Puertos USB habilitados | **V028** | Sustracción de información |
| **A010** | Sistema operativo Windows 7 | 1 | 2 | 2=Bajo | **AM029** | Uso no autorizado de software | **V029** | Sistema desprotegido mediante acceso no autorizado |
| | | 4 | 2 | 8=Medio | **AM030** | Sustracción de información | **V030** | Nivel de confidencialidad no definido con claridad |
| **A011** | Computadora portátil COMPAQ | 3 | 2 | 6=Medio | **AM031** | Intercepción de información. | **V031** | Conexión de red pública sin conexión. |
| | | 3 | 2 | 6=Medio | **AM032** | Contrato de confidencialidad | **V032** | Salvaguardas los intereses institucionales de toda la información que custodian |
| **A012** | UPS | 3 | 2 | 6=Medio | **AM033** | Intercepción de información | **V033** | Las copias de seguridad no se disponen en lugar fuera de la Institución |
| | | 4 | 3 | 12=Medio | **AM034** | Robo | **V034** | Equipamiento móvil proclive para robar |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A013** | Swich | 4 | 2 | 8=Medio | **AM035** | Interrupción de servicio eléctrico | **V035** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 4 | 2 | 8=Medio | **AM036** | Falla de equipos | **V036** | Uso de equipamiento obsoleto |
| **A014** | Sistema de cámara video vigilancia | 4 | 2 | 8=Medio | **AM037** | Interrupción de servicio eléctrico | **V037** | Susceptibilidad del equipamiento a alteraciones en el voltaje |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2 | 3 | 6=Medio | **AM038** | Deterioro de soportes | **V038** | Mantenimiento insuficiente |
| **A015** | Alarma de incendio | 4 | 2 | 8=Medio | **AM039** | Interrupción de servicio eléctrico | **V039** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 2 | 6=Medio | **AM040** | Falla de equipos | **V040** | Uso de equipamiento obsoleto |
| **A016** | Sistema de enfriamiento | 3 | 2 | 6=Medio | **AM041** | Interrupción de servicio eléctrico | **V041** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 2 | 6=Medio | **AM042** | Falla de equipos | **V042** | Uso de equipamiento obsoleto |
| | | 3 | 2 | 6=Medio | **AM043** | Error de mantenimiento | **V043** | Mantenimiento inadecuado |
| **A017** | Mikrotik | 3 | 3 | 9=Medio | **AM044** | Interrupción de servicio eléctrico | **V044** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 5 | 1 | 5=Medio | **AM045** | Fallas de los vínculos de comunicación | **V045** | Inadecuada gestión de redes |
| | | 5 | 3 | 15=Alto | **AM046** | Falla de equipos | **V046** | Uso de equipamiento obsoleto |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A018** | KVM – 440 DLink | 3 | 1 | 3=Bajo | **AM047** | Interrupción de servicio eléctrico | **V047** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 2 | 2 | 4=Bajo | **AM048** | Falla de equipos | **V048** | Uso de equipamiento obsoleto |
| **A019** | Sistema eléctrico | 2 | 3 | 6=Medio | **AM049** | Interrupción de servicio eléctrico | **V049** | Susceptibilidad del equipamiento a alteraciones en el voltaje |
| | | 3 | 2 | 6=Medio | **AM050** | Deterioro de soportes | **V050** | Mantenimiento insuficiente |
| | | 3 | 3 | 9=Medio | **AM051** | Errores de mantenimiento | **V051** | Mantenimiento inadecuado |
| **A020** | | 3 | 2 | 6=Medio | **AM052** | Errores de mantenimiento | **V052** | Mantenimiento inadecuado |
| | Liberty Data Center | 3 | 2 | 6=Medio | **AM053** | Interrupción de suministro eléctrico | **V053** | Susceptibilidad del equipamiento a alteraciones en el voltaje |

Tabla 14 Evaluación y cálculo de riesgo de Seguridad de la Información

| **Proceso:** | | | **Seguridad de la Información** | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Responsable:** | | | **Analista de Sistema** | | | | | |
| **Activo** | | **Probabilidad de la amenaza explote la vulnerabilidad** | **Impacto de materializarse la amenaza** | **Riesgo del Activo** | **Amenaza** | | **Vulnerabilidad** | |
| **A021** | Copia Respaldo del Data Center | 4 | 3 | 12=Medio | **AM054** | Intercepción de Información | **V054** | Falta de control en datos de entrada y salidas |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 4 | 2 | 8=Medio | **AM055** | Modificación accidental de datos del sistema de información | **V055** | Sesiones activas después del horario laboral |
| **A022** | Registro de Actividades de Base de Datos | 3 | 3 | 9=Medio | **AM056** | Acceso no autorizado al sistema de información | **V056** | Contraseñas inseguras |
| | | 4 | 2 | 8=Medio | **AM057** | Daños ocasionados durante pruebas de intrusión | **V057** | Sesiones activas después del horario laboral |
| **A023** | Respaldo de Configuración de Mikrotik | 4 | 2 | 8=Medio | **AM058** | Modificación accidental de datos del sistema de información | **V058** | Sesiones activas después del horario laboral |
| **A024** | Respaldo de Máquina Virtual Cabild | 3 | 2 | 6=Medio | **AM059** | Acceso físico no autorizado | **V059** | Sistemas desprotegidos ante acceso no autorizado |
| | | 4 | 3 | 12=Medio | **AM060** | Código Malicioso | **V060** | Protección desactualizada contra códigos malicioso |
| **A025** | Respaldo de Máquina Virtual Centos 7-Servicios | 4 | 2 | 8=Medio | **AM061** | Instalación no autorizada de software | **V061** | Falta de inventario de licencias instaladas |
| **A026** | Respaldo de Máquina Virtual Elastix | 5 | 2 | 10=Medio | **AM062** | Destrucción de registros | **V062** | Inadecuada gestión de redes |
| | | 5 | 2 | 10=Medio | **AM063** | Interceptación de información | **V063** | Ubicación susceptible a perdidas |
| **A027** | Respaldo de Máquina Virtual Ipcop-Proxy | 5 | 2 | 10=Medio | **AM064** | Errores de aplicaciones | **V064** | Inadecuada capacitación |
| **A028** | Respaldo de Máquina Virtual Windows 7 Cloud | 5 | 2 | 10=Medio | **AM065** | Interceptación de información | **V065** | Mantenimiento inadecuado |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A029** | Respaldo de Máquina Virtual Storage Manager (localhost) | 3 | 2 | 6=Medio | **AM066** | Interceptación de información | **V066** | Poderes de gran alcance |
| **A030** | Respaldo de Máquina Virtual Cabildo-Principal | 5 | 2 | 10=Medio | **AM067** | Interceptación de información | **V067** | Ubicación susceptible a perdidas |
| **A031** | Respaldo de Máquina Virtual SisRiesgo | 4 | 2 | 8=Medio | **AM068** | Destrucción de registros | **V068** | Inadecuada gestión de redes |
| **A032** | Respaldo de Máquina Virtual FreeNas | 3 | 3 | 9=Medio | **AM069** | Incumplimiento de leyes | **V069** | Poderes de gran alcance |
| **A033** | Respaldo de Máquina Virtual Pruebas-Cabildo-Técnicos | 3 | 3 | 9=Medio | **AM070** | Sustracción de información | **V070** | Acceso no autorizado a instalaciones |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A034** | Respaldo de Máquina Virtual Server-antivirus | 5 | 2 | 10=Medio | **AM071** | Interceptación de información | **V071** | Ubicación susceptible a perdidas |
| **A035** | Respaldo de Máquina Virtual 2003 SERVER | 4 | 2 | 8=Medio | **AM072** | Sustracción de información | **V072** | Acceso no autorizado a instalaciones |
| **A036** | Respaldo de Máquina Virtual servidor.ime.org | 4 | 1 | 4=Medio | **AM073** | Fuga o revelación de información | **V073** | Solo una copia de la información |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A037** | Respaldo de Máquina Virtual SIGCES | 5 | 2 | 10=Medio | **AM074** | Fuga o revelación de información | **V074** | Solo una copia de la información |
| **A041** | Ordenador personal Jefe de TI | 4 | 2 | 8=Medio | **AM075** | Interceptación de información | **V075** | Información disponible para personas no autorizada |
| | | 5 | 3 | 15=Alto | **AM076** | Contagio de virus | **V076** | Falta de antivirus con licencia |
| **A042** | Ordenador personal Jefe de Infraestructura | 5 | 3 | 15=Alto | **AM077** | Falsificación de registros | **V077** | Inadecuados derechos de usuario |
| | | 5 | 2 | 10=Medio | **AM078** | Contagio de virus | **V078** | Falta de antivirus con licencia |
| | | 5 | 3 | 15=Alto | **AM079** | Sustracción de información | **V079** | Puertos USB habilitados |
| **A043** | Ordenador personal jefe de desarrollo | 3 | 2 | 6=Medio | **AM080** | Contagio de virus | **V080** | Falta de antivirus con licencia |
| | | 5 | 1 | 5=Medio | **AM081** | Interceptación de información | **V081** | Información disponible para personas no autorizada |
| **A044** | Ordenador personal de mantenimiento | 5 | 2 | 10=Medio | **AM082** | Contagio de virus | **V082** | Falta de antivirus con licencia |
| | | 4 | 3 | 12=Medio | **AM083** | Instalación no autorizada de software | **V083** | Falta de inventario de licencias instaladas |
| **A045** | | 4 | 2 | 8=Medio | **AM084** | Sustracción de información | **V084** | Puertos USB habilitados |
| | Respaldo de Base de Datos | 5 | 2 | 10=Medio | **AM085** | Contagio de virus | **V085** | Falta de antivirus con licencia |

Tabla 15 Evaluación y cálculo de riesgo de Soporte Técnico y Redes

| **Proceso:** | | | **Soporte Técnico y Redes** | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Responsable:** | | | **Infraestructura Tecnológica** | | | | | |
| **Activo** | | **Probabilidad de la amenaza explote la vulnerabilidad** | **Impacto de materializarse la amenaza** | **Riesgo del Activo** | **Amenaza** | | **Vulnerabilidad** | |
| **A046** | Ordenador Apple | 5 | 1 | 5=Medio | **AM086** | Modificación accidental de datos del sistema de información | **V086** | Sesiones activas después del horario laboral |
| **A047** | Ordenador Portátil Toshiba | 5 | 2 | 10=Medio | **AM087** | Sustracción de información | **V087** | Puertos USB habilitados |
| | | 5 | 3 | 15=Alto | **AM088** | Modificación accidental de datos del sistema de información | **V088** | Sesiones activas después del horario laboral |
| **A048** | Ordenador Aditk | 5 | 4 | 20=Alto | **AM089** | Daños provocados por actividades de tercero | **V089** | Eliminación de Registros y datos de funcionamiento de la información |
| **A049** | Ordenador Altek | 3 | 2 | 6=Medio | **AM090** | Errores de mantenimiento | **V090** | Inadecuado control de cambios |
| **A050** | Sistema de Contabilidad Olimpo | 5 | 3 | 15=Alto | **AM091** | Robo | **V091** | Inadecuada gestión del empleador |
| **A051** | Sistema de Automatización de Temperatura | 5 | 2 | 10=Medio | **AM092** | Modificación accidental de datos del sistema de información | **V092** | Sesiones activas después del horario laboral |
| **A052** | Backup | 3 | 1 | 3=Bajo | **AM093** | Intercepción de información | **V093** | Ubicación susceptible a perdidas |
| **A053** | Reporte Trafico de Red | 3 | 3 | 9=Medio | **AM094** | Sustracción de información | **V094** | Nivel de confidencialidad no definido con claridad |
| **A054** | Red de Datos | 3 | 4 | 12=Medio | **AM095** | Fuga o revelación de información | **V095** | Falta de control en datos de entrada y salida |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A055** | Diccionario de Datos | 4 | 3 | 12=Medio | **AM096** | Fuga o revelación de información | **V096** | Falta de control en datos de entrada y salida |
| **A056** | Esquema de Datos | 2 | 4 | 8=Medio | **AM097** | Fuga o revelación de información | **V097** | Falta de control en datos de entrada y salida |
| **A057** | Programa Roles de Pago | 2 | 3 | 6=Medio | **AM098** | Modificación accidental de datos del sistema de información | **V098** | Sesiones activas después del horario laboral |
| **A058** | Código Fuente Sistema de Intranet | 3 | 4 | 12=Medio | **AM099** | Mala utilización de la aplicación | **V099** | Mala redacción del manual |
| | | 3 | 5 | 15=Alto | **AM100** | Plagio | **V100** | Falta de control de desarrollo |
| **A059** | Información Respaldada | 4 | 3 | 12=Medio | **AM101** | Perdida de servicios | **V101** | Solo una copia de la información |
| **A060** | Sistemas de Procesos Programadas | 1 | 3 | 3=Medio | **AM102** | Otros desastres (causados por el hombre) | **V102** | Falta de separación de entornos de prueba y operativos |

A continuación, conforme a la ilustración 8, se mostrará el mapa de calor de los riesgos encontrados dentro de los activos asociados al sistema de intranet, ubicándose cada riesgo de acuerdo con su evaluación.

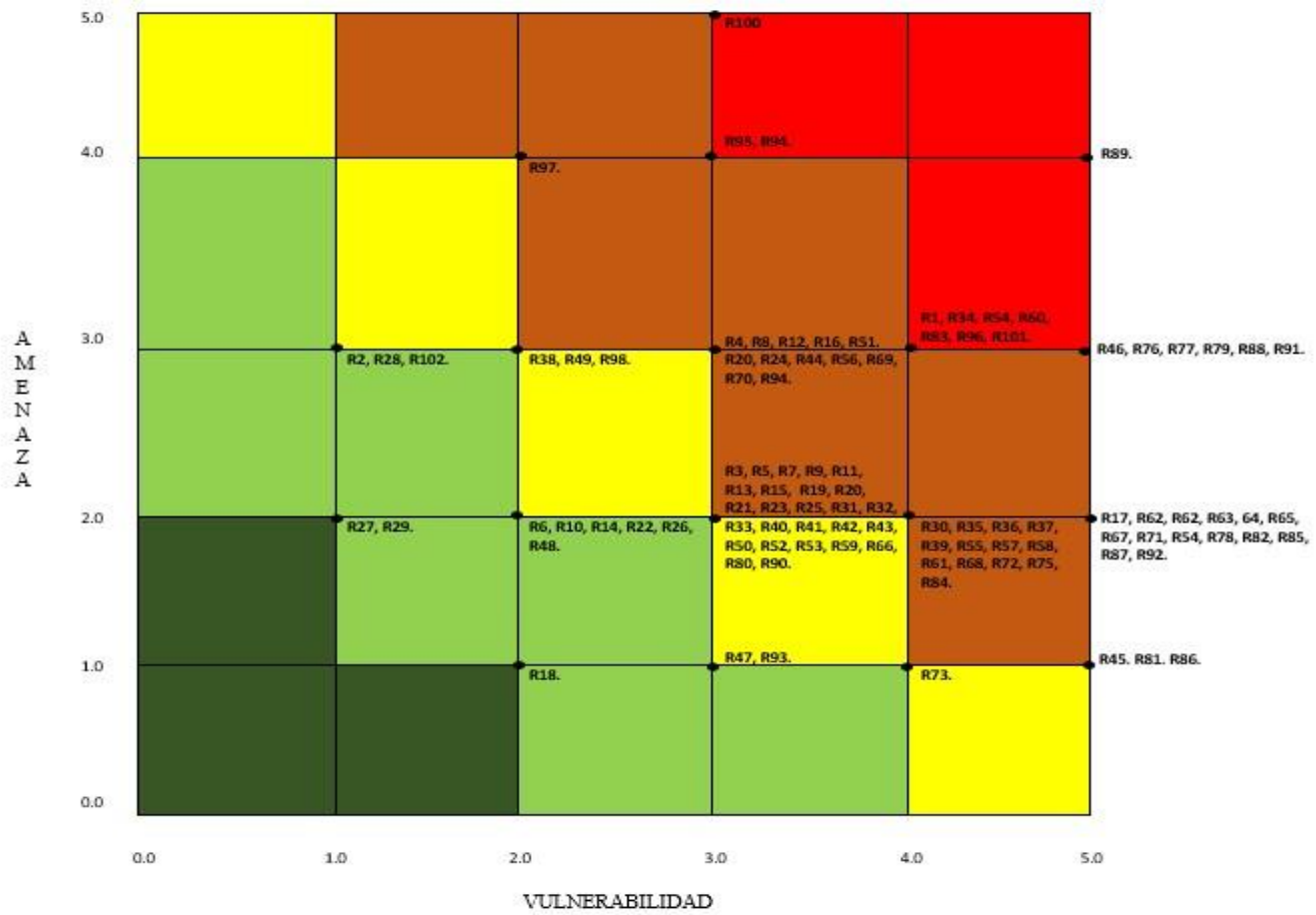



Ilustración 8 Mapa de Riesgo

Se encontraron **14 riesgos bajos** (R2, R5, R10, R14, R18, R22, R26, R27, R28, R29, R47, R48, R93, R102), **80 riesgos medios** (R1, R3, R4, R5, R7, R8, R9, R11, R12, R13, R15, R16, R17, R19, R20, R21, R23, R24, R25, R30, R31, R32, R33, R34, R35, R36, R37, R38, R39, R40, R41, R42,

R43, R44, R45, R49, R50, R51, R52, R53, R54, R55, R56, R57, R58, R59, R60, R61, R62, R63, R64, R65, R66, R67, R68, R69, R70, R71, R72, R73, R74, R75, R78, R80, R81, R82, R83, R84, R85, R86, R87, R90, R92, R94, R95, R96, R97, R98, R99, R101) **y 8 riesgos altos** (R46, R76, R77, R79, R88, R89, R91, R100) de los cuales se aplicará los controles pertinentes para eliminar o mitigarlos.

Dentro del apetito se seleccionaron aquellos riesgos que están sobre el promedio de 9, siendo así los siguientes:

Medios: R1, R17, R34, R54, R60, R62, R63, R64, R65, R67, R71, R74, R78, R82, R83, R85, R87, R92, R95, R96, R99.

Altos: R46, R76, R77, R79, R88, R89, R91, R100.

Con el propósito de evitar o eliminar, reducir o mitigar y minimizar los riesgos se aplicarán los siguientes controles a aquellos riesgos que están sobre el apetito del riesgo. A continuación, se proponen los controles según la ISO/IEC 27002:2013.

- Se recomienda aplicar el control A.11.1.4 en cuanto a la protección contra las amenazas externas y ambientales, lo cual se deberá diseñar y aplicar la protección física contra desastres naturales, ataques provocados por el hombre o incidentes (R1, R88, R89, R92).
- Se recomienda aplicar en los equipos, el mantenimiento debido a su necesidad, que asegure su perfecta continuidad, disponibilidad e integridad, por lo tanto, se aplicará el control A.11.2.4 de mantenimiento a los equipos (R17, R34, R46, R60, R76, R78, R82, R83, R85).
- Con el fin de tener la información respaldada por otros medios, se recomienda instalar un sistema raid de replicación de discos duros, políticas de seguridad y se aplicaran los controles A.5.1.1, A12.3.1 de copias de seguridad de la información, A.3 de control de acceso (R63, R65, R67, R71, R79, R87, R91, R95, R96, R101).
- Para que no exista la pérdida de código fuente del sistema de intranet, se recomienda implementar una arquitectura (modelo vista presentador), para tener un mejor control del código, también una metodología que contenga todas las pruebas de software. Agregar toda la documentación de usuario y necesaria de los módulos, fases y diseños a programar. Se debe aplicar los controles A.9.4.5 para el control de acceso al código fuente de los programas, A.9.4.2 de procedimientos seguro de inicio de sesión (R64, R99, R100).
- Se recomienda utilizar seguridad de activos para que no exista ingreso de dispositivos USB, modificaciones de escritorio, preferencias de Windows; como también para respaldos de información.

# CAPÍTULO IV: PROPUESTA

**Plan de gestión de seguridad de la información para el sistema de intranet, de la prefectura de Esmeraldas, basado en el estándar internacional de la ISO 27001:**

Dentro de la propuesta se presentará cada una de las normas a seguir para tener un buen diseño de gestión de la seguridad de la información, según lo que establece la ISO/IEC 27001, aplicando de manera clara las clausulas, normas, objetivos de control, políticas, procesos y procedimientos para la seguridad de la información, según el anexo A. La estructura de esta ISO 27001, tiene 10 cláusulas en 1 anexo, donde las normas aplicables de esta norma es de la cláusula 4 a la 10.

## ALCANCE

La prefectura de Esmeraldas, cuenta con un grupo de trabajo especializado en el área de tecnologías de la información, donde su propósito es brindar soluciones informáticas a las demás áreas del establecimiento.

Su propósito es brindar seguridad plena en todos los procesos que se realice dentro y fuera de la organización, salvaguardado, integrando, confiando y disponiendo todo lo referente a la seguridad de la información, es por ello, que se estableció un alcance que satisfaga la necesidad de tener una información segura, solucionando problemas y confiando plenamente en el procesamiento del sistema de intranet, realizado por dicho departamento de TI.

Dentro de la aplicación del alcance se debe tener:

- Un documento en la planificación para poder implementar la norma, es muy obligatorio (si no se cumple este paso no se podrá seguir al siguiente).
- Enumerar todos los procesos del sistema de intranet, instalaciones, medios técnicos, así como el tipo de información dentro del SGSI.
- Definir el alcance de cumplimiento, declarando de manera clara las dependencias e interfaces entre la organización y las entidades externas.

Como base fundamental de esta implementación es poder regirse a requisitos que presenta la norma ISO 27001, y tomar parámetros tales como requerimientos obligatorios, objetivos de control, controles del anexo A, clausulas, políticas que ayuden al sistema de intranet de la prefectura a ser muy eficaz y eficiente en la información que procesa cada

uno de sus áreas; pudiendo así determinar acciones correctivas de conformidad, que den soluciona alguna eventualidad catastrófica en la seguridad de la información.

## CONTEXTO DE LA ORGANIZACIÓN

**Objetivo:**

En esta cláusula se va a determinar las cuestiones externas e internas que ayuden para el propósito y capacidad plena para lograr resultados previsto del SGSI en el sistema de intranet de la organización.

Cada uno de los parámetros a establecer se presentan a continuación, conforme a la ilustración 9:

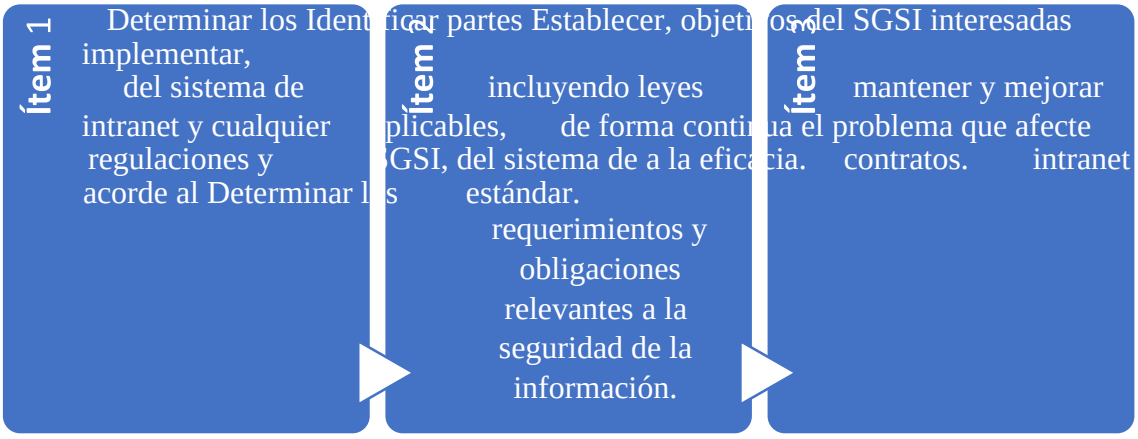



*Ilustración 9 Clausula Contexto de la Organización*

**Responsable:**

Jefe de desarrollo de sistemas y director del área.

## LIDERAZGO

**Objetivo:**

Toda la organización debe estar comprometida para cambios que se ejecuten en el interfaz del sistema, cumpliendo todas las políticas y manejando un liderazgo pertinente. Este objetivo se debe cumplir por medio de la alta dirección, asegurando que la seguridad de la información y los objetivos sean compatibles para la dirección estratégica de la organización.

El liderazgo debe contener la siguiente aplicación, conforme a la ilustración 10:

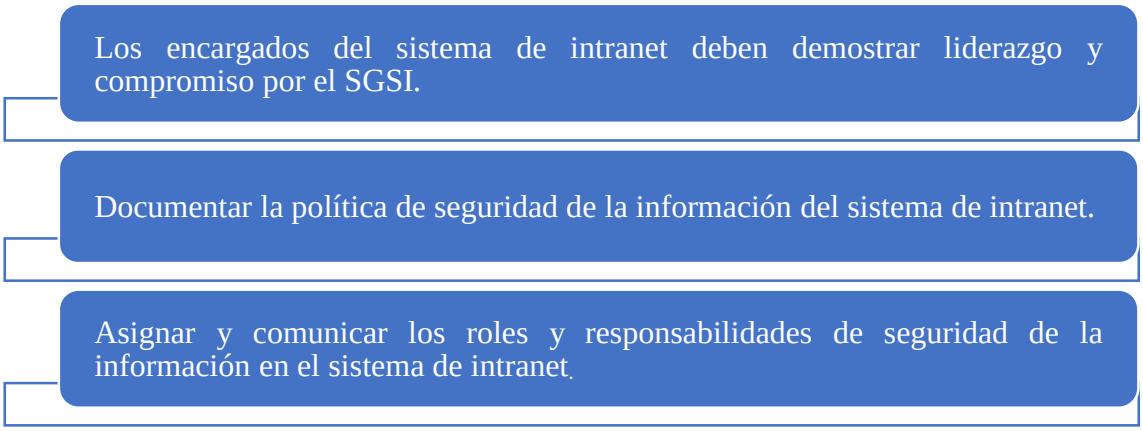



Ilustración 10 Clausula Liderazgo y Compromiso

**Responsable:**

Toda el área de TI.

## PLANIFICACIÓN

**Objetivo:**

Para la realización de este clausula se debe tener la comprensión de la organización y se su contexto, tomar acciones para tratar los riesgos y oportunidades. Se seguirá los siguientes pasos para su ejecución, conforme a la ilustración 11:

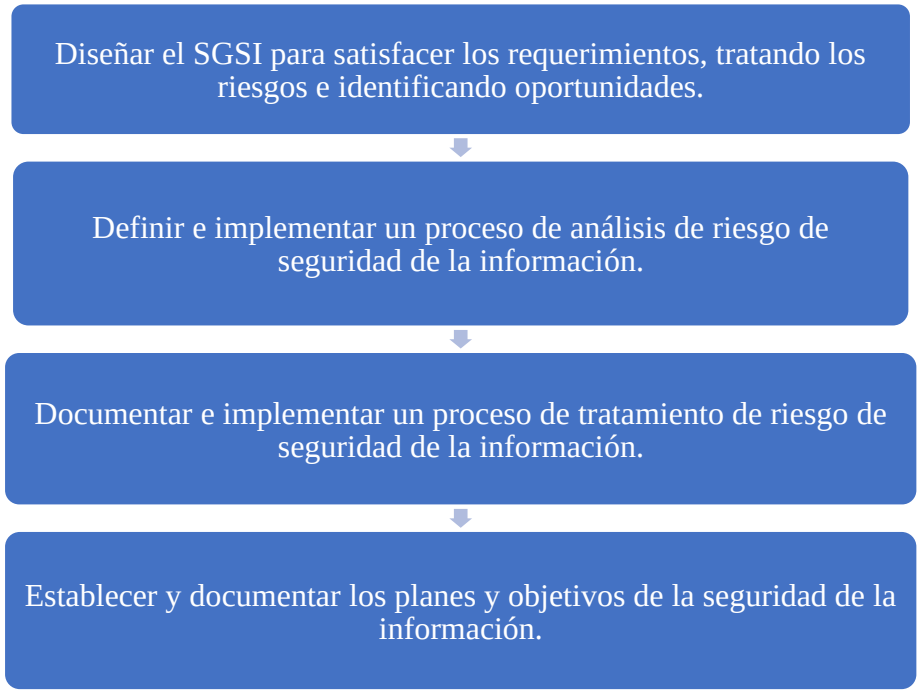



Ilustración 11 Clausula Planificación

**Responsable:**

Jefe de desarrollo de sistemas, director del área de TI.

## APOYO / SOPORTE

**Objetivo:**

Dentro de esta cláusula se definen parámetros tales como: recursos que se debe utilizar en el momento de establecer el SGSI en el sistema de intranet, de igual manera, competencia, concienciación, comunicación de las partes involucradas e información documentada, en conformidad a la ilustración 12.

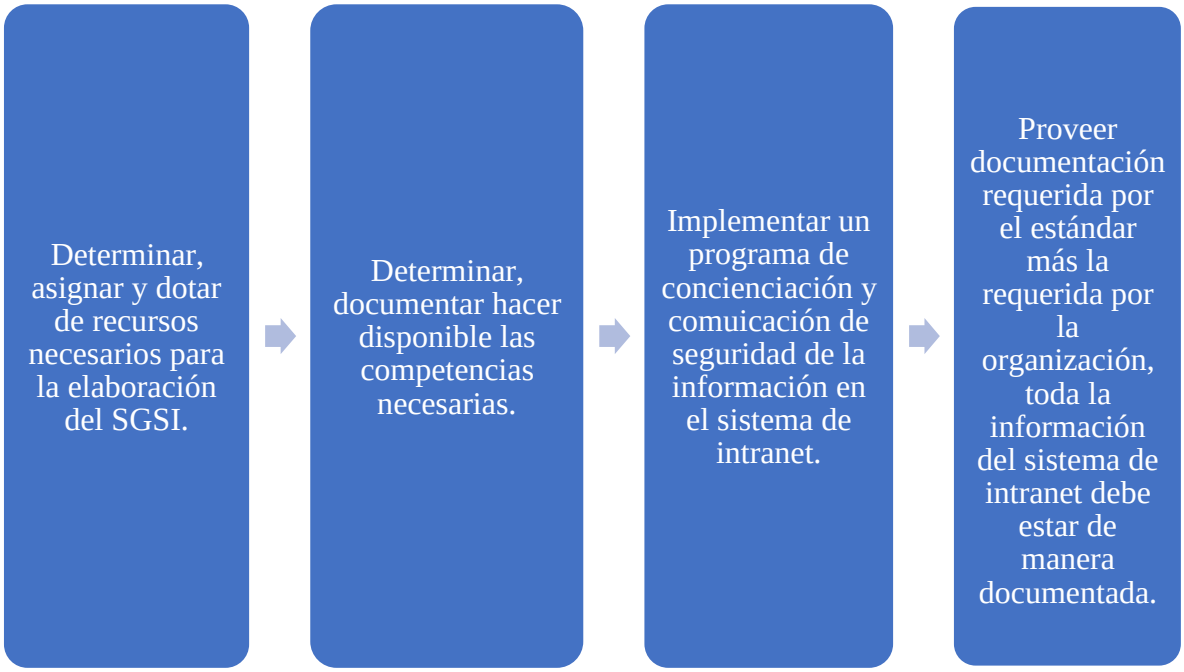



Ilustración 12 Clausula Apoyo y Soporte

**Responsable:**

Jefe de desarrollo de sistema y director de TI.

## OPERACIÓN

**Objetivo:**

La ejecución en práctica de esta cláusula, es gestionar los riesgos, determinar la apreciación de aquellos riesgos y realizar un tratamiento de riesgos para darle soluciona los mismos, en conformidad a la ilustración 13.


Ilustración 13 Clausula Operación

**Instrumento para la Gestión de Riesgos:**

Para la gestión de los riesgos se debe tomar en cuenta, la identificación de los riesgos, determinar la causa, evaluar el riesgo (impacto y probabilidad), y determinación de la consecuencia, a continuación, se presenta conforme a la ilustración.

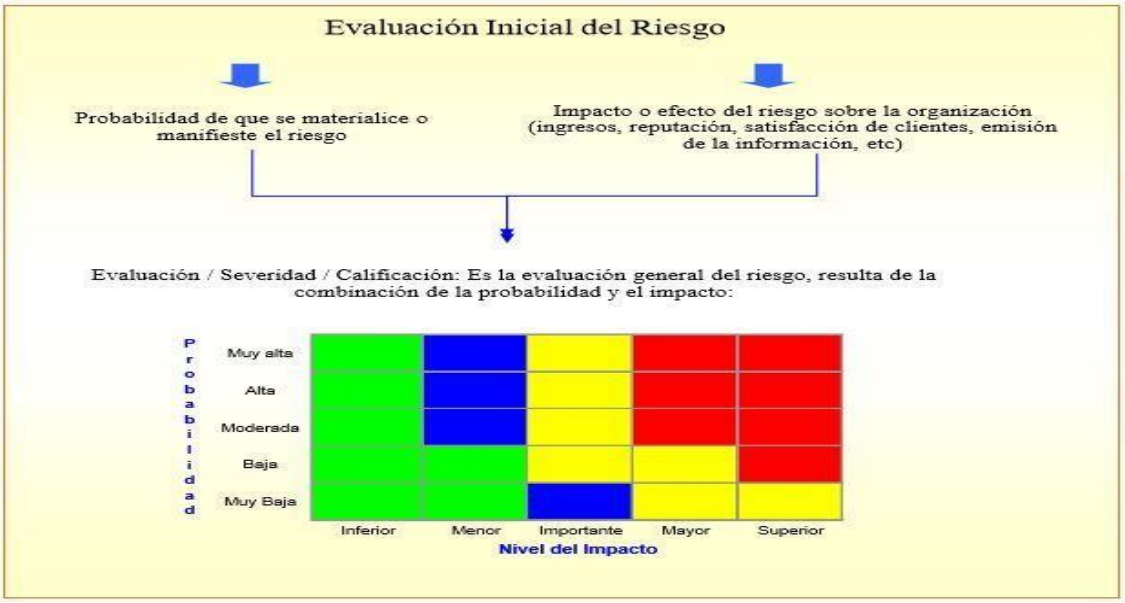



Ilustración 14 Gestión de Riesgo

Existirá un resultado de la obtención de la probabilidad de que se materialice e impacto del riesgo, conforme a la tabla.

| | |
|---|---|
| **Alto** | **Moderado** |
| **Extremo** | **Bajo** |

Ilustración 15 Resultado de la Evaluación de Riesgo **Responsable:**

Jefe de desarrollo de sistemas y los dueños de los procesos**.**

**Resultado de Evaluación de Riesgos**

A continuación, se especificará cada uno de los riesgos, con su respectivo activo, nombre, amenaza y vulnerabilidad:

**Riesgo 1 →** (Alto)
**Activo 001:** Data center Liebert.

| | | | |
|---|---|---|---|
| **AM001** | Terremoto | **V001** | Susceptible a desastres naturales |

**Riesgo 17 →** (Alto)
**Activo 006**: Sensores de Calor.

| | | | |
|---|---|---|---|
| **AM017** | Falla de sensor | **V017** | Uso de equipamiento obsoleto |

**Riesgo 34 →** (Alto) **Activo 012**: UPS.

| | | | |
|---|---|---|---|
| **AM034** | Robo | **V034** | Equipamiento móvil proclive para robar |

**Riesgo 46 →** (Extremo)
**Activo 017:** Mikrotik

| | | | |
|---|---|---|---|
| **AM046** | Falla de equipos | **V046** | Uso de equipamiento obsoleto |

**Riesgo 54 →** (Alto)
**Activo 021:** Copia del respaldo data center.

| | | | |
|---|---|---|---|
| **AM054** | Intercepción de Información | **V054** | Falta de control en datos de entrada y salidas |

**Riesgo 60 →** (Alto)
**Activo 024:** Respaldo de Máquina Virtual Centos 7.

| | | | |
|---|---|---|---|
| **AM060** | Código | **V060** | Protección desactualizada contra códigos |

Malicioso malicioso

→ (Alto)

**Riesgo 62**
**Activo 026:** Respaldo de Máquina Virtual Elastix.

| | | | |
|---|---|---|---|
| **AM062** | Destrucción de registros | **V062** | Inadecuada gestión de redes |

**Riesgo 63** → (Alto)
**Activo 026:** Respaldo de Máquina Virtual Elastix.

| | | | |
|---|---|---|---|
| **AM063** | Interceptación de información | **V063** | Ubicación susceptible a perdidas |

**Riesgo 64** → (Alto)
**Activo 027**: Respaldo de Máquina Virtual Ipcop-Proxy.

| | | | |
|---|---|---|---|
| **AM064** | Errores de aplicaciones | **V064** | Inadecuada capacitación |

**Riesgo 65** → (Alto)
**Activo 028:** Respaldo de Máquina Virtual Windows 7 Cloud.

| | | | |
|---|---|---|---|
| **AM065** | Interceptación de información | **V065** | Mantenimiento inadecuado |

**Riesgo 67** → (Alto)
**Activo 030:** Respaldo de Máquina Virtual Cabildo-Principal.

| | | | |
|---|---|---|---|
| **AM067** | Interceptación de información | **V067** | Ubicación susceptible a perdidas |

**Riesgo 71** → (Alto)
**Activo 034**: Respaldo de Máquina Virtual Server-antivirus.

| | | | |
|---|---|---|---|
| **AM071** | Interceptación de información | **V071** | Ubicación susceptible a perdidas |

**Riesgo 74** → (MEDIO)
**Activo 037:** Respaldo de Máquina Virtual SIGCES.

| | | | |
|---|---|---|---|
| **AM074** | Fuga o revelación de información | **V074** | Solo una copia de la información |

**Riesgo 76** → (Extremo)
**Activo 041:** Ordenador personal Jefe de TI.

| | | | |
|---|---|---|---|
| **AM076** | Contagio de | **V076** | Falta de antivirus con |

→ (Alto)

virus licencia

**Riesgo 77** → (Extremo)
**Activo 042:** Ordenador personal Jefe de Infraestructura.

| | | | |
|---|---|---|---|
| **AM077** | Falsificación de registros | **V077** | Inadecuados derechos de usuario |

**Riesgo 78**
**Activo 042:** Ordenador personal Jefe de Infraestructura.

| | | | |
|---|---|---|---|
| **AM078** | Contagio de virus | **V078** | Falta de antivirus con licencia |

**Riesgo 79** → (Extremo)
**Activo 042:** Ordenador personal Jefe de Infraestructura.

| | | | |
|---|---|---|---|
| **AM079** | Sustracción de información | **V079** | Puertos USB habilitados |

**Riesgo 82** → (Alto)
**Activo 044:** Ordenador personal de mantenimiento.

| | | | |
|---|---|---|---|
| **AM082** | Contagio de virus | **V082** | Falta de antivirus con licencia |

**Riesgo 83** → (Alto)
**Activo 044:** Ordenador personal de mantenimiento.

| | | | |
|---|---|---|---|
| **AM082** | Contagio de virus | **V082** | Falta de antivirus con licencia |

**Riesgo 85** → (Alto)
**Activo 045:** Respaldo de Base de Datos.

| | | | |
|---|---|---|---|
| **AM085** | Contagio de virus | **V085** | Falta de antivirus con licencia |

**Riesgo 87** → (Alto)
**Activo 047:** Ordenador Portátil Toshiba.

Sustracción de Puertos USB

→ (Alto)

| | | | |
|---|---|---|---|
| **AM087** | información | **V087** | habilitados |

**Riesgo 88** → (Extremo)
**Activo 047:** Ordenador Portátil Toshiba.

| | | | |
|---|---|---|---|
| **AM088** | Modificación accidental de datos del sistema de información | **V088** | Sesiones activas después del horario laboral |

**Riesgo 89** → (Extremo) **Activo 048:** Ordenador Aditk.

| | | | |
|---|---|---|---|
| **AM089** | Daños provocados por actividades de tercero | **V089** | Eliminación de Registros y datos de funcionamiento de la información |

**Riesgo 91** → (Extremo)
**Activo 050:** Sistema de Contabilidad Olimpo.

| | | | |
|---|---|---|---|
| **AM091** | Robo | **V091** | Inadecuada gestión del empleador |

**Riesgo 92**
**Activo 051:** Sistema de Automatización de Temperatura.

| | | | |
|---|---|---|---|
| **AM092** | Modificación accidental de datos del sistema de información | **V092** | Sesiones activas después del horario laboral |

**Riesgo 95** → (Alto)
**Activo 054:** Red de Datos.

| | | | |
|---|---|---|---|
| **AM095** | Fuga o revelación de información | **V095** | Falta de control en datos de entrada y salida |

**Riesgo 96** → (Alto)
**Activo 055:** Diccionario de Datos.

| | | | |
|---|---|---|---|
| **AM096** | Fuga o revelación de información | **V096** | Falta de control en datos de entrada y salida |

**Riesgo 99** → (Alto)
**Activo 058:** Código Fuente Sistema de Intranet.

| | | | |
|---|---|---|---|
| | Mala utilización de la | | Mala redacción del |

→ (Alto)

| | | | |
|---|---|---|---|
| **AM099** aplicación | | **V099** | manual |

**Riesgo 100** → (Extremo)
**Activo 058:** Código Fuente Sistema de Intranet.

| | | | |
|---|---|---|---|
| **AM100** Plagio | | **V100** | Falta de control de desarrollo |

**Riesgo 101** → (Alto)
**Activo 059:** Información Respaldada.

| | | | |
|---|---|---|---|
| **AM101** | Perdida de servicios | **V101** | Solo una copia de la información |

## EVALUACIÓN DEL DESEMPEÑO

**Objetivo:**

Ya establecido el SGSI, se debe verificar que todas las normas establecidas en él, estén acorde a lo que dice el estándar, con revisión periódicas y sujetas a cambios si en esta existe alguna anomalía**.**

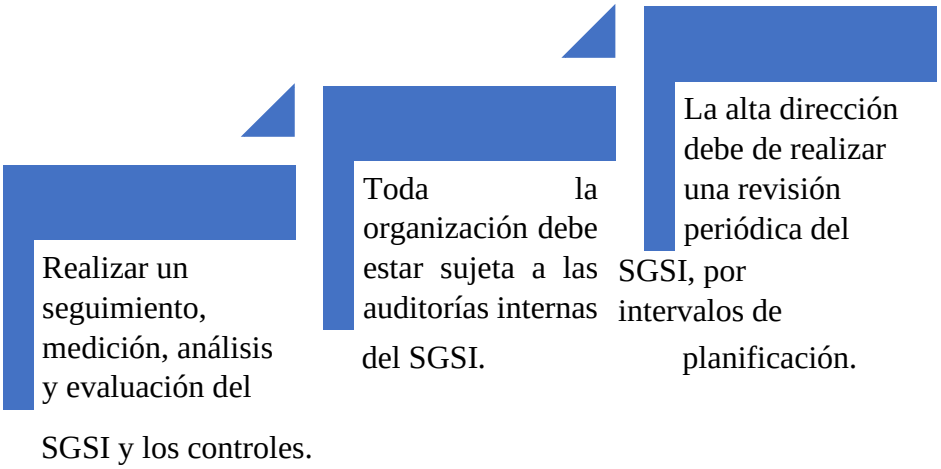



Ilustración 16 Clausula Evaluación de Desempeño

**Controles:**

Para realizar los controles hay que tener bien en claro, cuales son y cómo se deben abordar en el momento de su utilización, en la cual la presentamos en la tabla 16**.**

Tabla 16 Controles[10]

| **Dominios** |
|---|
| **A.5** Política de seguridad de la información. |
| **A.6** Organización de la seguridad de la información. |
| **A.7** Seguridad de los recursos humanos. |
| **A.8** Gestión de los activos. |
| **A.9** Control de Acceso |
| **A.10** Criptografía |
| **A.11** Seguridad física y ambiental. |
| **A.12** Seguridad de las operaciones. |
| **A.13** Seguridad de las comunicaciones. |
| **A.14** Adquisición, desarrollo y mantenimiento del sistema. |
| **A.15** Relación con proveedores. |
| **A.16** Gestión de incidentes de seguridad de la información. **A.17** Gestión de los aspectos de la seguridad |

de la información para la continuidad del negocio. **A.18** Cumplimiento.

Se necesita especificar algunas métricas, las cuales están en coordinación con los controles y los requerimientos de las clausulas, en donde la proporción será de 0% a 100%, como lo explica la tabla 17. Según lo investigado, todas las métricas se encuentran en 0% ya que la organización no ha implementado ninguna.

Tabla 17 Métricas de Controles[10]

| Estado | Significado | Proporción de requerimientos del SGSI | Proporción de controles se seguridad de la información |
|---|---|---|---|
| Desconocido | No ha sido verificado. | 0% - 100% | 0% - 100% |
| Inexistente | No se lleva a cabo el control de seguridad en los sistemas de información. | 0% - 100% | 0% - 100% |
| Inicial | Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad. | 0% - 100% | 0% - 100% |
| Repetible | La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación. | 0% - 100% | 0% - 100% |

| | | | |
|---|---|---|---|
| Definido | El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección. | 0% - 100% | 0% - 100% |
| Administrado | El control se lleva a cabo de acuerdo a un procedimiento documentado, | 0% - 100% | 0% - 100% |
| | aprobado y formalizado. | | |
| Optimizado | El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores. | 0% - 100% | 0% - 100% |
| No Aplicable | A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración. | 0% - 100% | 0% - 100% |
| | **Total** | **0% - 100%** | **0% - 100%** |

También para verificar la tendencia de los controles y requerimientos de cláusulas a aplicar, como ejemplo se mostrarán un gráfico; como conformidad a la ilustración 16 y 17.


Ilustración 17 Ejemplo de Estado Clausulas

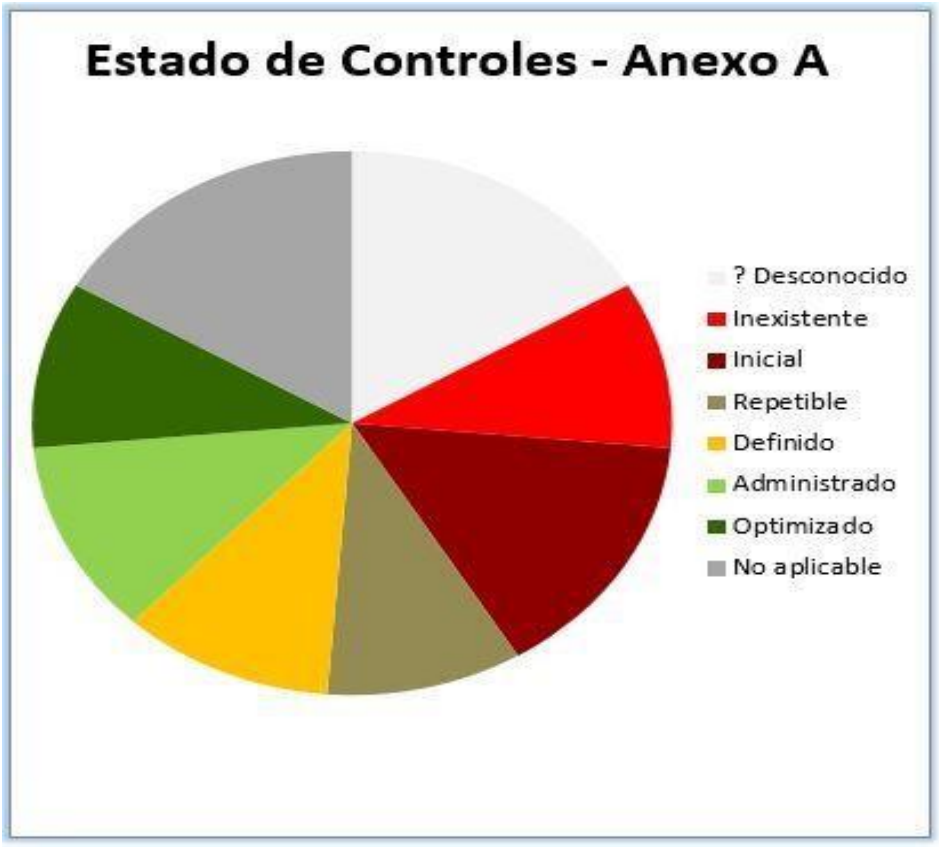



Ilustración 18 Ejemplo de Estado Controles

## Selecciones de controles y objetivos de control

Verificar que controles según la ISO 27001, son aplicables para la seguridad de la información, conforme a la tabla 18 se especifica cada uno de los controles con su objetivo y establecimiento de aplicabilidad y no aplicabilidad.

Tabla 18 Controles Según ISO 27001[10].

| | | |
|---|---|---|
| **A.5 Planteamiento de Políticas** | | |
| **A.5.1 Verificar directrices de gestión de políticas de la información** | | |
| **Objetivo:** El sistema de intranet tendrá la orientación y apoyo a la gestión de seguridad de la información en concordancia con las normativas, leyes y requisitos que debe tener la organización. | | |
| A.5.1.1 | Políticas para la seguridad de la información | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable**. |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| **A.6 Organización de la seguridad de la información** | | |
| **A.6.1 Organización Interna** | | |
| **Objetivo:** La organización debe contener un marco de gestión, para tener muy bien establecido, implementado y operado la seguridad de la información dentro del sistema de intranet. | | |
| A.6.1.1 | Roles y responsabilidades en seguridad de la información | **Control**<br><br>No es aplicable |
| A.6.1.2 | Segregación de tareas | **Control**<br><br>No es aplicable |
| A.6.1.3 | Contacto en las autoridades | **Control**<br><br>No es aplicable. |
| A.6.1.4 | Contacto con grupos de interés especial | **Control**<br><br>No es aplicable. |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | **Control**<br>No es aplicable. |
| **A.6.2 Los dispositivos móviles y el teletrabajo** | | |
| **Objetivo:** El teletrabajo es muy importante ya que ocupa cualquier eventualidad que tenga uno de los encargados del sistema y poder desde el lugar donde se encuentra cubrir alguna falencia en el sistema de intranet, mediante la utilización de dispositivo móviles. | | |

| | | |
|---|---|---|
| A.6.2.1 | Contacto con las autoridades | **Control**<br><br>No es aplicable |
| A.6.2.2 | Teletrabajo | **Control**<br><br>No es aplicable |

| | | |
|---|---|---|
| **A.7 Seguridad relativa de los recursos humanos** | | |
| **A.7.1 Antes del empleo** | | |
| **Objetivo:** Cada uno de los encargados de los procesos, deben tener muy claro su responsabilidad y adecuarlas para necesidades que se los requiera. | | |
| A.7.1.1 | Investigación de antecedentes | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| A.7.1.2 | Términos y condiciones de empleo | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| **A.7.2 Durante el empleo** | | |
| **Objetivo:** Cada uno de los encargados de los procesos, deben conocer y cumplir su responsabilidad en cuanto a la seguridad de la información. | | |
| A.7.2.1 | Responsabilidades de gestión | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| A.7.2.2 | Concienciación, educación y capacitación en seguridad de la información | **Control**<br><br>Este control se deberá establecer para todos los activos, **R79,** por lo tanto, **es aplicable.** |
| A.7.2.3 | Proceso disciplinario | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| **A.7.3 Finalización del empleo o cambio de trabajo** | | |
| **Objetivo:** Tener la claridad de los intereses institucionales, en el proceso de cambio del empleo. | | |

| | | |
|---|---|---|
| A.7.3.1 | Responsabilidades ante la finalización o cambio | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| **A.8 Gestión de activos** | | |
| **A.8.1 Responsabilidad sobre los activos** | | |
| **Objetivo:** La utilización de los activos en el sistema de intranet ayuda a la organización y definición de responsabilidades de protección pertinente. | | |
| A.8.1.1 | Inventario de los activos | **Control**<br><br>**Aplicable** para el riesgo R83, R84 |
| A.8.1.2 | Propiedad de los activos | **Control** |

| | | |
|---|---|---|
| | | Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| A.8.1.3 | Uso aceptable de los activos | **Control**<br><br>No es aplicable. |
| A.8.1.4 | Devolución de activos | **Control**<br><br>No es aplicable**.** |
| **A.8.2 Clasificación de la información** | | |
| **Objetivo:** La información dentro del sistema de intranet debe de estar en una adecuada protección en concordancia a la importancia de la institución**.** | | |
| A.8.2.1 | Clasificación de la información | **Control**<br><br>No es aplicable**.** |
| A.8.2.2 | Etiquetado de la información | **Control**<br><br>No es aplicable**.** |
| A.8.2.3 | Manipulado de la información | **Control**<br><br>No es aplicable**.** |
| **A.8.3 Manipulación de los soportes** | | |
| **Objetivo:** Se tendrá que salvaguardar la seguridad de los soportes, en donde no exista su revelación, modificación, eliminación de no autorización. | | |
| A.8.3.1 | Gestión de soportes extraíbles | **Control**<br><br>**Aplicable** para el activo **A014** y **A009** |

| | | |
|---|---|---|
| A.8.3.2 | Eliminación de soportes | **Control**<br><br>No es aplicable**.** |
| A.8.3.3 | Soportes físicos en transito | **Control**<br><br>No es aplicable**.** |
| **A.9 Controlar la autenticación** | | |
| **A.9.1 Controlar los accesos en conjunto con los requisitos** | | |
| **Objetivo:** Se debe tener un límite establecido para los recursos de tratamiento de la información. | | |
| A.9.1.1 | Política de control de acceso | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de administración de redes, por lo tanto, **es aplicable. A022** |
| A.9.1.2 | Servicios en la infraestructura de redes | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de administración de redes, por lo tanto, **es aplicable. A022** |
| **A.9.2 Gestión de acceso de usuario** | | |

| | | |
|---|---|---|
| **Objetivo:** La autorización a los accesos de usuarios, solo debe ser para los autorizados y evitar el acceso a los no autorizados en el sistema de intranet y sus servicios. | | |
| A.9.2.1 | Registro y baja de usuario | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable. A023, A046, A051** |
| A.9.2.2 | Provisión de acceso de usuario | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.9.2.3 | Gestión de privilegios de acceso | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable. A023, A046, A051** |

| | | |
|---|---|---|
| A.9.2.4 | Gestión de la información secreta de autenticación de los usuarios | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.9.2.5 | Revisión de los derechos de acceso de usuario | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable. A023, A046, A051** |
| A.9.2.6 | Retirada o reasignación de los derechos de acceso | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| **A.9.3 Responsabilidades del usuario** | | |
| **Objetivo:** Es muy importante para que los usuarios tengas responsabilidad de salvaguardar su información de autenticación**.** | | |
| A.9.3.1 | Uso de la información secreta de autenticación | **Control**<br><br>No es aplicable**.** |
| **A.9.4 Control de acceso a sistemas y aplicaciones** | | |
| **Objetivo:** Prevención a los accesos no autorizados del sistema de intranet y sus aplicaciones. | | |
| A.9.4.1 | Retracción del acceso a la información | **Control**<br><br>Aplicable para el **R79, R88, R89, R91**. |
| A.9.4.2 | Procedimientos seguros de inicio de sesión | **Control**<br><br>**Aplicable** para el activo **A022.** |
| A.9.4.3 | Sistema de gestión de contraseñas | **Control** |

| | | |
|---|---|---|
| | | Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.9.4.4 | Uso de utilidades con privilegios del sistema | **Control** |
| A.9.4.5 | Control de acceso al código fuente de los programas | **Control**<br><br>No es aplicable**.** |
| **A.10 Criptografía** | | |
| **A.10.1 Controles criptográficos** | | |

| | | |
|---|---|---|
| **Objetivo:** Tener la garantía absoluta en el sistema de intranet, en el momento de autenticación de la criptografía para su protección de confidencialidad e integridad de la información. | | |
| A.10.1.1 | Política de uso de los controles criptográficos | **Control**<br><br>Este control se deberá establecer para todos los activos con proceso de sistemas informáticos de autenticación, **R91**, por lo tanto, **es aplicable.** |
| A.10.1.2 | Gestión de claves | **Control**<br><br>Este control se deberá establecer para todos los activos con proceso de sistemas informáticos de autenticación, por lo tanto, **es aplicable.** |
| **A.11 Seguridad física y del entorno** | | |
| **A.11.1 Áreas seguras** | | |
| **Objetivo:** Prevención del acceso físico no autorizado, en daños que puede ocurrir a la información y recursos de tratamiento de la información. | | |
| A.11.1.1 | Perímetro de seguridad física | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de infraestructura, por lo tanto, **es aplicable.** |
| A.11.1.2 | Controles físicos de entrada | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de infraestructura, el **R46**, por lo tanto, **es aplicable.** |
| A.11.1.3 | Seguridad de oficinas, despachos y recursos | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de infraestructura, por lo tanto, **es aplicable.** |

| | | |
|---|---|---|
| A.11.1.4 | Protección contra las amenazas externas y ambientales | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de infraestructura, por lo tanto, **es aplicable.** |

| | | |
|---|---|---|
| A.11.1.5 | El trabajo en áreas seguras | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de infraestructura, por lo tanto, **es aplicable.** |
| A.11.1.6 | Áreas de carga y descarga | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de infraestructura, por lo tanto, **es aplicable.** |
| **A.11.2 Seguridad de los equipos** | | |
| **Objetivo:** Se debe evitar la pérdida, daño, robo dentro de los activos que posee el sistema de intranet e interrupciones de las operaciones. | | |
| A.11.2.1 | Emplazamiento y protección de equipos | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.2 | Instalaciones de suministro | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.3 | Seguridad del cableado | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico y redes, por lo tanto, **es aplicable.** |
| A.11.2.4 | Mantenimiento de los equipos | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.5 | Retirada de materiales propiedad de la empresa | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.6 | Seguridad de los equipos fuera de las instalaciones | **Control** |

| | | |
|---|---|---|
| | | Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.7 | Reutilización o eliminación segura de equipos | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.8 | Equipo de usuario desatendido | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.11.2.9 | Política de puesto de trabajo despejado y pantalla limpia | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| **A.12 Seguridad de las operaciones** | | |
| **A.12.1 Procedimientos y responsabilidades operacionales** | | |
| **Objetivo:** Las instalaciones de tratamiento de la información dentro del sistema de intranet, deben en un correcto funcionamiento. | | |
| A.12.1.1 | Documentación de procedimientos operacionales | **Control**<br><br>No es aplicable. |
| A.12.1.2 | Gestión de cambios | **Control**<br><br>No es aplicable. |
| A.12.1.3 | Gestión de capacidades | **Control**<br><br>No es aplicable. |
| A.12.1.4 | Separación de los recursos de desarrollo, prueba y operación | **Control**<br><br>No es aplicable. |
| **A.12.2 Protección contra el software malicioso (malware)** | | |
| **Objetivo:** Tener la plena seguridad de que los recursos de tratamiento de información deben estar protegidos contra el malware. | | |
| A.12.2.1 | Controles contra el código malicioso | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, **R76**, por lo tanto, **es aplicable.** |
| **A.12.3 Copias de seguridad** | | |

| | | |
|---|---|---|
| **Objetivo:** Tener las copias de seguridad de toda la información y código para evitar pérdidas. | | |
| A.12.3.1 | Copiad de seguridad de la información | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte |

| | | |
|---|---|---|
| | | técnico y **R100**, por lo tanto, **es aplicable.** |
| **A.12.4 Registros de supervisión** | | |
| **Objetivo:** Tener las evidencias de los eventos. | | |
| A.12.4.1 | Registro de eventos | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| A.12.4.2 | Protección de la información del registro | **Control**<br><br>**Aplicable** para el activo **A022, R77.** |
| A.12.4.3 | Registros de administración y operación | **Control**<br><br>No es aplicable. |
| A.12.4.4 | Sincronización del reloj | **Control**<br><br>No es aplicable. |
| **A.12.5 Control del software en explotación** | | |
| **Objetivo:** Tener la seguridad de la integridad del sistema de intranet en explotación. | | |
| A.12.5.1 | Instalación del software en explotación | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| **A.12.6 Gestión de la vulnerabilidad técnica** | | |
| **Objetivo:** Reducción de los riesgos en la explotación de las vulnerabilidades técnicas**.** | | |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |

| | | |
|---|---|---|
| A.12.6.2 | Restricción en la instalación de software | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| **A.12.7 Consideraciones sobre auditorias** | | |
| **Objetivo:** Asegurar que las auditorias en los sistemas operativos se encuentren estables, teniendo la actualización y activación en cada uno de los departamentos de la organización**.** | | |
| A.12.7.1 | Controles de auditoria de sistemas de información | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de soporte técnico, por lo tanto, **es aplicable.** |
| **A.13 Administración de comunicaciones** | | |
| **A.13.1 Aseguramiento de buena gestión de las redes** | | |
| **Objetivo:** La administración de redes de la organización debe asegurarse la protección de la información y los recursos de tratamiento de la información**.** | | |

| | | |
|---|---|---|
| A.13.1.1 | Controles de red | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de redes, por lo tanto, **es aplicable.** |
| A.13.1.2 | Seguridad de los servicios de red | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de redes, por lo tanto, **es aplicable.** |
| A.13.1.3 | Segregación en redes | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de redes, por lo tanto, **es aplicable.** |
| **A.13.2 Intercambio de información** | | |
| **Objetivo:** Asegurar que los limites en transferir información mantenga seguridad. | | |
| A.13.2.1 | Políticas y procedimientos de intercambio de información | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |

| | | |
|---|---|---|
| A.13.2.2 | Acuerdos de intercambio de información | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| A.13.2.3 | Mensajería electrónica | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| A.13.2.4 | Acuerdos de confidencialidad o no revelación | **Control**<br><br>Este control se deberá establecer para todos los activos, por lo tanto, **es aplicable.** |
| **A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información**[10] | | |
| **A.14.1 Requisitos de seguridad en los sistemas de información**[10] | | |
| **Objetivo:** Asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida, de igual manera proporcionar requisitos para los sistemas de información a los servicios a través de redes públicas[10]. | | |
| A.14.1.1 | Análisis de requisitos y especificaciones de seguridad de la información | **Control**<br><br>No es aplicable. |
| A.14.1.2 | Asegurar los servicios de aplicaciones en redes publicas | **Control** |

| | | |
|---|---|---|
| | | Este control se deberá establecer para todos los activos del proceso de redes, por lo tanto, **es aplicable.** |
| A.14.1.3 | Protección de las transacciones de servicios de aplicaciones | **Control**<br><br>No es aplicable. |
| **A.14.2 Seguridad en el desarrollo y en los procesos de soporte** | | |
| **Objetivo:** Tener la garantía que se haya diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información, la seguridad de la información**.** | | |
| A.14.2.1 | Política de desarrollo seguro | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |

| | | |
|---|---|---|
| A.14.2.2 | Procedimiento de control de cambios en sistemas | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| A.14.2.3 | Cambios en el sistema operativo de forma técnica | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| A.14.2.4 | Restricciones a los cambios en los paquetes de software | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| A.14.2.5 | Principios de ingeniería de sistemas seguros | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| A.14.2.6 | Entorno de desarrollo seguro | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| A.14.2.7 | Externalización del desarrollo de software | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de |

| | | |
|---|---|---|
| | | desarrollo de software, por lo tanto, **es aplicable.** |
| A.14.2.8 | Pruebas funcionales de seguridad de sistemas | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |

| | | |
|---|---|---|
| A.14.2.9 | Pruebas de aceptación de sistemas | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| **A.14.3 Datos de prueba** | | |
| **Objetivo:** Asegurar la protección de los datos de prueba. | | |
| A.14.3.1 | Protección de los datos de prueba | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de software, por lo tanto, **es aplicable.** |
| **A.15 Relación con proveedores** | | |
| **A.15.1 Aseguramiento de una buena seguridad con los proveedores** | | |
| **Objetivo:** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores[10]**.** | | |
| A.15.1.1 | Relaciones con los proveedores | **Control**<br><br>No es aplicable**.** |
| A.15.1.2 | Requisitos de seguridad en contratos con terceros | **Control**<br><br>No es aplicable**.** |
| A.15.1.3 | Cadena de suministro de tecnología de la información y de las comunicaciones | **Control**<br><br>No es aplicable. |
| **A.15.2 Gestión de la provisión de servicios del proveedor** | | |
| **Objetivo:** Mantener un nivel acordado de seguridad y de provisión de servicios en línea**.** | | |
| A.15.2.1 | Prohibición de interferencias en los servicios a proveedores | **Control**<br><br>No es aplicable**.** |
| A.15.2.2 | Gestión de cambios en la provisión del servicio del proveedor | **Control**<br><br>No es aplicable**.** |
| **A.16 Gestión de incidentes de seguridad de la información**[10] | | |
| **A.16.1 Gestión de incidentes de seguridad de la información y mejoras**[10] | | |
| **Objetivo:** El sistema de intranet deberá de tener un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información y de igual manera la comunicación de eventos de seguridad y debilidades[10]**.** | | |
| A.16.1.1 | Responsabilidades y procedimientos | **Control** |

| | | |
|---|---|---|
| | | **Aplicable** para los activos **A002, A021, A041, A042, A043, A045 y** riesgos **R88, R89, R91.** |
| A.16.1.2 | Notificación de los eventos de seguridad de información | **Control**<br><br>No es aplicable**.** |
| A.16.1.3 | Notificación de puntos débiles de seguridad | **Control**<br><br>**Aplicable** para los activos **A002, A021, A041, A042, A043, A045.** |
| A.16.1.4 | Evaluación y decisión sobre los eventos de seguridad de información | **Control**<br><br>No es aplicable**.** |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | **Control**<br><br>**Aplicable** para los activos **A002, A021, A041, A042, A043, A045.** |
| A.16.1.6 | Aprendizaje de los incidentes de seguridad de la información | **Control**<br><br>Este control se deberá aplicar para todos los activos que intervienen en el sistema de intranet, por lo tanto, **es aplicable.** |
| A.16.1.7 | Recopilación de evidencias. | **Control**<br><br>No es aplicable**.** |
| **A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio**[10] | | |
| **A.17.1 Continuidad de la seguridad de la información**[10] | | |
| **Objetivo**: Dentro de los sistemas de gestión de continuidad, la seguridad de la información debe formar parte ideal de la organización[10]. | | |
| A.17.1.1 | La seguridad de la información sujeto a mejoras | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de la infraestructura de la organización, por lo tanto, **es aplicable.** |
| A.17.1.2 | Implementación de la seguridad de la información sujeto a mejoras | **Control**<br><br>No es aplicable. |
| A.17.1.3 | Verificación, revisión y evaluación de la seguridad de la información sujeta a mejoras | **Control**<br><br>No es aplicable. |
| **A.17.2 Redundancias** | | |
| **Objetivo:** Asegurar la disponibilidad de los recursos de tratamiento de la información**.** | | |

| | | |
|---|---|---|
| A.17.2.1 | Disponibilidad de los recursos de tratamiento de información | **Control**<br><br>No es aplicable. |
| **A.18 Cumplimiento** | | |
| **A.18.1 Cumplimiento de los requisitos legales y contractuales** | | |

| | | |
|---|---|---|
| **Objetivo:** La documentación necesaria debe estar al día, no evitar las obligaciones legales, estatutarias, reglamentarias o contractuales relativas de la seguridad de la información[10]**.** | | |
| A.18.1.1 | Normas de leyes aplicables y de contratos | **Control**<br><br>Este control se deberá aplicar para todo el sistema intranet, ya que posee un objetivo de tener los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales de forma explícita, documentada y actualizada para cada sistema de información de la prefectura, por lo tanto, **es aplicable**. |
| A.18.1.2 | Derechos de Propiedad Intelectual (DPI) | **Control**<br><br>**No es aplicable,** ya que la organización si lo posee**.** |
| A.18.1.3 | Protección de los registros de la organización | **Control**<br><br>**No es aplicable,** ya que la organización si lo posee**.** |
| A.18.1.4 | Protección y privacidad de la información de carácter personal | **Control**<br><br>**No es aplicable,** ya que la organización si lo posee**.** |
| A.18.1.5 | Regulación de los controles criptográficos | **Control**<br><br>Este control se deberá establecer para todos los activos del proceso de desarrollo de sistemas, por lo tanto, **es aplicable.** |
| **A.18.2 Revisiones del SGSI** | | |
| **Objetivo:** Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización[10]**.** | | |

| | | |
|---|---|---|
| A.18.2.1 | Revisión independiente de la seguridad de la información | **Control**<br><br>Este control se deberá aplicar para todo el sistema de intranet, ya que se podrá tener los objetivos de control, control de políticas, políticas y procedimientos para la seguridad de la información de la ISO 27001, por lo tanto**, es aplicable.** |
| A.18.2.2 | Cumplimiento de las políticas y normas de seguridad | **Control**<br><br>**No es aplicable,** ya que la organización si lo posee**.** |
| A.18.2.3 | Comprobación del cumplimiento técnico | **Control** |
| | | Este control se deberá establecer para todos los activos del proceso soporte técnico, por lo tanto, **es aplicable.** |

**Responsable:**

Jefe de desarrollo de sistema y director del área de TI.

## MEJORA

**Objetivo:**

Realizar la mejora continua al SGSI, para que en este no exista no conformidades por medio de los auditores internos**.**

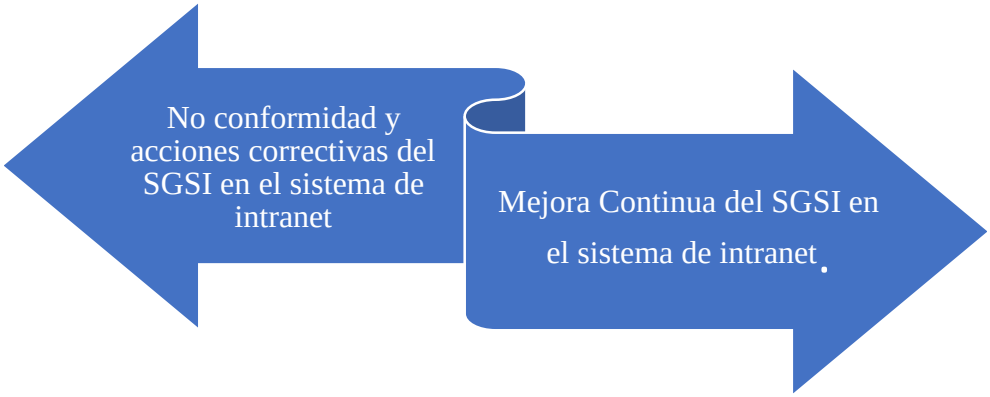



Ilustración 19 Clausula Mejora Continua

**Responsable:**

Todo el personal del área de TI**.**

# CAPÍTULO V: CONCLUSIONES

- Los objetivos delimitados en esta investigación se cumplieron en su totalidad, diseñando un plan de seguridad de la información para el sistema de intranet de la prefectura de esmeraldas, mediante la ISO 27001 que nos brinda una serie de requisitos para su perfecta elaboración**.**

- Se estudió la situación actual del sistema de intranet, verificando cada uno de los activos que se encuentran involucrados, evidenciando sus falencias y determinando los niveles de riesgos, abordando soluciones para minimizar los mismos**.**

- Debido a que existe una serie de amenazas y vulnerabilidades, provocando riesgos altos al momento de efectuar el procesamiento de información en sistemas de intranet, se utilizó herramientas tales como matrices inherentes capaces de minimizar los mismos, contribuyendo de manera significativa en la protección de los activos**.**

- Se desarrolló un plan de tratamiento de riesgo conforme a lo que establece la norma de la ISO 27001, permitiendo colocar cada una de sus cláusulas con métricas y herramientas a utilizar para su perfecta implementación, más sin embargo dando la posibilidad de que otras investigaciones la utilicen**.**

# CAPÍTULO VI: RECOMENDACIONES

- Tomar en consideración que la presente investigación servirá de manera significativa para que la prefectura de esmeraldas pueda tomar decisiones acertadas en cuanto al tema en mención, debido a la elaboración de un plan de seguridad de información.

- Dentro del departamento deben de tener liderazgo al momento de ejecutar las cláusulas de la norma ISO 27001, el compromiso debe ser totalmente efectivo comunicando los roles y responsabilidades de seguridad de la información.

- Todo el personal interno debe tener conocimiento de la ISO 27001, ya que esto ayuda a minimizar los riesgos y gastos al momento de realizar auditorías externas.

- Aplicar la norma ISO 27001, estableciendo cada una de sus cláusulas, los objetivos de control, contar con dos los documentos necesarios que establece el estándar, tener las políticas de seguridad bien establecidas, con cada uno de los controles necesarios si llegase a ocurrir alguna eventualidad de fuga de información.

## REFERENCIA


[1] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *J. Inf. Secur.*, vol. 04, no. 02, pp. 92–100, 2013.

[2] R. Posso, “Desarrollo De Políticas De Seguridad Informática E Implementación De Tres Dominios En Base a La Norma 27002 Para El Área De Hardware En La Empresa Uniplex Systems S.a. En Quito,” 2009.

[3] “Ecuador - Tesis - Análisis y diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa YOUPHONE Cía. Ltda. Utilizando Hacking Ético,” 2016.

[4] J. G. Cervantes, “Vulnerabilidades de Seguridad en las Empresas,” *Celerinet*, 2013.

[5] Ó. Navarro Carrasco and A. Villalón Puerta, “Una visión global de la ciberseguridad de los sistemas de control,” *106*, pp. 53–55, 2013.

[6] G. Pallas, “Metodología de Implantacion de un SGSI en un grupo empresarial jerárquico,” p. 186, 2009.

[7] G. Pallas and M. Corti, “Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica,” *Fing.Edu.Uy*, p. 186, 2009.

[8] S. G. Gui, “Desarrollo de algunos objetivos de control del SGSI.”

[9] D. C. Allende and S. G. Gui, “Sistema de gestión de la seguridad de la información.”

[10] C. Apítulo and I. A. L. O. S. A. D. E. Riesgos, “Análisis De Riesgos,” pp. 125– 140.

[11] R. Alexander, A. Martínez1, A. Abel, and G. Hernández2, “Plataforma De Gestión De Servicios Telemáticos En Gnu/Linux,” *Rev. Telem@tica*, vol. 11, no. 3, pp. 46–57, 2012.

[12] R. Services, “Planes de continuidad de negocio,” 2016.

[13] J. C. González Cervantes, “Vulnerabilidades de Seguridad en las Empresas,” *Celerinet*, 2013.

[14] Alberto, “Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005,” *Inf. Secur.*, vol. 116, no. 511, pp. 1– 6, 2005.

[15] I. Heras Saizarbitoria, M. Bernardo, and M. Casadesús, “La Integración De Sistemas De Gestión Basados En Estándares Internacionales,” *Rev. Dir. y Adm. Empres. - España*, vol. 14, pp. 155–174, 2007.

[16] J. A. Puente, “Implicaciones De La Integración De Los Sistemas De Gestión De Calidad, Medio Ambiente Y Seguridad Y Salud Laboral Basados En Estándares Internacionales,” p. 241, 2011.

[17] R. J. Martelo, J. E. Maderay, and A. D. Betín, “Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI),” *Inf. Tecnol.*, vol. 26, no. 2, pp. 129–134, 2015.

[18] D. C. Allende and S. G. Gui, “Sistema de gestión de la seguridad de la información.”

[19] S. G. Gui, “Introducción a la seguridad de la información.”

[20] “Informe : Lista de documentación obligatoria requerida por ISO / IEC 27001,” 2014.

[21] V. M. Orrego, “La gestión en la seguridad de la información según Cobit, Itil e Iso 27000,” *Rev. Pensam. Am.*, 2013.

[22] I. S. O. Iec, “Norma ISO/IEC 27001,” 2015.

# ANEXOS

**Anexo 1**

**ENTREVISTA**

Fecha: _____

Nombre del entrevistado/a_____

CC. No _____Edad _____

Sexo_____ Dirección actual _____

Teléfono _____ Formación académica _____

**Preguntas dirigidas al director de TI y programador del sistema de intranet.**
**Objetivo:** Conocimiento pleno de la infraestructura tecnológica y normativas de seguridad del sistema de intranet y descripción del mismo.

**1.-** ¿Considera usted que el sistema de intranet cuanta con la seguridad pertinente para cumplir eficientemente su función?

**2.-** ¿El sistema de intranet cuenta con los controles y cláusulas de la ISO 27001:2013?

**3.-** ¿El programador del sistema de intranet cuenta con conocimiento acerca de las normativas internacionales ISO 27001:2013?

**4.-** ¿Qué tipo de seguridad tiene el sistema de intranet?

**5.-** ¿El sistema de intranet ha sufrido una pérdida de información de gran importancia dentro de la organización?

**6.-** ¿El sistema de intranet ha sufrido algún ataque de algunos hackers maliciosos?

**7.-** ¿Se ha establecido medidas de seguridad dentro del sistema de intranet?

**8.-** ¿Los funcionarios de la organización han recibido alguna capacitación entorno a la perfecta utilización del sistema de intranet?

**9.-** ¿Se han establecido políticas de seguridad en el sistema de intranet?

**Objetivo:** Conocimiento del tipo de información que se maneja dentro del sistema de intranet.

**1.-** ¿Qué tipo de información maneja el sistema de intranet?

**2.-** ¿Dentro del sistema de intranet, que departamentos de la organización no más maneja?

**3.-** ¿L a información que se maneja dentro de la intranet es de manera confidencial?

**4.-** ¿Quiénes son los encargados de visualizar la información confidencial que se maneja dentro de la intranet?

**5.-** ¿El sistema de intranet posee un conjunto de reglas para los funcionarios de la información confidencial que se maneja?

**Objetivo:** Conocimiento de los controles dentro del sistema de intranet**.**

**1.-** ¿Cuáles son las especificaciones técnicas del equipo de TI, que cuenta la dirección para el manejo del sistema de intranet?

**2.-** ¿Con que tiempo y frecuencia se le da mantenimiento y actualización al sistema de intranet?

**3.-** ¿Los activos se encuentran asociados con los procesos, y si así lo es; lo tienen correctamente identificados?

**4.-** ¿Cuáles son los procesos que se maneja dentro del sistema de intranet para el buen cumplimiento de sus funciones?

**5.-** ¿En qué condiciones internas y externas se encuentra el sistema de intranet para la buena utilización del mismo?

6.- ¿Utiliza algún método de encriptación de claves?, ¿Cuál?

7.- ¿Qué tipo de base de datos utiliza y por qué?

**Objetivo:** Conocimiento de los controles que establece la ISO 27001.