**UNIVERSIDAD NACIONAL DE SAN MARTÍN - T**

**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

# TESIS

# IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, APLICADO A LOS RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA NET – CONSULTORES S.A.C

**Para optar el Título de:**

**INGENIERO DE SISTEMAS E INFORMÁTICA**

**Presentado por el Bachiller**

**ADRIÁN GARCÍA PAREDES**

**Tarapoto - Perú**

**2016**

# UNIVERSIDAD NACIONAL DE SAN MARTÍN - T

## FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

### ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

# IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, APLICADO A LOS RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA NET – CONSULTORES S.A.C

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE**

## INGENIERO DE SISTEMAS E INFORMÁTICA

**Presentado por:**

**Bachiller** : **Adrián García Paredes**

**Asesor** : **Ing. Alberto Alva Arévalo**

.....

**Firma**

**SUSTENTADO Y APROBADO ANTE EL HONORABLE JURADO:**

**Presidente** : **Ing. MBA. Miguel Ángel Valles Coral**

.....

**Firma**

**Secretario** : **Ing. Cristian Werner García Estrella**

.....

**Firma**

**Miembro** : **Ing. Gilberto Paredes García**

.....

**Firma**

# DEDICATORIA

A Dios por brindarme la oportunidad y la dicha de la vida, además por poner en mi camino a las personas indicadas siempre.

A mis padres Oswaldo García y Luzmila Paredes; además a mis hermanos Andrés García y Katia García con todo el amor del mundo: Por todo su apoyo, esfuerzo, confianza y consejos que me brindaron y me siguen brindando en este camino largo de formación profesional y personal.

A mi amada novia Elsa Giovanna Sánchez, mi compañera inseparable, por ser mi apoyo, mi inspiración y por estar siempre a mi lado.

# AGRADECIMIENTO

Agradecer en primer lugar a Dios por brindarnos el bienestar familiar y estar siempre acompañándonos en nuestras actividades diarias.

A mis amados padres Oswaldo García y Luzmila Paredes; además a mis hermanos Andrés García y Katia García, quienes me acompañaron en cada momento de mi vida, brindándome apoyo moral y económico durante mi formación universitaria, porque son la fuente de mi motivación para superarme cada día.

Agradezco a todo el personal docente de la facultad de ingeniería de sistemas por compartir sus conocimientos y enseñanzas desinteresadamente el cual me permite a lo largo de mi vida profesional ser competente y llegar a lograr mis metas.

A mi amada novia Elsa Giovanna Sánchez, por escucharme, preguntarme, corregirme, darme ánimos y compartir conmigo la experiencia de desarrollar en su compañía la presente tesis.

## RESUMEN

Este proyecto se lleva a cabo para la empresa NET-Consultores S.A.C la cual pretende cada día implementar políticas y controles de seguridad para proteger la información; mejorar la atención a sus clientes, brindándoles eficiencia y calidad en la prestación de su servicio y asegurar la continuidad del negocio.

Este trabajo tiene como objetivo fundamental, diseñar un SGSI para la empresa NET-Consultores bajo la Norma ISO/IEC 27001 con el fin de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento de la empresa, instrucciones de los procedimientos a realizarse y la documentación que se debe desarrollar en todo el proceso para la posterior implementación del SGSI, aplicando el modelo PDCA (Planificar, hacer, verificar y actuar).

Como primera medida se recolecta información de la empresa a través de la observación y la técnica de la encuesta que permiten tener una idea general del manejo de la seguridad en la organización.

Seguidamente se realiza un análisis de riesgos paso a paso desarrollando el inventario de activos, la valoración cualitativa de los activos, identificación de amenazas, identificación de salvaguardas para los activos, valoración y evaluación del riesgo y el informe de calificación del riesgo, que permiten identificar los riesgos más apremiantes a los que está expuesta la empresa.

Posteriormente se definen las políticas y controles de seguridad, que tienen como finalidad contribuir a la disminución de riesgos de los elementos del área de informática y fortalecer la seguridad con medidas que se ven reflejadas en la empresa y a sus clientes en la prestación de un servicio ágil, eficiente, eficaz y con calidad.

Finalmente se realiza la primera fase de la implementación que es el plan de gestión del riesgo donde se concreta de forma clara cómo se va a actuar en el control de los riesgos, se identifica los controles seleccionados, los responsables y el tiempo. Listo para ser adoptado por la empresa.

## SUMMARY

The following research is made for NET CONSULTORES enterprise SAC, which implement security control policies to protect information; improving client's services, offering quality and efficiency in service to assure business continuing.

The following research has as main objective to design an SGSI system with NET-consulters under ISO/IEC 27001 Standard aiming to classify information, identify weaknesses and menace to the communication area; value risks defining security control and policies based on it, which would be manage by the company, procedure instructions and documentation that must be developed during the process in order to implement SGCI system, under PDCA (Planning, Doing, Control and Acting).

As a first step, observation for information gathering must be done and also interview technic to let have a general idea of security management on the organization.

After, a risk analysis step by step developing the assets inventory is done, quality value of assets, menaces identification, assets safeguard identification, valuation and evaluation of risks and its report which let identify the most relevant risks where the company is exposed.

Following is defining security control and policies which will contribute in less incidence of risk in the communication area empower security that will be reflected in the company and its clients giving nimble, efficient, and accurate services.

Finally, the first phase of implementation is done, consisting on a risk management plan where it is specifying how the risk must be control, selecting the controls, the responsible and the time, ready to be used by the company.

# ÍNDICE

# NOMENCLATURAS

## a) Lista de tablas



## b) Lista de Ilustraciones

## c) Lista de siglas, abreviaturas y símbolos

**SGSI**: Sistema de Gestión de Seguridad de la Información.

**S.A.C**: Sociedad Anónima Cerrada.

**ISO**: Organización Internacional para la Estandarización.

**IEC**: Comisión Electrotécnica Internacional.

**P-D-C-A**: Planear-Hacer-Chequear-Actuar.

# INTRODUCCIÓN

Desde hace ya algunos años la información se considera uno de los activos más valiosos de una compañía (los costes derivados de pérdida de seguridad no son sólo costes económicos directos, sino que también afectan a la imagen de la empresa), por lo que, cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones y, sin embargo, y a pesar de esa concienciación generalizada, muchas empresas no se enfrentan a este aspecto con la profundidad con la que debiera tratarse.

La continua evolución, crecimiento y sofisticación de la tecnología, al igual que los ataques cibernéticos en las organizaciones, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger a la compañía ante las amenazas a los activos informáticos. De esta manera se hace necesario diseñar un sistema de seguridad Informática que permita salvaguardar los activos de información de la empresa NET - Consultores, ayudando a la organización a cumplir sus objetivos. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La empresa NET- Consultores S.A.C, a través del diseño e implementación de un SGSI busca minimizar los riesgos a los que se encuentra expuesta la información de la organización desarrollo que se documenta paso a paso.

Para el desarrollo de la primera fase se aplica la metodología Magerit con la cual se realiza el análisis de riesgos que es uno de los procesos más importantes que se debe realizar dentro de la empresa ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales esta expuestos cada uno de ellos. Además permite identificar amenazas y vulnerabilidades.

Para el análisis de riesgos se realiza un inventario de activos, valoración cualitativa de dichos activos, identificación de amenazas, definición de salvaguardas. Una vez realizado estos procesos se procede a realizar una evaluación de los riesgos el cual permite determinar que activos se encuentran en peligro.

Una vez identificado claramente los activos que se encuentran en riesgo y que generarían mayor impacto en caso de sufrir un ataque, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles y el plan de gestión del riesgo, para cada uno de estos activos teniendo en cuenta lo expuesto por la Norma ISO/IEC 27002. Dichas políticas y controles deben ser implementadas en la organización para cumplir el objetivo fundamental del SGSI que es proteger la información y disminuir los riesgos, garantizando la continuidad del negocio.

# CAPÍTULO I

# I. EL PROBLEMA

## 1.1. Antecedentes del problema

Desde hace varias décadas la información ha pasado de ser un producto del desarrollo de las actividades de las organizaciones a ser un insumo de alto valor, fundamental para el cumplimiento de los objetivos y subsistencia de las mismas. De esta manera, toda organización se encuentra constantemente expuesta a una serie de riesgos mientras que resulta imposible establecer un entorno totalmente seguro de su información.

La empresa NET - Consultores S.A.C es una sociedad de consultoría de sistemas que inició sus operaciones el 01 de abril de 2007 en la ciudad de Lima. Desde su creación, hasta nuestros días NET - Consultores S.A.C ha evolucionado enfocándose en la entrega y realización de proyectos de mayor valor agregado, de la mano con diversas tecnologías líderes en el mercado, siempre orientados a las necesidades y requerimientos de sus clientes y de acuerdo a las características específicas de sus negocios.

La evolución y crecimiento de la empresa NET - Consultores SAC en cuanto a la consultoría de sistemas, ha hecho que la empresa cuente con información importante y valiosa para su funcionamiento, además ha adquirido competidores importantes dedicados al mismo rubro del negocio; por lo que la información en ciertas ocasiones ha sido interceptada, robada y/o modificada por personas que dañan el trabajo y la imagen de la empresa.

Analizando el problema se encontró que existe un alto riesgo de los activos de información con la que cuenta la empresa NET - Consultores SAC, entre sus causas podemos mencionar que existen incumplimiento de las normativas y legislación vigente; desconocimiento de las política, normas, buenas prácticas de seguridad de información, personal no concientizado en seguridad de información, carencia de controles de seguridad de información y numerosas vulnerabilidades en la seguridad de la información que no son atendidas.

## 1.2. Definición del problema

Tomando en consideración el gran volumen de información que se genera y registra diariamente en la empresa NET - Consultores S.A.C, en donde un ataque simple puede originar daños significativos cuando no se cuenta con controles que mitiguen los riesgos de la probabilidad de ocurrencia de sus amenazas. Por lo que existe la necesidad de proteger la información, ya que se pudo evidenciar que en la empresa se han presentado durante el periodo 2013–2014 las amenazas que mencionamos a continuación:

Se ha podido evidenciar que dentro de las áreas de tecnologías es frecuente observar que existen distintos problemas, tales como:

a) Frecuentes incidentes de seguridad:

1. Uso indebido de información crítica para la empresa.
2. Uso prohibido de un recurso informático o de red dentro de la empresa.
3. Destrucción no autorizada de información.
4. Pérdida de información.
5. Interrupción prolongada en un sistema o servicio de red.
6. Modificación, instalación o eliminación no autorizada de software.
7. Acceso o intento de acceso no autorizado a un sistema informático.
8. Modificaciones no autorizadas de los sistemas informáticos.
9. Eliminación insegura de información.
10. Modificación no autorizada de información.
11. Infecciones por código malicioso (virus).

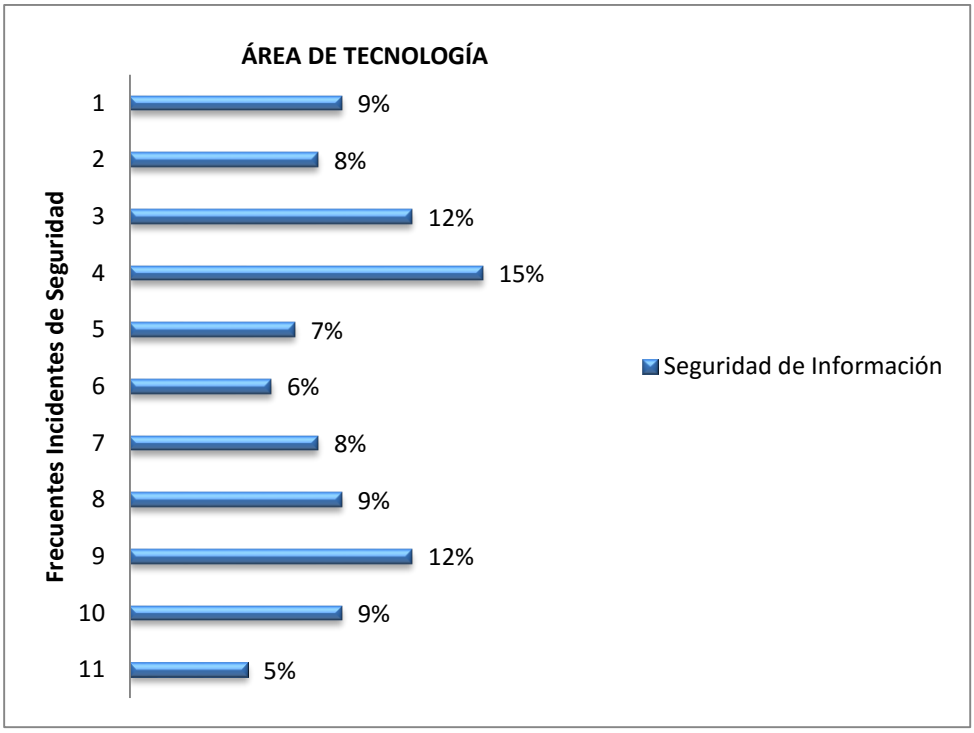



***Ilustración 1: Frecuentes Incidentes de Seguridad.***

***Funte: Elaboración Propia***

Dentro del 100% de incidentes de seguridad que se suscitaron durante el periodo 2013 – 2014 dentro de la empresa NET - Consultores en problemas de seguridad de información; el problema más relevante del 15% es de pérdida de información y el menos relevante del 5% es de infecciones por códigos malicioso (virus).

b) Numerosas vulnerabilidades asociadas a la seguridad de la información:

1. Control de acceso inadecuado.
2. Puntos de accesos remotos no seguros y no vigilados.
3. Contraseñas reutilizadas, sencillas o fáciles de adivinar a nivel de estación de trabajo.
4. Cuentas de usuarios con privilegios exclusivos.
5. Servidores con malas configuraciones.
6. Inadecuada implementación de políticas de seguridad.

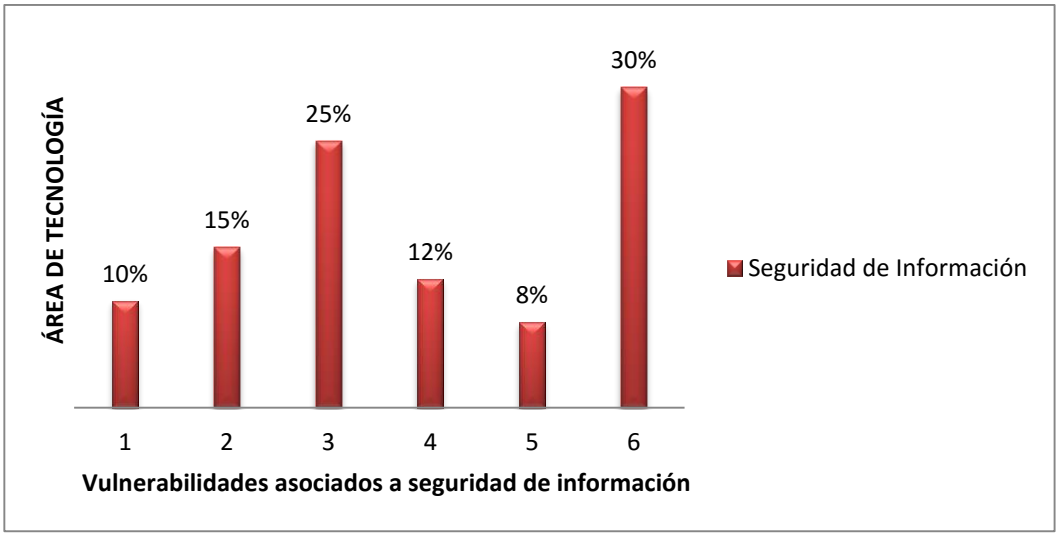



***Ilustración 2: Vulnerabilidades asociados a seguridad de información.***

***Fuente: Elaboración Propia***

Dentro del 100% de vulnerabilidades asociado a seguridad de información que se suscitaron durante el periodo 2013 – 2014 dentro de la empresa NET-Consultores; el problema más relevante del 30% es la inadecuada implementación de políticas de seguridad y el menos relevante del 8% es de servidores con malas configuraciones.

c) Altos niveles de riesgo de los activos de información.

1. Datos o información.
2. Aplicaciones.
3. Servicios.
4. Tecnología.
5. Local.

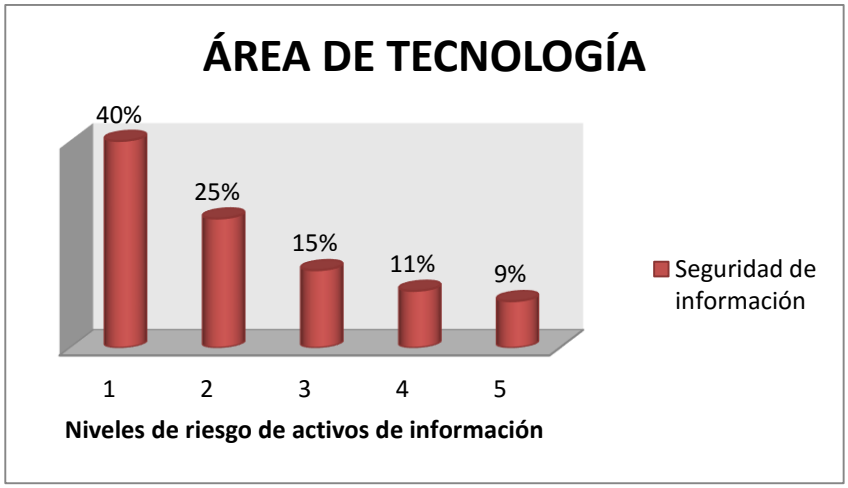



***Ilustración 3: Niveles de riesgo de activos de información.***

***Fuente: Elaboración Propia***

Dentro del 100% de activos de información de la empresa NET-Consultores dentro del periodo 2013 - 2014; el activo más importante del 40% es la información y el activo menos importante del 9% es el local donde funciona la empresa.

d) Personal no capacitado en seguridad de la información.

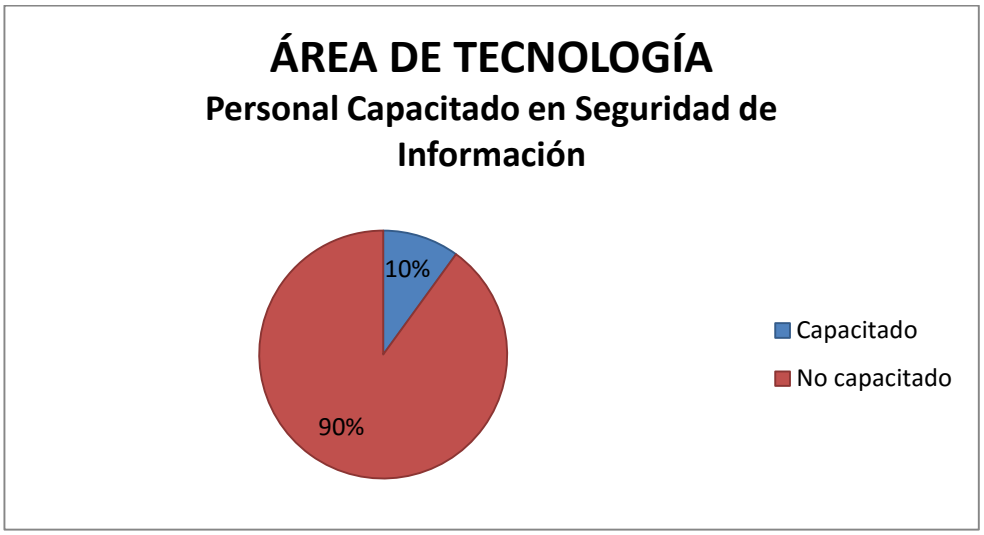



***Ilustración 4: Personal Capacitado en Seguridad de la Información.***

***Fuente: Elaboración Propia***

Dentro del 100% del personal de la empresa NET-Consultores dentro del periodo 2013 - 2014; se evidencio que el 90% de los trabajadores no se encuentra capacitado en lo que se refiere a seguridad de la información, mientras que el 10% si está capacitado en seguridad de la información.

e) No cuenta con la documentación necesaria

Se pudo evidenciar que NET-Consultores S.A.C no cuenta con la documentación necesaria en cuanto a políticas de gestión de seguridad de la información, el cual es un peligro latente para la empresa.

Se pudo evidenciar el incumpliendo las normativas y legislaciones vigentes en cuanto a seguridad de la información dentro de la empresa NET-Consultores S.A.C.

Un antecedente presentado en la empresa producto de la intersección de varios problemas mencionados que acontecen dentro de la organización, podemos mencionar la pérdida 80% de la información de una máquina, producto de un problema técnico de hardware; el cual genero grandes atrasos concerniente a lo trabajado en la computadora deteriorada; además genero la pérdida de tiempo y de dinero el cual se detalla de S/. 3,000.00 en reparación de la computadora y S/. 8,000.00 en sueldo de 2 trabajadores, haciendo un total de pérdida monetaria de S/. 11,000.00.

Además la empresa firma con sus clientes un contrato de confidencialidad de información, en el cual se estipula una multa a pagar por el uso indebido de la información, el cual lo establece la empresa que requiere el servicio; los montos a pagar por divulgar o perder la información superan los $150,000.00 y de presentarse este acontecimiento dentro de NET-Consultores S.A.C por no tener las debidas políticas de seguridad de la información dentro de la empresa; tendría como consecuencia la bancarrota de la empresa; así como también el desprestigio de la misma.

En base a este contexto, presento como una alternativa de solución la implementación de un Sistema de Gestión de Seguridad de la Información en la empresa NET-Consultores S.A.C.

## 1.3. Formulación del problema

¿Cuál es la influencia de la implementación de un Sistema de Gestión de Seguridad de la Información, aplicado al impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C?

## 1.4. Justificación e importancia

Se puede evidenciar que la empresa NET-Consultores S.A.C, no cuenta con la documentación necesaria en cuanto a políticas de gestión de seguridad de la información, demostrando el incumpliendo de las normativas y legislaciones vigentes en cuanto a seguridad de la información, por lo que presento esta investigación con la finalidad de analizar el impacto que generará la implementación de un Sistema de Gestión de Seguridad de la Información.

La investigación permitirá establecer los procesos para la identificación, análisis, evaluación y tratamiento de los riesgos considerando la seguridad de la información en la empresa, evitando un impacto negativo en la organización. También permitirá poner en práctica los conocimientos sobre el manejo de gestión de riesgos, y las técnicas pertinentes a las buenas prácticas.

## 1.5. Alcance y limitaciones

El alcance de la investigación comprende a la empresa “NET-Consultores S.A.C”, ubicada en la ciudad de Lima y está dirigido a los procesos, activos, riesgos y demás consideraciones, de la empresa en mención.

Entre las limitaciones consideramos los siguientes:

- Estará limitado a los riesgos de los activos de información, el cual comprende los siguientes procesos: Activos esenciales, Datos o información (catalogados como fundamentales), Claves Criptográficas, Servicios, Las aplicaciones de software, Equipos informáticos, Personal, Redes de Comunicación, Soportes de Información, Equipamiento Auxiliar e Instalaciones.

- Los objetivos de control y el proceso de evaluación serán seleccionados o alineados a la norma ISO/IEC 27001.
- El Sistema de Gestión de Seguridad de la Información, no será automatizado.

# II. MARCO TEÓRICO

## 2.1. Antecedentes de la investigación

**Justino (2015),** en su tesis titulada "Diseño de un Sistema de Gestión de Seguridad de Información para una Empresa Inmobiliaria Alineado a la Norma ISO/IEC 27001:2013" concluye que:

- Es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad.

**Espinoza (2013)** Estipula en su investigación "Análisis y Diseño de un Sistema de Gestión de Seguridad de Información Basado en la Norma ISO/IEC 27001:2005 para una empresa de Producción y Comercialización de Productos de Consumo Masivo" lo siguiente:

- Se debe establecer que los dueños de cada uno de los procesos que fueron analizados para el diseño del SGSI de este proyecto, empiecen a darle mayor importancia a la seguridad de la información, y que velen para que de alguna manera se pueda levantar los riesgos encontrados dentro de sus actividades.

**Barrantes & Hugo (2012)** en su tesis "Diseño e Implementación de un Sistema de Seguridad de Información en Procesos Tecnológicos" concluye que:

- Aún después de implementar un buen sistema de gestión de seguridad de información, en el futuro se presentan más activos de información, más

amenazas, vulnerabilidades y por lo tanto, mayores riesgos. Este escenario no se puede evitar; es por ello que se concluye, que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad que se identifique.

**Mantilla Guerra (2009),** menciona en su investigación titulada “Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001”:

- La seguridad de la información es un aspecto importante que debe ser parte de la cultura organizacional; cursos; seminarios y talleres no bastan, hay que interiorizar en las personas que la organización, la necesidad y beneficios de dicha cultura, así como los riesgos de no tenerla.

## 2.2. Definición de términos

- Activo: (ISO/IEC 13335-1:2004) Algo que presenta valor para la organización.
- Disponibilidad: (ISO/IEC 13335-1:2004) Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.
- Confidencialidad: (ISO/IEC 13335-1:2004) Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.
- Integridad: (ISO/IEC 13335-1:2004) Salvaguardar la exactitud e integridad de la información y activos asociados.
- Seguridad de la Información: (ISO/IEC 17799:2005) Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.
- Evento de la seguridad de la información: (ISO/IEC 18044:2004) Ocurrencia identificada en un sistema, servicio o red indicando una posible brecha de la política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.

- Incidente de la seguridad de la información: (ISO/IEC 18044:2004) Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.

- Riesgo residual:(ISO/IEC Guide 73:2002) Riesgo remanente después de un tratamiento del riesgo.

- Aceptación del riesgo: (ISO/IEC Guide 73:2002) Decisión de aceptar el riesgo.

- Análisis del riesgo: (ISO/IEC Guide 73:2002) Uso sistemático de información para identificar amenazas y estimar el riesgo.

- Estimación del riesgo:(ISO/IEC Guide 73:2002) Proceso total de análisis y evaluación del riesgo.

- Evaluación del riesgo: (ISO/IEC Guide 73:2002) Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado del riesgo.

- Gestión del riesgo: (ISO/IEC Guide 73:2002) Actividades coordinadas para dirigir y controlar el riesgo en una organización.

- Tratamiento del riesgo: (ISO/IEC Guide 73:2002) Proceso de selección e implementación de controles para minimizar el riesgo.

- Vulnerabilidad: es toda debilidad en un activo de información, dada comúnmente por la inexistencia o ineficacia de un control.

- Amenaza: es todo elemento que, haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, e independientemente de que se comprometa o no la seguridad de un sistema.

## 2.3. Bases teóricas

### 2.3.1. Sistema de gestión de la seguridad de la información (SGSI)

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

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

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización.

La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos. Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

### 2.3.2. Norma ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC, que proporcionan un marco de gestión de seguridad de la información, utilizable por cualquier tipo de organización pública o privada, grande o pequeña.

La norma ISO 27000 comprende un amplio rango de numeración para los estándares, que va desde 27000 a 27019 y de 27030 a 27044.

Para el caso de desarrollo del proyecto propuesto se toma en consideración el estudio de los estándares 27001 y 27002 que están directamente relacionados con la implementación y controles del Sistema de Gestión de Seguridad de la Información.

El estándar ISO 27002 es un conjunto de buenas prácticas en seguridad de la información. Contiene controles aplicables en relación a la gestión de la continuidad de actividades, la gestión de incidentes de seguridad, control de accesos o regulación de las actividades del personal interno o externo, que ayudan a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información, mientras que el estándar ISO 27001 contiene un anexo A, que considera los controles del estándar ISO 27002 para su posible aplicación en el SGSI que implante cada organización; de esta manera existe una relación de controles necesarios para garantizar la seguridad de la información.

### 2.3.3. Estándar internacional ISO/IEC 27001

Este estándar fue publicado el 15 de octubre de 2005 por la ISO e IEC que conforman un sistema especializado para la estandarización universal. Es la norma principal de la serie ISO 27000 y contiene los requisitos de implementación del sistema de gestión de seguridad de la información.

El estándar ha sido preparado para proporcionar un modelo que permite establecer, implementar, monitorear, revisar y mejorar un SGSI. La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI en una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, procesos empleados, tamaño y estructura de la empresa.

#### 2.3.3.1. Enfoque del proceso

Este estándar fomenta que los usuarios enfaticen la importancia de:

a. Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la misma.

b. Implementar y operar controles para manejar los riesgos de la seguridad de la información.

c. Monitorear y revisar el desempeño y la efectividad del SGSI.

d. Mejoramiento continúo en base a la medición del objetivo.

Este estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. PDCA es un ciclo de vida continuo.

La figura 01 muestra cómo se desarrolla el proceso de implantación de un SGSI.


***Ilustración 5: Modelo de desarrollo PDCA***

***Fuente: http://www.gestion-calidad.com/implantacion-iso-27001.html***

A continuación se detalla cada una de las fases del modelo PDCA.

- **Planificar (Plan).** Dentro de esta fase se establecen políticas, objetivos, procesos y procedimientos relevantes para manejar el riesgo y mejorar la seguridad de la información. Se debe definir una política de seguridad que considere los requerimientos legales relativos a la seguridad de la información; además debe establecerse los criterios con los que se va a evaluar el riesgo y finalmente debe ser aprobada por la dirección o gerencia.

  Aquí se define una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos de la institución, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

- **Hacer (Do).** En esta fase se seleccionan e implementan los controles que reduzcan el riesgo a los niveles considerados como aceptables.

  Se debe efectuar el cambio y/o las pruebas proyectadas según la decisión que se haya tomado y la planificación que se ha realizado.

- **Verificar (Check).** Una vez realizada la acción e implantado el control, se debe verificar, evaluar y medir el desempeño del proceso en comparación con la política, objetivos, experiencias prácticas y reportar los resultados a la gerencia para su revisión.

- **Actuar (Act).** Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

  Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar la forma de proceder, además es importante tener la seguridad de que las mejoras introducidas alcanzan los objetivos previstos.

#### 2.3.3.2. Alcance del estándar

Este estándar internacional abarca todos los tipos de organizaciones. Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos generales de la organización. El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

#### 2.3.3.3. Referencias normativas

El estándar internacional ISO/IEC 27001:2013 está basado en la norma ISO/IEC 17799:2005, cuyo contenido trata sobre: Tecnología de la información, técnicas de seguridad y código de práctica para la gestión de la seguridad de la información.

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

Un SGSI es un Sistema de Gestión de la Seguridad de la Información, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración. Esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

##### 2.3.3.4.1. Requerimientos generales

La institución debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado, es decir que todas las políticas establecidas, procedimientos de administración y el uso de las herramientas de gestión deben estar reflejadas de manera escrita, dentro del contexto de las actividades generales de la organización. Para propósitos de este estándar, los procesos utilizados se basan en el modelo PDCA.

##### 2.3.3.4.2. Requerimiento de documentación

a. Documentados de la política SGSI y los objetivos.

b. Alcance, Procedimientos y controles de soporte del SGSI.

c. Metodología de evaluación del riesgo.

d. Reporte de evaluación del riesgo.

e. Plan de tratamiento del riesgo.

f. Los procedimientos documentados necesarios por la organización.

g. Registros requeridos por este Estándar Internacional.

#### 2.3.3.4.3. Responsabilidad de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al establecer una política.

**Gestión de recursos:**

**a. Provisión de recursos.** La organización debe determinar y proporcionar los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI y brindar una seguridad adecuada mediante la correcta aplicación de todos los controles.

**b. Capacitación, conocimiento y capacidad.** La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas.

#### 2.3.3.5. Auditorías internas SGSI

La organización debe realizar auditorías internas a intervalos planeados para determinar si los objetivos de control y procedimientos del SGSI cumplen con los requerimientos de este estándar internacional, la legislación y regulaciones a las que está sometida la norma ISO 27000.

#### 2.3.3.6. Mejoramiento del SGSI

**Mejoramiento continúo.** La organización debe mejorar continuamente la efectividad del SGSI a través del uso de políticas de seguridad de la información, objetivos de seguridad de la información, resultados de auditoría, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

**Acción correctiva.** La organización debe realizar las acciones para eliminar la causa de las no conformidades con los requerimientos del SGSI para poder evitar la recurrencia.

**Acción preventiva.** La organización debe determinar la acción para eliminar la causa de las no conformidades potenciales de los requerimientos SGSI para evitar ocurrencias.

#### 2.3.3.7. Objetivos de control y controles

**Anexo A (Normativo).** Los objetivos de control y los controles de este anexo deben seleccionarse como parte del proceso SGSI.

Las cláusulas enumeradas desde A5 a A18 proporcionan lineamientos para la implementación de las mejores prácticas en soporte de los controles.

**Tabla 1: Objetivos de control de la norma ISO/IEC 27001**

| Anexo | Objetivo de Control |
|---|---|
| A.05. | Políticas de seguridad de la Información |
| A.06. | Organización de la seguridad de la información |
| A.07. | Seguridad de los recursos humanos |
| A.08. | Gestión de activos |
| A.09. | Control de accesos |
| A.10. | Criptografía |
| A.11. | Seguridad física y del entorno |
| A.12. | Seguridad en las operaciones |
| A.13. | Seguridad de las comunicaciones |
| A.14. | Adquisiciones, desarrollo y mantenimiento de los sistemas |
| A.15. | Relación con los proveedores |
| A.16. | Gestión de incidentes en la seguridad de la información |
| A.17. | Gestión de la continuidad comercial |
| A.18. | Cumplimiento |

***Fuente: http://www.iso27000.es/***

### 2.3.4. Estándar internacional ISO/IEC 27002

Es una guía de buenas prácticas que fue publicada en el 2013 basándose en la norma ISO 17799:2005 por lo que mantiene a 2013 como año de edición y describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es una norma certificable. Contiene 35 objetivos de control y 114 controles, agrupados 14 dominios.

El objetivo del estándar ISO/IEC 27002 es servir de guía a los responsables de la implementación de seguridad de la información de una organización. En este estándar se describe los 14 dominios referentes a la seguridad de la información.

Los objetivos de control y los controles, deben ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos.

#### 2.3.4.1. Alcances del estándar

Este estándar internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Sirve como un lineamiento práctico para desarrollar estándares de seguridad organizacional, prácticas de gestión de seguridad efectivas y para ayudar a crear confianza en las actividades inter-organizacionales.

#### 2.3.4.2. Cláusulas

Cada cláusula contiene un número de categorías de seguridad principales.

**Tabla 2: Cláusulas del estándar ISO/IEC 27002**

| Cláusula o Dominios | Objetivo de Control |
|---|---|
| Políticas de seguridad de la Información | 1 |
| Organización de la seguridad de la información | 2 |
| Seguridad de los recursos humanos | 3 |
| Gestión de activos | 3 |
| Control de accesos | 4 |
| Criptografía | 1 |
| Seguridad física y del entorno | 2 |
| Seguridad en las operaciones | 7 |
| Seguridad de las comunicaciones | 2 |

***Fuente: http://www.iso27000.es/***

a. **Política de seguridad de la información.** Esta cláusula se enfoca en brindar apoyo y orientación a la gerencia o dirección, con respecto a la seguridad de la información, de acuerdo con los requisitos de la institución y los reglamentos y leyes pertinentes.

b. Organización de la Seguridad de la Información. Está orientada a gestionar y mantener la seguridad de la información y de los servicios de procesamiento de información a los cuales tienen acceso.

c. **Seguridad de Recursos Humanos.** Este punto trata de asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones para las cuales están considerados.

d. **Gestión de Activos.** El objetivo de la cláusula es mantener la protección adecuada de los activos de la institución y asegurar que la información reciba el nivel de protección adecuado.

e. **Control de Acceso**. Esta cláusula permite controlar el acceso a la información con base en los requisitos de seguridad y de la institución evitando el acceso no autorizado a servicios de red.

f. **Criptografía.** Esta cláusula permite hacer uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

g. **Seguridad Física y Ambiental (Entorno físico).**Esta cláusula hace referencia a evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la institución.

h. **Seguridad en las Operaciones.** Se refiere a asegurar la operación correcta de los servicios de procesamiento de información para minimizar el riesgo de fallas en los sistemas manteniendo la integridad y disponibilidad de la información.

i. **Seguridad en las Comunicaciones.** Se refiere a asegurar la operación correcta de los servicios de procesamiento de información para minimizar el riesgo de fallas en los sistemas manteniendo la integridad y disponibilidad de la información.

j. **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.** Este punto hace referencia a que se debe garantizar que la seguridad es parte integral de los sistemas de información.

k. **Relación con los proveedores**. Esta cláusula permite implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

l. **Gestión de Incidentes de Seguridad de la Información**. Esta cláusula asegura que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

m. **Gestión de la Continuidad Comercial.** Este punto considera la disminución de interrupciones en las actividades de la institución para proteger los procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

n. **Cumplimiento.** Se refiere a evitar el incumplimiento de normativas legales, estatutos y requisitos de seguridad que se encuentre en vigencia dentro de la institución.

### 2.3.5. Riesgo

Es la probabilidad de que una amenaza aproveche o explote una potencial vulnerabilidad en un activo de información, y de la magnitud del daño resultante de tal evento adverso en la organización.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

**Identificar los riesgos comprende:**

- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
- Identificar las amenazas en relación a los activos.

  Son ejemplos de amenazas:

  - De origen natural: eventos tales como inundaciones, terremotos, tornados, incendios, tormentas eléctricas y otros desastres naturales.
  - De origen humano: eventos que son permitidos o causados por seres humanos, sean estos actos involuntarios tales como errores en la operatoria, errores de programación, ausencia de personal técnico responsable; o bien acciones intencionales tales como la comisión de robo o fraude, el acceso no autorizado a la información, la suplantación de identidad, etc.
  - Del entorno: tales como interrupciones prolongadas de servicios eléctricos o de comunicaciones, fallas por obsolescencia o mal funcionamiento de equipamiento, etc.
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.

Son ejemplos de vulnerabilidades, entre muchas otras:

- La falta de mantenimiento en las instalaciones.
- La falta de capacitación al personal.
- La falta de manuales de procedimientos.
- La inexistencia de respaldos de información y equipamiento redundante.
- La falta de políticas de acceso a los sistemas informáticos.
- La divulgación o utilización de contraseñas inseguras.
- La transmisión de información por medios inseguros.
- Los errores de programación en las aplicaciones.
- La falta de mobiliario de oficina con llave.
- El acceso irrestricto al lugar de trabajo.
- La eliminación insegura de la información.

- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

**Analizar y evaluar los riesgos:**

- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
- Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.
- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

**Identificar y evaluar, las distintas opciones de tratamiento de los riesgos para:**

- Aplicar controles adecuados.
- Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.
- Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan.
- Transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

Seleccionar los objetivos de control y los controles, del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

Definir una declaración de aplicabilidad que incluya:

- Los objetivos de control y controles seleccionados y los motivos para su elección.
- Los objetivos de control y controles que actualmente ya están implantados.
- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

## 2.4. Hipótesis

### 2.4.1. Hipótesis alterna (H1)

Si implementamos un Sistema de Gestión de Seguridad de la Información entonces se minimizará el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

### 2.4.2. Hipótesis nula (Ho)

Si implementamos un Sistema de Gestión de Seguridad de la Información entonces no se minimizará el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

## 2.5. Sistema de variables

### 2.5.1. Variable independiente:

Sistema de Gestión de Seguridad de la Información.

### 2.5.2. Variable dependiente:

Riesgos asociados a los activos de información.

## 2.6. Escala de medición

**Variable Independiente:** Sistema de Gestión de Seguridad de la Información. Tendrá como escala de medición a las tres características básicas de la seguridad de la información: la confidencialidad, la integridad, y la disponibilidad a la que debe estar sometido; el cual se aplicara en la valorización cualitativa de los activos, según la Metodología MAGERIT:

**Tabla 3: Escala de medición variable independiente**

| Dimensión | Escala | Indicadores |
|---|---|---|
| **Confidencialidad** | 0, 1, 2, 3 | **(0)** Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la empresa. |
| | | **(1)** Información que puede ser conocida y utilizada por todos los agentes de la empresa. |
| | | **(2)** Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo. |
| | | **(3)** Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la empresa o terceros. |
| **Integridad** | 0, 1, 2, 3 | **(0)**Información cuya modificación no autorizada puede repararse fácilmente. |
| | | **(1)** Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para la empresa o terceros. |
| | | **(2)** Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo. |
| | | **(3)** Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades. |

| | | |
|---|---|---|
| **Disponibilidad** | 0, 1, 2, 3 | **(0)** Información cuya inaccesibilidad no afecta la actividad normal de la empresa. |
| | | **(1)** Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la empresa. |
| | | **(2)** Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la empresa. |
| | | **(3)** Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la empresa. |

***Fuente: www.seguridadinformatica.unlu.edu.ar***

**Variable Dependiente:** Riesgos asociados a los activos de información.

Tendrá como escala de medición a las siguientes situaciones de ocurrencia de los riesgos:

**Tabla 4: Escala de medición variable dependiente**

| Escala | Indicador | Valor | |
|---|---|---|---|
| | | Numérico | Porcentual |
| 1 | Poco frecuente, cada varios años | 10 | 10% |
| 2 | Normal, una vez al año | 50 | 50% |
| 3 | Frecuente, mensualmente | 70 | 70% |
| 4 | Muy frecuente A diario | 100 | 100% |

***Fuente: www.fing.edu.uy***

## 2.7. Objetivos

### 2.7.1. Objetivo general

Determinar la influencia de la implementación de un Sistema de Gestión de Seguridad de la Información sobre el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.

### 2.7.2. Objetivos específicos

- Diseñar el Sistema de Gestión de Seguridad de la Información, aplicado a los riesgos asociados a los activos de información.
- Aplicar el Sistema de Gestión de Seguridad de la Información, a los riesgos asociados a los activos de información.
- Determinar el grado de variación o significancia de la minimización de los riesgos asociados con el uso de la información.

# CAPÍTULO II

# III. MATERIALES Y MÉTODOS

## 3.1. Universo y muestra

### 3.1.1. Universo

El universo de estudio está conformado por todos los activos de información y sus correspondientes riesgos asociados de la empresa NET- Consultores S.A.C ubicada en la ciudad de Lima.

**Tabla 5: Activos de información y los riesgos asociados**

| Activos de Información | Riesgos asociados |
|---|---|
| Activos esenciales | 20 |
| Datos o información | 14 |
| Claves criptográficas | 8 |
| Servicios | 14 |
| Aplicaciones de software | 14 |
| Equipos informáticos | 17 |
| Personal | 9 |
| Redes de comunicación | 12 |
| Soportes de información | 10 |
| Equipamiento auxiliar | 13 |
| Instalaciones | 11 |
| **Total de Muestra** | **142** |

***Fuente: Elaboración propia***

### 3.1.2. Muestra

La muestra es el 100% del universo, es decir, los 142 riesgos asociados a los activos de información.

## 3.2. Ámbito geográfico

La investigación se centra en la empresa NET- Consultores S.A.C ubicada en la ciudad de Lima, siendo el lugar principal de contexto en donde se realizará el estudio. Para más detalles, se presenta la descripción exacta en donde se realizará la investigación.

- Departamento : Lima.
- Provincia : Lima.
- Distrito : San Borja.
- Dirección : Av. Aviación #2478

## 3.3. Diseño de investigación

En la presente investigación se aplicará el diseño pre experimental con pre test y pos test con un solo grupo.

Cuyo diagrama es el siguiente:

G ---------- $O_1$---------- X ----------$O_2$

Dónde:

**G :** Es el grupo al que se le hará el seguimiento.

**$O_1$:** Es el pre test, que permitirá diagnosticar el estado de los riesgos antes de la aplicación del Sistema de Gestión de Seguridad de la Información.

**X :** Es la aplicación del Sistema de Gestión de Seguridad de la Información.

**$O_2$:** Es el pos test, que permitirá determinar el estado de los riesgos después de la aplicación del Sistema de Gestión de Seguridad de la Información.

## 3.4. Procesamiento y técnicas

### 3.4.1. Procedimientos

En cuanto al procesamiento y presentación de datos de pre test y pos test se utilizará el programa de Microsoft Office Excel, se usará fórmulas para sacar resultados de las mediciones realizadas en la empresa NET- Consultores S.A.C, ubicada en la ciudad de Lima.

Se utilizará la metodología MAGERIT para el análisis, gestión y evaluación de los riesgos asociados a los activos de información.

Toda información obtenida de los diversos instrumentos serán para obtener los datos necesarios para realizar la investigación, los cuales serán graficados y procesados, la mejor forma de demostrar el fruto de la investigación es reflejarlo en resultados.

### 3.4.2. Técnicas

#### 3.4.2.1. Observación directa

Esta técnica se utilizó para captar los hechos que acontecen en la empresa para obtener los datos más próximos que ocurren en la realidad.

#### 3.4.2.2. Entrevista

Por medio de esta técnica, se recaudó la información proveniente de la Gerencia con el fin de realizar análisis, gestión y evaluación de los riesgos asociados a los activos de información el cual nos permitirá obtener toda la información empírica necesaria para determinar los valores o respuestas de las variables motivo de estudio.

#### 3.4.2.3. Cuestionario

Se realizó una serie de preguntas, a fin de obtener toda la información empírica necesaria para determinar los valores o respuestas de las variables motivo de estudio.

## 3.5. Instrumento

### 3.5.1. Instrumento de recolección de datos

El instrumento que se utilizó fue el siguiente: 24 formatos de observación directa impresos los cuales se aplicaron semanalmente durante 6 meses (12 en el pre test y 12 en el pos test) para la obtención de datos de la variable dependiente.

### 3.5.2. Instrumento de procesamiento de datos

El procesamiento de los datos obtenidos se realizó mediante el programa Excel, para calcular los indicadores estadísticos, que serán presentados en forma de cuadros y gráficos.
Para determinar la significancia de la variable independiente sobre la variable dependiente se realizó a través de la estadística inferencial, mediante las siguientes herramientas estadísticas:

**Para hallar que hay en los datos:**

- **La media aritmética o promedio ( $\overline{X}$ ):** Es el estadístico de tendencia central más significativo y corresponde variables de cualquier nivel de medición pero particularmente a las mediciones de intervalo y de razón.

$$\bar{X} = \sum_{i=1}^{n} \frac{x_i}{\mathrm{n}}$$

**Para conocer que tanto varían los datos:**

- **Desviación estándar (S):** Es el promedio de las desviaciones o dispersiones de las puntuaciones respecto a la media o promedio, permite medir el grado de homogeneidad o heterogeneidad de los datos de la población objeto de medición. Cuanto mayor sea la dispersión de los datos respecto a la media mayor será la desviación estándar, lo cual significa mayor heterogeneidad entre las mediciones. La fórmula para calcular la desviación estándar de una muestra de observaciones de datos es:

$$S = \sqrt{\frac{\sum_{i=1}^{n}(X_i - \bar{X})^2}{n-1}}$$

- **Prueba estadística**.- Para la verificación de hipótesis se usará la prueba Z, que es una prueba de distribución normal que tiene como fin comparar las probabilidades de los riegos asociados de cada activo de información obtenidos en el pre-test y pos-test.

Se contrastará los “Riesgos asociados a los activos de información” antes y después del Sistema de Gestión de Seguridad de la Información.

## 3.6. Prueba de hipótesis

### 3.6.1. Hipótesis

H1: Si implementamos un Sistema de Gestión de Seguridad de la Información entonces se minimizará el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

Ho: Si implementamos un Sistema de Gestión de Seguridad de la Información entonces no se minimizará el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

### 3.6.2. Regla de decisión

Se rechaza la Ho si : Zc > Zt o –Zc < -Zt

Se acepta la Ho si : Zc <= Zt o –Zc >= -Zt

### 3.6.3. Encontrar la Z tabulada (Zt)

Trabajamos a un nivel de significancia (α)= 0.05

Establecemos las hipótesis estadísticas:

Ho : $\mu 1 = \mu 2$

H1 : $\mu 1 \neq \mu 2$

Se trabajará con cola bilateral por lo tanto el nivel de significancia será $\alpha/2 = 0.025$.

Consultando el valor z de la tabla a 2.5% de probabilidad se tiene que:

$Zt = \pm 1.96$

### 3.6.4. Matriz resumen de las encuestas aplicadas, calculó de las diferencias de cada par (pre test – pos test)

Luego de realizar las respectivas observaciones del Pre test y Pos test aplicado a los activos de información de la empresa NET-Consultores S.A.C y habiendo obtenido los resultados, se procedió a llenar el siguiente tabla para la respectiva verificación de la hipótesis, de acuerdo a la probabilidad con la que ocurre cada riesgo correspondiente a cada activo de información; la evaluación se llevó a cabo de acuerdo a los 142 riesgos asociados a los activos encontrados en la empresa y de los cuales se hizo la respectiva evaluación.

Los resultados de las observaciones (Pre test y Pos test) realizadas a los se encuentra en el punto (4.2. Resultados obtenidos en la aplicación de las observaciones) del documento.

**Tabla 6: Diferencia entre el pre test y el pos test**

| Riesgo | Activo | Pre test (%) | Pos test (%) | Dif. (Pre-Pos) % |
|---|---|---|---|---|
| [N.1] Fuego<br>[N.2] Daños por agua | Equipos informáticos.<br>Instalaciones. | 50 | 10 | 40 |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipos informáticos.<br>Instalaciones. | 70 | 50 | 20 |
| N.1] Fuego<br>[N.2] Daños por agua | Soporte de almacenamiento. | 50 | 10 | 40 |
| [I.1] Fuego<br>[I.2] Daños por agua | Soporte de almacenamiento. | 50 | 10 | 40 |
| [N.1] Fuego<br>[N.2] Daños por agua | Equipamiento Auxiliar. | 50 | 10 | 40 |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipamiento Auxiliar. | 50 | 10 | 40 |
| [N.*] Desastres naturales | Equipos informáticos. | 70 | 50 | 20 |
| | Soporte de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |
| | Instalaciones. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [I.*] Desastres industriales | Equipos informáticos. | 70 | 50 | 20 |
| | Soporte de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |
| | Instalaciones. | 50 | 10 | 40 |
| [I.3] Contaminación mecánica | Equipos informáticos. | 70 | 70 | 0 |
| | Soporte de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |
| I.4] Contaminación electromagnética | Router de acceso inalámbrico. | 100 | 70 | 30 |
| [I.5] Avería de origen físico o lógico | Software - Aplicaciones Informáticas. | 100 | 70 | 30 |
| | Equipos informáticos. | 70 | 50 | 20 |
| | Soportes de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [I.6] Corte del suministro eléctrico | Equipos Informáticos. | 100 | 70 | 30 |
| | Soporte de Información (electrónicos). | 50 | 10 | 40 |
| | Ups computadores | 50 | 10 | 40 |
| [I.7] Condiciones inadecuadas de temperatura o humedad | Equipos Informáticos. | 100 | 70 | 30 |
| [I.8] Fallo de servicios de comunicaciones | Redes de comunicaciones (Red inalámbrica, red local e internet) | 100 | 70 | 30 |
| [I.9] Interrupción de otros servicios y suministros esenciales. | Equipamiento Auxiliar. | 50 | 10 | 40 |
| [I.10] Degradación de los soportes de almacenamiento de la información. | Soportes de Información. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios | Archivos de proyectos. | 100 | 70 | 30 |
| | Archivos de Clientes | 50 | 10 | 40 |
| | Archivo de Contabilidad | 50 | 10 | 40 |
| | Archivos de Informes y licencias expedidas | 100 | 50 | 50 |
| | Archivo de Copias de seguridad de la información | 50 | 10 | 40 |
| | Datos de configuración de servidores y equipos | 50 | 10 | 40 |
| | Datos de Gestión de proyectos radicados | 50 | 10 | 40 |
| | Contraseñas de acceso de empleados | 50 | 10 | 40 |
| [E.1] Errores de los usuarios | Claves Criptográficas | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios | Servicios prestados a usuarios externos bajo relación contractual | 50 | 10 | 40 |
| | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | 50 | 10 | 40 |
| | Servicio de internet que acceden los empleados. | 70 | 50 | 20 |
| | Manejo de correos electrónicos | 50 | 10 | 40 |
| | Servicio de almacenamiento de información en el servidor de bases de datos. | 70 | 50 | 20 |
| | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios Aplicaciones | Servidor de aplicaciones | 50 | 10 | 40 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 50 | 10 | 40 |
| | Office 2010 | 50 | 10 | 40 |
| | Kaspersky original con actualizaciones automáticas. | 50 | 10 | 40 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas. | 70 | 50 | 20 |
| [E.1] Errores de los usuarios. Soporte de información | Soportes de Información. | 70 | 50 | 20 |
| [E.4] Errores de configuración | Datos de configuración de servidores y equipos | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.7] Deficiencias en la organización | Personal | 100 | 70 | 30 |
| | Administrador de sistemas | 50 | 10 | 40 |
| [E.8] Difusión de software dañino | Software – Aplicaciones Informáticas | 50 | 10 | 40 |
| [E.9] Errores de [re-]encaminamiento | Servicios | 50 | 10 | 40 |
| | Software – Aplicaciones Informáticas | 50 | 10 | 40 |
| | Redes de comunicaciones | 50 | 10 | 40 |
| [E.14] Escapes de información | Activos esenciales | 50 | 10 | 40 |
| | Datos / información | 50 | 10 | 40 |
| [E.15] Alteración accidental de la información | Datos / información | 70 | 50 | 20 |
| [E.18] Destrucción de la información | Datos / información | 70 | 50 | 20 |
| | Aplicaciones | 50 | 10 | 40 |
| | Soporte Información | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.19] Fugas de información | Datos / información | 70 | 50 | 20 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 70 | 50 | 20 |
| | Aplicaciones | 70 | 50 | 20 |
| | Personal | 70 | 50 | 20 |
| [E.20] Vulnerabilidades de los programas (software) | Servidor de aplicaciones | 50 | 10 | 40 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 70 | 50 | 20 |
| | Office 2010 | 50 | 10 | 40 |
| | Kaspersky original con actualizaciones automáticas. | 50 | 10 | 40 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 70 | 50 | 20 |

| | | | | |
|---|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | Servidor de aplicaciones | 50 | 10 | 40 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 70 | 50 | 20 |
| | Office 2010 | 50 | 10 | 40 |
| | Kaspersky original con actualizaciones automáticas. | 70 | 50 | 20 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 70 | 50 | 20 |
| [E.24] Caída del sistema por agotamiento de recursos | Servicios | 50 | 10 | 40 |
| | Equipos Informáticos | 70 | 50 | 20 |
| | Redes de comunicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.25] Pérdida de equipos -Robo | Equipos Informáticos | 50 | 10 | 40 |
| | Soporte Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| [E.28] Indisponibilidad del personal | Personal de recepción, área técnica, administrativa y archivo | 70 | 50 | 20 |
| [A.5] Suplantación de la identidad del usuario | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 50 | 10 | 40 |
| | Redes de comunicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.6] Abuso de privilegios de acceso | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Equipos Informáticos | 100 | 70 | 30 |
| | Redes de comunicaciones | 70 | 50 | 20 |
| [A.7] Uso no previsto | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 70 | 50 | 20 |
| | Equipos Informáticos | 100 | 70 | 30 |
| | Redes de comunicaciones | 70 | 50 | 20 |
| | Soporte de Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| | Instalaciones | 70 | 50 | 20 |
| [A.8] Difusión de software dañino | Aplicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.11] Acceso no autorizado | Datos / información | 70 | 50 | 20 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 70 | 50 | 20 |
| | Equipos Informáticos | 70 | 50 | 20 |
| | Redes de comunicaciones | 70 | 50 | 20 |
| | Soporte de Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| | Instalaciones | 50 | 10 | 40 |
| [A.13] Repudio | Servicios | 50 | 10 | 40 |
| [A.14] Interceptación de información | Redes de comunicaciones | 50 | 10 | 40 |
| [A.15] Modificación deliberada de la información | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicio | 50 | 10 | 40 |
| | Aplicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.18] Destrucción de información | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 50 | 10 | 40 |
| | Soporte de la información | 50 | 10 | 40 |
| [A.19] Divulgación de información | Datos / información | 70 | 50 | 20 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Soporte de la información | 50 | 10 | 40 |
| [A.22] Manipulación de programas | Aplicaciones | 70 | 50 | 20 |
| [A.23] Manipulación de los equipos | Equipos Informáticos | 100 | 70 | 30 |
| | Soportes de Información | 50 | 10 | 40 |
| | Equipamiento auxiliar | 50 | 10 | 40 |
| [A.24] Denegación de servicio | Equipos Informáticos | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Redes de Comunicación | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.25] Robo | Equipos informáticos | 50 | 10 | 40 |
| | Soporte de Información | 50 | 10 | 40 |
| [A.26] Ataque destructivo | Equipo Informáticos | 50 | 10 | 40 |
| | Soporte de Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| | instalaciones | 50 | 10 | 40 |
| [A.28] Indisponibilidad del Personal | Personal | 50 | 10 | 40 |
| [A.29] Extorsión | Personal | 50 | 10 | 40 |
| [A.30] Ingeniería Social | Personal | 50 | 10 | 40 |
| **SUMA** | | **8 290** | **3 360** | **4 930** |
| **MEDIAS** | | **58.38** | **23.66** | **34.72** |
| **DESVIACIÓN ESTÁNDAR** | | **14.66** | **21.35** | **8.89** |

***Fuente: Tabla33 Relación de amenazas por activo***

Como podemos observar la media del pre test es de 58,38 corresponden a la probabilidad de ocurrencias de las amenazas de los riesgos, mientras que la media del pos test es de 23,66 haciendo una diferencia de 34,72, demostrando así que la implementación del sistema de seguridad de los activos de información, ha permitido disminuir las amenazas de los riesgos identificados en la empresa.

### 3.6.5. Cálculo de Z calculada (Zc)

Se usa la fórmula: $Zc = \frac{\mu 2 - \mu 1}{\sqrt{\frac{\sigma 2^2}{n} + \frac{\sigma 1^2}{n}}}$

Entonces se tiene:

$$Zc = \frac{23.6620 - 58.3803}{\sqrt{\frac{21.3541^2}{142} + \frac{14.6659^2}{142}}} = -15.97$$

### 3.6.6. Justificación y decisión

Se observa que : - Zc < - Zt.

Como -15.97 < -1.96, entonces se rechaza Ho y aceptamos H1: Si implementamos un Sistema de Gestión de Seguridad de la Información entonces se minimiza el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

Se concluye con un nivel de significancia de 0.05 que los datos indican que el Sistema de Gestión de Seguridad de la Información utilizado disminuyó las amenazas de riesgos asociados a los activo de información de la empresa.

## 3.7. Prueba Z bilateral

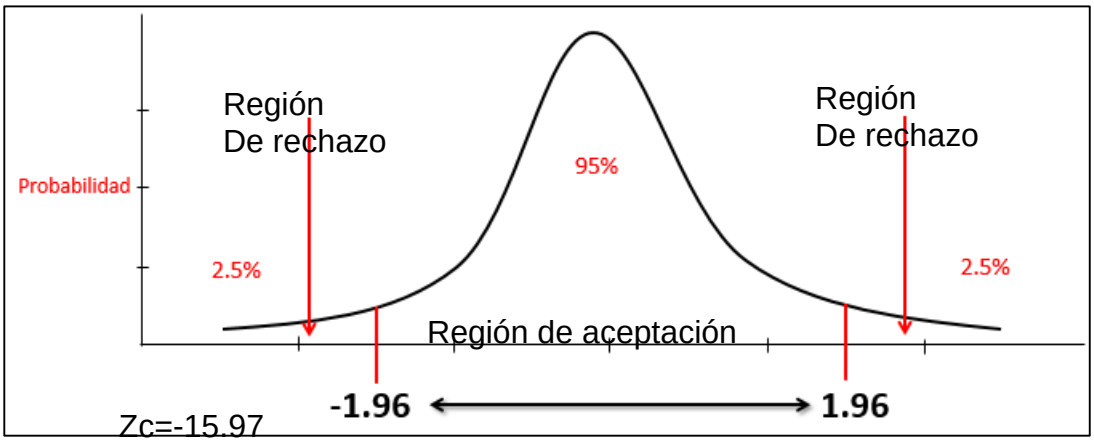



***Ilustración 6: La región crítica o de rechazo a $H_0$***

***Fuente: Elaboración Propia***

Se observa que la Zc queda en la región crítica o región de rechazo a la hipótesis Nula (Ho), a un nivel de confianza del 5% se rechaza la hipótesis nula y por consiguiente se acepta la hipótesis alternativa.

Por lo tanto podemos afirmar que**:** SI IMPLEMENTAMOS UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ENTONCES SE MINIMIZA EL IMPACTO DE LOS RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA NET–CONSULTORES S.A.C.

# CAPÍTULO III

# IV. RESULTADOS

## 4.1. SGSI para la empresa NET-Consultores S.A.C

Teniendo en cuenta el ciclo PDCA que permite realizar una serie de pasos y procesos para la construcción de un SGSI, a continuación se procede a realizar cada una de estas etapas:

### 4.1.1. Establecer el SGSI

#### 4.1.1.1. Alcance

Con el fin de mejorar la calidad en la prestación del servicio se aplica el SGSI a los procesos, recursos informáticos y tecnológicos que forman parte de la empresa NET-Consultores S.A.C, con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información, el cual debe ser aplicada y cumplida por todos los empleados de la organización.

#### 4.1.1.2. Política del sistemas de gestión

La empresa NET-Consultores S.A.C pretende que la información manejada por la entidad; esté debidamente protegida con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información, ya que es una entidad privada encargada de realizar consultorías de software.

La empresa NET-Consultores S.A.C es la responsable de la implementación de los requerimientos de seguridad con el fin de proteger la información por lo tanto en su organización se debe elaborar un análisis y evaluación del riesgo para gestionarlos adecuadamente y disminuir eventos indeseados.

#### 4.1.1.3. Metodología de Evaluación del Riesgo

Se elige la metodología Magerit para el análisis y gestión de los riesgos porque:

- Los pasos para su ejecución están claramente definidos.
- La documentación es clara, amplia y permite realizar una identificación adecuada del entorno donde va a ser aplicada.
- Permite enfocar los esfuerzos al análisis de riesgos críticos para la empresa, por lo tanto se puede trabajar más claramente en las posibles soluciones para dichos riesgos.
- Se puede decir que por estar incluida en los estándares ISO, sirve como punto de partida para procesos de certificación y mejoramiento del sistema de gestión para la empresa.
- Permite el análisis a riesgos, donde se identifican y valoran los diferentes componentes que pueden tener los riesgos.
- Permite la minimización de riesgos mediante la implementación de medidas de seguridad.
- MAGERIT le permita una empresa saber cuánto valor está en juego y le ayudará a protegerlo.
- Con MAGERIT los resultados de análisis de riesgos se pueden expresar en valores cualitativos y cuantitativos, lo que permite a los directivos tomar decisiones.

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

Paso 1: Inventario de Activos

Paso 2: Valoración de los activos

Paso 3: Amenazas (identificación y valoración)

Paso 4: Salvaguardias

Paso 5: Impacto residual y riesgo residual

#### 4.1.1.4. Análisis de riesgos de la empresa NET-Consultores S.A.C.

##### 4.1.1.4.1. Inventario de activos

Las empresas deben proteger la confidencialidad, integridad y disponibilidad de la información para velar por la continuidad del negocio independientemente de su actividad social. Para proteger dicha información de riesgos y amenazas la empresa NET-Consultores S.A.C realiza un inventario de sus activos y los clasificamos en los siguientes grupos.

**Tabla 7: Inventario de Activos de la Empresa NET – Consultores S.A.C**

| Activos | Código grupo activo Magerit | Nombre grupo Activo Magerit | Código Activo NET-Consultores | Nombre activo de acuerdo a la empresa |
|---|---|---|---|---|
| Activos Esenciales | [vr] | Datos vitales | [I_Proyectos] | Información de Proyectos radicados (base de datos y registro de proyectos ) |
| | | | [I_Licencias] | Información de Licencias |
| | | | [I_Normativa] | Información de Normativa ( Normas locales, nacionales, POT, acuerdos, decretos, Cartografía) |
| | [per] | Datos de Carácter Personal | [I_Contabilidad] | Contabilidad de la empresa |
| | [classified] | Datos clasificados | [D_Históricos] | Datos Históricos de proyectos realizados |
| | | | [D_Proyectos] | Documentación de proyectos. |

| | | | | |
|---|---|---|---|---|
| Datos o Información | [files] | Ficheros | [A_ proyectos] | Archivos de proyectos |
| | | | [A_ Clientes] | Archivos de Clientes |
| | | | [A_ Contabilidad] | Archivo de Contabilidad |
| | [backup] | Copias de Respaldo | [A_ Copias de Seguridad] | Archivo de Copias de seguridad de la información |
| | [conf] | Datos de configuración | [D_ Configuración _ser] | Datos de configuración de servidores y equipos |
| | [int] | Datos de gestión interna | [D_ Gestión Proyectos] | Datos de Gestión de proyectos |
| | [password] | Credenciales | [Pass_ usuarios] | Contraseñas de acceso de empleados |
| Claves Criptográficas | [encrypt] | Claves de cifra | [CC_ Aplicaciones_ bancarias] | Claves de cifra de aplicaciones bancarias |

| | | | | |
|---|---|---|---|---|
| Servicios | [ext] | A usuarios externos (bajo una elación contractual) | [S _ U _Externo] | Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos) |
| | [int] | Interno (a usuarios de la propia organización) | [S _ U _ Interno] | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. |
| | [www] | World wide web | [S _ Internet] | Servicio de internet al que pueden acceder los empleados. |
| | [email] | Correo electrónico | [S_ correo] | Manejo de correos electrónicos |
| | [file] | Almacenamiento de ficheros | [S_ A_ Basesde datos] | Servicio de almacenamiento de información en el servidor de bases de datos. |
| | [ipm] | Gestión de privilegios | [G_ privilegios] | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando. |

| | | | | |
|---|---|---|---|---|
| Aplicaciones de Software | [app] | Servidor de aplicaciones | [Server _App] | Servidor de aplicaciones |
| | [dbms] | Sistema de gestión de bases de datos | [S_ Base De Datos] | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. |
| | [Oficce] | Ofimática | [Office] | Office 2010 |
| | [av] | Antivirus | [Antivirus] | Kaspersky original con actualizaciones automáticas. |
| | [os] | Sistema operativo | [OS_Win7] | Sistema operativoWindows7, en su versión professional con actualización es automáticas activadas. |

| | | | | |
|---|---|---|---|---|
| Equipos Informáticos | [host] | Grandes equipos (Servidor de bases de datos, servidores de aplicación) | [S_ Aplicaciones] | Servidor Aplicaciones |
| | | | [S_ Data base] | Servidor de Base de Datos |
| | [mid] | Equipos medios (Equipos de trabajo conectados a través de red) | [PC_ trabajadores] | Equipos de mesa |
| | [pc] | Equipos que son fácilmente transportados | [PC_ portátiles] | Equipos Portátiles |
| | [print] | Equipos de impresión | [E_ Impresoras] | Impresoras |
| | [router] | Enrutadores | [R_ enrutadores] | Enrutadores |
| Personal | [ui] | Usuarios internos | [E_ personal] | Personal de gerencia, gestión, administrativa, desarrollo, diseño, documentación y seguridad y soporte |

| | | | | |
|---|---|---|---|---|
| Redes de Comunicación | [wifi] | Red inalámbrica | [R_ wifi] | Red Inalámbrica |
| | [LAN] | Red local | [R_ Local] | Red local |
| | [Internet] | Internet | [Internet] | Internet |
| Soportes de Información | [cd] | Discos | [A_CD] | Almacenamientos en Disco Duro |
| | [cd] | Cederrón (CD_ROM) | [A_CD] | Almacenamiento en CD |
| | [USB] | Memorias | [A_ Memorias] | Almacenamiento en Memorias |
| | [dvd] | DVR | [A_DVD] | Almacenamiento en DVD |
| | [printed] | Material impreso | C_ Documentación proyecto | Carpetas con la documentación de cada proyecto |
| | | | C_ Reportes e informes | Carpetas de reportes e informes impresos |
| | | | C_ Soportes Contabilidad | Carpetas facturas y soportes contabilidad |
| | | | C_ varios | Carpetas varios |

| | | | | |
|---|---|---|---|---|
| Equipamiento Auxiliar | [printed] | Sistemas de Alimentación ininterrumpida | U_ Computadores | Ups computadores |
| | [suplly] | Suministros Esenciales | Esenciales | Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc. |
| | [Furniture] | Mobiliario | M_ Mobiliario | Mobiliario: Estantes, armarios, escritorios, archivadores, etc. |
| Instalaciones | [building] | Edificio | [E_ empresa] | Edificio de la empresa (NET-Consultores) |

***Fuente: Elaboración propia***

#### 4.1.1.4.2. Valorización cualitativa de los activos

Teniendo en cuenta que todos los activos no tienen la misma relevancia e importancia para la empresa y que cada uno de estos en caso de ser atacado o sufrir un incidente genera un impacto diferente en la organización, se procede a realizar una valoración cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como confiabilidad, integridad y disponibilidad de acuerdo a la siguiente Tabla.

**Tabla 8: Escala de la variable independiente**

| Dimensión | Indicadores |
|---|---|
| **Confidencialidad** | **(0)** Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la empresa. |
| | **(1)** Información que puede ser conocida y utilizada por todos los agentes de la empresa. |
| | **(2)** Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo. |
| | **(3)** Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la empresa o terceros. |

| | |
|---|---|
| **Integridad** | **(0)**Información cuya modificación no autorizada puede repararse fácilmente. |
| | **(1)** Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para la empresa o terceros. |
| | **(2)** Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo. |
| | **(3)** Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades. |
| **Disponibilidad** | **(0)** Información cuya inaccesibilidad no afecta la actividad normal de la empresa. |
| | **(1)** Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la empresa. |
| | **(2)** Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la empresa. |
| | **(3)** Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la empresa. |

***Fuente: www.seguridadinformatica.unlu.edu.ar***

**Tabla 9: Valoración cualitativa de los Activos de NET-Consultores**

| Activos | Código grupo activo Magerit | Nombre grupo Activo Magerit | Código Activo NET-Consultores | Nombre activo NET-Consultores | Dimensión Seguridad | | |
|---|---|---|---|---|---|---|---|
| | | | | | Confidencialidad | Integridad | Disponibilidad |
| Activos Esenciales | [vr] | Datos vitales | [I_Proyectos] | Información de Proyectos radicados | 3 | 3 | 0 |
| | | | [I_Licencias] | Información de Licencias | 3 | 3 | 1 |
| | | | [I_Normativa] | Información de Normativa | 0 | 2 | 1 |
| | [per] | Datos de Carácter Personal | [I_Contabilidad] | Contabilidad de la empresa | 3 | 3 | 0 |
| | [classified] | Datos clasificados | [D_Históricos] | Datos Históricos de proyectos realizados | 2 | 2 | 0 |
| | | | [D_Proyectos] | Documentación de proyectos. | 0 | 0 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Datos o Información | [files] | Ficheros | [A_ proyectos] | Archivos de proyectos | 3 | 3 | 0 |
| | | | [A_ Clientes] | Archivos de Clientes. | 3 | 3 | 0 |
| | | | [A_ Contabilidad] | Archivo de Contabilidad. | 3 | 3 | 0 |
| | [backup] | Copias de Respaldo | [A_ Copias de Seguridad] | Archivo de Copias de seguridad de la información. | 0 | 3 | 0 |
| | [conf] | Datos de configuración | [D_ Configuración _ser] | Datos de configuración de servidores y equipos | 3 | 3 | 0 |
| | [int] | Datos de gestión interna | [D_ Gestión Proyectos] | Datos de Gestión de proyectos. | 0 | 0 | 1 |
| | [password] | Credenciales | [Pass_ usuarios] | Contraseñas de acceso de empleados. | 3 | 0 | 3 |
| Claves Criptográficas | [encrypt] | Claves de cifra | [CC_ Aplicaciones_ bancarias] | Claves de cifra de aplicaciones bancarias. | 3 | 3 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Servicios | [ext] | A usuarios externos (bajo una relación contractual) | [S_U_ Externo] | Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos). | 3 | 3 | 0 |
| | [int] | Interno (a usuarios de la propia organización) | [S_U_ Interno] | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | 3 | 3 | 0 |
| | [www] | World wide web | [S_ Internet] | Servicio de internet al que pueden acceder los empleados. | 3 | 3 | 0 |
| | [email] | Correo electrónico | [S_ correo] | Manejo de correos electrónicos. | 3 | 3 | 0 |
| | [file] | Almacenamiento de ficheros | [S_A_ Bases de datos] | Servicio de almacenamiento de información en el servidor de bases de datos. | 3 | 3 | 0 |
| | [ipm] | Gestión de privilegios | [G_ privilegios] | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando. | 3 | 3 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Aplicaciones de Software | [app] | Servidor de aplicaciones | [Server _App] | Servidor de aplicaciones | 3 | 3 | 0 |
| | [dbms] | Sistema de gestión de bases de datos | [S_ Base De Datos] | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 3 | 3 | 0 |
| | [Oficce] | Ofimática | [Office] | Office 2010 | 0 | 0 | 3 |
| | [av] | Antivirus | [Antivirus] | Kaspersky original con actualizaciones automáticas. | 3 | 0 | 1 |
| | [os] | Sistema operativo | [OS_Win7] | Sistema operativoWindows7, en su versión professional con actualizaciones automáticas activadas. | 0 | 0 | 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Equipos Informáticos | [host] | Grandes equipos (Servidor de bases de datos, servidores de aplicación) | [S_ Aplicaciones] | Servidor Aplicaciones | 3 | 3 | 1 |
| | | | [S_ Data base] | Servidor de Base de Datos | 3 | 3 | 1 |
| | [mid] | Equipos medios (Equipos de trabajo conectados a través de red) | [PC_ trabajadores] | Equipos de mesa | 3 | 3 | 0 |
| | [pc] | Equipos que son fácilmente transportados | [PC_ portátiles] | Equipos Portátiles | 3 | 3 | 0 |
| | [print] | Equipos de impresión | [E_ Impresoras] | Impresoras | 0 | 0 | 2 |
| | [router] | Enrutadores | [R_ enrutadores] | Enrutadores | 3 | 3 | 1 |
| Personal | [ui] | Usuarios internos | [E_ personal] | Personal de gerencia, gestión, administrativa, desarrollo, diseño, documentación y seguridad y soporte | 0 | 0 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Redes de Comunicación | [wifi] | Red inalámbrica | [R_ wifi] | Red Inalámbrica | 3 | 3 | 1 |
| | [LAN] | Red local | [R_ Local] | Red local | 3 | 3 | 1 |
| | [Internet] | Internet | [Internet] | Internet | 0 | 0 | 1 |
| Soportes de información | [cd] | Discos | [A_CD] | Almacenamientos en Disco Duro | 0 | 2 | 2 |
| | [cd] | Cederrón (CD_ROM) | [A_CD] | Almacenamiento en CD | 1 | 1 | 0 |
| | [USB] | Memorias | [A_ Memorias] | Almacenamiento en Memorias | 0 | 2 | 2 |
| | [dvd] | DVR | [A_DVD] | Almacenamiento en DVD | 0 | 2 | 2 |
| | [printed] | Material impreso | C_ Documentación proyecto | Carpetas con la documentación de cada proyecto | 0 | 3 | 0 |
| | | | C_ Reportes e informes | Carpetas de reportes e informes impresos | 0 | 3 | 0 |
| | | | C_ Soportes Contabilidad | Carpetas facturas y soportes contabilidad | 0 | 3 | 0 |
| | | | C_ varios | Carpetas varios | 0 | 3 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Equipamiento Auxiliar | [printed] | Sistemas de Alimentación ininterrumpida | U_ Computadores | Ups computadores | 0 | 0 | 2 |
| | [suplly] | Suministros Esenciales | Esenciales | Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc. | 0 | 0 | 3 |
| | [Furniture] | Mobiliario | M_ Mobiliario | Mobiliario: Estantes, armarios, escritorios, archivadores, etc. | 0 | 2 | 0 |
| Instalaciones | [building] | Edificio | [E_ empresa] | Edificio de la empresa (NET-Consultores) | 0 | 0 | 2 |

***Fuente: Elaboración propia***

#### 4.1.1.4.3. Identificación de Amenazas y valor de impacto

La valoración de amenazas se realiza teniendo en cuenta la frecuencia con la que ocurre, las dimensiones de seguridad según Magerit y la escala de rango porcentual de impactos en los activos.

**Tabla 10: Escala de la variable dependiente**

| Escala | Indicador | Valor | |
|---|---|---|---|
| | | Numérico | Porcentual |
| 1 | Poco frecuente, cada varios años | 10 | 10% |
| 2 | Normal, una vez al año | 50 | 50% |
| 3 | Frecuente, mensualmente | 70 | 70% |
| 4 | Muy frecuente A diario | 100 | 100% |

***Fuente: www.fing.edu.uy***

**Tabla 11: Escala porcentual del impacto**

| Impacto | Valor |
|---|---|
| 1) Muy alto | 75% - 100% |
| 2) Medio | 50% - 75% |
| 3) Bajo | 20% - 50% |
| 4) Muy Bajo | 0% - 20% |

***Fuente: www.fing.edu.uy***

En la siguiente tabla se procede a identificar las amenazas para el inventario de activos realizado. En algunos casos se toma los activos más críticos o la categoría, identificando su frecuencia e impacto.

**Tabla 12: Relación de amenazas por activo y su valor de impacto**

| Relación de amenazas por activo identificando su frecuencia e impacto | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Amenaza | Activo | Frecuencia de la amenaza antes de la implementación | Frecuencia de la amenaza después de la implementación | Probabilidad | Antes SGSI | | Después SGSI | |
| | | | | | Valor Impacto | Impacto | Valor Impacto | Impacto |
| [N.1] Fuego<br>[N.2] Daños por agua | Equipos informáticos<br>Instalaciones | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipos informáticos<br>Instalaciones | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |
| N.1] Fuego<br>[N.2] Daños por agua | Soporte de almacenamiento | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [I.1] Fuego<br>[I.2] Daños por agua | Soporte de almacenamiento | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| [N.1] Fuego<br>[N.2] Daños por agua | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [N.*] Desastres naturales | Equipos informáticos | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| | Instalaciones | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [I.*] Desastres industriales | Equipos informáticos, | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| | Instalaciones | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| [I.3] Contaminación mecánica | Equipos informáticos, | 0.7 | 0.7 | 0.9 | 0.63 | Medio | 0.63 | Medio |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [I.4] Contaminación electromagnética | Router de acceso inalámbrico. | 1 | 0.7 | 0.8 | 0.8 | Muy Alto | 0.56 | Medio |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [I.5] Avería de origen físico o lógico | Software - Aplicaciones Informáticas | 1 | 0.7 | 0.7 | 0.7 | Medio | 0.49 | Bajo |
| | Equipos informáticos | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |
| | Soportes de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [I.6] Corte del suministro eléctrico | Equipos Informáticos | 1 | 0.7 | 0.9 | 0.9 | Muy Alto | 0.63 | Medio |
| | Soporte de Información (electrónicos) | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Ups computadores | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [I.7] Condiciones inadecuadas de temperatura o humedad | Equipos Informáticos | 1 | 0.7 | 0.9 | 0.9 | Muy Alto | 0.63 | Medio |
| [I.8] Fallo de servicios de comunicaciones | Redes de comunicaciones (Red inalámbrica, red local e internet) | 1 | 0.7 | 0.8 | 0.8 | Muy Alto | 0.56 | Medio |
| [I.9] Interrupción de otros servicios y suministros esenciales. | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [I.10] Degradación de los soportes de almacenamiento de la información. | Soportes de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.1] Errores de los usuarios Datos/Información | Archivos de proyectos | 1 | 0.7 | 0.2 | 0.2 | Muy Bajo | 0.14 | Muy Bajo |
| | Archivos de Clientes | 0.5 | 0.1 | 0.2 | 0.1 | Muy Bajo | 0.02 | Muy Bajo |
| | Archivo de Contabilidad | 0.5 | 0.1 | 0.2 | 0.1 | Muy Bajo | 0.02 | Muy Bajo |
| | Archivos de Informes y licencias expedidas | 1 | 0.5 | 0.8 | 0.8 | Muy Alto | 0.4 | Bajo |
| | Archivo de Copias de seguridad de la información | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Datos de configuración de servidores y equipos | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Datos de Gestión de proyectos radicados | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Contraseñas de acceso de empleados | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.1] Errores de los usuarios | Claves Criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| [E.1] Errores de los usuarios Servicios | Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos) | 0.5 | 0.1 | 0.2 | 0.1 | Medio | 0.02 | Muy Bajo |
| | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | 0.5 | 0.1 | 0.2 | 0.1 | Medio | 0.02 | Muy Bajo |
| | Servicio de internet al que pueden acceder los empleados. | 0.7 | 0.5 | 0.5 | 0.35 | Bajo | 0.25 | Bajo |
| | Manejo de correos electrónicos | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Servicio de almacenamiento de información en el servidor de bases de datos. | 0.7 | 0.5 | 0.5 | 0.35 | Bajo | 0.25 | Bajo |
| | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo. | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.1] Errores de los usuarios Aplicaciones | Servidor de aplicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Office 2010 | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Kaspersky original con actualizaciones automáticas. | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas. | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| [E.1] Errores de los usuarios. Soporte de información | Soportes de Información. | 0.7 | 0.5 | 0.5 | 0.35 | Bajo | 0.25 | Bajo |
| [E.4] Errores de configuración | Datos de configuración de servidores y equipos | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.7] Deficiencias en la organización | Personal de recepción, área técnica, administrativa y archivo | 1 | 0.7 | 0.4 | 0.4 | Bajo | 0.28 | Bajo |
| | Administrador de sistemas | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [E.8] Difusión de software dañino | Software –Aplicaciones Informáticas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| [E.9] Errores de [re-]encaminamiento | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Software –Aplicaciones Informáticas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Redes de comunicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| [E.14] Escapes de información | Activos esenciales | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Datos / información | 0.5 | 0.1 | 1 | 0.5 | Bajo | 0.1 | Muy Bajo |
| [E.15] Alteración accidental de la información | Datos / información | 0.7 | 0.5 | 1 | 0.7 | Medio | 0.5 | Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.18] Destrucción de la información | Datos / información | 0.7 | 0.5 | 1 | 0.7 | Medio | 0.5 | Bajo |
| | Aplicaciones | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Soporte Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| [E.19] Fugas de información | Datos / información | 0.7 | 0.5 | 1 | 0.7 | Medio | 0.5 | Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Servicios | 0.7 | 0.5 | 0.6 | 0.42 | Bajo | 0.3 | Bajo |
| | Aplicaciones | 0.7 | 0.5 | 0.7 | 0.49 | Bajo | 0.35 | Bajo |
| | Personal | 0.7 | 0.5 | 0.4 | 0.28 | Bajo | 0.2 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.20] Vulnerabilidades de los programas (software) | Servidor de aplicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| | Office 2010 | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Kaspersky original con actualizaciones automáticas. | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | Servidor de aplicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| | Office 2010 | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| | Kaspersky original con actualizaciones automáticas. | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| [E.24] Caída del sistema por agotamiento de recursos | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Equipos Informáticos | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |
| | Redes de comunicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.25] Pérdida de equipos - Robo | Equipos Informáticos | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| | Soporte Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [E.28] Indisponibilidad del personal | Personal de recepción, área técnica, administrativa y archivo | 0.7 | 0.5 | 0.4 | 0.28 | Bajo | 0.2 | Muy Bajo |
| [A.5] Suplantación de la identidad del usuario | Datos / información | 0.5 | 0.1 | 1 | 0.5 | Bajo | 0.1 | Muy Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Aplicaciones | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Redes de comunicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.6] Abuso de privilegios de acceso | Datos / información | 0.5 | 0.1 | 1 | 0.5 | Bajo | 0.1 | Muy Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Equipos Informáticos | 1 | 0.7 | 0.9 | 0.9 | Muy Alto | 0.63 | Medio |
| | Redes de comunicaciones | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| [A.7] Uso no previsto | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Aplicaciones | 0.7 | 0.5 | 0.7 | 0.49 | Bajo | 0.35 | Bajo |
| | Equipos Informáticos | 1 | 0.7 | 0.9 | 0.9 | Muy Alto | 0.63 | Medio |
| | Redes de comunicaciones | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| | Instalaciones | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.8] Difusión de software dañino | Aplicaciones | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| [A.11] Acceso no autorizado | Datos / información | 0.7 | 0.5 | 1 | 0.7 | Medio | 0.5 | Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Aplicaciones | 0.7 | 0.5 | 0.7 | 0.49 | Bajo | 0.35 | Bajo |
| | Equipos Informáticos | 0.7 | 0.5 | 0.9 | 0.63 | Medio | 0.45 | Bajo |
| | Redes de comunicaciones | 0.7 | 0.5 | 0.8 | 0.56 | Medio | 0.4 | Bajo |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| | Instalaciones | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| [A.13] Repudio | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| [A.14] Interceptación de información (escucha pasiva) | Redes de comunicaciones | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.15] Modificación deliberada de la información | Datos / información | 0.5 | 0.1 | 1 | 0.5 | Bajo | 0.1 | Muy Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Servicio | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Aplicaciones | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| [A.18] Destrucción de información | Datos / información | 0.5 | 0.1 | 1 | 0.5 | Bajo | 0.1 | Muy Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Aplicaciones | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |
| | Soporte de la información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| [A.19] Divulgación de información | Datos / información | 0.7 | 0.5 | 1 | 0.7 | Medio | 0.5 | Bajo |
| | Claves criptográficas | 0.5 | 0.1 | 0.7 | 0.35 | Bajo | 0.07 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Soporte de la información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| [A.22] Manipulación de programas | Aplicaciones | 0.7 | 0.5 | 0.7 | 0.49 | Bajo | 0.35 | Bajo |
| [A.23] Manipulación de los equipos | Equipos Informáticos | 1 | 0.7 | 0.9 | 0.9 | Muy Alto | 0.63 | Medio |
| | Soportes de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [A.24] Denegación de servicio | Equipos Informáticos | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| | Servicios | 0.5 | 0.1 | 0.6 | 0.3 | Bajo | 0.06 | Muy Bajo |
| | Redes de Comunicación | 0.5 | 0.1 | 0.8 | 0.4 | Bajo | 0.08 | Muy Bajo |
| [A.25] Robo | Equipos informáticos | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.26] Ataque destructivo | Equipo Informáticos | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| | Soporte de Información | 0.5 | 0.1 | 0.5 | 0.25 | Bajo | 0.05 | Muy Bajo |
| | Equipamiento Auxiliar | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| | instalaciones | 0.5 | 0.1 | 0.9 | 0.45 | Bajo | 0.09 | Muy Bajo |
| [A.28] Indisponibilidad del Personal | Personal | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [A.29] Extorsión | Personal | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |
| [A.30] Ingeniería Social | Personal | 0.5 | 0.1 | 0.4 | 0.2 | Muy Bajo | 0.04 | Muy Bajo |

***Fuente: Elaboración Propia***

Como podemos observar el impacto de los riesgos en el pre test y en el pos test demostrando hay una variación significativa para cada riesgo asociado a un activo; de donde podemos demostrar que la implementación de un sistema de gestión de seguridad de la información influye significativamente sobre el impacto de los riesgos asociados a los activos de información en la empresa.

#### 4.1.1.4.4. Salvaguardas

Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definen las salvaguardas que son procedimiento tecnológico que reduce el riesgo, de acuerdo a los activos que se van proteger, en este caso se tiene en cuenta las salvaguardas definidas en Magerit.

**Tabla 13: Tipos de salvaguardas Magerit**

| Efecto | Tipo |
|---|---|
| Preventivas: reducen la probabilidad | [PR] preventivas<br>[DR] disuasorias<br>[EL] eliminatorias |
| Acotan la degradación | [IM] dinamizadoras<br>[CR] correctivas<br>[RC] recuperativas |
| Consolidan el efecto de las demás | [MN] de monitorización<br>[DC] de detección<br>[AW] de concienciación<br>[AD] administrativas |

***Fuente: Magerit V 3.0 Libro 1***

**Tabla 14: Salvaguarda de Activos Esenciales**

| Activos | Código grupo activo Magerit | Nombre grupo Activo Magerit | Código Activo NET-Consultores | Nombre activo NET-Consultores | Tipo Protección | Des. Salvaguarda |
|---|---|---|---|---|---|---|
| Activos esenciales | [vr] | Datos vitales | [I_Proyectos] | Información de Proyectos radicados | PR | Políticas de seguridad para el personal |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan Director |
| | | | | | EL | Gestión de contraseñas |
| | | | [I_Licencias] | Información de Licencias | PR | Políticas de seguridad para el personal |
| | | | | | RC | Copias de Seguridad de los archivos de licencias |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan Director |
| | | | | | EL | Gestión de contraseñas |
| | | | [I_Normativa] | Información de Normativa | PR | Políticas de seguridad para el personal |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan Director |

| | | | | | | |
|---|---|---|---|---|---|---|
| Activos esenciales | [per] | Datos de Carácter Personal | [I_Contabilidad] | Contabilidad de la empresa | PR | Políticas de seguridad para el personal que tiene acceso a la información |
| | | | | | RC | Copias de Seguridad de la información de contabilidad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan Director |
| | [classified] | Datos clasificados | [D_Históricos] | Datos Históricos de proyectos realizados | PR | Políticas de seguridad para el personal |
| | | | | | RC | Copias de Seguridad de datos históricos guardadas en sitios seguros |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan Director |
| | | | [D_Proyectos] | Documentación de proyectos. | PR | Políticas de seguridad para el personal |
| | | | | | RC | Copias de Seguridad de datos históricos guardadas en sitios seguros |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan Director |
| | | | | | PR | Políticas de seguridad para el personal |
| | | | | | PR | Políticas de seguridad para el personal. Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |

| | | | | | | |
|---|---|---|---|---|---|---|
| Activos esenciales | [classified] | Datos clasificados | [A_ Clientes] | Archivos de Clientes | PR | Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |
| | | | [A_ Contabilidad] | Archivo de Contabilidad | PR | Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |
| | | | [A_ Copias de Seguridad] | Archivo de Copias de seguridad de la información | PR | Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |

| | | | | | | |
|---|---|---|---|---|---|---|
| Activos esenciales | [conf] | Datos de configuración | [D_ Configuración _ser] | Datos de configuración de servidores y equipos | PR | Políticas de seguridad para el personal que tiene ACCESO A LA INFORMACIÓN. |
| | | | | | | Gestión de privilegios. |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |
| | [int] | Datos de gestión interna | [D _ Gestión Proyectos] | Datos de Gestión de proyectos | PR | Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |
| | [password] | Credenciales | [Pass _ usuarios] | Contraseñas de acceso de empleados | PR | Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | | | | | EL | Gestión de contraseñas |

| | | | | | | |
|---|---|---|---|---|---|---|
| Claves criptográficas | [encrypt] | Claves de cifra | [CC_ Aplicaciones _ bancarias] | Claves de cifra de aplicaciones bancarias | PR | Clasificación y Encriptación de la información |
| | | | | | | Gestión de privilegios. |
| | | | | | IM | Detención del servicio en caso de ataque. |
| | | | | | MN | Gestión de incidentes. |
| | | | | | DC | Registro de descarga. |
| | | | | | DC | Activación de IDS y Firewall, software de monitorización y escaneo, manejo de antivirus. |
| Servicios | [ext] | A usuarios externos(bajo una relación contractual) | [S _ U _ Externo] | Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos) | PR | Clasificación de la información en este caso catalogada como confidencial. |
| | | | | | | Políticas de seguridad, Gestión de privilegios. |
| | | | | | RC | Copias de Seguridad. |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Servicios | [int] | Interno (a usuarios de la propia organización) | [S _ U _ Interno] | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | PR | Clasificación de la información en este caso catalogada como confidencial. |
| | | | | | | Políticas de seguridad, Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |
| | [www] | World wide web | [S _ Internet] | Servicio de internet al que pueden acceder los empleados. | MN | Registro de descarga |
| | | | | | PR | Clasificación de la información en este caso catalogada como confidencial. |
| | | | | | | Políticas de seguridad, Gestión de privilegios |
| | | | | | RC | Copias de Seguridad |
| | | | | | AW | Capacitación al personal en el manejo de la información. |
| | | | | | AD | Puesta en marcha del Plan |

| | | | | | | |
|---|---|---|---|---|---|---|
| Servicios | [email] | Correo electrónico | [S _ correo] | Manejo de correos electrónicos | MN | Registro de descarga. |
| | | | | | | Clasificación de la información en este caso catalogada como confidencial. |
| | | | | | PR | Políticas de seguridad, Gestión de privilegios |
| | | | | | | Copias de Seguridad |
| | | | | | RC | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Registro de descarga |
| | [file] | Almacenamiento de ficheros | [S _ A _ Bases de datos] | Servicio de almacenamiento de información en el servidor de bases de datos. | MN | Clasificación de la información en este caso catalogada como confidencial. |
| | | | | | PR | Políticas de seguridad, Gestión de privilegios |
| | | | | | | Copias de Seguridad |
| | | | | | RC | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Clasificación de la información en este caso catalogada como confidencial. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Servicios | [ipm] | Gestión de privilegios | [G _ privilegios] | Manejo de privilegios. | PR | Políticas de seguridad, Gestión de privilegios. |
| | | | | | | Copias de Seguridad |
| | | | | | RC | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Eliminación de cuentas sin contraseña |
| | | | | | EL | Políticas de seguridad, Gestión de privilegios |
| Aplicaciones de Software | [app] | Servidor de aplicaciones | [Server _ App] | Servidor de aplicaciones | PR | Clasificación de la información en este caso catalogada como confidencial |
| | | | | | PR | Copias de Seguridad |
| | | | | | RC | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Activación de IDS y Firewall, software de monitorización y escaneo, manejo de antivirus. |
| | [dbms] | Sistema de gestión de bases de datos | [S_ Base De Datos] | Gestor base de datos. | DC | Políticas de seguridad, Gestión de privilegios |
| | | | | | PR | Capacitación al personal |
| | | | | | AW | Registro de uso y descarga |
| | | | | | MN | Eliminación de cuentas sin contraseña |
| | | | | | EL | Capacitación al personal en el manejo de la información. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Aplicaciones de Software | [Office] | Ofimática | [Office] | Office 2010 | AW | Registro de uso y descarga |
| | | | | | MN | Eliminación de cuentas sin contraseña |
| | | | | | EL | Políticas de seguridad, Gestión de privilegios |
| | | | | | PR | Capacitación al personal en el manejo de la información. |
| | [av] | Antivirus | [Antivirus] | Kaspersky original | AW | Registro de uso y descarga |
| | | | | | MN | Eliminación de cuentas sin contraseña |
| | | | | | EL | Políticas de seguridad, Gestión de privilegios |
| | | | | | PR | Capacitación al personal en el manejo de la información. |
| | [os] | Sistema operativo | [OS_Win7] | Sistema operativo Windows con actualizaciones automáticas | AW | Registro de uso y descarga. |
| | | | | | MN | Eliminación de cuentas sin contraseña |
| | | | | | EL | Políticas de seguridad, Gestión de privilegios |
| | | | | | PR | Políticas de seguridad, Gestión de privilegios |

| | | | | | | |
|---|---|---|---|---|---|---|
| Equipos informáticos | [host] | Grandes equipos (Servidor de bases de datos, servidores de aplicación) | [S_ Aplicaciones] | Servidor Aplicaciones | PR | Eliminación de cuentas sin contraseña |
| | | | | | EL | Detención del servicio en caso de ataque |
| | | | | | IM | Gestión de incidentes |
| | | | | | CR | Registro descarga, registro acceso |
| | | | | | MN | Activación de Firewall, software de monitorización y escaneo, manejo de antivirus |
| | | | | | DC | Capacitación al personal en el manejo. |
| | | | | | AW | Políticas de seguridad, Gestión de privilegios |
| | | | [S_ Data base] | Servidor de Base de Datos | PR | Eliminación de cuentas sin contraseña |
| | | | | | EL | Detención del servicio en caso de ataque |
| | | | | | IM | Gestión de incidentes |
| | | | | | CR | Registro de descarga, registro de acceso |
| | | | | | MN | Activación de Firewall, software de monitorización y escaneo, manejo de antivirus |
| | | | | | DC | Capacitación al personal en el manejo. |
| | | | | | AW | Activación de IDS y Firewall, manejo de antivirus |

| | | | | | | |
|---|---|---|---|---|---|---|
| Equipos informáticos | [mid] | Equipos medios | [PC_ trabajadores] | Equipos de mesa | DC | Políticas de seguridad, Gestión de privilegios |
| | | | | | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Copias de Seguridad |
| | | | | | RC | Eliminación de cuentas sin contraseña |
| | | | | | EL | Gestión de incidentes |
| | | | | | CR | Activación de IDS y Firewall, manejo de antivirus |
| | [pc] | Equipos que son fácilmente transportados | [PC_ portátiles] | Equipos Portátiles | DC | Políticas de seguridad, Gestión de privilegios |
| | | | | | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Copias de Seguridad |
| | | | | | RC | Eliminación de cuentas sin contraseña |
| | | | | | EL | Gestión de incidentes |
| | | | | | CR | Políticas de seguridad. |
| | [print] | Equipos de impresión | [E_ Impresoras] | Impresoras | PR | Gestión de incidentes |
| | | | | | CR | Políticas de seguridad, Gestión de privilegios |

| | | | | | | |
|---|---|---|---|---|---|---|
| Equipos informáticos | [router] | Enrutadores | [R_ enrutadores] | Enrutadores | PR | Detención del servicio en caso de ataque |
| | | | | | IM | Gestión de incidentes |
| | | | | | CR | Registro de descarga, registro de acceso |
| | | | | | MN | Activación de Firewall, software de monitorización y escaneo, manejo de antivirus |
| | | | | | DC | Cursos de capacitación y entrenamiento |
| Personal | [ui] | Usuarios internos | [E_ personal] | Personal de las áreas de la empresa | AW | Puesta en marcha del Plan |
| | | | | | AD | Políticas de seguridad, Gestión de privilegios |
| Redes de comunicación | [wifi] | Red inalámbrica | [R_ wifi] | Red Inalámbrica | PR | Detención del servicio en caso de ataque |
| | | | | | IM | Gestión de incidentes |
| | | | | | CR | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad, Gestión de privilegios |
| | [LAN] | Red local | [R_ Local] | Red local | PR | Detención del servicio en caso de ataque |
| | | | | | IM | Gestión de incidentes |
| | | | | | CR | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad, Gestión de privilegios |

| | | | | | | |
|---|---|---|---|---|---|---|
| Redes de comunicación | [Internet] | Internet | [Internet] | Internet | PR | Detención del servicio en caso de ataque |
| | | | | | IM | Gestión de incidentes |
| | | | | | CR | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad para el personal que tiene acceso a la información |
| Soportes de información | [cd] | Discos | [A_CD] | Almacenamientos en Disco Duro | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas seguridad para personal que tiene acceso a información. |
| | [cd] | Cederrón (CD_ROM) | [A_CD] | Almacenamiento en CD | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad para el personal que tiene acceso a la información |

| | | | | | | |
|---|---|---|---|---|---|---|
| Soportes de información | [USB] | Memorias | [A_ Memorias] | Almacenamiento en Memorias | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad para el personal que tiene acceso a la información |
| | [dvd] | DVR | [A_DVD] | Almacenamiento en DVD | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas seguridad para personal que tiene acceso a la información |
| | [printed] | Material impreso | C_ Documentación proyecto | Carpetas con la documentación de cada proyecto | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan Director |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas seguridad para el personal que tiene acceso a la información |

| | | | | | | |
|---|---|---|---|---|---|---|
| Soportes de información | [printed] | Material impreso | C_ Reportes e informes | Carpetas de reportes e informes impresos | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan Director |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad para el personal que tiene acceso a la información |
| | | | C_ Soportes Contabilidad | Carpetas facturas y soportes contabilidad | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan Director |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas seguridad para personal que tiene acceso a la información |
| | | | C_ varios | Carpetas varios | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan Director |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas seguridad para personal que tiene acceso a la información |

| | | | | | | |
|---|---|---|---|---|---|---|
| Equipamiento auxiliar | [printed] | Sistemas de Alimentación ininterrumpida | U_ Computadores | Ups computadores | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad para el personal que tiene acceso a la información |
| Equipamiento auxiliar | [suplly] | Suministros Esenciales | Esenciales | Suministros esenciales | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan Director |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Políticas de seguridad para el personal que tiene acceso a la información |
| | [Furniture] | Mobiliario | M_ Mobiliario | Mobiliario | PR | Capacitación al personal en el manejo de la información. |
| | | | | | AW | Puesta en marcha del Plan Director |
| | | | | | AD | Guardias de seguridad |
| | | | | | DR | Alarma de seguridad |
| Instalaciones | [building] | Edificio | [E_ empresa] | Edificio de la empresa | DR | Detección de Incendios |

***Fuente: Elaboración propia***

#### 4.1.1.4.5. Informe de Calificación del Riesgo

Teniendo en cuenta el análisis de riesgos se puede observar que existen activos la Empresa NET-Consultores que presentan riesgos catalogados como críticos y su probabilidad de frecuencia es alta tal es el caso de los equipos informáticos, datos e información, este riesgo puede generar pérdida de la información, divulgación de la información confidencial, daño en equipos y servidor, manipulación y daños en la base de datos, propagación de virus y el cese de actividades de la empresa.

Referente a los activos de redes de comunicaciones (routers de acceso inalámbrico), software y aplicaciones informáticas también se puede decir que el riesgo es catalogado como crítico, el cual puede ser causado por errores de usuarios y de administrador; de allí la importancia de establecer políticas de seguridad encaminadas a proteger los activos de la organización y minimizarlos riesgos para que en caso de presentarse el impacto sea mínimo.

Condiciones inadecuadas de temperatura y humedad, corte del suministro eléctrico, avería de orden físico y lógico y amenazas como manipulación no autorizada de equipos puede ocasionar daños en las aplicaciones, en el servidor y los equipos que pueden originar pérdida de información vital.

Deficiencias en la organización, abuso de privilegios de acceso y uso no previsto son amenazas que se deben de tener en cuenta ya que de acuerdo al análisis de riesgos están catalogadas como importantes y pueden ocasionar grandes daños a la empresa.

Por otra parte los impactos generados por los desastres naturales como fuego e inundaciones son críticos en el caso de que se llegasen a presentar afortunadamente la posibilidad de que ocurra es muy baja, esto no quiere decir que no se deba de tener en cuenta al contrario también se debe considerar como una posibilidad y se debe establecer políticas y medidas de seguridad encaminadas a minimizar cada riesgo.

En este orden de ideas los activos con mayor necesidad de ser protegidos son: Equipos informáticos, datos e información, software y aplicaciones, redes de comunicación puesto que son vulnerables y blanco fácil de los atacantes.

De que se los debe proteger: Del uso no previsto, del abuso de privilegios, fallos en los servicios de comunicaciones, errores de usuarios y administradores del sistema, condiciones inadecuadas de seguridad, contaminación electromagnética y mecánica etc.

Como se los debe proteger: Definiendo e implementando políticas de seguridad que permitan capacitar al usuario y al administrador en el manejo y clasificación de la información, gestión de contraseñas, control de acceso, implementación de equipos y software que

permitan mejorar la seguridad, seguridad física y lógica, actualizaciones permanentes del software, elaboración permanente de backups. Etc.

#### 4.1.1.4.6. ¿Cómo quedarían reducidos los riesgos de seguridad a los que está expuesta NET-Consultores?

Una vez realizado el análisis de riesgos para los activos de la empresa NET-Consultores y teniendo en cuenta los resultados obtenidos, se procede a especificar las políticas y objetivos de la seguridad del área de informática, teniendo como guía la norma ISO/IEC-27002.

Políticas y controles que se definen y se pretender implementar en la empresa con el fin de minimizar los riesgos encontrados.

**a) Políticas y objetivos de seguridad del área de informática.**

**Generalidades:**

La información actualmente es considerada como uno de los activos más importante de una empresa por lo tanto se puede decir que la seguridad de la misma es un pilar fundamental que contribuye al logro de la misión y cumplimiento de los objetivos en este caso de la empresa NET-Consultores S.A.C que es prestar un servicio eficiente y de calidad en consultoría de software.

**Objetivo:**

Definir políticas de seguridad para la empresa NET-Consultores, que sirvan como estrategias

de apoyo para lograr disminuir riesgos, evitar incidentes, mantener la confidencialidad, brindar un servicio eficiente y de calidad, manteniendo permanentemente una excelente imagen empresarial.

**Alcance:**

Esta política se debe aplicar a todas las áreas de la empresa.

**Responsables:**

La responsabilidad de la seguridad de la información está a cargo de la empresa, seguida por el responsable de la seguridad y el responsable del mantenimiento y todo el equipo de trabajo; es decir todos los empleados que hacen parte de la organización.

Para la aplicación de estas políticas de seguridad la empresa debe designar un responsable de seguridad informática y tendrá las siguientes funciones:

- Aprobación de las políticas de seguridad, monitorear riesgos y amenazas, plantear modificaciones en las políticas de seguridad, velar y controlar que sean cumplidas por todos los empleados de la empresa.

- Practicar auditorias periódicas sobre el manejo de los sistemas de información y la aplicación de las políticas de seguridad, estas deben estar debidamente documentas y son las responsables de encontrar fallas y brindar soluciones para corregir dichas fallas.

- Documentación, mantenimiento, actualización y gestión de políticas de seguridad para todos los recursos tecnológicos de la organización (Hardware, software, red, servidores etc).

- Clasificar la información de acuerdo a su grado de confidencialidad y definir los permisos de acceso a los usuarios.

- Divulgar las políticas de seguridad y la obligatoriedad del cumplimiento de las mismas por todos los empleados de la empresa.

- Cumplimiento de todas las políticas de seguridad en todos los contratos laborales.

- Conocer y cumplir con todos los requerimientos y políticas de seguridad estipuladas por la empresa y encargado de contribuir con la confidencialidad, disponibilidad e integridad de la información.

**Política:**

Esta política define aspectos específicos y pautas sobre la seguridad en la empresa tales como:

- Organización de la seguridad:

  Su objetivo es guiar la administración y dirección de la seguridad para su posterior implementación.

- Clasificación y Control de Activos:

  Su objetivo es clasificar jerárquicamente los activos de la organización y protegerlos de manera apropiada.

- Control de Acceso:

  Su objetivo es controlar y restringir el acceso a la información que es vital para la organización o es catalogada como confidencial.

- Desarrollo y mantenimiento de los sistemas:

  Su objetivo es implementar medidas de seguridad en el desarrollo (confidencialidad, copias de seguridad, acceso restringido), implementación y mantenimiento de los sistemas de información.

- Administrador de Operaciones:

  Su objetivo es contrarrestar las interrupciones en los procesos productivos, solucionar fallas y desastres.

- Seguridad de los usuarios:

  Su objetivo es reducir el riesgo que generan los errores humanos y también velar por la buena utilización de las instalaciones. (Capacitación permanente y adecuada para disminuir errores producidos por un manejo incorrecto o por desinformación).

- Seguridad Física:

  Su objetivo es impedir el acceso no autorizado y evitar daños y robos en la empresa. (Proteger la empresa).

- Cumplimiento:

  Su objetivo es hacer cumplir las políticas de seguridad anteriormente establecidas y hacer cumplir las obligaciones establecidas por las leyes, el reglamento, los contratos e imponer sanciones por incumplimiento de las mismas.

- Recursos:

  La empresa NET-Consultores cada año debe disponer de un rubro destinado a la seguridad de la información.

**b) Organización de la Seguridad de la Información**

**Generalidades:**

Establecer la seguridad de la información como una de los objetivos vitales para la Empresa.

**Objetivo:**

Organizar, controlar y administrar la información dentro de la organización.

**Alcance:**

Esta política se debe aplicar a todos los procesos de la empresa NET-Consultores tanto internos como externos.

**Responsables:**

La responsabilidad de la organización de seguridad de la información está a cargo de la empresa y todos sus miembros.

Para la organización de seguridad de la información la empresa debe designar un responsable y tendrá las siguientes funciones:

- Desarrollar la implementación de las políticas de seguridad. Se encargara de realizar seguimiento, monitoreo, análisis de riesgo, implementación de controles, velar por la continuidad y hacer conocer de los avances, cambios y dificultades a la dirección general.
- Dirigir la implementación de políticas de seguridad con la asesoría de profesionales especializados, e implementar medidas de seguridad como la restricción del acceso a la información que sea catalogada como confidencial.
- Revisar la vigencia y el cumplimiento de las políticas de seguridad.
- Destinar y disponer de recursos necesario para la adquisición de elementos necesarios para el cumplimiento de dichas políticas (Hardware, software, elementos de logística, asesoría especializada).
- Informar a proveedores, y equipo de trabajo sobre las modificaciones en las políticas de seguridad.

**Política**

- Infraestructura de la seguridad de la información:

Designar a un responsable de la seguridad de la información que garantice el apoyo a la implementación de todas las medidas de seguridad.

- Funciones del encargado de la seguridad:
  - Revisar y proponer políticas de seguridad al director general.
  - Monitorear e identificar cambios que generen riesgos para la organización.
  - Identificar amenazas y posibles vulnerabilidades.
  - Documentar y monitorear los incidentes concernientes a la seguridad.
  - Evaluar las posibles soluciones y elegir la más adecuada encaminada a contribuir con la seguridad de la información.
  - Asegurase de que la seguridad haga parte del proceso de planificación de la organización.
  - Determinar y organizar la implementación de controles de seguridad.

- Asignación de responsabilidades para la seguridad de la información:

  La empresa asigna las funciones referentes a la seguridad informática al responsable encargado de la seguridad quien de ahora en adelante será el directo garante de la seguridad de la información de la empresa y responsable del cumplimiento de lo tratado en la presente política.

- Proceso de autorización para los servicios de procesamiento de información:

  Los nuevos servicios de procesamiento de información deben ser autorizados previamente por el responsable de la seguridad de la información y deben ser autorizados para el usuario apropiado; de igual manera al implementar hardware y software se debe verificar que sean compatibles con el sistema actual e identificar e implementar controles de seguridad para portátiles y computadores personales nuevos que ingresan a la empresa.

- Acuerdos sobre confidencialidad:

  Identificar y revisar con regularidad los requisitos de confidencialidad (suscribir contratos de confidencialidad y no divulgación para la protección de la información vital para la empresa.), que deben ser encaminados a proteger la información legalmente, para lo cual se debe tener en cuenta la clasificación de la información, en este caso se debe

proteger la información confidencial, se debe definir por cuánto tiempo se va a proteger y designar un responsable para hacer buen uso de esta.

- Contactos con las especialistas:

  La empresa debe mantener contactos adecuados con las autoridades que especializadas en seguridad y delitos informáticos para comunicarse de manera inmediata en caso de ser necesario. (Saber cuándo y a quién dirigirse en caso de incidentes).

- Contactos con grupos de interés especiales:

  Los responsables de la seguridad deben estar en contacto permanente con foros y empresas especializadas en seguridad ya que estos están a la vanguardia de las nuevas formas de ataque.

- Revisión independiente de la seguridad de la información:

  El encargado de la seguridad se encargara de realizar revisiones independientes para garantizar el cumplimiento de las políticas de seguridad. El responsable debe informar las fallas encontradas y de las mejoras y cambios que son necesarios implementarse. (La revisión la deben realizar profesionales idóneos o expertos en seguridad, de ser necesario se debe contratar personal externo para realizar dicha revisión).

- Partes externas y coordinación de la seguridad de la información:

  Se debe controlar todo acceso a los servicios, comunicación, procesamiento de la información y comunicación que provienen de partes externas así:

  - Se debe definir un convenio con la parte externa para compartir información.
  - Se deben identificar los riesgos provenientes de las partes externas e implementar controles adecuados antes de autorizar el acceso.
  - Identificar los servicios de los que va disponer la parte externa.
  - Definir el tipo de acceso que va a tener la parte externa: ya sea acceso físico, acceso lógico, acceso a la red etc.
  - Identificar el valor y la sensibilidad de la información a la que van a tener acceso.
  - Implementar controles necesarios para proteger la información de terceros.
  - Conocer los controles y medidas que implementara la parte externa para el manejo y uso de la información.
  - Definir unos requisitos legales que está obligada a cumplir la parte externa.
  - para compartir información y servicios.

- Establecer y definir posibles medidas de contingencia en caso de fallos, errores, ataques etc.

- Todo servicio con terceros se debe hacer mediante contrato y en cada contrato se deben definir claramente las obligaciones, las políticas de seguridad y las implicaciones legales en caso de incumplimiento.

Estas medidas deben ser tomadas para: Proveedores de servicios de red, de internet, de telefonía, de mantenimiento, de soporte, de auditoría, de gestión, de negocios, personal de trabajo temporal, clientes etc.

**c) Gestión de Activos**

**Generalidades:**

Una vez realizado el inventario de activos y la evaluación de riesgos se clasifican los activos de acuerdo a su sensibilidad y vulnerabilidad.

**Objetivo:**

Clasificar la información de acuerdo a su grado de confidencialidad, definir niveles de protección y garantizar que los activos de la organización sean protegidos de manera adecuada.

**Alcance:**

Esta política se debe aplicar a todos los activos de la organización.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encarga de:

- Clasificar la información de acuerdo a su grado de confidencialidad, mantener actualizada y documentada la clasificación y de definir los permisos de acceso a los usuarios. Cada dependencia debe supervisar que la clasificación y rotulado de la información sea correcto.

**Política**

- Inventario de Activos:

  Se realiza un inventario de activos los cuales debe estar debidamente clasificados y ordenados según su importancia, propietario, ubicación e información almacenada, este inventario debe ser actualizado constantemente y conservarse de manera ordenada.

- Clasificación de la información: Para clasificar la información de deben tener en cuenta los criterios básicos de seguridad.

- Rotulado de la información:

  Definir procedimientos de rotulado, almacenamiento y físico y electrónico de la información de acuerdo a su Nivel De Criticidad.

**d) Seguridad de los recursos humanos**

**Generalidades:**

Es fundamental educar y concienciar al personal sobre la importancia de la aplicación de las políticas de seguridad, desde el primer instante que se ingresa a la empresa y de las sanciones que conlleva el incumplimiento de las mismas. Por lo tanto es importante que el personal este consiente de la importancia, esté capacitado y en caso de ocurrir un incidente informar en qué condiciones ocurrió para establecer mecanismos que conduzcan a que dichas fallas o incidentes no vuelvan a ocurrir y establecer los correctivos necesarios.

**Objetivo:**

Minimizar los riesgos ocasionados por errores humanos y promover un uso adecuado de los recursos informáticos así como capacitar y concienciar sobre la importancia de la aplicación de las políticas de seguridad e información oportuna de incidentes para ser corregidos en debida forma.

**Alcance:**

Esta política se debe aplicar a todo el personal de la organización, interno y externo.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encarga de:

- Informará, capacitara y establecerá acuerdos de confidencialidad y de cumplimiento de todas las políticas de seguridad con el personal que ingrese a la empresa.

- Establecer términos y condiciones laborales. Mediante cláusulas en los contratos los acuerdos de confidencialidad y cumplimiento de políticas de seguridad con todo el personal y con terceros.

- Capacitar y concienciar al personal con asesoría de profesionales especializados, sobre el uso correcto de los recursos informáticos y el cumplimiento de las políticas de seguridad así como del acuerdo de confidencialidad.

**Política**

- Antes de la contratación Laboral:

  La organización antes de la contratación laboral debe documentar los roles y responsabilidades que estos van a desempeñar.

  En la selección del personal se debe revisar antecedentes (hoja de vida, experiencia laboral, experiencia crediticia etc.). Se debe seleccionar y clasificar que información va estar disponible para estos tanto para personal como para terceros.

**Términos y condiciones laborales:**

Tanto para empleados como para terceros estos deben conocer los términos y las condiciones del contrato laboral haciendo énfasis en los aspectos relativos a la seguridad, la confidencialidad y se debe verificar que los contratos estén firmados. (El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento).

- Durante la Vigencia del contrato:

  La dirección debe exigir que los empleados y terceras partes cumplan a cabalidad con las políticas de seguridad establecidas por la empresa. Para esto debe darles a conocer las políticas de seguridad, motivarlos y verificar que estén de acuerdo con los términos y condiciones establecidas en el contrato laboral.

**Capacitación y formación:**

La organización capacitara e informara sobre las políticas de seguridad establecidas en la organización, así mismo capacitara e informara cuando se presenten cambios y modificaciones.

La capacitación al personal y a terceras partes se realizara por personal especializado de la organización que resalte la importancia del cumplimiento de las políticas de seguridad y les enseñe como detectar posibles fallas e incidentes y les explique cómo comunicar estas fallas a la organización.

La organización lleva a cabo verificaciones del cumplimiento de las obligaciones en los puestos de trabajo.

**El empleado debe someterse a:**

Cumplir con el control y la política de seguridad, formar y cumplir el compromiso de confidencialidad, cumplir los términos y condiciones del contrato, capacitarse, comunicar sobre incidentes y anomalías.

Para el personal y terceras partes que violen o incumplan las políticas de seguridad se llevara a cabo un proceso disciplinario de acuerdo a los estatutos de la empresa.

- Terminación o Cambio del contrato laboral: La organización gestiona de manera adecuada la terminación del contrato o cambio de contrato y una vez terminado el contrato verifica la suspensión de los servicios, la devolución de los activos, devolución de documentos, dispositivos (pc, celulares, usb, etc), verifica y gestiona el cambio de contraseñas. Los responsables de realizar estos procesos son el responsable de seguridad y el área de recursos humanos.

**e) Seguridad física y del entorno**

**Generalidades:**

Para la seguridad física se deben tener en cuenta los siguientes aspectos: La protección física de acceso, protección y mantenimiento de equipos de acuerdo a su importancia, los

posibles daños e interferencias; El mantenimiento de las instalaciones se debe hacer bajo estrictas normas de seguridad.

**Objetivo:**

Evitar el daño, interferencias y el acceso no autorizado a la información de la empresa.

**Alcance:**

Esta política se debe aplicar en la Empresa y todos sus equipos, expedientes, cableados, documentación etc.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encarga de:

- Dirigir las políticas a seguir en el resguardo de los equipos, su mantenimiento y control de acceso etc. También se encargara de clasificar las áreas (Para servidores se creara un área restringida que tendrá un tratamiento especial).
- Adopta todas las políticas establecidas y verificara el cumplimiento de las mismas.

**Política**

- Perímetro de Seguridad Física:

  Se define un perímetro de seguridad para el área considerada como crítica que si no existen se debe crear (almacena todos los dispositivos considerados vitales como

servidores y almacenamiento de información confidencial) y se deben adoptar las siguientes medidas:

- Definir claramente el perímetro de seguridad.
- Establecer barreras de seguridad.
- Definir el personal autorizado para el acceso al área restringida.

- Controles de Acceso Físico:

  El responsable de la seguridad establecerá controles de acceso al área restringida:

  - Limitar el acceso al área donde se encuentra almacena la información, llevar un registro solo del personal autorizado.
  - Verificar que el personal que ingrese porte un documento visible que lo catalogue como personal autorizado.
  - Revisar periódicamente los registros del personal que accede.
  - Actualizar constantemente la lista de personal autorizado.
  - Seguridad de Oficinas e instalaciones; Se debe tener en cuenta las condiciones de iluminación ventilación salubridad, equipamiento anti incendios, medidas que prevengan inundaciones robos etc.

- Ubicación y protección de copias de seguridad y equipamiento:

  El equipamiento se ubicara en un sitio donde se minimice el riesgo, es decir en un lugar aislado y protegido tanto de amenazas naturales ambientales, físicas y humanas, adicional a esta medida se restringirá el acceso. Por lo tanto solo podrá acceder personal autorizado con su credencial y los ingresos y tareas a realizar serán debidamente documentadas por el responsable de la seguridad; las labores de aseo serán verificadas para evitar daños y hurtos.

- Suministro de Energía:

  Periódicamente se deben revisar el buen funcionamiento de las instalaciones eléctricas para evitar incidentes, la organización debe optar por contrarrestar fallas en el suministro de energía tales como la adquisición de una planta eléctrica, la compra de ups para los pc etc.

- Seguridad en el Cableado:

  Proteger el cableado que transporta datos de daños e interceptación cumpliendo con las normas, que el cableado baya por conductos seguros, separa los cables de energía de los cables de comunicación etc. Mantenimiento de Equipos:

  El responsable de la seguridad debe someter todos los equipos periódicamente e

mantenimiento preventivo, este mantenimiento debe ser registrado y documentado, cada equipo debe tener un inventario de dispositivos para saber qué cambio se hicieron y que dispositivos se retiraron.

- Seguridad en la reutilización o eliminación de equipos:

  Cuando un equipos es cambiado de sitio o eliminado se debe tener total precaución con los dispositivos de almacenamiento como discos duros los cuales deben ser formateados o destruidos de forma segura para evitar incidentes con la información.

**f) Gestión de operaciones y comunicaciones**

**Generalidades:**

La empresa debe crear condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información que se produce y se recibe a través de diferentes canales de comunicación.

**Objetivo:**

Adoptar medidas de seguridad encaminadas a prevenir la proliferación y expansión de software malicioso que son catalogadas como amenazas en potencia, garantizar el adecuado funcionamiento de los sistemas de información y designar responsables encargados de adoptar todas las medidas de seguridad necesarias para prevenir posibles ataques.

**Alcance:**

Esta política se debe aplicar a todo el sistema informático (red, servidores, comunicaciones y equipos) etc.

**Responsables:**

La responsabilidad de la seguridad está en manos del encargado de seguridad de la empresa y se encargan de:

- Definir procedimientos para el control actualización y modificación de los sistemas operativos tanto de servidores como pcs.
- Adoptar todas las políticas establecidas por el responsable de la seguridad y verificara el cumplimiento de las mismas.
- Verificar y hacer cumplir a cabalidad los contratos y acuerdos.

**Política**

- Procedimientos y responsabilidades operativas

  **Documentación de los procedimientos operativos:**

  Los S.O. Se actualizarán permanentemente y toda actualización y modificación de los S.O. será autorizada por el responsable de seguridad y debidamente documentada y realizada por el área de informática.

  Control de Cambios en las Operaciones: Todo cambio debe ser evaluado y aprobado

previamente y se tendrán en cuenta los siguientes aspectos: Evaluación del cambio y posible impacto, planificación, prueba, e identificación de responsabilidades en caso de que el cambio sea fallido.

**Procedimientos de Manejo de incidentes:**

El responsable de la seguridad establecerá protocolo para el manejo de incidentes tales como: Definir los posibles tipos de incidentes (Fallas operativas, código malicioso, intrusiones, fraude informático, error humano, desastres naturales).

En caso de presentarse incidentes comunicarlos a la dirección y seguir el plan de contingencia, implementar controles de acceso a los sistemas y medidas de recuperación.

- Planificación y Aprobación de sistemas.

  **Planificación de la Capacidad:**

  El responsable de seguridad es el encargado de evaluar constantemente las necesidades a futuro de los S.O. para evitar posibles fallas.

  **Aprobación del sistema:**

  El responsable de la seguridad sugiere a la dirección la posible especificación necesaria para actualizar los sistemas Operativos.

- Protección Contra software malicioso:

  El responsable de la seguridad y el responsable del área de informática definen los siguientes criterios de seguridad y el cumplimiento de los mismos:

  - Prohibir las instalaciones y descargas en los pc de la empresa.
  - Verificar constantemente el contenido del software.
  - Escanear constantemente el software.
  - Monitorear constantemente el software de los servidores.
  - Antes de realizar instalaciones o cambios verificar que toda información entrante esté libre de virus.
  - Concientizar al personal de la importancia de la protección en el manejo de la información.

- Mantenimiento

  **Resguardo de la información:**

  Los responsables de la información definirán un esquema de protección de la información entre ellas: Copias de seguridad y prueba de restauración, definir un esquema de rotulado de copias, almacenar copias de seguridad en una ubicación remota, el almacenamiento de copias de seguridad debe estar

físicamente protegida con un esquema de seguridad especial.

**Registro de actividades del personal operativo:**

El responsable de seguridad debe llevar un registro del uso de los sistemas como: Tiempo de inicio, cierre, errores del sistema, intentos de acceso al sistema, medidas tomadas etc.

**Registro de fallas:**

El responsable de seguridad debe llevar un registro fallas en los sistemas, como fueron resueltas, medidas correctivas etc (documentar todas las fallas de los sistemas).

- Administración de la Red:

  El responsable de la seguridad define y toma las medidas necesarias para proteger la red de datos para evitar posibles daños, interferencias etc.

  - Establece procedimiento de administración y delega un responsable que debe documentar todos los procedimientos realizados en la red.
  - Establecer controles para asegurar la disponibilidad, la confidencialidad y la integridad de la información.

- Garantizar mediante actividades de supervisión que los controles se apliquen.

- Administración de medios de almacenamiento:

  El responsable de la seguridad y el responsable del área de informática establecerán y verificaran el cumplimiento del correcto almacenamiento de respaldos de seguridad y eliminación de información de cintas magnéticas, discos duros para evitar incidentes con el manejo de la información.

  **Eliminación de medios de información:**

  El responsable de la seguridad y el responsable del área de informática deben verificar la correcta eliminación de información desde dispositivos de almacenamiento.

  **Procedimientos de manejo de información:**

  Para almacenar la información los empleados deben seguir el siguiente procedimientos tales como: Proteger documentos, redes y dispositivos informáticos, restringir el acceso a personal no autorizado, conservar los dispositivos de almacenamiento en medios seguros.

**Seguridad de la documentación del sistema:**

La documentación del sistema debe estar almacenada en un lugar seguro y el acceso a esta debe ser restringido.

- Intercambios de Información y de Software:

  Se debe utilizar medios de mensajería confiable, se deben de tener en cuenta las siguientes recomendaciones:

  - Uso adecuado por de la mensajería electrónica por parte del personal.
  - No abrir mensajes de remitentes desconocidos.
  - Toda información que llega debe ser escaneada.
  - Se debe conocer los posibles riesgos de seguridad a los que se enfrenta un usuario al utilizar mensajería electrónica y transferir por este medio la información confidencial.

**g) Control del Acceso**

**Generalidades:**

La política de control debe ser documentada, revisada y actualizada constantemente con el fin de evitar el acceso a los sistemas de información, bases de datos y documentos por personal no autorizado que pongan en peligro la información de la empresa.

**Objetivo:**

Controlar el acceso a la información.

**Alcance:**

Esta política se aplica a todas los procesos o formas de acceso a los sistemas de información, bases de datos o servicios de información de la empresa.

**Responsables:**

La responsabilidad de la seguridad está en manos del encargado de seguridad de la empresa y se encargan de:

- Definir normas, pautas y procedimientos para los accesos a los sistemas, bases de datos y servicios de información.
- También debe realizar un control de los privilegios de los usuarios y concientizar a los usuarios de la importancia de la no divulgación de las contraseñas.
- Dirigir normas y procedimientos para implementar Sistemas operativos, Gateway, firewall, servicios de red etc.
- Debe verificar que todos estos dispositivos y servicios queden debidamente configurados, debe realizar pruebas de escaneo, monitoreo para evitar intromisión.
- Promover y realizar la gestión de contraseñas y privilegios, capacitar y concientizar a los usuarios de la utilización de las medidas de control de acceso.

**Política**

- Política de Control de acceso:

  El responsable cumplirá con las siguientes funciones:

  - Implementar métodos de autenticación y control de acceso.
  - Segmentar la red.
  - Implementar control de puertos y ruteo de red.
  - Efectuar control de los registros de auditoría.
  - Definir perfiles de acceso.
  - Controlar los cambios en los accesos.

- Administración de accesos de usuarios.

  **Registración de usuarios:**

  Definir un registro formal de usuarios para otorgar y revocar accesos, utilizar identificadores de usuarios únicos.

  **Administración de Privilegios:**

  Identificar los privilegios, asignar los privilegios de acuerdo a las necesidades del trabajo, mantener un registro actualizado de los privilegios.

  **Administración de contraseñas de usuario:**

Los usuarios deben comprometerse a utilizar y mantener en secreto sus contraseñas esto debe estar estipulado en el contrato laboral, cambiar periódicamente las contraseñas, las contraseñas deben cumplir con todos los criterios de seguridad.

**Administración de contraseñas críticas:**

Para realizar configuraciones, asignaciones y cambios en los servidores, enrutadores etc., se utilizara contraseñas con un nivel de complejidad más alto.

- Responsabilidad de los usuarios:

  Los usuarios deben usar contraseñas, deben mantener la contraseña en secreto, pedir cambio de contraseña en caso de riesgo, usar contraseñas de calidad etc. El usuario está obligado a proteger los equipos asignados, no debe dejar los equipos abandonados o desatendidos, una vez terminado un servicio debe cerrar cesión, cerrar cesión después de utilizar correos electrónicos, apagar el equipo en forma correcta.

- Control de acceso a la red:

  El responsable de la seguridad es el encargado de otorgar los permisos para el acceso a la red y sus recursos, realizar normas y procedimientos de autorización, establecer controles y procedimientos de control de acceso, para autenticación de usuarios para conexiones externas debe

de escogerse un método de autenticación, un protocolo de autenticación, a autenticar las conexiones a sistemas informáticos remotos, protección de puertos para evitar accesos no autorizados, en lo posible subdividir o segmentar la red para realizar procesos separados con el fin de que si se presenta un incidente no se contamine toda la red o si un espía ingresa a esta no tenga acceso a toda la información, por otra parte se debe controlar el acceso lógico a los servicios, configurar los servicios de manera segura etc. El acceso a internet solo será autorizado por el jefe del área de informática.

- Se debe restringir algunos servicios como: Utilización de correo electrónico, transferencias de archivos, acceso interactivo y acceso a red fuera del horario laborar.

- Control de Acceso al sistema operativo:

  El responsable de seguridad debe definir los procedimientos para realizar la protección de los sistemas operativos, el acceso a los servicios de información solo se realizara a través de un proceso de conexión seguro, limitar el tiempo para los procesos de conexión, limitar el número de intentos de conexión; todos los usuarios utilizaran contraseñas seguras.

- Control de Acceso a las aplicaciones:

  Controlar los accesos de los usuarios, restringir la información, controlar el acceso a las funciones de los sistemas, revisar las salidas de información es decir que solo se envié la información solicitada.

- Monitoreo de acceso y uso de los sistemas:

  Revisar y monitorear que los usuarios solo estén realizando actividades que hayan sido autorizadas previamente, se debe monitorear, el acceso, la identificación de usuarios, fecha y hora de eventos, archivos accedidos, se debe supervisar el inicio y cierre del sistema, las operaciones con privilegios, cambios de configuración del sistema, intentos de acceso no autorizado, alertas fallas del sistema etc.

**h) Adquisición, desarrollo y mantenimiento de sistemas de información**

**Generalidades:**

Se debe documentar y aprobar los requerimientos de seguridad a aplicar en la implementación de los sistemas de información; se debe llevar a cabo adecuadas políticas de seguridad para las bases de datos, los sistemas operativos, todo esto con el fin de evitar que personas conocedoras de los procesos puedan cometer fraudes o ilícitos y si es el caso identificarlos de manera inmediata.

**Objetivo:**

Adoptar medidas de seguridad en la implementación de los sistemas de información.

**Alcance:**

Esta política se debe aplicar a todos los sistemas informáticos tanto sistemas operativos como software requerido para la entidad.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encargan de:

- Definir e implementar controles en el desarrollo y mantenimiento de sistemas de información.
- Definir el procedimiento para asignar claves, de garantizar el cumplimiento de los requisitos de seguridad del software, de controlar los cambios en los sistemas etc.
- Licenciamiento del software adquirido y en el caso del software desarrollado por la organización de establecer las políticas de derechos de autor y fijar las condiciones de los contratos y de entrega.

**Política**

- Requerimientos de seguridad de los sistemas:

  **Análisis y especificaciones de los requerimientos de seguridad:**

Identificar y definir los requerimientos y controles necesarios en materia seguridad desde las etapas de análisis y diseño del sistema ya que implementar medidas de seguridad desde estas etapas sale menos costoso que hacerlo después.

**Seguridad en los sistemas de aplicaciones:**

Se debe establecer controles de los registro de auditoría para evitar la pérdida de los datos de los sistemas de información (validación y autenticación de los datos de entrada y de salida).

**Validación de datos de entrada:**

Se debe establecer un control de validación de los datos de entrada como: Revisión periódica de contenidos de campos claves, se debe establecer cómo se realizará y con qué método, además se definirá las responsabilidades del personal.

**Controles de procedimientos interno:**

El responsable de la seguridad junto con el jefe del área de sistemas deben establecer controles para la etapa del diseño, se deben implementar procedimientos que permitan identificar el uso y localización en los aplicativos, controles y verificaciones, revisión periódica de los registros, controles de integridad de los registros y de los archivos, controles que verifique la

consecución y orden en la ejecución de los aplicativos.

También se deben implementar controles para la autenticación de mensajes y para la validación de datos de salida.

- Controles criptográficos

**Política controles criptográficos:**

Se debe utilizar controles criptográficos para los siguientes casos: Protección de claves de acceso a sistemas, datos y servicios, transmisión de información clasificada, resguardo de información. El responsable de la seguridad se encargara de definir la política de controles criptográficos, el método y el responsable de administración de claves (Uso de algoritmo de cifrado y firma digital, servicios de no repudio).

**Administración de claves:**

El responsable de administrar las claves debe aplicar las políticas de protección de las claves implementando un sistema de administración de claves criptográficas que permitan usar técnicas de clave secreta, estas claves serán protegidas contra copia, destrucción, divulgación, modificación etc.

- Seguridad de los procesos de soporte

**Procedimiento de control de cambios:**

Verificar que los cambios sean propuestos por personal autorizado, mantener un registro

del nivel de autorización, identificar todos los elementos que requieren modificaciones, obtener aprobación por parte del responsable del área de informática para cumplir con los requerimientos del software.

**Revisión técnica de los cambios en el sistema operativo:**

Antes de realizar cambios en el sistema operativo se debe revisar y verificar que los cambios son necesarios, que impacto genera, informar al área involucrada y verificar la continuidad del negocio.

**Restricción del cambio de paquetes de software:**

Se debe evaluar la necesidad, los costos, la parte legal (licencias) y el impacto del cambio que este genera en la organización.

**Canales ocultos y código malicioso:**

Se debe adquirir software a personal confiable y conocido, examinar códigos fuentes que estén libres de virus, llevar un control de acceso al software y las modificaciones instaladas, utilizar antivirus y software de monitoreo y escaneo.

**Adquisición de software:**

Para la adquisición de software a terceros se deben establecer condiciones puntuales rigurosas tales como: acuerdos de licencias, procedimientos certificación de calidad, calidad en el software, verificación del

cumplimiento de las condiciones de seguridad.

i) **Gestión de los incidentes de seguridad de la información**

**Generalidades:**

Todos los empleados de la empresa deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

**Objetivo:**

Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata.

**Alcance:**

Esta política la deben cumplir todos los empleados de la empresa.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encargan de:

- Establecer un protocolo el cual deben conocer todos empleados para conozcan cual es el procesos a seguir en caso de presentarse una falla. Es decir cómo y a quien reportarlo para que se tomen los correctivos necesarios.

- Concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

**Política**

- Reportes sobre los eventos de seguridad de la información:

  Se debe establecer un punto de contacto que siempre esté disponible y brinde respuesta oportuna y adecuada a los incidentes. Todos los empleados deben estar informados sobre la obligatoriedad de reportar e informar sobre incidentes, fallas, vulnerabilidades y debilidades observadas en el sistema (los empleados para reportar los incidentes deben diligencian un formato).

- Gestión de incidentes y las mejoras en la seguridad de la información:

  La organización en cabeza del responsable de la seguridad establece procedimientos para el manejo de eventos y debilidades de la seguridad. Se debe evaluar y gestionar todos los incidentes de seguridad de la información así:

  **Responsabilidades y procedimientos:**

  Establecer procedimientos para manejar eventos como: Fallas en el sistema, virus, negación del servicio, violación de confidencialidad, integridad y disponibilidad, uso inadecuado de los sistemas informáticos,

código malicioso; identificar la causa, implementar acciones correctivas y reportar todo el procesos realizado al responsable de la seguridad.

**Aprendizaje debido a los incidentes de seguridad informática:**

El responsable del área de informática, debe llevar un registro de los incidentes presentados, de cómo se han manejado, las posibles causas y cuanto le cuestan a la empresa resolverlos, para en un futuro no cometer los mismos errores.

**Recolección de Evidencia:**

En el caso de llevar a cabo una acción disciplinaria, se debe recolectar la evidencia siguiendo las siguientes pautas: No se debe manipular la evidencia, se debe crear una copia intacta de la evidencia y esta debe ser resguarda a través de una cadena de custodia.

**j) Gestión de la continuidad del negocio**

**Generalidades:**

Es indispensable que toda empresa disponga de un proceso de gestión de continuidad del negocio en caso de llegarse a presentar una eventualidad como un desastre natural, robo, daños en los servidores etc.

**Objetivo:**

Asegurar el funcionamiento continuo de la organización.

**Alcance:**

Esta política se debe aplicar a todos los procesos críticos y prioritarios de la empresa.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encargan de:

- Identificar las amenazas, evaluar los riesgos identificar controles preventivos, desarrollar un plan estratégico y un plan de contingencia.
- Participar en la elaboración y documentación del plan de contingencia.

**Política**

- Proceso de la administración de la continuidad de la empresa:

  El encargado de seguridad identificará los procesos críticos, asegurarse de que todos los empleados de la empresa comprendan y conozcan los riesgos, elaborar y documentar una estrategia de continuidad del negocio y proponer la adquisición de pólizas y seguros.

- Continuidad de las actividades y análisis de los impactos:

  Antes de elaborar el plan de contingencia el comité de seguridad debe identificar los eventos o amenazas, evaluar los riesgos e

identificar controles preventivos. Todo esto debe estar debidamente documentado.

- Elaboración e implantación de los planes de continuidad de las actividades de la empresa:

  El responsable de la seguridad debe elaborar el plan de contingencia que debe contemplar los siguientes aspectos: Responsables de los procedimientos de emergencia, definir acciones y correctivos, implementar procedimientos de emergencia, documentar estos procedimientos e instruir al personal; actualizar constantemente el plan de contingencia.

- Marco para la planificación de la continuidad de las actividades de la empresa:

  Se debe especificar claramente los requisitos y condiciones para su puesta en marcha, los responsables y los requerimientos etc. Adicionalmente debe prever las condiciones de implementación, definir los procedimientos de emergencia, y las acciones a realizarse, describir los procedimientos de recuperación, definir un cronograma de mantenimiento y documentar las responsabilidades y funciones de las personas. (Elaborar un documento muy completo del plan de contingencia.).

- Ensayo, mantenimiento y reevaluación de los planes de continuidad de la empresa:

  El encargado de la seguridad establecerá un cronograma de pruebas, el cronograma

señalara quienes son los responsables, efectuara pruebas, realizara simulaciones y pruebas completas en las instalaciones, involucrando procesos y con todo el personal.

**k) Cumplimiento**

**Generalidades:**

Todas las empresas deben cumplir con las obligaciones estipuladas por la ley.

**Objetivo:**

Cumplir con todas las obligaciones estipuladas por la ley Alcance: Esta política se debe aplicar a todo el personal de la empresa.

**Responsables:**

La responsabilidad de la seguridad de la información está en manos del encargado de seguridad de la empresa y se encargan de:

- Definir procedimientos encaminados a cumplir con todas las normas y restricciones legales.
- Realizar revisiones periódicas a la empresa para verificar el cumplimiento de las políticas de seguridad, solicitar auditorias periódicas, documentar y dar a conocer los requisitos normativos.

Todos los empleados están obligados a conocer y dar a conocer a cumplir y hacer cumplir la presente política y la normativa vigente.

**Política**

- Cumplimiento de requisitos legales:

  **Identificación de la legislación aplicable:**

  Se definirán claramente los requisitos normativos contractuales.

  **Derechos de propiedad intelectual:**

  Solo se podrá utilizar material autorizado, respetando la propiedad intelectual.

  **Derecho de propiedad intelectual del software:**

  El responsable de la seguridad junto con el responsable del área de informática implementar controles y procedimientos para el manejo de licencias.

  **Protección de los registros de la empresa:**

  Los registros críticos serán debidamente protegidos contra pérdida, falsificación o robo. Para el almacenamiento y protección de los registros contables, base de datos y otros de estos se debe realizar un inventario, implementar controles, y establecer procedimientos de almacenamiento, divulgación, manipulación o eliminación.

  **Protección de datos:**

  Todos los empleados están obligados a cumplir un compromiso de confidencialidad es decir a utilizar la información solo para bien de la empresa.

**Prevención del uso inadecuado de los recursos de procesamiento de información:**

Cuando un empleado utilice la información o los recursos de la organización sin ser autorizado será considerado como uso indebido y esto va en contra de las normas de la empresa y puede estar sujeto a sanciones.

**Regulación de controles para el uso de criptografía:**

Para hacer usos de herramientas criptográficas el responsable del área legal junto con el responsable del área de seguridad debe cumplir con las leyes de firma digital y encriptación vigentes en el país, una vez conozcan las normas de uso, se implementan los controles y se dan a conocer al encargado.

**Recolección de Evidencia:**

Cuando una acción indebida o inapropiada involucre la aplicación de la ley, la evidencia presentada debe cumplir con lo establecido en las leyes que rigen a nuestro país.

Para la recolección de la evidencia se debe cumplir con las siguientes condiciones: Realizar una copia de seguridad para que la evidencia original no sea modificada, guardar la evidencia en un sitio seguro.

- Revisión de las políticas de seguridad y la compatibilidad técnica.

**Cumplimiento de las políticas de seguridad:**

El responsable del área de informática realizara revisiones del cumplimiento de las políticas de seguridad en la empresa.

**Verificación de la compatibilidad técnica:**

El responsable de la seguridad revisara que los controles para el hardware y el software sean implementados correctamente.

- Auditorías de sistemas

**Controles de auditoría de sistemas:**

Cuando se realicen auditorías a los sistemas, el responsable de la seguridad debe definir el área a auditar, controlar el alcance de las comprobaciones, limitar la auditoria para evitar modificaciones.

**Protección de los elementos utilizados por la auditoria de sistemas:**

El responsable de la seguridad debe definir instrucciones y procedimientos para el acceso archivos, datos o software.

- Sanciones previstas por incumplimiento:

El incumplimiento o violación de las políticas de seguridad implica sanciones, de acuerdo a los contratos suscritos con la empresa y en caso de acciones legales se procederá de acuerdo a la ley.

### 4.1.2. Implantar el SGSI

Declaración de Aplicabilidad. En la declaración de aplicabilidad se define como se implementaran los sistemas de seguridad de la información, ya que este documento aplica la relación entre la calificación y el tratamiento del riesgo y la implementación de un sistema de seguridad de la información y es un documento fundamental desde donde parte una auditoria.

Para la declaración de aplicabilidad en la empresa NET-Consultores S.A.C, se ha tenido en cuenta los siguientes documentos: l Anexo A de la norma ISO 27001 Se tomó el Inciso (A.8) del Anexo cuyo contenido es la Gestión de Activos.

La declaración de aplicabilidad se realizó sobre el análisis de activos teniendo en cuenta los siguientes parámetros:

- Dominio: Que indica el número del control de acuerdo al anexo A de la Norma ISO/IEC 27001.
- Controles según la ISO/IEC 27001: Se identifica el nombre del control.
- Aplicabilidad: Se identifica si es o no es aplicable en la empresa.
- Justificación: Explica porque es o no es aplicable dicho control.
- Objetivo del Control
- Actividades para la implementación del control
- Estado del control.

#### 4.1.2.1. Aplicabilidad de los controles

**Tabla 15: Aplicabilidad de Controles Anexo (A.8) de la ISO 27001**

| Dominios | Controles según la norma ISO/IEC 27001 | Aplicabilidad (Sí/No) | Justificación de elección/ no elección | Objetivo del control | Actividades para la implementación de los controles | Estado |
|---|---|---|---|---|---|---|
| 8 | Gestión de Activos | | | | | |
| 8.1 | Responsabilidad sobre los activos | | | | | |
| 8.1.1 | Inventario de activos | Si | Es importante identificar los activos de acuerdo a su grado de importancia dentro de la empresa, en la que se deja claro que el activo más relevante es la base de datos donde se registran los proyectos, el archivo de licencias y el archivo físico. | Jerarquizar la importancia de los activos al interior de la | Clasificación de los activos y establecimiento del nivel de importancia de los mismos. | IMPLEMENTAD |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.1.2 | Propietario de activos | Si | Cada activo dentro de la empresa debe tener relacionado un responsable de la seguridad. | Tener responsables de los activos que forman parte de la empresa. | Asignar responsables tanto para los activos de información a través del área de gestión de proyectos, como para activos físicos que forman parte de los sistemas de información. | IMPLEMENTADO |
| 8.1.3 | Uso aceptable de los activos | Si | Las políticas sobre manejo de la información deben permitir tener claridad acerca del manejo adecuado de activos. | Definir políticas para el manejo de activos. | Políticas de manejo de activos. | IMPLEMENTADO |
| 8.1.4 | Devolución de activos | No | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.2 | Clasificación de la información | | | | | |
| 8.2.1 | Directrices de clasificación | Si | La información debe ser clasificada de acuerdo a su grado de importancia para establecer los controles adecuados para el manejo de la misma. | Identificar el nivel de importancia de los activos de información al interior de la empresa. | Establecimiento de prioridades en el manejo de la información. | IMPLEMENTADO |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.2.2 | Etiquetado y manipulado de la información | Si | Cada tipo de información debe ser identificado para que cada persona conociendo su naturaleza respete su nivel de confidencialidad, es decir debe ser etiquetada relacionando sus restricciones. | Identificar el nivel de confidencialidad y acceso a la información. | Políticas de acceso a la información. | IMPLEMENTADO |
| 8.2.3 | Manipulación de activos | Si | Cada tipo de información debe ser identificado para que cada persona conociendo su naturaleza respete su nivel de confidencialidad, es decir debe ser etiquetada relacionando sus restricciones. | Identificar el nivel de confidencialidad y acceso a la información. | Políticas de acceso a la información. | IMPLEMENTADO |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.3 | Manejo de los soportes de almacenamiento | | | | | |
| 8.3.1 | Gestión de soportes extraíbles | No | | | | |
| 8.3.2 | Eliminación de soportes | No | | | | |
| 8.3.3 | Soportes físicos en tránsito | No | | | | |

***Fuente: Elaboración propia***

#### 4.1.2.2. Plan de Tratamiento del Riesgo

**Tabla 16: Plan de tratamiento del Riesgo**

| Descripción de las actividades | Responsables | Tiempo | Hallazgos |
|---|---|---|---|
| Documentación de todos los procesos a desarrollarse para la implementación de la seguridad | NET- Consultores Encargado de la Seguridad | 2 meses | Es necesario que se defina una política para la documentación de todos los procedimientos en relación con las políticas de manejo de la información. |
| Revisión de las políticas de seguridad de la información. | | 2 meses | Se revisara periódicamente las políticas de la seguridad de la información. |
| Políticas de gestión de privilegios. | | 1 mes | Es necesario que se definan políticas para la verificación de acceso a los sistemas de información y verificar los privilegios con los que tiene acceso. |
| Políticas de seguridad para el personal que maneja la información al interior de la empresa. | | 1 mes | Es necesario que los empleados que manejan la información conozcan y apliquen las políticas seleccionadas para el manejo de la información. |

| | | | |
|---|---|---|---|
| Planes de capacitación para el personal a cargo del manejo de la información. | NET- Consultores | 2 meses | Planes de capacitación para el personal a cargo del manejo de la información. |
| Políticas de seguridad para nuevos activos de información. | Encargado de la Seguridad | 2 meses | Es necesaria la definición de políticas de seguridad para nuevos y futuros activos dentro de la empresa. |
| Acuerdos de confidencialidad para los empleados de la empresa. | | 1 mes | Es necesario que los acuerdos de confidencialidad para el manejo de la información queden establecidos en el contrato laboral. |
| Definir canales seguros para el manejo de la información. | | 3 meses | Definir políticas de seguridad para evitar fallas en los canales de comunicación. |
| Políticas para el manejo de la información al interior de la organización. | | 2 meses | Es necesario definir, documentar e informar sobre la implementación y cumplimiento de las políticas de seguridad para el manejo de la información al interior de la empresa. |
| Políticas pensadas en futuros activos que formaran parte de la empresa. | | 3 meses | Es necesaria la definición de políticas de seguridad para nuevos y futuros activos dentro de la empresa. |
| Clasificación de los activos y establecimiento del nivel de importancia de los mismos. | | 3 meses | Es necesario que se clasifiquen los activos de acuerdo al nivel de seguridad. |

| | | | |
|---|---|---|---|
| Políticas de manejo de activos. | NET- Consultores Encargado de la Seguridad | 3 meses | Es necesario definir, documentar e informar sobre el manejo de los activos y las políticas de seguridad a aplicarse a dichos activos. |
| Establecimiento de prioridades en el manejo de la información. | | 3 meses | Es necesario definir |
| Políticas de acceso a la información. | | 2 meses | Es necesario definir, documentar e informar sobre la implementación y cumplimiento de las políticas de seguridad para el acceso a la información. |
| Claridad en las políticas de contratación. | | 1 mes | Es necesario definir e informar las políticas de confidencialidad dentro de la organización, |
| Definición de políticas de manejo de la información, acompañadas de planes de capacitación. | | 3 meses | Aunque existen políticas de seguridad para la información, se debe definir la competencia de manejo de la misma y garantizar el conocimiento de las mismas por parte de todas las personas que tienen acceso a la misma. |
| Implementación de políticas de manejo de privilegios sobre la información. | | 3 meses | Es necesario que se definan políticas para la verificación de acceso a los sistemas de información y verificar los privilegios con los que tiene acceso. |
| Políticas de control de acceso físico a áreas que contienen información sensible. | | 3 meses | Ya se encuentran implementados controles para acceso a la empresa mediante clave y al archivo solo a personal autorizado, es ideal que es extiendan a las áreas. |

| | | | |
|---|---|---|---|
| Políticas de control de acceso físico. | NET- Consultores<br>Encargado de la Seguridad | 1 mes | Ya se encuentran implementados controles para acceso a la empresa mediante clave y al archivo solo a personal autorizado, es ideal que es extiendan a todas las áreas. |
| Protección contra factores atmosféricos como temperatura, humedad, etc. | | 3 meses | Es necesario establecer controles ambientales para evitar el deterioro de activos derivado de estos factores. |
| Verificación del nivel de seguridad de las áreas de trabajo. | | 3 meses | Es necesario establecer controles que permitan verificar de seguridad a aplicar en cada área de trabajo de acuerdo a la información que se maneje en cada dependencia. |
| Control de acceso físico a determinadas áreas de la empresa. | | 1 mes | Es necesario establecer controles de seguridad para áreas críticas donde se debe seleccionar el personal que tiene acceso a esta y las responsabilidades que esto implica ejemplo: Área de archivo |
| Implementar controles para el control de factores ambientales como humedad, polvo, etc. | | 1 mes | Es necesario establecer controles ambientales para evitar el deterioro de activos derivado de estos factores. |
| Implementar UPS. | | 3 meses | Deben existir sistemas de respaldo ante caídas del suministro eléctrico. Para cada uno de los equipos. |

| | | | |
|---|---|---|---|
| Implementar planes de mantenimiento de equipos al interior de la empresa | NET- Consultores Encargado de la Seguridad | 3 meses | Es necesario que se establezca un plan para el mantenimiento de equipos al interior de la empresa. |
| Políticas para la documentación de procedimientos. | | 3 meses | Es necesario iniciar el proceso de implementación de un plan director debidamente documentado de seguridad de la información que permita cubrir cada uno de los aspectos que han sido enumerados. |
| Implementación de políticas de manejo de privilegios sobre la información. | | 3 meses | Es necesario implementar controles y políticas de seguridad aplicados a los grupos de trabajos y adicionalmente realizar controles que permitan gestionar la gestión de privilegios dentro del sistema. |
| Definición de políticas para la integración de nuevos elementos al sistema de información. | | 3 meses | Es necesario definir controles que se deben tener en cuenta en el caso de que ingresen nuevos elementos al sistema de información. |
| Definición de políticas de administración y uso de redes. | | 3 meses | Es necesario definir políticas de seguridad para el manejo y administración de la red. |
| Definición de políticas para que la información no sea extraída | | 3 meses | Aunque existen restricciones que se deben tener en cuenta en cuanto al manejo de la información es necesario definir políticas de seguridad para evitar que la información sea extraída, además concientizar de las implicaciones legales a las que se expone quien lo haga. |

| | | | |
|---|---|---|---|
| Definir políticas para la gestión y eliminación de medios de almacenamientos. | NET- Consultores Encargado de la Seguridad | 3 meses | Se debe definir políticas a tener en cuenta para la eliminación de medios de almacenamiento tales como discos duros, CD, DVD, memorias usb y papel firmado o sellado ya que si es desechado de forma incorrecta puede ser utilizado de forma indebida por terceros y ocasionar problemas a la organización. |
| Implementar mecanismos de protección de información como por ejemplo encriptación (se garantiza con los controles con que cuenta la empresa). | | 6 meses | Es necesario definir políticas de seguridad para el manejo de herramientas criptográficas, en caso de ser implementadas. |
| Políticas de implementación y control de registros de actividad. | | 3 meses | Es necesario que sean definidos sistemas de registros de actividad para tener control de cualquier cambio en los sistemas de información. |
| Políticas de control y gestión de fallas en el sistema. | | 3 meses | Es necesario definir políticas de seguridad para implantar la gestión de fallos (notifican, visualización y reparación de fallos). |
| Políticas de implementación y control de registros de actividad. | | 3 meses | Es necesario definir políticas de seguridad para la administración del registro de actividades. |
| Definir políticas para el control de acceso teniendo en cuenta áreas críticas. | | 1 mes | Es necesario definir políticas a seguir para controlar el acceso a áreas restringidas (llevar un registro detallado de ingreso a estas áreas) |

| | | | |
|---|---|---|---|
| Definir políticas para el ingreso o eliminación de usuarios del sistema. | NET- Consultores Encargado de la Seguridad | 3 meses | Es necesario definir políticas de seguridad a seguir en los procesos de eliminación de usuarios. |
| Definir políticas para la gestión de privilegios. | | 3 meses | Es necesario definir políticas de seguridad para la gestión de privilegios, esta labor la debe realizar el administrador del sistema que se encargara de definir los roles y permisos a los usuarios del sistema. |
| Establecer políticas para la asignación de contraseñas. | | 3 meses | Es necesario establecer políticas de seguridad que permitan implementar el uso de contraseñas. Es decir para cada usuario y equipo una contraseña la cual debe cumplir con todas las condiciones de una contraseña segura. |
| Establecer políticas para la verificación regular del acceso a sistemas de información. | | 3 meses | Implementar políticas de seguridad que permitan verificar los accesos a los sistemas de información. |
| Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa. | | 3 meses | Es necesario definir políticas que los trabajadores de la empresa deben poner en práctica para la utilización de los sistemas de información de la empresa adicionales a los ya existentes. |
| Establecer políticas de enrutamiento de la información. | | 3 meses | Es necesario definir políticas de enrutamiento de red. |

| | | | |
|---|---|---|---|
| Establecer políticas de acceso a los sistemas operativos. | NET- Consultores Encargado de la Seguridad | 3 meses | Es necesario establecer políticas para el acceso y manejo del sistema operativo. |
| Establecer políticas de manejo de credenciales de usuarios. | | 3 meses | Es necesario definir políticas de seguridad para el manejo de credenciales de usuarios. |
| Establecer políticas de uso de aplicaciones de carácter administrativo propias del sistema. | | 3 meses | Es necesario definir políticas de seguridad para el uso de aplicaciones de carácter administrativo propias del sistema. |
| Establecer políticas para la integración de sistemas de información. | | 3 meses | Es necesario definir políticas de seguridad para la integración de sistemas de información para que la información sea compartida de forma segura. |
| Establecer políticas para garantizar la seguridad de las aplicaciones en funcionamiento. | | 3 meses | Es necesario definir políticas de seguridad para a cada aplicación manejada en la empresa. |
| Definir políticas para la gestión de vulnerabilidades de aplicaciones o sistemas usados por la empresa. | | 3 meses | Es necesario definir políticas de seguridad para la gestión de vulnerabilidades de aplicaciones usadas por la empresa. |
| Definir políticas para la gestión de incidentes de seguridad de la información. | | 3 meses | Es necesario definir políticas de seguridad para la gestión de incidentes de seguridad de la información. |

| | | | |
|---|---|---|---|
| Definir políticas de seguridad de la información que garanticen la continuidad del negocio. | NET- Consultores Encargado de la Seguridad | 6 meses | Es necesario y de suma importancia definir políticas de seguridad de la información a implementarse encaminadas a garantizar la continuidad del negocio |
| Definir políticas de protección de información alineadas con requerimientos de carácter legal. | | 6 meses | Es necesario definir políticas de seguridad a implementarse con el fin de proteger la información teniendo en cuenta las normas legales. |
| Revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares. | | 6 meses | Es necesario establecer políticas de seguridad que permitan verificar que los procedimientos se estén realizando de acuerdo a las políticas y estándares definidos por la empresa. |
| Establecer políticas para el desarrollo de procesos de auditoria. | | 6 meses | Es necesario definir políticas de seguridad que permitan desarrollar futuras auditorias. |

***Fuente: Elaboración propia***

## 4.2. Resultados obtenidos en la aplicación de las encuestas

Para la prueba de hipótesis se realizó dos encuestas (Pre test y Pos test) a los 23 trabajadores de la empresa NET-Consultores S.A.C; De lo cual se seleccionó el resultado más alto (pre test y post test) de la encuesta aplicada de acuerdo a la frecuencia con la que se presenta cada amenaza por cada activo de información y se le asignó un respectivo valor de acuerdo a la siguiente tabla y a la metodología aplicada:

**Tabla 17: Escala de medición variable dependiente**

| Escala | Indicador | Valor | |
|---|---|---|---|
| | | Numérico | Porcentual |
| 1 | Poco frecuente, cada varios años | 10 | 10% |
| 2 | Normal, una vez al año | 50 | 50% |
| 3 | Frecuente, mensualmente | 70 | 70% |
| 4 | Muy frecuente A diario | 100 | 100% |

***Fuente: www.fing.edu.uy***

De lo cual se obtuvo los siguientes resultados que se muestra a continuación.

**Tabla 18: Evaluación de frecuencia de amenazas respecto a los activos**

| Amenaza | Activo | Frecuencia de la Amenaza (Indicador) | Antes SGSI | | Después SGSI | |
|---|---|---|---|---|---|---|
| | | | N° Enc. | Valor | N° Enc. | Valor |
| [N.1] Fuego [N.2] Daños por agua | Equipos informáticos Instalaciones | 1 | 2 | 50 | 10 | 10 |
| | | 2 | 10 | | 2 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [I.1] Fuego [I.2] Daños por agua | Equipos informáticos Instalaciones | 1 | 1 | 70 | 2 | 50 |
| | | 2 | 2 | | 9 | |
| | | 3 | 9 | | 1 | |
| | | 4 | 0 | | 0 | |
| [N.1] Fuego [N.2] Daños por agua | Soporte de almacenamiento | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [I.1] Fuego [I.2] Daños por agua | Soporte de almacenamiento | 1 | 3 | 50 | 7 | 10 |
| | | 2 | 8 | | 5 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [N.1] Fuego [N.2] Daños por agua | Equipamiento Auxiliar | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 4 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [I.1] Fuego<br>[I.2] Daños por agua | Equipamiento Auxiliar | 1 | 2 | 50 | 7 | 10 |
| | | 2 | 7 | | 4 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| N.*] Desastres naturales | Equipos informáticos | 1 | 1 | 70 | 1 | 50 |
| | | 2 | 4 | | 7 | |
| | | 3 | 7 | | 4 | |
| | | 4 | 0 | | 0 | |
| | Soporte de Información | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 4 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Equipamiento Auxiliar | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Instalaciones | 1 | 2 | 50 | 10 | 10 |
| | | 2 | 9 | | 2 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [I.*] Desastres industriales | Equipos informáticos | 1 | 1 | 70 | 1 | 50 |
| | | 2 | 2 | | 8 | |
| | | 3 | 9 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Soporte de Información | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 2 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Equipamiento Auxiliar | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Instalaciones | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 4 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [I.3] Contaminación mecánica | Equipos informáticos | 1 | 2 | 70 | 2 | 70 |
| | | 2 | 1 | | 2 | |
| | | 3 | 9 | | 8 | |
| | | 4 | 0 | | 0 | |
| | Soporte de Información | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Equipamiento Auxiliar | 1 | 4 | 50 | 8 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [I.4] Contaminación electromagnética | Router de acceso inalámbrico. | 1 | 0 | 100 | 0 | 70 |
| | | 2 | 2 | | 4 | |
| | | 3 | 3 | | 6 | |
| | | 4 | 7 | | 2 | |
| [I.5] Avería de origen físico o lógico | Software - Aplicaciones Informáticas | 1 | 0 | 100 | 0 | 70 |
| | | 2 | 2 | | 1 | |
| | | 3 | 1 | | 9 | |
| | | 4 | 9 | | 2 | |
| | Equipos informáticos | 1 | 0 | 70 | 0 | 50 |
| | | 2 | 1 | | 7 | |
| | | 3 | 10 | | 4 | |
| | | 4 | 1 | | 1 | |
| | Soportes de Información | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Equipamiento Auxiliar | 1 | 2 | 50 | 7 | 10 |
| | | 2 | 9 | | 4 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [I.6] Corte del suministro eléctrico | Equipos informáticos | 1 | 1 | 100 | 1 | 70 |
| | | 2 | 2 | | 1 | |
| | | 3 | 3 | | 7 | |
| | | 4 | 6 | | 3 | |
| | Soporte de Información (electrónicos) | 1 | 4 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Ups computadores | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [I.7] Condiciones inadecuadas de temperatura o humedad | Equipos Informáticos | 1 | 1 | 100 | 0 | 70 |
| | | 2 | 3 | | 1 | |
| | | 3 | 2 | | 8 | |
| | | 4 | 6 | | 3 | |
| [I.8] Fallo de servicios de comunicaciones | Redes de comunicaciones (Red inalámbrica, red local e internet) | 1 | 2 | 100 | 1 | 70 |
| | | 2 | 1 | | 2 | |
| | | 3 | 2 | | 8 | |
| | | 4 | 7 | | 1 | |
| [I.9] Interrupción de otros servicios y suministros esenciales. | Equipamiento Auxiliar | 1 | 2 | 50 | 6 | 10 |
| | | 2 | 9 | | 5 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [I.10] Degradación de los soportes de almacenamiento de la información | Soportes de Información | 1 | 3 | 50 | 7 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.1] Errores de los usuarios Datos/Información | Archivos de proyectos | 1 | 0 | 100 | 0 | 70 |
| | | 2 | 0 | | 1 | |
| | | 3 | 3 | | 9 | |
| | | 4 | 9 | | 2 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.1] Errores de los usuarios Datos/Información | Archivos de Clientes | 1 | 3 | 50 | 7 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 2 | |
| | | 4 | 1 | | 1 | |
| | Archivo de Contabilidad | 1 | 5 | 50 | 9 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [E.1] Errores de los usuarios Datos/Información | Archivos de Informes y licencias expedidas | 1 | 0 | 100 | 0 | 70 |
| | | 2 | 1 | | 1 | |
| | | 3 | 3 | | 8 | |
| | | 4 | 8 | | 3 | |
| | Archivo de Copias de seguridad de la información | 1 | 1 | 50 | 9 | 10 |
| | | 2 | 9 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Datos de configuración de servidores y equipos | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Datos de Gestión de proyectos radicados | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 2 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Contraseñas de acceso de empleados | 1 | 2 | 50 | 6 | 10 |
| | | 2 | 9 | | 5 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.1] Errores de los usuarios | Claves Criptográficas | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.1] Errores de los usuarios Servicios | Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos) | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 9 | | 4 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Servicio de internet al que pueden acceder los empleados. | 1 | 0 | 70 | 0 | 50 |
| | | 2 | 4 | | 10 | |
| | | 3 | 7 | | 2 | |
| | | 4 | 1 | | 0 | |
| [E.1] Errores de los usuarios Servicios | Manejo de correos electrónicos | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Servicio de almacenamiento de información en el servidor de bases de datos. | 1 | 2 | 70 | 0 | 50 |
| | | 2 | 1 | | 9 | |
| | | 3 | 9 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo. | 1 | 1 | 50 | 6 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 3 | | 2 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.1] Errores de los usuarios Aplicaciones | Servidor de aplicaciones | 1 | 1 | 50 | 6 | 10 |
| | | 2 | 8 | | 5 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Gestor base de datos, aplicación destinada al proceso de gestión de las bases de datos manejadas al interior de la empresa. | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Office 2010 | 1 | 3 | 50 | 7 | 10 |
| | | 2 | 6 | | 4 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Kaspersky original con actualizaciones automáticas. | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 10 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas. | 1 | 2 | 70 | 2 | 50 |
| | | 2 | 1 | | 7 | |
| | | 3 | 9 | | 3 | |
| | | 4 | 0 | | 0 | |
| [E.1] Errores de los usuarios. Soporte de información | Soportes de Información. | 1 | 2 | 70 | 3 | 50 |
| | | 2 | 1 | | 8 | |
| | | 3 | 9 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.4] Errores de configuración | Datos de configuración de servidores y equipos | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [E.7] Deficiencias en la organización | Personal de recepción, área técnica, administrativa y archivo | 1 | 0 | 100 | 0 | 70 |
| | | 2 | 1 | | 2 | |
| | | 3 | 3 | | 7 | |
| | | 4 | 8 | | 3 | |
| | Administrador de sistemas | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.8] Difusión de software dañino | Software – Aplicaciones Informáticas | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.9] Errores de [re-]encaminamiento | Servicios | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Software – Aplicaciones Informáticas | 1 | 3 | 50 | 7 | 10 |
| | | 2 | 6 | | 4 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Redes de comunicaciones | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 2 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.14] Escapes de información | Activos esenciales | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Datos / información | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.15] Alteración accidental de la información | Datos / información | 1 | 1 | 70 | 1 | 50 |
| | | 2 | 3 | | 7 | |
| | | 3 | 8 | | 4 | |
| | | 4 | 0 | | 0 | |
| [E.18] Destrucción de la información | Datos / información | 1 | 3 | 70 | 1 | 50 |
| | | 2 | 1 | | 9 | |
| | | 3 | 8 | | 2 | |
| | | 4 | 0 | | 0 | |
| | Aplicaciones | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 7 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Soporte Información | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 11 | | 5 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [E.19] Fugas de información | Datos / información | 1 | 3 | 70 | 4 | 50 |
| | | 2 | 1 | | 6 | |
| | | 3 | 8 | | 2 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.19] Fugas de información | Claves criptográficas | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Servicios | 1 | 3 | 70 | 0 | 50 |
| | | 2 | 1 | | 9 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Aplicaciones | 1 | 1 | 70 | 3 | 50 |
| | | 2 | 3 | | 6 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Personal | 1 | 3 | 70 | 2 | 50 |
| | | 2 | 2 | | 9 | |
| | | 3 | 7 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.20] Vulnerabilidades de los programas (software) | Servidor de aplicaciones | 1 | 3 | 50 | 7 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 1 | 3 | 70 | 3 | 50 |
| | | 2 | 1 | | 8 | |
| | | 3 | 8 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Office 2010 | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Kaspersky original con actualizaciones automáticas. | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 1 | 3 | 70 | 3 | 50 |
| | | 2 | 1 | | 8 | |
| | | 3 | 8 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.21] Errores de mantenimiento / actualización de programas (software) | Servidor de aplicaciones | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Gestor base de datos | 1 | 3 | 70 | 3 | 50 |
| | | 2 | 1 | | 8 | |
| | | 3 | 8 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Office 2010 | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Kaspersky original con actualizaciones automáticas. | 1 | 0 | 70 | 0 | 50 |
| | | 2 | 3 | | 10 | |
| | | 3 | 8 | | 2 | |
| | | 4 | 1 | | 0 | |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 1 | 3 | 70 | 1 | 50 |
| | | 2 | 1 | | 9 | |
| | | 3 | 8 | | 2 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [E.24] Caída del sistema por agotamiento de recursos | Servicios | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Equipos Informáticos | 1 | 3 | 70 | 3 | 50 |
| | | 2 | 1 | | 8 | |
| | | 3 | 8 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Redes de comunicaciones | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 11 | | 5 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [E.25] Pérdida de equipos -Robo | Equipos Informáticos | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Soporte Información | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Equipamiento Auxiliar | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 10 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [E.28] Indisponibilidad del personal | Personal de la empresa | 1 | 1 | 70 | 3 | 50 |
| | | 2 | 3 | | 5 | |
| | | 3 | 8 | | 4 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.5] Suplantación de la identidad del usuario | Datos / información | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Claves criptográficas | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Servicios | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Aplicaciones | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Redes de comunicaciones | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 11 | | 4 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.6] Abuso de privilegios de acceso | Datos / información | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Claves criptográficas | 1 | 1 | 50 | 9 | 10 |
| | | 2 | 10 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Servicios | 1 | 1 | 50 | 9 | 10 |
| | | 2 | 10 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.6] Abuso de privilegios de acceso | Equipos Informáticos | 1 | 1 | 100 | 0 | 70 |
| | | 2 | 2 | | 3 | |
| | | 3 | 3 | | 8 | |
| | | 4 | 6 | | 1 | |
| | Redes de comunicaciones | 1 | 1 | 70 | 0 | 50 |
| | | 2 | 3 | | 9 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| [A.7] Uso no previsto | Servicios | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Aplicaciones | 1 | 0 | 70 | 0 | 50 |
| | | 2 | 3 | | 10 | |
| | | 3 | 8 | | 2 | |
| | | 4 | 1 | | 0 | |
| | Equipos Informáticos | 1 | 1 | 100 | 1 | 70 |
| | | 2 | 2 | | 3 | |
| | | 3 | 3 | | 7 | |
| | | 4 | 6 | | 1 | |
| | Redes de comunicaciones | 1 | 1 | 70 | 2 | 50 |
| | | 2 | 3 | | 7 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Soporte de Información | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 8 | | 4 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| [A.7] Uso no previsto | Equipamiento Auxiliar | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.7] Uso no previsto | Instalaciones | 1 | 1 | 70 | 1 | 50 |
| | | 2 | 3 | | 8 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| [A.8] Difusión de software dañino | Aplicaciones | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 10 | | 5 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.11] Acceso no autorizado | Datos / información | 1 | 1 | 70 | 2 | 50 |
| | | 2 | 3 | | 7 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Claves criptográficas | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Servicios | 1 | 2 | 50 | 10 | 10 |
| | | 2 | 10 | | 2 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Aplicaciones | 1 | 1 | 70 | 2 | 50 |
| | | 2 | 3 | | 7 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| | Equipos Informáticos | 1 | 3 | 70 | 3 | 50 |
| | | 2 | 1 | | 8 | |
| | | 3 | 8 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Redes de comunicaciones | 1 | 0 | 70 | 0 | 50 |
| | | 2 | 3 | | 9 | |
| | | 3 | 9 | | 3 | |
| | | 4 | 1 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.11] Acceso no autorizado | Soporte de Información | 1 | 1 | 50 | 9 | 10 |
| | | 2 | 10 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Equipamiento Auxiliar | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Instalaciones | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 1 | |
| | | 4 | 0 | | 0 | |
| [A.13] Repudio | Servicios | 1 | 5 | 50 | 9 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.14] Interceptación de información | Redes de comunicaciones | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.15] Modificación deliberada de la información | Datos / información | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Claves criptográficas | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 10 | | 3 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Servicio | 1 | 1 | 50 | 7 | 10 |
| | | 2 | 7 | | 4 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 1 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.14] Interceptación de información (escucha | Aplicaciones | 1 | 4 | 50 | 9 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.18] Destrucción de información | Datos / información | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Claves criptográficas | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Servicios | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Aplicaciones | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| | Soporte de la información | 1 | 2 | 50 | 9 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.19] Divulgación de información | Datos / información | 1 | 2 | 70 | 3 | 50 |
| | | 2 | 1 | | 7 | |
| | | 3 | 9 | | 2 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Claves criptográficas | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 6 | | 2 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Soporte de la información | 1 | 2 | 50 | 7 | 10 |
| | | 2 | 9 | | 5 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.22] Manipulación de programas | Aplicaciones | 1 | 1 | 70 | 2 | 50 |
| | | 2 | 3 | | 7 | |
| | | 3 | 8 | | 3 | |
| | | 4 | 0 | | 0 | |
| [A.23] Manipulación de los equipos | Equipos Informáticos | 1 | 1 | 100 | 2 | 70 |
| | | 2 | 2 | | 2 | |
| | | 3 | 3 | | 6 | |
| | | 4 | 6 | | 2 | |
| | Soportes de Información | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Equipamiento auxiliar | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 9 | | 4 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.24] Denegación de servicio | Equipos Informáticos | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 6 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Servicios | 1 | 2 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Redes de Comunicación | 1 | 3 | 50 | 9 | 10 |
| | | 2 | 8 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.25] Robo | Equipos informáticos | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 6 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 1 | | 0 | |
| | Soporte de Información | 1 | 1 | 50 | 8 | 10 |
| | | 2 | 9 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| [A.26] Ataque destructivo | Equipo Informáticos | 1 | 3 | 50 | 8 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 2 | | 1 | |
| | | 4 | 0 | | 0 | |
| | Soporte de Información | 1 | 2 | 50 | 7 | 10 |
| | | 2 | 10 | | 5 | |
| | | 3 | 0 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.26] Ataque destructivo | Equipo Informáticos | 1 | 1 | 50 | 9 | 10 |
| | | 2 | 8 | | 2 | |
| | | 3 | 3 | | 1 | |
| | | 4 | 0 | | 0 | |
| | instalaciones | 1 | 4 | 50 | 10 | 10 |
| | | 2 | 7 | | 2 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.28] Indisponibilidad del Personal | Personal | 1 | 4 | 50 | 10 | 10 |
| | | 2 | 7 | | 2 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.29] Extorsión | Personal | 1 | 4 | 50 | 8 | 10 |
| | | 2 | 7 | | 4 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |
| [A.30] Ingeniería Social | Personal | 1 | 4 | 50 | 9 | 10 |
| | | 2 | 7 | | 3 | |
| | | 3 | 1 | | 0 | |
| | | 4 | 0 | | 0 | |

***Fuente: Elaboración Propia***

## 4.3. Matriz resumen de las encuestas aplicadas, calculó de las diferencias de cada par (pre test – pos test)

Luego de realizar las respectivas observaciones del Pre test y Pos test aplicado a los riesgos asociados de los activos de información de la empresa NET-Consultores S.A.C y habiendo obtenido los resultados, se procedió a llenar el siguiente cuadro para la respectiva verificación de la hipótesis, de acuerdo a la probabilidad con la que ocurre cada riesgo correspondiente a cada activo de información; la evaluación se llevará a cabo de acuerdo a los 142 activos encontrados en la empresa NET-Consultores S.A.C.

**Tabla 19: Diferencia entre el pre test y el pos test**

| Riesgo | Activo | Pre test (%) | Pos test (%) | Dif. (Pre-Pos) % |
|---|---|---|---|---|
| [N.1] Fuego<br>[N.2] Daños por agua | Equipos informáticos.<br>Instalaciones. | 50 | 10 | 40 |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipos informáticos.<br>Instalaciones. | 70 | 50 | 20 |
| N.1] Fuego<br>[N.2] Daños por agua | Soporte de almacenamiento. | 50 | 10 | 40 |
| [I.1] Fuego<br>[I.2] Daños por agua | Soporte de almacenamiento. | 50 | 10 | 40 |
| [N.1] Fuego<br>[N.2] Daños por agua | Equipamiento Auxiliar. | 50 | 10 | 40 |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipamiento Auxiliar. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [N.*] Desastres naturales | Equipos informáticos. | 70 | 50 | 20 |
| | Soporte de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |
| | Instalaciones. | 50 | 10 | 40 |
| [I.*] Desastres industriales | Equipos informáticos. | 70 | 50 | 20 |
| | Soporte de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |
| | Instalaciones. | 50 | 10 | 40 |
| [I.3] Contaminación mecánica | Equipos informáticos. | 70 | 70 | 0 |
| | Soporte de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |
| I.4] Contaminación electromagnética | Router de acceso inalámbrico. | 100 | 70 | 30 |
| [I.5] Avería de origen físico o lógico | Software - Aplicaciones Informáticas. | 100 | 70 | 30 |
| | Equipos informáticos. | 70 | 50 | 20 |
| | Soportes de Información. | 50 | 10 | 40 |
| | Equipamiento Auxiliar. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [I.6] Corte del suministro eléctrico | Equipos Informáticos. | 100 | 70 | 30 |
| | Soporte de Información (electrónicos). | 50 | 10 | 40 |
| | Ups computadores | 50 | 10 | 40 |
| [I.7] Condiciones inadecuadas de temperatura o humedad | Equipos Informáticos. | 100 | 70 | 30 |
| [I.8] Fallo de servicios de comunicaciones | Redes de comunicaciones (Red inalámbrica, red local e internet) | 100 | 70 | 30 |
| [I.9] Interrupción de otros servicios y suministros esenciales. | Equipamiento Auxiliar. | 50 | 10 | 40 |
| [I.10] Degradación de los soportes de almacenamiento de la información. | Soportes de Información. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios | Archivos de proyectos. | 100 | 70 | 30 |
| | Archivos de Clientes | 50 | 10 | 40 |
| | Archivo de Contabilidad | 50 | 10 | 40 |
| | Archivos de Informes y licencias expedidas | 100 | 50 | 50 |
| | Archivo de Copias de seguridad de la información | 50 | 10 | 40 |
| | Datos de configuración de servidores y equipos | 50 | 10 | 40 |
| | Datos de Gestión de proyectos radicados | 50 | 10 | 40 |
| | Contraseñas de acceso de empleados | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios | Claves Criptográficas | 50 | 10 | 40 |
| [E.1] Errores de los usuarios | Servicios prestados a usuarios externos bajo relación contractual | 50 | 10 | 40 |
| | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | 50 | 10 | 40 |
| | Servicio de internet que acceden los empleados. | 70 | 50 | 20 |
| | Manejo de correos electrónicos | 50 | 10 | 40 |
| | Servicio de almacenamiento de información en el servidor de bases de datos. | 70 | 50 | 20 |
| | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo. | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.1] Errores de los usuarios Aplicaciones | Servidor de aplicaciones | 50 | 10 | 40 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 50 | 10 | 40 |
| | Office 2010 | 50 | 10 | 40 |
| | Kaspersky original con actualizaciones automáticas. | 50 | 10 | 40 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas. | 70 | 50 | 20 |
| [E.1] Errores de los usuarios. Soporte de información | Soportes de Información. | 70 | 50 | 20 |
| [E.4] Errores de configuración | Datos de configuración de servidores y equipos | 50 | 10 | 40 |
| [E.7] Deficiencias en la organización | Personal | 100 | 70 | 30 |
| | Administrador de sistemas | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.8] Difusión de software dañino | Software –Aplicaciones Informáticas | 50 | 10 | 40 |
| [E.9] Errores de [re-]encaminamiento | Servicios | 50 | 10 | 40 |
| | Software –Aplicaciones Informáticas | 50 | 10 | 40 |
| | Redes de comunicaciones | 50 | 10 | 40 |
| [E.14] Escapes de información | Activos esenciales | 50 | 10 | 40 |
| | Datos / información | 50 | 10 | 40 |
| [E.15] Alteración accidental de la información | Datos / información | 70 | 50 | 20 |
| [E.18] Destrucción de la información | Datos / información | 70 | 50 | 20 |
| | Aplicaciones | 50 | 10 | 40 |
| | Soporte Información | 50 | 10 | 40 |
| [E.19] Fugas de información | Datos / información | 70 | 50 | 20 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 70 | 50 | 20 |
| | Aplicaciones | 70 | 50 | 20 |
| | Personal | 70 | 50 | 20 |

| | | | | |
|---|---|---|---|---|
| [E.20] Vulnerabilidades de los programas (software) | Servidor de aplicaciones | 50 | 10 | 40 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 70 | 50 | 20 |
| | Office 2010 | 50 | 10 | 40 |
| | Kaspersky original con actualizaciones automáticas. | 50 | 10 | 40 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 70 | 50 | 20 |

| | | | | |
|---|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | Servidor de aplicaciones | 50 | 10 | 40 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 70 | 50 | 20 |
| | Office 2010 | 50 | 10 | 40 |
| | Kaspersky original con actualizaciones automáticas. | 70 | 50 | 20 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 70 | 50 | 20 |
| [E.24] Caída del sistema por agotamiento de recursos | Servicios | 50 | 10 | 40 |
| | Equipos Informáticos | 70 | 50 | 20 |
| | Redes de comunicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [E.25] Pérdida de equipos -Robo | Equipos Informáticos | 50 | 10 | 40 |
| | Soporte Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| [E.28] Indisponibilidad del personal | Personal de recepción, área técnica, administrativa y archivo | 70 | 50 | 20 |
| [A.5] Suplantación de la identidad del usuario | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 50 | 10 | 40 |
| | Redes de comunicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.6] Abuso de privilegios de acceso | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Equipos Informáticos | 100 | 70 | 30 |
| | Redes de comunicaciones | 70 | 50 | 20 |
| [A.7] Uso no previsto | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 70 | 50 | 20 |
| | Equipos Informáticos | 100 | 70 | 30 |
| | Redes de comunicaciones | 70 | 50 | 20 |
| | Soporte de Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| | Instalaciones | 70 | 50 | 20 |

| | | | | |
|---|---|---|---|---|
| [A.8] Difusión de software dañino | Aplicaciones | 50 | 10 | 40 |
| [A.11] Acceso no autorizado | Datos / información | 70 | 50 | 20 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 70 | 50 | 20 |
| | Equipos Informáticos | 70 | 50 | 20 |
| | Redes de comunicaciones | 70 | 50 | 20 |
| | Soporte de Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| | Instalaciones | 50 | 10 | 40 |
| [A.13] Repudio | Servicios | 50 | 10 | 40 |
| [A.14] Interceptación de información | Redes de comunicaciones | 50 | 10 | 40 |
| [A.15] Modificación deliberada de la información | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicio | 50 | 10 | 40 |
| | Aplicaciones | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.18] Destrucción de información | Datos / información | 50 | 10 | 40 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Aplicaciones | 50 | 10 | 40 |
| | Soporte de la información | 50 | 10 | 40 |
| [A.19] Divulgación de información | Datos / información | 70 | 50 | 20 |
| | Claves criptográficas | 50 | 10 | 40 |
| | Soporte de la información | 50 | 10 | 40 |
| [A.22] Manipulación de programas | Aplicaciones | 70 | 50 | 20 |
| [A.23] Manipulación de los equipos | Equipos Informáticos | 100 | 70 | 30 |
| | Soportes de Información | 50 | 10 | 40 |
| | Equipamiento auxiliar | 50 | 10 | 40 |
| [A.24] Denegación de servicio | Equipos Informáticos | 50 | 10 | 40 |
| | Servicios | 50 | 10 | 40 |
| | Redes de Comunicación | 50 | 10 | 40 |
| [A.25] Robo | Equipos informáticos | 50 | 10 | 40 |
| | Soporte de Información | 50 | 10 | 40 |

| | | | | |
|---|---|---|---|---|
| [A.26] Ataque destructivo | Equipo Informáticos | 50 | 10 | 40 |
| | Soporte de Información | 50 | 10 | 40 |
| | Equipamiento Auxiliar | 50 | 10 | 40 |
| | instalaciones | 50 | 10 | 40 |
| [A.28] Indisponibilidad del Personal | Personal | 50 | 10 | 40 |
| [A.29] Extorsión | Personal | 50 | 10 | 40 |
| [A.30] Ingeniería Social | Personal | 50 | 10 | 40 |
| | **SUMA** | **8 290** | **3 360** | **4 930** |
| | **MEDIAS** | **58.38** | **23.66** | **34.72** |
| | **DESVIACIÓN ESTÁNDAR** | **14.66** | **21.35** | **8.89** |

***Fuente: Tabla33 Relación de amenazas por activo***

Como podemos observar el promedio del pre test es de 58,38 corresponden a la frecuencia de ocurrencias de las amenazas de los riesgos, mientras que el promedio del pos test es de 23,66 haciendo una diferencia de 34,72, demostrando así que la implementación del sistema de seguridad de los activos de información, ha permitido disminuir las amenazas de los riesgos identificados en la empresa.

# V. DISCUSIÓN DE LOS RESULTADOS

A través del desarrollo de la presente tesis, se ha logrado establecer cuál es la situación actual de los activos de información de la empresa NET-Consultores S.A.C., de esta manera se pudo evidenciar los riesgos derivado de cada activo de información, y proponiendo una alternativa de solución denominada Sistema de Gestión de Seguridad de la Información.

Se ha logrado realizar la fase de análisis diseño del Sistema de Gestión de Seguridad de Seguridad, obteniendo la clasificación de los activos y los riesgos asociados a ellos dentro de la empresa NET-Consultores S.A.C.

Se logró diseñar el Sistema de Gestión de Seguridad de la Información para la empresa NET-Consultores S.A.C.; Se utilizó la metodología MAGERIT; lo cual fue necesario establecer Políticas de Seguridad de Información que contengan lineamientos para una correcta administración de la información con el fin de garantizar la seguridad de los activos esenciales e importantes para la empresa.

Se implementó satisfactoriamente el Sistema de Gestión de Seguridad de la Información en la empresa NET-Consultores S.A.C.; aplicado a los riesgos asociados a los activos de información; pero la empresa debe estar preparada para para actuar de manera inmediata ante cualquier eventualidad que pueda poner en peligro el normal funcionamiento y el futuro de la empresa, debido que constantemente se presentan más activos de información, más riesgos o amenazas.

Se ha logrado determinar a través de la prueba Z de verificación de hipótesis, que luego de la implementación del Sistema de Gestión de Seguridad de la Información aplicado a los riesgos asociados a los activos de información de la empresa NET-Consultores, se han obtenido excelentes resultados, afirmando que la implementación de un Sistema de Gestión de Seguridad de la Información minimizará el impacto de los riesgos asociados a los activos de información en la empresa NET-Consultores S.A.C.

Además se determinó que si influye significativamente la implementación de un Sistema de Gestión de Seguridad de la Información sobre el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

Según Justino (2015), en su tesis titulada “Diseño de un Sistema de Gestión de Seguridad de Información para una Empresa Inmobiliaria Alineado a la Norma ISO/IEC 27001:2013” concluye que: Es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad. Este resultado concuerda con los resultados obtenidos en el estudio respecto al diseño de un Sistema de Gestión de Seguridad de la Información.

Barrantes & Hugo (2012) en su tesis “Diseño e Implementación de un Sistema de Seguridad de Información en Procesos Tecnológicos” concluye que: Aún después de implementar un buen sistema de gestión de seguridad de información, en el futuro se presentan más activos de información, más amenazas, vulnerabilidades y por lo tanto, mayores riesgos. Este escenario no se puede evitar; es por ello que se concluye, que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad que se identifique. Este estudio concluye con un resultado similar a la investigación realizada.

# CAPÍTULO IV

# VI. CONCLUSIONES

- ✓ Se logró diseñar el Sistema de Gestión de Seguridad de la Información para la empresa NET-Consultores S.A.C.; Se utilizó la metodología MAGERIT; lo cual fue necesario establecer Políticas de Seguridad de Información que contengan lineamientos para una correcta administración de la información con el fin de garantizar la seguridad de los activos esenciales e importantes para la empresa.

- ✓ Se implementó satisfactoriamente el Sistema de Gestión de Seguridad de la Información en la empresa NET-Consultores S.A.C.; aplicado a los riesgos asociados a los activos de información; pero la empresa debe estar preparada para para actuar de manera inmediata ante cualquier eventualidad que pueda poner en peligro el normal funcionamiento y el futuro de la empresa, debido que constantemente se presentan más activos de información, más riesgos o amenazas.

- ✓ La implementación del Sistema de Gestión de Seguridad de la Información en la empresa NET-Consultores S.A.C permitió minimizar los riesgos asociados a los activos de información. Al realizar la prueba Z de contrastación de hipótesis se encontró que -Zc < -Zt (-15.97 < -1.96), lo que permitió rechazar la hipótesis nula y aceptar la hipótesis alterna a un nivel de significancia de 0.05 esto confirmó que la implementación de un Sistema de Gestión de Seguridad de la Información minimizó el impacto de los riesgos asociados a los activos de información en la empresa NET-Consultores S.A.C.

- ✓ Se ha cumplido con el objetivo general y se determinó que si influye significativamente la implementación de un Sistema de Gestión de Seguridad de la Información sobre el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C.

# VII. RECOMENDACIONES

- ✓ Se recomienda a las empresas implementar un sistema de gestión de seguridad de la información, ya que esto les permitirá minimizar los riesgos.
- ✓ Se recomienda considerar al Sistema de Gestión de Seguridad de la Información como un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.
- ✓ Se recomienda realizar más investigaciones sobre el tema tratado en la presente investigación.
- ✓ Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se va a proporcionar con un SGSI es permanente para lo cual es necesario de un proceso continuo.

## VIII. REFERENCIAS BIBLIOGRÁFICAS


1. Arias, F. (2004) “El proyecto de investigación: Introducción a la Metodología científica”.

2. Alexander G, A. (2007). “Diseño de un Sistema de Gestión de Seguridad de Información/Óptica ISO/IEC 27001:2005”. Primera edición. Bogotá: Alfaomega Colombiana S.A.

3. Barrantes Porras, C. E; & Hugo Herrera, J. R. (2012). Diseño e Implementación de un Sistema de Seguridad de Información en Procesos Tecnológicos, Lima.

4. Buenaño, J. L; & Granda, M. A. (2009). Planeación Y Diseño De Un Sistema De Gestión De Seguridad De La Información Basado En La Norma Iso/Iec 27001 - 27002 Guayaquil – Ecuador.

5. Donado, Siler A.& Flechas, A.(2001)“Seguridad Computacional” .Primera edición Cauca.

   http://www.govannom.org/seguridad/seg_general/seg_com.pdf

6. De la Cruz Guerrero, C. W; & Vásquez Montenegro, J. C. (2008). “Elaboración Y Aplicación De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Para La Realidad Tecnológica De La USAT”, Chiclayo.

7. Espinoza, A; & Hans, R. (2013). Análisis y Diseño de un Sistema de Gestión de Seguridad de Información Basado en la Norma Iso/Iec 27001:2005 para una empresa de Producción y Comercialización de Productos de Consumo Masivo, Lima.

8. Fernández, E. & Piattini, M.(2003)“Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada”. Primera edición. Madrid: Ediciones Aenor.

9. García, A. & Alegre, M.(2011)“Seguridad Informática”. Primera edición. Madrid: Ediciones Paraninfo SA.

10. ISMS International User Group 2012 ISMS Certificates.

    http://www.iso27001certificates.com/

11. INTERNATIONAL STANDARD ISO/IEC 27001 2005 Information technology — Security techniques — Information security management system— Requirements. Primer Edition.

12. INTERNATIONAL STANDARD ISO/IEC 27002 2005 Information technology — Security techniques — Code of practice for information security management. Primer Edition.

13. ISO/IEC 13335-1:2004, Information Technology – Security techniques – Management of information and communications technology security – Part1: Concepts and models for information and communications technology security management.

14. ISO/IEC 17799:2005, Information Technology – Security techniques – Code of practice for information security management.

15. ISO/IEC 18044:2004, Information Technology – Security techniques – Information security incident management.

16. ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards.

17. ISO27000.es 2005 ISO 27001: “Auditoria y Certificación”.

    http://www.iso27000.es/certificacion.html#section5b.

18. Justino Salinas, Z. I.(2015)“Diseño de un Sistema de Gestión de Seguridad de Información para una Empresa Inmobiliaria Alineado a la Norma Iso/Iec 27001:2013”, Lima.

19. López, A. A. (2011). Diseño de un plan de gestión de seguridad de la información. Caso: dirección de informática de la alcaldía del municipio Jiménez del estado Lara, Barquisimeto.

20. Mantilla Guerra, A. R. (2009). Diseño de un Sistema de Gestión de Seguridad de la Información para Cooperativas De Ahorro y Crédito en Base a la Norma Iso 27001, Quito.

21. Qualitas Consultores 2012 Normas: ISO/ IEC 27001.

    http://qualitas.com.pe/normas/iso-27001

22. Talavera Álvarez, V. R. (2015). “Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la Iso/Iec 27001:2013”, Lima.

23. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012). “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, Madrid.

23. Córdoba Suárez, A. E. (2015). "Diseño e Implementación de un SGSI para el Área de Informática de la Curaduría Urbana Segunda de Pasto Bajo la Norma ISO/IEC 27001", Colombia.

# IX. ANEXO

## 9.1. Anexo N° 01 – Cuestionario

### ENCUESTA PARA LA APLICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Por medio del presente instrumento se va a verificar la frecuencia con la que sucede una amenaza o riesgo con respecto a un determinado activo dentro de la empresa NET-Consultores S.A.C.

**INDICACIONES:** Marcar la siguiente cartilla de observación con una “X” la frecuencia con la que ocurre un riesgo respecto a un activo dentro de la empresa; donde (1: Poco Frecuente, cada varios años; 2: Normal, una vez al año; 3: Frecuente, mensualmente y 4: Muy frecuente, A diario).

**PREGUNTAS ESPECÍFICAS**

**A. RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN**

| Amenaza | Activo | Frecuencia de la amenaza | | | |
|---|---|---|---|---|---|
| [N.1] Fuego<br>[N.2] Daños por agua | Equipos informáticos<br>Instalaciones | 1 | 2 | 3 | 4 |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipos informáticos<br>Instalaciones | 1 | 2 | 3 | 4 |
| N.1] Fuego<br>[N.2] Daños por agua | Soporte de almacenamiento | 1 | 2 | 3 | 4 |
| [I.1] Fuego<br>[I.2] Daños por agua | Soporte de almacenamiento | 1 | 2 | 3 | 4 |
| [N.1] Fuego<br>[N.2] Daños por agua | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| [I.1] Fuego<br>[I.2] Daños por agua | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| [N.*] Desastres naturales | Equipos informáticos | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| | Instalaciones | 1 | 2 | 3 | 4 |
| [I.*] Desastres industriales | Equipos informáticos, | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| | Instalaciones | 1 | 2 | 3 | 4 |
| [I.3] Contaminación mecánica | Equipos informáticos, | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| [I.4] Contaminación electromagnética | Router de acceso inalámbrico. | 1 | 2 | 3 | 4 |
| [I.5] Avería de origen físico o lógico | Software - Aplicaciones Informáticas | 1 | 2 | 3 | 4 |
| | Equipos informáticos | 1 | 2 | 3 | 4 |
| | Soportes de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| [I.6] Corte del suministro eléctrico | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Soporte de Información (electrónicos) | 1 | 2 | 3 | 4 |
| | Ups computadores | 1 | 2 | 3 | 4 |
| [I.7] Condiciones inadecuadas de temperatura o humedad | Equipos Informáticos | 1 | 2 | 3 | 4 |
| [I.8] Fallo de servicios de comunicaciones | Redes de comunicaciones (Red inalámbrica, red local e internet) | 1 | 2 | 3 | 4 |
| [I.9] Interrupción de otros servicios y suministros esenciales. | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| [I.10] Degradación de los soportes de almacenamiento de la información. | Soportes de Información | 1 | 2 | 3 | 4 |
| [E.1] Errores de los usuarios Datos/Información | Archivos de proyectos | 1 | 2 | 3 | 4 |
| | Archivos de Clientes | 1 | 2 | 3 | 4 |
| | Archivo de Contabilidad | 1 | 2 | 3 | 4 |
| | Archivos de Informes y licencias expedidas | 1 | 2 | 3 | 4 |
| | Archivo de Copias de seguridad de la información | 1 | 2 | 3 | 4 |
| | Datos de configuración de servidores y equipos | 1 | 2 | 3 | 4 |
| | Datos de Gestión de proyectos radicados | 1 | 2 | 3 | 4 |
| | Contraseñas de acceso de empleados | 1 | 2 | 3 | 4 |
| [E.1] Errores de los usuarios | Claves Criptográficas | 1 | 2 | 3 | 4 |
| [E.1] Errores de los usuarios Servicios | Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos) | 1 | 2 | 3 | 4 |
| | Servicios prestados a trabajadores tanto al interior como haciendo uso de internet. | 1 | 2 | 3 | 4 |
| | Servicio de internet al que pueden acceder los empleados. | 1 | 2 | 3 | 4 |
| | Manejo de correos electrónicos | 1 | 2 | 3 | 4 |
| | Servicio de almacenamiento de información en el servidor de bases de datos. | 1 | 2 | 3 | 4 |
| | Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde | 1 | 2 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | esté ingresando, considerando el desempeño como teletrabajo. | | | | |
| [E.1] Errores de los usuarios Aplicaciones | Servidor de aplicaciones | 1 | 2 | 3 | 4 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 1 | 2 | 3 | 4 |
| | Office 2010 | 1 | 2 | 3 | 4 |
| | Kaspersky original con actualizaciones automáticas. | 1 | 2 | 3 | 4 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas. | 1 | 2 | 3 | 4 |
| [E.1] Errores de los usuarios. Soporte de información | Soportes de Información. | 1 | 2 | 3 | 4 |
| [E.4] Errores de configuración | Datos de configuración de servidores y equipos. | 1 | 2 | 3 | 4 |
| [E.7] Deficiencias en la organización | Personal de recepción, área técnica, administrativa y archivo | 1 | 2 | 3 | 4 |
| | Administrador de sistemas | 1 | 2 | 3 | 4 |
| [E.8] Difusión de software dañino | Software–Aplicaciones Informáticas | 1 | 2 | 3 | 4 |
| [E.9] Errores de [re-]encaminamiento | Servicios | 1 | 2 | 3 | 4 |
| | Software–Aplicaciones Informáticas | 1 | 2 | 3 | 4 |
| | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| [E.14] Escapes de información | Activos esenciales | 1 | 2 | 3 | 4 |
| | Datos / información | 1 | 2 | 3 | 4 |
| [E.15] Alteración accidental de la información | Datos / información | 1 | 2 | 3 | 4 |

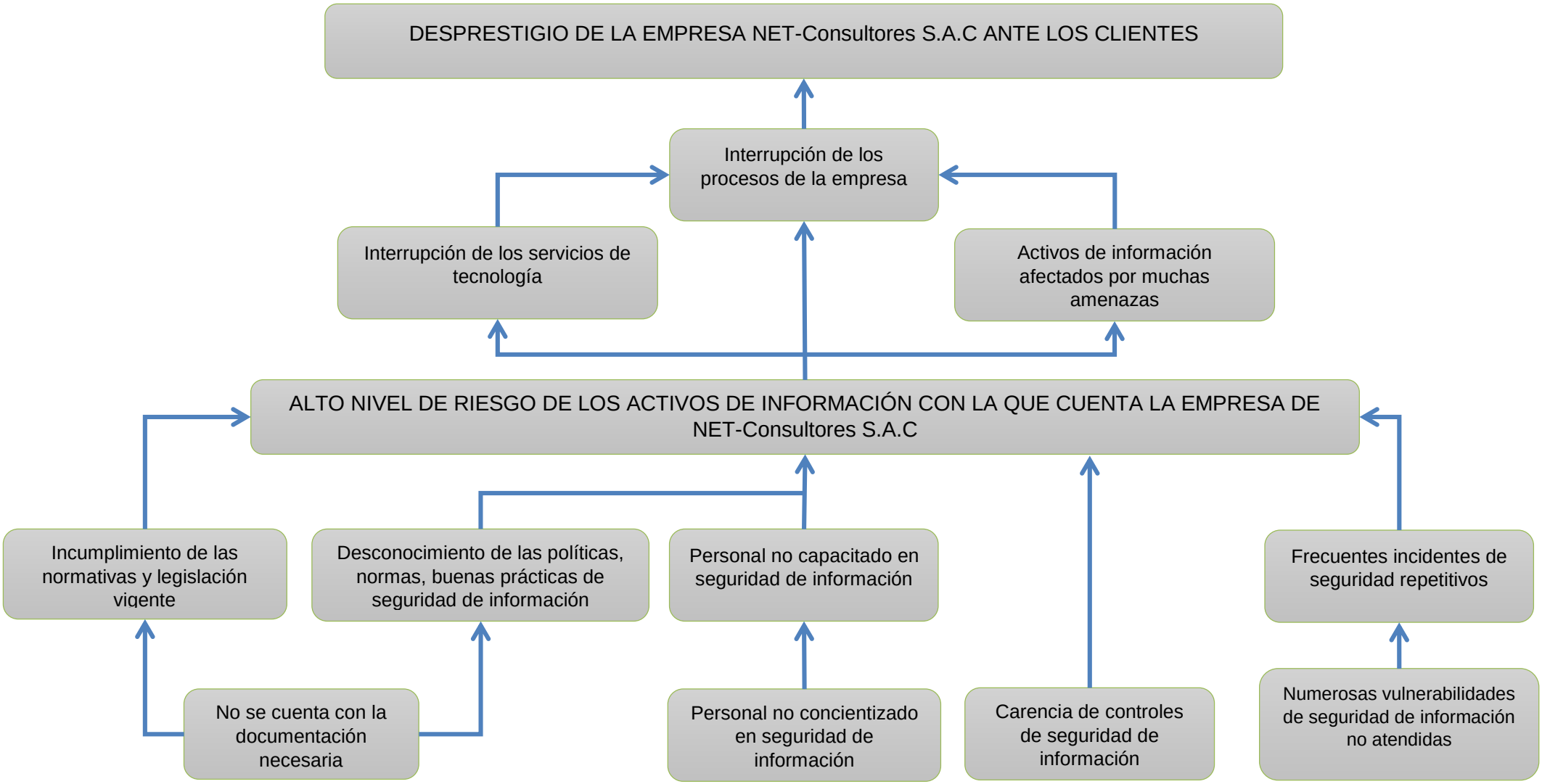
| | | | | | |
|---|---|---|---|---|---|
| [E.18] Destrucción de la información | Datos / información | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| | Soporte Información | 1 | 2 | 3 | 4 |
| [E.19] Fugas de información | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Servicios | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| | Personal | 1 | 2 | 3 | 4 |
| [E.20] Vulnerabilidades de los programas (software) | Servidor de aplicaciones | 1 | 2 | 3 | 4 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 1 | 2 | 3 | 4 |
| | Office 2010 | 1 | 2 | 3 | 4 |
| | Kaspersky original con actualizaciones automáticas. | 1 | 2 | 3 | 4 |
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 1 | 2 | 3 | 4 |
| [E.21] Errores de mantenimiento / actualización de programas (software) | Servidor de aplicaciones | 1 | 2 | 3 | 4 |
| | Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa. | 1 | 2 | 3 | 4 |
| | Office 2010 | 1 | 2 | 3 | 4 |
| | Kaspersky original con actualizaciones automáticas. | 1 | 2 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas | 1 | 2 | 3 | 4 |
| [E.24] Caída del sistema por agotamiento de recursos | Servicios | 1 | 2 | 3 | 4 |
| | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| [E.25] Pérdida de equipos -Robo | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Soporte Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| [E.28] Indisponibilidad del personal | Personal de recepción, área técnica, administrativa y archivo | 1 | 2 | 3 | 4 |
| [A.5] Suplantación de la identidad del usuario | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Servicios | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| [A.6] Abuso de privilegios de acceso | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Servicios | 1 | 2 | 3 | 4 |
| | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| [A.7] Uso no previsto | Servicios | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| | Instalaciones | 1 | 2 | 3 | 4 |
| [A.8] Difusión de software dañino | Aplicaciones | 1 | 2 | 3 | 4 |

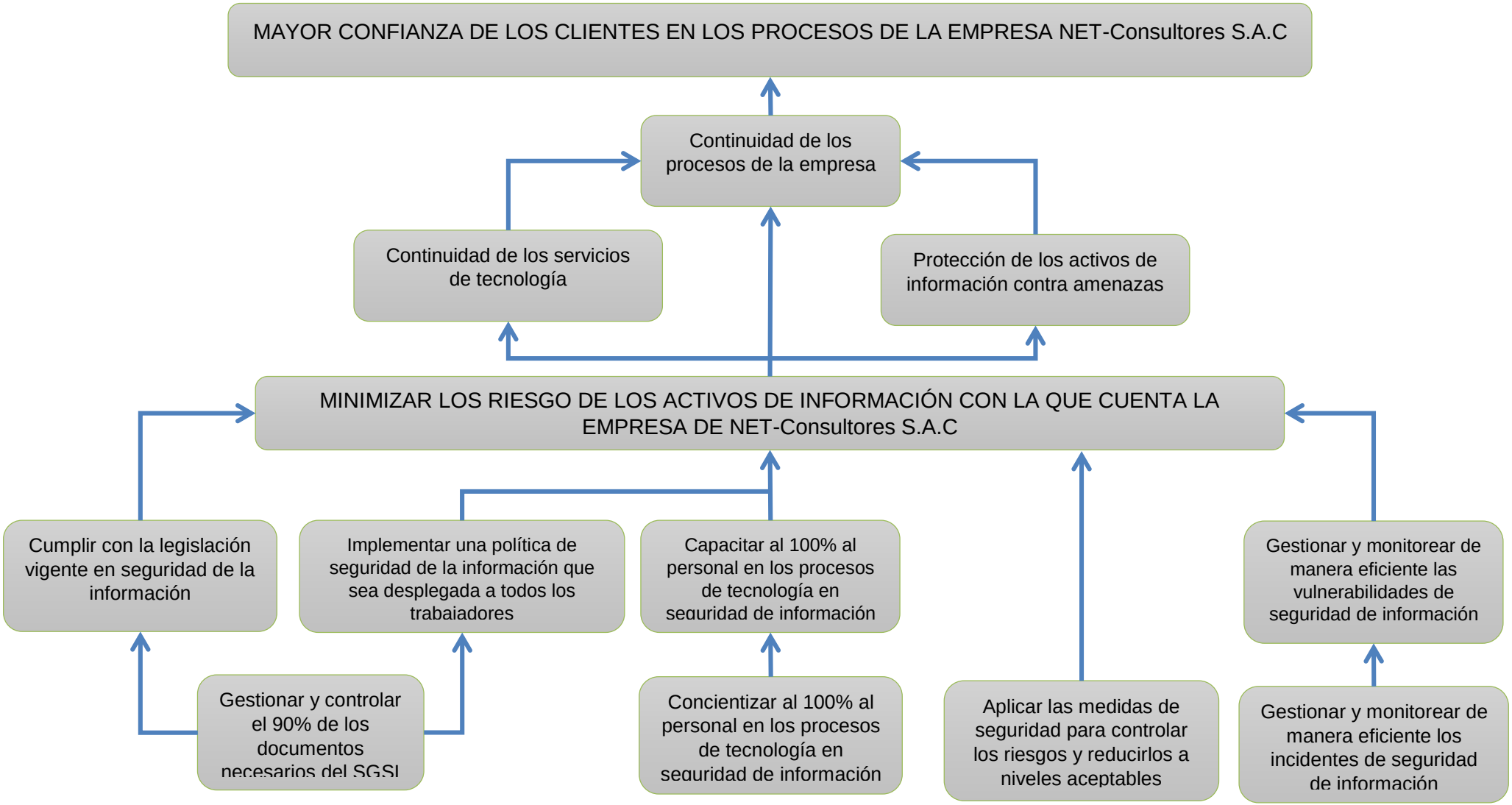
| | | | | | |
|---|---|---|---|---|---|
| [A.11] Acceso no autorizado | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Servicios | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| | Instalaciones | 1 | 2 | 3 | 4 |
| [A.13] Repudio | Servicios | 1 | 2 | 3 | 4 |
| [A.14] Interceptación de información (escucha pasiva) | Redes de comunicaciones | 1 | 2 | 3 | 4 |
| [A.15] Modificación deliberada de la información | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Servicio | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| [A.18] Destrucción de información | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Servicios | 1 | 2 | 3 | 4 |
| | Aplicaciones | 1 | 2 | 3 | 4 |
| | Soporte de la información | 1 | 2 | 3 | 4 |
| [A.19] Divulgación de información | Datos / información | 1 | 2 | 3 | 4 |
| | Claves criptográficas | 1 | 2 | 3 | 4 |
| | Soporte de la información | 1 | 2 | 3 | 4 |
| [A.22] Manipulación de programas | Aplicaciones | 1 | 2 | 3 | 4 |
| [A.23] Manipulación de los equipos | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Soportes de Información | 1 | 2 | 3 | 4 |
| | Equipamiento auxiliar | 1 | 2 | 3 | 4 |
| [A.24] Denegación de servicio | Equipos Informáticos | 1 | 2 | 3 | 4 |
| | Servicios | 1 | 2 | 3 | 4 |
| | Redes de Comunicación | 1 | 2 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| [A.25] Robo | Equipos informáticos | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| [A.26] Ataque destructivo | Equipo Informáticos | 1 | 2 | 3 | 4 |
| | Soporte de Información | 1 | 2 | 3 | 4 |
| | Equipamiento Auxiliar | 1 | 2 | 3 | 4 |
| | instalaciones | 1 | 2 | 3 | 4 |
| [A.28] Indisponibilidad del Personal | Personal | 1 | 2 | 3 | 4 |
| [A.29] Extorsión | Personal | 1 | 2 | 3 | 4 |
| [A.30] Ingeniería Social | Personal | 1 | 2 | 3 | 4 |

## 9.2. Anexo N° 02 - Árbol de Problemas



## 9.3. Anexo N° 03 - Árbol de Objetivos



## 9.4. Anexo N° 04 – Diagrama de Implementación de un Sistema de Gestión de Seguridad de la Información