# ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

## Guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados

**FABRICIO ALFREDO JIMÉNEZ CAICEDO**

**Trabajo de titulación: Proyecto de Investigación y Desarrollo, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:**

**MAGÍSTER EN SEGURIDAD TELEMÁTICA**

**RIOBAMBA-ECUADOR**

**NOVIEMBRE 2022**

**©2022, Fabricio Alfredo Jiménez Caicedo**

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el derecho del autor.

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado: Guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados, de responsabilidad de Fabricio Alfredo Jiménez Caicedo, ha sido prolijamente revisado y se autoriza su presentación.

Ing. M.Sc. OSWALDO GEOVANNY MARTÍNEZ GUASHIMA
**PRESIDENTE**

Firmado electrónicamente por:
OSWALDO GEOVANNY MARTINEZ GUASHIMA

Ing. Mag. MARCO VINICIO RAMOS VALENCIA
**DIRECTOR**

Firmado electrónicamente por:
MARCO VINICIO RAMOS VALENCIA

Ing. Mag. NANCY PAOLA VELOZ PARRA
**MIEMBRO**

Firmado electrónicamente por:
NANCY PAOLA VELOZ PARRA

Ing. Mag. MAYRA ALEJANDRA OÑATE ANDINO
**MIEMBRO**

Firmado electrónicamente por:
MAYRA ALEJANDRA OÑATE ANDINO

Riobamba, noviembre 2022

## DERECHOS INTELECTUALES

Yo, Fabricio Alfredo Jiménez Caicedo, con cédula de identidad 080291741-9, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.


FABRICIO ALFREDO JIMÉNEZ CAICEDO
N° de Cédula: 0802917419

## DECLARACIÓN DE AUTENTICIDAD

Yo, **Fabricio Alfredo Jiménez Caicedo**, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Firmado electrónicamente por:
**FABRICIO ALFREDO JIMENEZ CAICEDO**

FABRICIO ALFREDO JIMÉNEZ CAICEDO
N° de Cédula: 0802917419

## DEDICATORIA

Al culminar esta etapa de mi vida profesional que ha sido el resultado de mi esfuerzo, entrega y constancia, dedico este trabajo:

A Dios por brindarme la sabiduría y guiarme en cada uno de mis pasos, a mi madre Lcda. Victoriana Eugenia Caicedo Ortiz, a mi familia y todas las personas que permanentemente me han brindado su apoyo y confianza, por ser quienes han estado conmigo sin importar distancia ni circunstancia.

**Fabricio Alfredo**

**AGRADECIMIENTO**

Agradezco a Dios por la vida, salud y fortaleza dadas para llegar hasta aquí, a mi familia que en todo momento ha sido el pilar fundamental; gracias a ellos por la confianza que depositaron en mí para formarme como profesional.

Agradezco a los docentes de la Escuela de Postgrado y Educación Continua de la Escuela Superior Politécnica del Chimborazo que supieron impartir sus conocimientos para alcanzar la Maestría en Seguridad Telemática.

**Fabricio Alfredo**

**TABLA DE CONTENIDO**

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

## ÍNDICE DE GRÁFICOS

## ÍNDICE DE ANEXOS

## RESUMEN

El presente trabajo de investigación tuvo como objetivo desarrollar una Guía metodológica de gestiónde riesgos de seguridad de la información en la administración de servidores virtualizados para mejorar el control de posibles eventos que afecten el nivel de seguridad. El tipo de investigación fuebibliográfica, documental y descriptiva, con enfoque cuali-cuantitativo, en un entorno particular, Fibratelecom, proveedor de servicios de internet de la provincia de Chimborazo, la población fueron45 profesionales encargados de la administración de servidores virtualizados, el grupo de estudio fueevaluado con el mismo instrumento antes y después de la aplicación de la guía. Se utilizó la prueba estadística T Student para el análisis de los resultados de la encuesta inicial y la encuesta final, en donde se observa que el valor p es menor al valor de la significancia y adicional a esto en la encuestafinal se obtiene que el 93% de los encuestados respondieron afirmativamente, lo que significa que laguía planteada tiene resultados favorables para identificar y mitigar los riesgos.



**Palabras claves:** <GUÍA METODOLÓGICA>, <GESTIÓN DE RIESGOS>, <SEGURIDAD DE INFORMACIÓN>, <SISTEMAS VIRTUALIZADOS>



Firmado electrónicamente por:
**LUIS ALBERTOCAMINOS VARGAS**

UNIDAD DE PROCESOS TÉCNICOS DBRA ESPOCH

27-10-2022

0155-DBRA-UPT-IPEC-2022

**ABSTRACT**

The objective of this research work was to develop a methodological guide for information security risk management in the administration of virtualized servers to improve the control of possible events that affect the level of security. The type of research was bibliographic, documentary, and descriptive, with a quali-quantitative approach, in a particular environment, FibraTelecom, an internet service provider in the province of Chimborazo, the population was 45 professionals in charge of the administration of virtualized servers, the study group was evaluated with the same instrument before and after the application of the guide. The statistical T Student test was used to analyze the results of the initial survey and the final survey, showing that the p-value is less than the significance value. Additionally, 93% of the respondents answered affirmatively in the final survey, so the proposed guide has favorable results for identifying and mitigating risks.

**Keywords:** <METHODOLOGICAL GUIDE>, <RISK MANAGEMENT>, <INFORMATION SECURITY>, <VIRTUALIZED SYSTEMS>.

# CAPÍTULO I

## 1. INTRODUCCIÓN

La seguridad telemática como un área específica de la TI, Tecnología de la Información ha tomado cuerpo y desarrollo en su proceso de tecnificación y especialmente en cuanto tiene que ver con la seguridad que las informaciones de los usuarios deben tener los servidores virtuales en una empresa, institución o de uso particular. De allí que esta tesis con el tema: "Guía Metodológica de análisis y de gestión de seguridad de la información para los servidores virtualizados" tiene trascendental importancia en que en los últimos años inescrupulosos operadores de estos sistemas han violentado de las seguridades apropiándose indebidamente información de exclusiva propiedad de los usuarios de un sistema virtualizado. El instrumento que como una guía metodológica es el resultado de esta investigación se entrega a los usuarios y operadores de los sistemas virtualizados será de mucha utilidad para asegurar su información dando tranquilidad y confianza en estos sistemas que cada día se apropian del quehacer de la humanidad en un mundo cada vez más inmediato y desarrollado en la información telemática.

### 1.1 Planteamiento del problema

La virtualización de servidores es la evolución de la tecnología informática que ha sido capaz de ayudar a cualquier usuario o empresa con la mayoría de sus necesidades o servicios de Tecnología de la Información desarrollando las capacidades de almacenamiento y procesamiento en una infraestructura cada vez más reducida a un costo total de propiedad más bajo y un retorno sobre la inversión, más elevado.

Sin embargo, la gran aceptación que ha tenido en esta perspectiva, quizás considere solamente los costos inmediatos de contratación, pero por otra parte surgen diversas cuestiones que deben ser consideradas, como por ejemplo el soporte técnico, calidad, geografía y la estrategia para mantener estos servicios confiables y disponibles. Por eso la seguridad es un elemento necesario para mitigar amenazas informáticas y se convierte en una preocupación para dar prioridad de evitar que la operación de los sistemas virtualizados se vea impactada ante un eventual incidente.

El ejercicio de protección o seguridad de la información se torna una controversia para los responsables o líderes de seguridad que deben recurrir a su creatividad para mantener un ambiente

o entorno adecuado e incentivando la puesta en práctica de innovadoras estrategias encaminadas a la protección de la información en todos los niveles de la empresa independientemente de su dimensión ya que las amenazas informáticas pueden afectar a los sistemas sin importar si se encuentran operando en ambientes físicos o virtuales; sin embargo para la eficacia de esta protección existen condiciones particulares de cada entorno sobre la forma de implementar las medidas de seguridad que conllevan a una actividad tecnológica particularizada.

Es importante señalar que las máquinas virtuales a diferencia de un equipo físico, están reducidas a un simple archivo; que, si bien representa flexibilidad para el administrador, también significa una vulnerabilidad que puede ser explotada para robar la máquina completa, incluyendo su contenido. Recordemos que, en los entornos virtuales, varias máquinas virtuales pueden compartir una sola interfaz física, en consecuencia, dichos equipos pueden ser víctimas de diversos tipos de ataques entre una máquina virtual y otra residente en el mismo equipo físico, ante esta situación, el administrador debe estar prevenido.

Recordemos por otro lado que la seguridad virtual se extiende más allá de las máquinas virtuales, por ejemplo, los sistemas de almacenamiento en red se ven expuestos a amenazas y constituyen otra línea de acción para los atacantes. Una recomendación es mantener los sistemas de almacenamiento separados del resto de las máquinas virtuales.

Además, en un esquema virtual, en donde se utilizan equipos para ejecutar las tareas de procesamiento de las máquinas virtuales y su almacenamiento se encuentra en un almacenamiento de red SAN es fácil ver cómo se ve comprometido todo el sistema de almacenamiento cuando no se contemplan este tipo de riesgos, sobre todo al momento de la instrumentación de entornos virtuales basados en sistemas de almacenamiento separado.
En este tipo de operación, existe un servidor denominado Servidor de procesamiento que puede contener una o varias máquinas virtuales y un “Sistema de almacenamiento” (por ejemplo, uno del tipo SAN). Este sistema es un equipo físico separado del servidor de procesamiento, cuya función es alojar los archivos de cada una de las máquinas virtuales a través de interfaces, ya sea de tipo iSCSI o Fiber Channel.

Consideraremos que el análisis es parte del proceso de gestión de riesgos en la que conocemos e inspeccionamos los riesgos y tiene como objetivo inicial la identificación del riesgo a fin de

conocer los sucesos que se pueden producir en la organización y las consecuencias que puedan tener sobre los objetivos de la empresa.

Por esta razón se plantea en este anteproyecto desarrollar una Guía Metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados para lograr la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información.

### 1.2 Situación problemática

Es evidente que en los últimos años la virtualización ha tenido una considerable aceptación dentro de las empresas y, más que una tendencia, se ha convertido en un estándar de la industria. Su adopción incluye beneficios relacionados principalmente con las capacidades de almacenamiento y procesamiento en una infraestructura cada vez más reducida.

En el proceso de adopción y migración hacia este tipo de soluciones, se busca mantener servicios confiables y disponibles. Por ello, la seguridad se convierte en un elemento necesario para mitigar amenazas informáticas como las de:

- No tener en cuenta la seguridad en los proyectos de virtualización ya que la seguridad del entorno debe realizarse previamente al proceso de virtualización en base a un plan de acción que se fundamente en la arquitectura inicial al proceso ya que se dará paso a cambios que permitan una adecuación de los conocimientos y técnicas para la lograr la protección necesaria para el flujo de trabajo, a los sistemas operativos y a los equipos con una nueva tecnología compatible con las máquinas virtuales que han de generar nuevas capas de software que no se toman en cuenta en los sistemas y software convencionales.
- Considerar que las amenazas de la capa de virtualización afectarían a todas las cargas de trabajo dependientes ya que la virtualización es un software sensible como cualquier otro y al presentar vulnerabilidad de considerarse la posibilidad de ataques que afecten las cargas de trabajo afectando todas las operaciones dependientes.
- La falta de sensibilidad y control de las redes internas virtuales señaladas por varios autores, que recomiendan se busque el mismo control en las redes virtuales como se lo hace en las físicas a fin de lograr mayor visibilidad y capacidad de gestión al pasar a la virtualización, reduciendo la mala configuración.

Debe centrarse adicionalmente, a más de la atención en las herramientas de seguridad que deben ser compatibles con las máquinas virtuales para proteger desde dentro en vista de que la administración de los sistemas virtualizados es una función del mencionado hipervisor el que se encuentra sometido a iguales riesgos que los componentes de los equipos clásicos, siendo igualmente un vector de ataque sin importar como opere la tecnología de virtualización, debiendo enfrentarse las amenazas antes de que estas aparezcan. Para el efecto:

- Las cargas de trabajo de los distintos niveles de seguridad han de consolidarse en un solo servidor físico sin la separación suficiente.
- Un control inadecuado de acceso administrativo a la capa de Hipervisor VMM y a las herramientas administrativas.
- La pérdida potencial por la separación de las funciones de red y los controles de seguridad.

A fin de evitar que la operación de los sistemas virtualizados se vea impactada ante un eventual incidente es necesario establecer la Guía Metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados, como objeto de este trabajo.

La Guía Metodológica de gestión de riesgos se compone de una serie de medidas que se deben tomar para prevenir la aparición, o incluso permitir la eliminación de los peligros señalados en párrafos anteriores. Esta gestión de riesgos no es más que un conjunto de procesos específicos y definidos con el fin de hacer todo lo posible para que no se produzcan riesgos en que se deberá tener en cuenta lo siguiente:

- Invertir parte del ahorro en controles
- Implementar un Programa de Seguridad de la Información para entornos virtuales
- Evaluar los procesos de gestión de TI
- Métricas de cumplimiento
- Exigir evaluaciones de vulnerabilidad y pentest
- Estrategia de gestión de riesgos
- Establecer revisiones y auditorias periódicas

Respecto a Educación y Cumplimiento:

- Verificar la capacitación continua del personal que administra entornos virtuales
- Asegurar la participación de personal debidamente certificado

- Verificar la capacitación en la plataforma ante cambio o ingreso de personal
- Establecer un cronograma anual de capacitación
- Verificar periódicamente la gestión de entornos virtuales
- Auditar políticas, procesos y procedimientos de continuidad
- Verificar el Marco Normativo y su cumplimiento en la gestión del servicio

Es importante recordar que las amenazas informáticas pueden afectar a los sistemas señalados, sin embargo, para la protección debe disponerse de una Guía Metodológica de gestión de riesgos propio para las condiciones del entorno e información para implementar estas medidas de seguridad.

El presente trabajo propone desarrollar una Guía Metodológica de gestión de riesgos de la información para los servidores virtualizados que mejore considerablemente las vulnerabilidades generales de seguridad existentes como ataques de HyperJacking, Hipervisor Escape o Ataques a VM entre otras. La misma que se aplicará en el entorno o ambientes de prueba y evaluará los resultados de la Guía Metodológica implementada.

Lo que será definido a través de la Guía Metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados que es el objeto del presente estudio.

### 1.3 Formulación del problema

¿Los recursos metodológicos de la gestión de riesgos de los entornos virtuales utilizados en los sistemas informáticos y de comunicación han tenido el desarrollo y renovación para que los procesos tengan el control necesario?

### 1.4 Preguntas directrices

¿Cuáles son los avances metodológicos en la gestión de riesgos de la seguridad de la información?

¿Cuáles son los componentes que debe contener una guía metodología de gestión riesgos de seguridad de la información para la administración de servidores virtualizados?

¿Se puede aplicar la guía metodológica en el caso de estudio establecido?

¿Se mejora con la aplicación de la guía metodología de gestión de riesgos de seguridad de la información el nivel de control?

## 1.5 Justificación de la investigación

### *1.5.1 Justificación teórica*

El presente trabajo investigativo se enmarca, justificándose en el desarrollo de una Guía Metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados que permitirá mejorar los sistemas de TI en donde la integridad, disponibilidad y confiabilidad sean los pilares fundamentales de la seguridad, como es su objetivo.

Tendrá un aporte bibliográfico ya que el diseño y elaboración de esta guía estará disponible para implementar en cualquier entorno particular o institucional.

### *1.5.2 Justificación metodológica*

La aplicación de un proceso metodológico ordenado y sistematizado, mediante la utilización de técnicas y herramientas permitirá identificar y analizar los riesgos de la seguridad de la información, posterior a esto se procederá a aplicar una Guía Metodológica de gestión de riesgos de seguridad de la información para la administración de servidores virtualizados, generando un instrumento aplicable en cualquier entorno.

### *1.5.3 Justificación práctica*

La aplicación de la Guía Metodológica de gestión de riesgos de seguridad de la información para la administración de servidores virtualizados contribuye con el desarrollo de los sistemas informáticos y computacionales de usuarios personales e instituciones de servicio público y/o empresas particulares, brindando tranquilidad a los usuarios o corporativos que tienen como fuente de su desarrollo económico, social, de servicio en estos sistemas.

## 1.6 Objetivos de Investigación

### *1.6.1 Objetivo General*

Desarrollar una Guía Metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados para mejorar el control de posibles eventos que afecten el nivel de seguridad.

### *1.6.2 Objetivos Específicos*

- Estudiar los fundamentos metodológicos de gestión de riesgos de seguridad de la información existente para adaptarlos a la administración de servidores virtualizados.
- Diseñar la guía metodología de gestión riesgos de seguridad de la información para la administración de servidores virtualizados.
- Aplicar la guía metodológica en un caso de estudio.

## 1.7 Hipótesis

El desarrollo de una guía metodológica para la gestión de riesgos en seguridad de la información, permitirá mejorar el nivel de control de seguridad de los servidores virtualizados.

# CAPÍTULO II

## 2. MARCO TEÓRICO

### 2.1. Antecedentes del problema

La virtualización de servidores se define como la evolución de la tecnología informática que ha ayudado a cualquier usuario o empresa con la mayoría de sus necesidades o servicios de TI (Tecnología de la Información) permitiendo mejorar de las capacidades de almacenamiento y procesamiento en una infraestructura cada vez más minúscula y a un costo total de propiedad más bajo y un retorno sobre la inversión, más elevado que garantiza el desarrollo empresarial tecnológico con visión de futuro.

Pese a ello, la inmensa aceptación que ha tenido en esta perspectiva, quizás considere solamente los costos inmediatos de contratación de los servicios, aparecen sin embargo diversas interrogantes que deben ser consideradas y resueltas como lo relacionado al soporte técnico, calidad y la estrategia para mantener estos servicios confiables y disponibles sin que puedan sufrir daños o enajenación de la información confiada a estos servidores virtuales; por lo que la seguridad, ante todo, es un elemento necesario para mitigar amenazas informáticas y es de gran preocupación apareciendo la necesidad de priorizarlo a fin de evitar que la operación de los sistemas virtualizados se vea impactada ante un eventual incidente interno o externo.

En estos últimos años la virtualización ha tenido una considerable aceptación dentro de las empresas de menor o mayor volumen de información y, más que un estilo de servicio, es un estándar de la industria y desarrollo de las empresas, ya que sus beneficios relacionados principalmente con las capacidades de almacenamiento y procesamiento de datos e información en una infraestructura cada vez más reducida. Evidenciándose permanentemente el proceso de adopción y migración hacia este tipo de soluciones informáticas que se dirigen a mantener servicios confiables y disponibles haciendo que la seguridad se convierte en un elemento fundamental para mitigar amenazas informáticas que puedan perjudicar al usuario.

Situaciones tecnológicas inherentes a la tecnología Informática determinantes para el tratamiento del tema: “Guía metodológica de gestión de riesgos de seguridad de la información para la

administración de los servidores virtualizados" en la presente tesis de Maestría en la Seguridad Telemática.

## 2.2. Bases teóricas

### *2.2.1. Conceptos de Virtualización*

La virtualización es una tecnología que para Martin.D, Marrero. M, Urbano. J, Barra.E y Moreiro. J R (2011) permite "la extracción del sofware de una computadora, encapsulándolo en algo que llamaremos máquina virtual, que será ejecutada en una máquina física ajena a la anterior (p.349), cuya principal ventaja consiste en una optimización del aprovechamiento del hardware que se traduce en una reducción de los costos de mantenimiento y administración de la red interna de la organización, ya que la misma permite transformar una intravet conformada por varios servidores, que en la mayoría de los casos están subutilizados a una estructura que se encuentra conformada por un número reducido de servidores que ofrecen los mismos (Emiliano, 2018).

La virtualización crea un entorno informático simulado, o virtual, en lugar de un entorno físico. A menudo, incluye versiones de hardware, sistemas operativos, dispositivos de almacenamiento, etc., generadas por un equipo. Esto permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones diferentes mientras comparten los recursos de una sola máquina host. (NETEC, 2018)

Entre las posibilidades que la virtualización de servidores y red proporcionan están las siguientes:

- Reducción de costos y mejora de los niveles de servicio.
- Gestión y administración simplificada de infraestructura.
- Facilidad de disponer de entornos de desarrollo/testing.
- Resuelve problemas de falta de capacidad o rendimiento de aplicación.
- Permite a las empresas facilidad de escalabilidad.
- Facilita las soluciones orientadas a la implementación de continuidad operativa.

Para lo cual la virtualización debe superar los retos de:

- Perfil de seguridad aprobado de acuerdo con las directivas establecidas.

- Control de versión adecuada de SO y sus actualizaciones correctas a la hora de implementar nuevas VM.
- Análisis de capacidad para verificar si hay recursos apropiados disponibles para las nuevas VM.
- Afectación de una nueva VM al rendimiento y a la seguridad de otras VM en la misma máquina anfitriona.
- Las vulnerabilidades de los entornos físicos son también aplicables a los entornos virtuales.
- Los hipervisores crean una nueva superficie susceptible de ataque. (Fabián, 2014)

De manera elemental se entiende como virtualización, a la acción de crear un entorno informático simulado, o virtual, en lugar de un entorno físico, en que se puede incluir versiones de hardware, sistemas operativos, dispositivos de almacenamiento, etc., generadas por un equipo. Esta acción permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Lógicamente cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones diferentes mientras comparte los recursos de una sola máquina host. (HART, 2018)

### *2.2.2. Servidor virtual*

Servidor VPS, es un servidor que se instala en una partición o fragmento de un servidor físico, pudiendo tener dentro de dicho servidor físico varios servidores virtuales que funcionan de manera independiente.

Principales ventajas de los servidores virtuales:

- Ahorro de costos.
- Posibilidad de ampliación de la capacidad de almacenamiento.
- Posibilidad de configurar nuevos servicios.
- Ahorro energético.
- Seguridad.
- Versatilidad, se pueden instalar todo tipo de programas y aplicaciones.

### 2.2.3. *El hipervisor*

En el glosario de MVware se define a un hipervisor como un monitor de máquinas virtuales, es un proceso que crea y ejecuta máquinas virtuales, el mismo que permite que un ordenador host preste soporte a varias máquinas virtuales invitadas mediante el uso compartido virtual de sus recursos, como la memoria y el procesamiento.

## 2.3 Tipos de virtualización

En la Tecnología Informática (TI) se define varios modelos de virtualización, entre los cuales están:

### *2.3.1. Virtualización de escritorios*

Ofrece un escenario de valor diferente mediante la sustitución de un grupo de escritorios físicos con la infraestructura de escritorio virtual (VDI), escritorios remotos basados en funciones, sucursales remotas sin necesidad de un servicio de IT especializado y todo el mantenimiento de cientos de lugares de trabajo limitado a varios servidores físicos.

### *2.3.2. Virtualización de red*

Diseñada para dividir el ancho de banda de una red en canales independientes que se asignan a servidores o dispositivos específicos.

### *2.3.3. Virtualización de aplicaciones*

En este caso, a diferencia de una infraestructura de escritorios remota basados en funciones; un entorno virtual se adopta solo para una sola aplicación. Para los enfoques de software como servicio, cada vez más populares, se trata de una elección natural y eficiente.

En la actualidad como resultado general de la aplicación de las tecnologías de la información y la comunicación, TIC’s la mayoría de los appliance están conectados a una entidad llamada “Cloud” cuyo significado es nube y que en términos informáticos se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que normalmente es Internet.

En la virtualización de aplicaciones el cloud computing o computación en la nube es un término amplio que abarca todo lo relacionado con los servicios que se encuentran alojados en internet.

Los de más utilización son:

#### *2.3.3.1. Software como Servicio (SaaS)*

Todo el desarrollo, mantenimiento, actualizaciones, copias de seguridad es responsabilidad del proveedor, es decir, si el servicio se cae es responsabilidad del proveedor volver a hacer que funcione.

Se trata de cualquier servicio basado en la web al que accedemos a través del navegador sin atender al software. Ejemplo: El Webmail de Gmail, Google Docs, Salesforce, Dropbox.

#### *2.3.3.2.Plataforma como servicio (PaaS)*

Reduce bastante la complejidad a la hora de desplegar y mantener aplicaciones ya que las soluciones PaaS gestionan automáticamente la escalabilidad usando más recursos si fuera necesario. (Platzi, 2017) Ejemplos: Google App Engine (Para desarrollar apps en Java o Python en la infraestructura de Google) o Heroku (Igual que la anterior, pero con Rails y Django).

#### **2.3.3.3.** *Infraestructura como servicio (IaaS)*

Es la forma más sencilla donde se proporcionan recursos informáticos básicos y el consumidor instala y administra el sofware necesario.

Ejemplos: Amazon Web Service (AWS) que nos permite decidir qué tipo de instancias queremos usar como Linux o Windows, así como la capacidad de memoria o procesador de cada una de nuestras maquinas, Microsoft Azure (Platzi, 2017).

### *2.3.4. Virtualización de servidores*

Permite que varias instancias de un sistema operativo funcionen de forma conjunta en un solo servidor. Esta es la mejor manera de aumentar la utilización de los recursos, hasta un 80 % con respecto a un nivel medio de utilización de un 10-20 % en el caso de servidores físicos habituales de una sola función. Virtualización del hardware de los servidores: ofrece un solo nivel intermedio (hipervisor) entre la máquina virtual (VM) y el metal. Ofrece un valor mayor que el de la virtualización del software de los servidores, donde el sistema operativo subyacente implica determinado consumo de recursos adicional. Para la mayoría de las aplicaciones empresariales se prefiere la virtualización de hardware. (IONOS, 2019)

## *2.4. Software de virtualización*

La virtualización utiliza el software para imitar las características del hardware y crear un sistema informático virtual. Esto permite a las organizaciones de TI ejecutar más de un sistema virtual, y múltiples sistemas operativos y aplicaciones, en un solo servidor. (Ayudaley, 2020)

Hay distintos tipos de software de virtualización que se utilizan y son versátiles debido a que engloba distintas herramientas; entre los más conocidos están:

### *2.4.1. VirtualBox*

La ventaja de este tipo de software es que está disponible de forma libre mediante licencia GNU de uso público. Es una herramienta que se puede ejecutar en sistemas operativos Windows, Mac OS, Linux y Solaris. Es muy versátil y sencillo de usar, y cuenta con funciones muy interesantes para usuarios principiantes.

### *2.4.2. VMware Workstation Pro*

VM Workstation Pro es la versión más avanzada de las herramientas de máquinas virtuales de VMware. Mientras que la versión VMware Player permite crear un sistema operativo virtualizado, dando la facilidad de crear varias máquinas virtuales.

### *2.4.3. Microsoft Hyper-V Server*

El gigante tecnológico Microsoft cuenta con su propio software de virtualización. Hyper-V Server es una herramienta que intenta emular el funcionamiento y las opciones de VMware, una de las herramientas más completas y conocidas.

### *2.4.4. Citrix XenServer*

Citrox XenServer es una plataforma para virtualización de servidores que se integra con la tecnología Xen y que proporciona un entorno de administración seguro y fiable. Cuenta con dos versiones, una gratuita y otra de pago que incluye funcionalidades más avanzadas.

### *2.4.5.* **Sandboxie**

Sandboxie es un software orientado a realizar pruebas con malware o código malicioso. Que permite crear un espacio aislado y protegido en el equipo para generar un entorno de pruebas en el que ejecutar software malicioso sin que afecte al resto del equipo. Una vez que se finalice la sesión, todo lo que haya en ese entorno de pruebas será eliminado y el equipo volverá a su funcionamiento normal.

### *2.4.6. Parallels*

Parallels es un software de virtualización para Mac, cuya principal ventaja es su capacidad para ejecutar otros sistemas operativos en equipos de la marca Apple.

## *2.5. Seguridad de la información*

Para la complementación de este estudio analizaremos la seguridad de la información.

ISO 27001, define como 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: (Bezerra, 2016)

- 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.

Los cambios tecnológicos son una presencia constante en la vida diaria de la organización. Estos cambios pueden hacer que surjan nuevas vulnerabilidades y riesgos o agravar los ya existentes, por lo cual deben ir acompañados de una evaluación de riesgos dinámica y actualizada, lo que permite el levantamiento de los niveles de riesgo y la forma de tratarlos. (Bezerra, 2016)

Al mismo tiempo, es necesario conocer las leyes que la organización está obligada a seguir y recopilar los requisitos de seguridad necesarios para cumplir con ella, y a partir de estos requisitos legales, identificar los controles necesarios y los designados por el análisis de riesgos, con el uso de las normas de seguridad. A partir de los controles identificados, es necesario generar políticas, normas y procedimientos para la aplicación de los controles. (Bezerra, 2016)

La proliferación de nuevas tecnologías en las distintas áreas que conforman las soluciones actuales de TIC (Tecnologías de Información y Comunicación), trae como consecuencia nuevos retos que las direcciones deben asumir y solventar llegado el momento de su instrumentación.

Uno de los retos actuales es el aseguramiento de este tipo de entornos, que, a diferencia de la infraestructura física, plantea nuevos desafíos. En contraste con los entornos físicos, los entornos virtuales basan su operación en infraestructura física unificada, es decir, un servidor físico puede contener uno o varios sistemas operativos hospedados en una misma plataforma. Es aquí donde el tema de seguridad de ambientes virtuales juega un papel muy importante. (Sánchez G., 2019)

### *2.6. Problemas de seguridad en la virtualización de servidores*

Ante la demanda de la interconexión computacional que es requerida por todo el mundo para sus permanentes y diarias actividades mucho se ha hablado y escrito sobre los beneficios de la virtualización de servidores. Todos hablan de las bondades y de los beneficios de la virtualización de sistemas, pero estos mismos beneficios traen asociados también nuevos problemas y preocupaciones. (CONSUSLTING, 2017)

A continuación, se detallan los que mayormente se presentan:

- **Facilidad y velocidad de implementación de servidores virtuales**

En entornos virtuales, todo se pude hacer o cambiar extremadamente más rápido. Por ejemplo, el ciclo de implementación de nuevos servidores virtuales o máquinas virtuales, puede realmente reducirse de días a minutos, o incluso, a segundos. La posibilidad de hacer estos despliegues de una forma mucho más rápida es, sin lugar a dudas, un beneficio extraordinario para cualquier centro de datos. (CONSUSLTING, 2017)

Pero también existe la necesidad de mitigar el riesgo de errores y de la actividad maliciosa con la misma rapidez. Si las organizaciones carecen de buenas prácticas de planificación, el factor velocidad puede exacerbar las debilidades en los procesos de su empresa.

Este factor de velocidad en un entorno de cambio continuo, puede resultar inexorablemente en la falta de entendimiento del estado actual de los activos en su centro de datos. (CONSULTING, 2015)

- **Consolidaciones de switches de red y servidores en un solo servidor físico**

En una infraestructura física, los servidores y las redes son gestionados a través de numerosas aplicaciones por separado. En una infraestructura virtual, los servidores y las redes pueden ser gestionados por el mismo software de la capa de virtualización. (CONSUSLTING, 2017)

Los administradores de red están familiarizados con el control de sus switches físicos a través de la aplicación de gestión de red que utilizan para su red física. Por consiguiente, deben adaptarse a las nuevas herramientas de gestión y mejores prácticas en un entorno de red virtual.

Estos mismos administradores de red deben actualizar sus conocimientos para operar el software de virtualización con soltura y evitar errores de configuración ya que los riesgos asociados con una mala configuración de red del entorno virtual son muy altos y las consecuencias pueden ser desastrosas para su centro de datos. (CONSULTING, 2015)

- **Encapsulación de las máquinas virtuales**

A diferencia de un servidor físico, una máquina virtual es un conjunto de ficheros que residen físicamente en un almacenamiento compartido. Esta propiedad de encapsulación permite métodos mucho más sencillos de asegurar la continuidad del servicio.

Sin embargo, este tipo de encapsulación de la máquina virtual ofrece un nuevo tipo de robo de datos. Como la máquina virtual es solo un conjunto de ficheros, un servidor entero puede ser copiado a un dispositivo USB o copiado durante un proceso de backup no autorizado a un lugar no protegido por su personal de seguridad o administrador de su entorno virtual. (CONSULTING, 2015)

- **Actualizaciones de parches de seguridad**

Es muy fácil despreocuparse de máquinas virtuales que no están en activo, particularmente en entornos de desarrollo. Un ejemplo podría de este posible escenario es el caso de un desarrollador de software que usa algunas máquinas virtuales por algún tiempo y luego las apaga. Un mes más tarde, este mismo desarrollador vuelve a usar las máquinas virtuales y las enciende (PowerOn) sin preocuparse de que estas máquinas virtuales deberían haber sido parcheadas con sus correspondientes parches de seguridad.

Así mismo, en un entorno virtual ya no existe la relación one-to-one entre servidor físico y aplicación. Ahora, una máquina virtual puede ejecutarte en cualquier servidor físico y cada servidor físico puede tener una gran variedad de máquinas virtuales. Esta asociación puede cambiar dinámicamente mediante el uso de tecnologías de migraciones en caliente de dichas máquinas virtuales lo que hace más difícil estar al día con todos los cambios en cuanto a los parches de seguridad se refiere. (CONSULTING, 2015)

- **Consolidación de servidores**

Las consolidaciones de servidores reducen los gastos de capital, así como los gastos de operaciones, pero también, no es menos cierto, ahora muchos más servicios que se están ejecutando en estas máquinas virtuales se basan en menos servidores físicos. Por consiguiente, si un servidor físico no es configurado de la forma correcta o es atacado, esto podría afectar a muchos más servidores virtuales. (CONSULTING, 2015)

## 2.7. *Normas, estándares y modelos de la seguridad de la información*

En cuanto a los estándares y normas para la gestión de riesgos de la seguridad de la información son múltiples los criterios de aplicabilidad que estas tienen y que de forma creciente se incrementan en cuanto a su número, características y resultados que se logran para este fin, por lo que en este trabajo a buen criterio se expondrán las más destacadas.

Muchos marcos, modelos y normas, explican cómo implementar la gestión del riesgo de una manera eficaz. Estos documentos cumplen con un amplio consenso en todo el mundo, lo cual pone de manifiesto una búsqueda creciente, en la armonización de las prácticas de gestión de riesgos a nivel internacional, a fin de tener en cuenta las particularidades de cada organización.

Entre los estándares o normas para la gestión de la seguridad de la información se destacan al momento las siguientes:

### *2.7.1. Norma ISO 27001*

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. (IsoTools, 2021)

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

Estructura de la norma ISO 27001

1. Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
2. Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001.
3. Términos y Definiciones: Describe la terminología aplicable a este estándar.

4. Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
5. Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
6. Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
7. Soporte: En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. Operación: Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.
9. Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.
10. Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre inconformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

### *2.7.2. Norma ISO 27002*

Es la normativa internacional que tiene como finalidad la protección de la confidencialidad de datos e información dentro de una organización. Esta norma proporciona el marco de trabajo para establecer un SGSI, que después puede ser certificado oficialmente por el organismo ISO.

La ISO 27002 contiene un inventario de prácticas donde se describe detalladamente los puntos clave de la ISO 27001. Estos dos estándares juntos contemplan tanto la ciberseguridad como también la protección de la información en todos los ámbitos posibles (EALDE, 2020)

### *2.7.3. Norma ISO 27005*

La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información.

Es compatible con los conceptos generales especificados en la norma ISO 27001 y se encuentra diseñada como soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de gestión de riesgo, es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información.

La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

ISO-27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, los usuarios elijen el método que mejor se adapte para, por ejemplo, una evaluación de riesgos de alto nivel seguido de un análisis de riesgos en profundidad sobre las zonas de alto riesgo.

La norma incorpora algunos elementos iterativos, por ejemplo, si los resultados de la evaluación no son satisfactorios.

### *2.7.4. Instituto Nacional de Estándares y Tecnología (NIST)*

El marco para la mejora de la seguridad cibernética en infraestructuras críticas, mejor conocida en inglés como NIST Cibersecurity Framework, fue emitido inicialmente en los Estados Unidos en febrero de 2014.

La orientación del marco es ayudar a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporcionando un lenguaje común y un resumen de las mejores prácticas en ciberseguridad. (R., 2020)

El marco es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la información (TI), sistemas de control

industrial (ICS), sistemas ciber físicos (CPS) o dispositivos conectados en general, incluido el Internet de las Cosas (IoT). Consta de tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco.

El Núcleo del Marco es un conjunto de funciones y actividades de seguridad cibernética, resultados esperados y referencias informativas que son comunes en todos los sectores y en la infraestructura crítica. El Núcleo del Marco consta de cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. Cuando se consideran juntas, estas funciones proporcionan una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de la seguridad cibernética de una organización. Cada función está compuesta de categorías, cada categoría se divide a su vez en subcategorías y cada subcategoría viene acompañada de referencias normativas a otros frameworks o estándares (ISO 27001, CobiT 5, NIST SP-83, ISA62443, entre otros) en los cuales se encuentra mayor nivel de detalle para la implementación de los controles de seguridad cibernética referidos.

### *2.7.5. Modelos para la gestión de riesgos de seguridad de información*

Para la concreción de la Gestión de la Seguridad de la Información durante su proceso de desarrollo se han planteado diversos modelos que han afianzado su eficacia en esta área de la información tecnológica, destacándose entre éstos: (Dirección General de Modernización Administrativa, 2013)

#### *2.7.5.1. Magerit*

La metodología de este modelo está basada en el análisis del impacto que puede tener la violación de la seguridad de un sistema desde el punto de vista de los activos; este proceso busca identificar las amenazas que pueden llegar a afectar al sistema y las vulnerabilidades que pueden ser empleadas por las amenazas identificadas, logrando de esta forma obtener una identificación concreta de las medidas preventivas y correctivas más apropiadas; el análisis de riesgos dentro de esta metodología comprende los siguientes aspectos:

- Los activos, que son los elementos que conforman el sistema de información y que le dan soporte a la misión de la organización.
- Las amenazas, que son los hechos que pueden producir un daño a los activos y que causan un perjuicio a la empresa o al usuario.

- Las salvaguardas, que son las medidas de protección destinadas a mitigar las amenazas que pueden causar un daño a los activos identificados.

Con estos tres aspectos se pueden determinar el impacto de lo que podría suceder y el riesgo que probablemente pase. (Dirección General de Modernización Administrativa, 2013)

#### *2.7.5.2. Octave*

Es una famework para el análisis y gestión de riesgo, en sus siglas en inglés Operationally Critical Threat, Asset and Vulnerability Evaluation. Esta metodología fue desarrollada por Computer Emergency Response Team (CEART) y tiene como objetivo facilitar la evaluación de riesgos de las tecnologías de la información en una organización o usuario. A su vez tiene tres fases:

- Construcción de perfiles de amenazas basadas en activos.
- Identificación de vulnerabilidades en la infraestructura.
- Desarrollo de estrategias y planes de seguridad. (Dirección General de Modernización Administrativa, 2013)

#### *2.7.5.3. Mehari*

Es conocido como un método de análisis de riesgo armonizado. En un inicio su enfoque era el de apoyar a los responsables de la seguridad de los sistemas de información en las tareas de gestión de riesgos; un aspecto importante de esta metodología es que se encuentra en permanente evolución para satisfacer la naturaleza cambiante del entorno de la organización o usuario, lo que facilita su implementación en ambientes como los virtuales que se caracterizan por ser cambiantes y fácilmente renovables.

Esta metodología nos provee de una serie de herramientas especialmente diseñadas para la gestión de los riesgos, en ella están incluidas una serie de pasos a seguir y que cada una de ellas tiene un objetivo específico, así:

- Desarrollo de planes de seguridad.
- Implementación de políticas o normas de seguridad.
- Relación de la situación detallada del estado de la seguridad.
- Evaluación y gestión de riesgo.
- Incluir la seguridad en la gestión de proyectos de desarrollo.

- Sensibilizar al personal de la organización sobre la seguridad a través de sesiones de formación.
- Gestión operativa de la seguridad por medio de la monitorización de las acciones ejecutadas.

Con esta metodología se espera conseguir la madurez en términos de seguridad informática a nivel empresarial y organizacional de igual manera que contribuya a mejorar la toma de decisiones por parte de las directivas y se acrecienta una cultura tecnocrática donde las normas están definidas y se deben cumplir.

Luego de este estudio Magerit y Octave han sido seleccionadas como metodologías que servirá de base para la formulación de la correspondiente guía metodológica, objeto de esta investigación en vista que son las más adecuadas a nuestro entorno. (Dirección General de Modernización Administrativa, 2013)

### *2.8. Sistema de Gestión de Seguridad de la Información (SGSI)*

El sistema de seguridad de la información o SGSI (Information Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa. El SGSI es un elemento fundamental de la norma internacional ISO 27001 (Sistemas de Gestión de la Seguridad de la Información), que persigue asegurar la integridad y confidencialidad de los datos y los sistemas encargados de procesarlos. (Ambit, Para qué sirve un SGSI? Controles y fases, 2021)

Para implantar el SGSI se debe utilizar el Ciclo de Deming o PDCA (Plan, Do, Check, Act) que hace referencia a la serie planea, implementa, comprueba y actúa. Se trata de un sistema que está diseñado para implementar una mejora continua en la gestión y ejecución de procesos.
El conocido como Ciclo de Deming cuenta con las siguientes fases:

- Planificar (Plan). En la fase inicial se realiza una evaluación de todos los riesgos y amenazas sobre la información que se producen en las distintas áreas de la empresa. Se deben establecer los controles oportunos para medir el nivel de riesgo de los datos en su flujo interno y externo y definir las políticas necesarias para el cumplimiento de las medidas de seguridad.

- Hacer (Do). En esta fase se implementa la selección de controles adecuados para medir los riesgos. En esta fase se pone en marcha el sistema SGSI para la detección y evaluación de los riesgos y amenazas. (Dirección General de Modernización Administrativa, 2013)

- Comprobar (Check). En esta fase se debe evaluar y revisar la eficiencia y la eficacia. Mediante KPI (métricas asociadas a objetivos) y el análisis de feedback se puede determinar si se están alcanzando los objetivos fijados. Es la etapa donde se detectan fallos o errores que deben ser corregidos.

- Actuar (Act). En esta última fase se aplican las correcciones o cambios necesarios en el sistema para sacar el máximo rendimiento y que fueron detectados en la fase anterior de comprobación.

Hay que tener en cuenta que el SGSI es un sistema dinámico que persigue una mejora continua en la detección, evaluación y reducción de amenazas y riesgos de la información. Por lo tanto, se trata de un ciclo que se repite, con cambios de planificación, nuevas implementaciones en seguridad, monitoreo y control continuo, y aplicaciones y ajustes constantes para alcanzar un alto nivel de seguridad de los datos de la empresa. (Dirección General de Modernización Administrativa, 2013)

Con la implementación de un sistema SGSI se consigue establecer una serie de procesos y controles para mejorar y proteger el acceso a la información que se maneja en el día a día de las empresas.

Los riesgos a los que se enfrenta una organización en la actualidad son muy amplios y peligrosos con ataques externos a sus servidores (como los de denegación de servicio) e infecciones de malware (como los peligrosos ransomware o phishing).

Con un SGSI la empresa incrementará de forma notable su nivel de protección reduciendo los riesgos de sufrir este tipo de ataques y estando preparada para minimizar sus consecuencias en caso de que se produzcan. (Dirección General de Modernización Administrativa, 2013)

El propósito de un sistema de gestión de la seguridad de la información SGSI 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.

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. (Alvarado, 2020)
En un Sistema de Gestión de Seguridad de la Información al materializarse una amenaza el activo cambia de estado, es decir, antes de producirse la amenaza tenemos un activo y después de que efectúe la amenaza tenemos la diferencia entre el estado anterior y el posterior a la amenaza.

Empleando una tipología de impactos orientada a la naturaleza de todas las consecuencias en las diferentes combinaciones activo-amenaza, el impacto puede ser cualitativo y cuantitativo.

Para los efectos correspondientes de esta investigación se determina la metodología para el análisis de riesgos y se define las matrices, a través de los siguientes puntos:

- Evaluación de riesgo. Se identifican las amenazas, vulnerabilidades y riesgos, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad. Se consideran los siguientes puntos:
  - La probabilidad de una amenaza.
  - La magnitud del impacto sobre el sistema.
- Determinación de la probabilidad. Se determina la probabilidad que una vulnerabilidad pueda ser explotada por una amenaza, pueden manejar diferentes tipos de clasificación. Se tienen en cuenta los siguientes factores:
  - Fuente de la amenaza y su capacidad.
  - Naturaleza de la vulnerabilidad.
- Identificación de Vulnerabilidades. Para la identificación de vulnerabilidades, se revisa la Norma ISO 27001.
- Análisis de Impacto y Factor de Riesgo. Se determina el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad.

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- La importancia crítica de los datos y el sistema (importancia a la organización).
- Sensibilidad de los datos y el sistema. (cibernética, 2018).

Las estrategias de gestión de riesgos son las tácticas que se utilizan para lidiar con ellos y para comprender sus posibles consecuencias. Dichas estrategias deben incluirse en un plan de gestión de riesgos, el cual consiste en un proceso documentado sobre la forma en la que su empresa o su equipo identificará y abordará los riesgos que surjan. (REDHART, 2019)

La gestión de riesgos empresariales es una parte fundamental de su estrategia comercial y de su relación con las partes interesadas, ya que lo ayuda a evitar las circunstancias que podrían impedir que su empresa alcance sus objetivos. (REDHAT, 2019)

### *2.9.1. Gestión de riesgos*

La gestión de riesgos se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse. (cibernética, 2018).

En su forma general contiene cuatro fases:

- Análisis: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- Reducción: Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas.
- Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento. (cibernética, 2018).

La gestión del riesgo debe considerar los siguientes tres niveles de aplicación: tecnologías, procesos y personas. La tecnología garantiza los ajustes técnicos necesarios para el tratamiento adecuado de los riesgos; los procesos de asegurar que las actividades que componen la gestión de los riesgos sean consideradas de forma sistemática, y, por último, las personas, de modo que los empleados y los gerentes identifiquen sus responsabilidades, conozcan los riesgos y puedan ayudar a su reducción y control. (cibernética, 2018).

Para comprender la gestión de riesgos es necesario establecer una breve definición de términos, entre los cuales tenemos: riesgo, amenaza, vulnerabilidad e impacto.

#### *2.9.1.1. Riesgo*

El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios o un virus. (cibernética, 2018).

##### *2.9.1.1.1. Tipos de riesgos en la administración de servidores virtuales*

Los riesgos existentes son elevados, ya que se puede poner en riesgo la continuidad de la operación y el acceso no autorizado a información confidencial, a continuación, se detalla una serie de carencias importantes que pueden hacer que su experiencia con infraestructuras de TI virtualizadas sea mucho menos satisfactoria. (cibernética, 2018).

- **Duplicación**

Cada máquina virtual tendrá un conjunto idéntico de componentes de seguridad y bases de datos, cada uno de los cuales tendrá que actualizarse de forma independiente. Por lo tanto, una parte significativa de sus recursos más preciados (potencia de procesamiento, memoria RAM y almacenamiento en disco) se consumirá de forma bastante inútil, reduciendo significativamente el índice de consolidación. (Ambit, 2020)

- **Tormentas**

Este término se utiliza para definir el análisis de la actividad de actualización de bases de datos simultáneos a través de varios equipos, que puede conducir a un repentino pico en el consumo de

recursos y el consiguiente descenso del rendimiento, e incluso a una denegación de servicio. La configuración manual puede ayudarle a resolver parcialmente este problema, pero con tantos resultados y cientos de máquinas virtuales, la intervención manual puede ser una tarea que consuma muchísimo tiempo. (Ambit, 2020)

- **Brechas de seguridad instantáneas**

Algunas máquinas virtuales permanecen latentes hasta que se las activa cuando surge la necesidad. Por desgracia, no es posible actualizar los componentes ni las bases de datos de la solución seguridad en una máquina virtual inactiva. Por lo tanto, inmediatamente después del arranque y antes de que la actualización de seguridad se haya completado, la máquina virtual es vulnerable a un ataque. (Ambit, 2020)

- **Problemas de incompatibilidad**

Las máquinas virtuales son en muchos aspectos similares a sus homólogos físicos, pero existen algunas diferencias importantes a tener en cuenta, tales como el uso de los discos no persistentes o el proceso de migración de máquinas virtuales en caliente, por lo que pueden causar retrasos y problemas técnicos inesperados, o incluso dejar de funcionar completamente. (cibernética, 2018).

- **Controles de red y de seguridad pueden entremezclarse**

Las herramientas utilizadas para administrar la máquina virtual no pueden tener la misma granularidad que se utilizan para gestionar la red. Esto podría llevar a una elevación de privilegios y un compromiso de la seguridad. (Ambit, 2020)

#### 2.9.1.2. Amenaza

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas. (cibernética, 2018).

Los tipos de amenazas a la seguridad de un sistema o red de computadores de conformidad con el estándar ISO 7498-3, se caracteriza de forma más sencilla, si se considera la función del sistema de computación como proveedor de información; en general, existe un flujo de información desde una fuente, existen cuatro categorías generales de amenazas que pueden presentarse: (Areitio Javier, 2008) . Ente las que encontramos:

- **Interrupción**

Ocurre cuando un factor estratégico del sistema se destruye o se hace no utilizable o no disponible, ésta es una amenaza a la disponibilidad. (Castro, 2018)

- **Intercepción**

Producida cuando una parte no autorizada obtiene acceso a un factor estratégico. Constituye, de hecho, una amenaza al secreto de confidencialidad. La parte no autorizada puede ser una persona, un programa o un computador. (Castro, 2018)

- **Modificación**

Se produce cuando una parte no autorizada, no sólo obtiene acceso, sino que modifica un factor estratégico, lo que constituye una amenaza a la integridad, así sucede con los cambios de valores en un fichero de datos, la alteración de un programa para que opere de una forma diferente y la modificación de los contenidos de los mensajes que se transmiten en una red. (Castro, 2018)

- **Fabricación**

Se debe a que cuando una parte no autorizada inserta objetos falsificados en el sistema, lo que constituye una amenaza a la integridad, esto sucede con la inserción de mensaje falsos en una red y la adición no autorizada de registros a un fichero. (Castro, 2018)

Es necesario en esta parte determinar la clasificación de las amenazas y que tiene relación a la forma en que se producen, así pueden ser:

- Accidentales, (intento no premeditado) como malfuncionamiento de sistemas, los errores de software y los fallos operacionales.
- Intencionales (intento premeditado), se consideran como un ataque.

La mayoría de las amenazas específicas en la virtualización se centran en el hipervisor, como conocemos el hipervisor es el monitor de máquina virtual, el software que permite a las máquinas virtuales existir. Si el hipervisor puede ser atacado con éxito, el atacante puede obtener acceso de nivel raíz a todos los sistemas virtuales. La solución a la mayoría de las amenazas de virtualización es aplicar siempre los parches más recientes y mantener el sistema al día. (Salazar, 2013)

#### *2.9.1.3. Vulnerabilidad*

Las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. El problema es que, en el mundo real, si existe una vulnerabilidad, siempre existirá alguien que intentará explotarla, es decir, sacar provecho de su existencia. (cibernética, 2018).

#### *2.9.1.4. Impacto*

El impacto generado sobre un activo de información según la norma ISO 27001 es la consecuencia de la materialización de una amenaza; es la diferencia entre las estimaciones del estado de seguridad del activo antes y después de materializar las amenazas.

### *2.10. Aplicación de la gestión de riesgos de la seguridad de la información en entornos virtuales*

Para la aplicación de seguridad en entornos virtuales se deben tomar en cuenta aspectos como:

- Clasificar el tráfico e información real entre máquinas virtuales.
- Mecanismo de autentificación y controles de acceso.
- Corrección de vulnerabilidades.
- Instalación de actualizaciones de seguridad.
- Configurar la auditoría y escaneo de vulnerabilidades.

Uno de los grandes retos de la virtualización, es el aseguramiento del servidor mainframe **(**un mainframe es una clase de computadora que es capaz de realizar cientos de millones de cálculos muy complejos a una velocidad asombrosa**)**, que representan flexibilidad para los administradores, pero a la par representa una vulnerabilidad que las convierte en presas fáciles de ataques.

La seguridad en entornos virtuales debe tomar en cuenta que los sistemas de almacenamiento en red se ven vulnerables a las amenazas construyendo otra línea de acción para los atacantes. Es recomendable mantener los sistemas de almacenamiento separados de las máquinas virtuales.

En cuanto al análisis de la criticidad, la vulnerabilidad y las amenazas, es la base de la identificación y evaluación del riesgo operacional. El mayor riesgo se encuentra siempre, en la intersección de las tres áreas de vulnerabilidad, amenazas y criticidad. (Areitio Javier, 2008)

El análisis de riesgos identifica y los estima, teniendo en cuenta el uso sistemático de la información. Abarca el análisis de las amenazas, vulnerabilidades e impactos y se considera el punto clave de la política de seguridad de la información de una organización.

La evaluación del riesgo compara el riesgo estimado en el análisis con los criterios predefinidos con el fin de identificar la importancia de cada riesgo para la organización. Aceptación de riesgos incluye la identificación del nivel aceptable de riesgos para una organización en función de sus necesidades específicas de negocio y seguridad. El tratamiento del riesgo corresponde a la selección y la aplicación de medidas para modificar un determinado riesgo. (Salazar, 2013)

Sin embargo, hay que señalar que de la investigación bibliográfica y digital realizada no existe una metodología de gestión de riesgos que esté específicamente destinada a sistemas virtuales, en los sistemas informáticos se han encontrado algunas como Magerit, Octave y Mehari, de las cuales habrá de seleccionarse la más adecuada que servirá de guía metodológica para cumplir los objetivos de este estudio.

# CAPÍTULO III

## 3. METODOLÓGÍA DE LA INVESTIGACIÓN

### 3.1. Tipo y diseño de la investigación

La investigación es de tipo bibliográfica y documental. Para tratar los aspectos teóricos necesarios para el desarrollo de la investigación se realizó consultas bibliográficas tanto de fuentes primarias y de fuentes secundarias, estas fueron:

**Primarias**. Se realizó mediante encuestas al personal encargado de la administración de los servidores virtuales además de la observación directa de los servidores virtualizados.

**Secundarias.** Se tomó en cuenta fuentes de investigación como el internet, boletines, libros relacionados con el tema.

**Investigación de campo.** La investigación se realizó en el entorno de la TI (Tecnología de la Información) particular, corporativo e institucional tanto pública como privada a través del contacto directo del investigador con la realidad, con el objeto de recolectar, registrar y analizar los datos obtenidos de primera mano, referentes al problema de estudio.

**Investigación descriptiva.** La investigación se basó en estudios descriptivos, ya que detallaron las características más importantes de las actividades en estudio, en lo que respecta a su origen y desarrollo, además identificó los diferentes elementos, componentes, y su interrelación.

### 3.2. Métodos de investigación

Para llevar a cabo esta investigación se utilizó un enfoque cuali-cuantitativo en razón que las teorías expresadas mediante variables cualitativas pueden ser medibles cuantitativamente a través de los indicadores de gestión

**Método inductivo - deductivo.** Permitió conocer la situación actual de la seguridad en los servidores virtualizados mediante instrumentos investigativos; proceso que se inició con el diseño de encuestas, aplicación, recopilación de los datos, análisis y resumen de la información obtenida,

con el propósito de emitir conclusiones generales sobre las deficiencias o aspectos negativos encontrados durante el proceso investigativo.

**Método analítico - sintético.** En la presente investigación se realizó un análisis comparativo y profundo de cada de los procedimientos ejecutados en relación a sus procedimientos planificados, poniendo mayor énfasis en aquellos que tengan mayor importancia de análisis o que presenten alguna deficiencia.

### 3.3. Enfoque de la investigación

**Enfoque cualitativo.** Muestra la realidad actual, esto es posible mediante la observación directa, la indagación, entrevistas, análisis de la información de las actividades realizadas en la misma.

**Enfoque cuantitativo.** La información que se requiere para el estudio está íntimamente ligada con datos numéricos, al momento en que se realizaron las encuestas especificando la composición de la población.

### 3.4. Alcance de la investigación

La Propuesta de un modelo de gestión de seguridad de la información para la administración de servidores virtualizados se ejecutó en el entorno particular, FIBRA TELECOM, que es un proveedor local de la provincia de Chimborazo.

### 3.5. Población de estudio

La población estuvo defina por los profesionales encargados de la administración de los servidores virtualizados del entorno.

### 3.6. Unidad de análisis

Encuestas realizadas a los profesionales encargados de la administración de los servidores virtualizados.

### 3.7. Selección de la muestra

No se realizó la selección de la muestra, porque la investigación se hizo a todos los profesionales encargados de la administración de los servidores virtualizados del entorno y que han sido

seleccionados en una muestra de 45, lo que no hace necesario el cálculo de la misma ya que se toma todo el universo como tal.

### 3.8. Tamaño de la muestra

No se realizó el cálculo del tamaño de la muestra, ya que la investigación se hará al total de los encargados de la administración de los servidores virtuales del entorno que son 45.

### 3.9. Técnica de recolección de datos primarios y secundarios

Se realizó mediante la vía digital enviando la encuesta al encargado de la administración de los servidores virtualizados de los proveedores de este servicio del entorno.

**Observación.** Se realizaron observaciones directas a las labores y operaciones que se realizan en FIBRA TELECOM, que es un proveedor local de la provincia de Chimborazo, con la finalidad de contar con suficiente y oportuna información para establecer las debidas recomendaciones.

### 3.10. Instrumentos de recolección de datos primarios y secundarios

- Encuesta
- Google Forms

### 3.11. Instrumentos para procesar datos recopilados

- Excel 2016
- Paquete estadístico informático SPSS 25.0

# CAPÍTULO IV

## 4. RESULTADOS Y DISCUSIÓN

### 4.1. Análisis de la Situación Actual

**Tabla 1-4:** Importancia del conocimiento sobre gestión de riesgos de seguridad de la información en la administración de servidores virtualizados

| Opciones | f | % |
|---|---|---|
| Si | 42 | 93% |
| No | 3 | 7% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

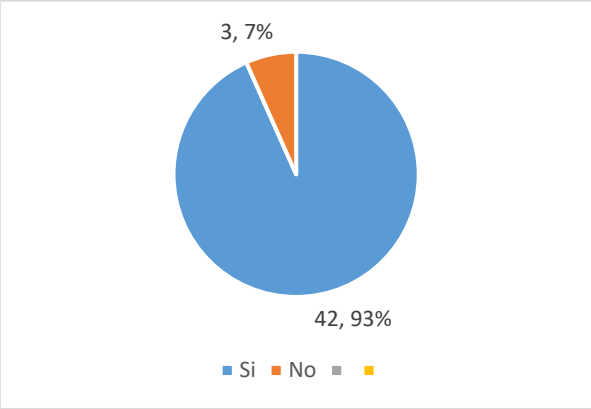



**Gráfico 1-4.** Importancia del conocimiento sobre gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

Respecto a la importancia del conocimiento de la gestión de riesgos de seguridad de la información en la administración de servidores virtualizados, un 93% de los encuestados afirman tener conocimiento.

**Tabla 2-4:** Factores de mayor trascendencia para lograr la seguridad de la información

| Opciones | f | % |
|---|---|---|
| Tecnologías | 28 | 47% |
| Procesos | 24 | 40% |
| Talento humano | 8 | 13% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

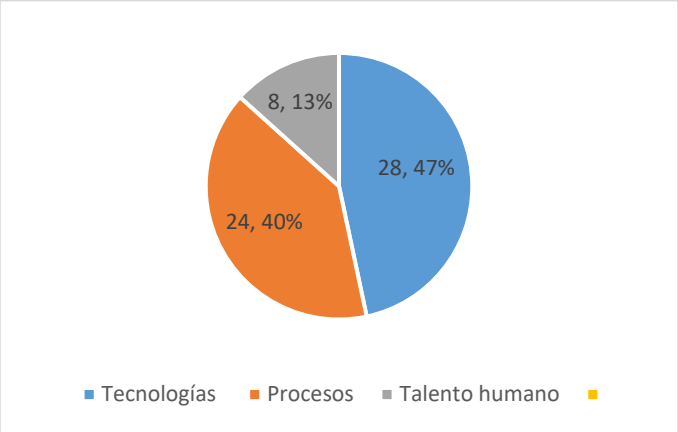



**Gráfico 2-4.** Factores de mayor trascendencia para lograr la seguridad de la información
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación;**

En cuanto a los factores importantes para la para lograr la seguridad de la información un 47% de los encuestados consideran a la tecnología en primer lugar, en segundo con 40% a los procesos y el talento humano en un 13%.

Estos resultados demuestran que la tecnología o modelos de gestión para determinar los riesgos de seguridad de la información son los más importantes.

**Tabla 3-4:** Fundamentos metodológicos de gestión de riesgos de seguridad de la información existentes

| Opciones | f | % |
|---|---|---|
| Si | 42 | 93% |
| No | 3 | 7% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

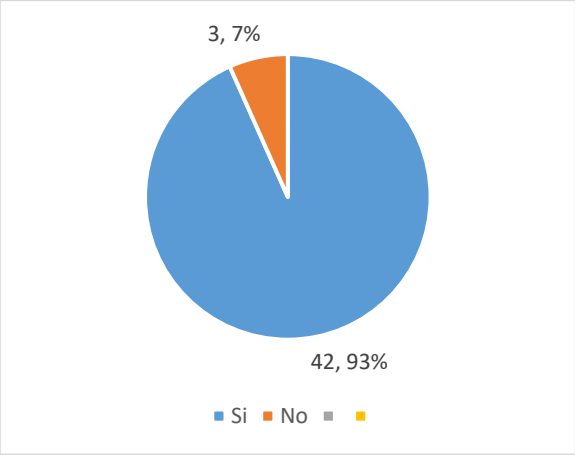



**Gráfico 3-4.** Fundamentos metodológicos de gestión de riesgos de seguridad de la información existentes
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

Los resultados de la encuesta reflejan que el 93% de encuestados consideran necesario conocer sobre los fundamentos metodológicos de la gestión de riesgos de la seguridad de la información, aspecto a tener en consideración para la guía metodológica respecto a la gestión de riesgos de la seguridad de la información.

**Tabla 4-4:** Medidas adoptadas para controlar los riesgos de la información en organizaciones

| Opciones | f | % |
|---|---|---|
| Análisis | 39 | 87% |
| Evaluación | 0 | 0% |
| El tratamiento | 3 | 7% |
| La aceptación | 3 | 6% |
| Comunicación | 0 | 0 |
| **Total** | **45** | **100%** |
| | | |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

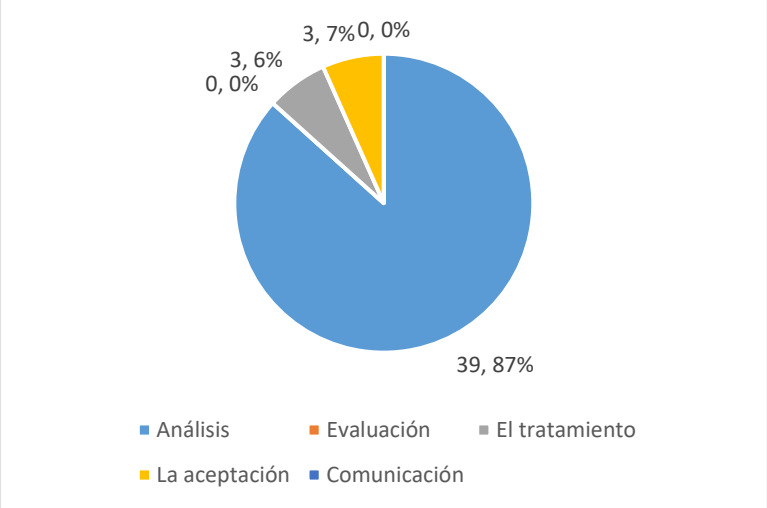



**Gráfico 4-4.** Medidas adoptadas para controlar los riesgos de la información en organizaciones
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

En cuanto a las medidas necesarias para controlar la gestión del riesgo que se adoptan en la organización los encuestados consideran el siguiente orden de importancia: el análisis, la aceptación y el tratamiento en porcentajes entre el 87%, 7% y 6% respectivamente. Lo que da la medida del conocimiento y necesidad de las mismas.

**Tabla 5-4:** Nivel de control de seguridad de los servidores virtualizados bajo responsabilidad

| Opciones | f | % |
|---|---|---|
| Si | 45 | 100% |
| No | 0 | 0% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

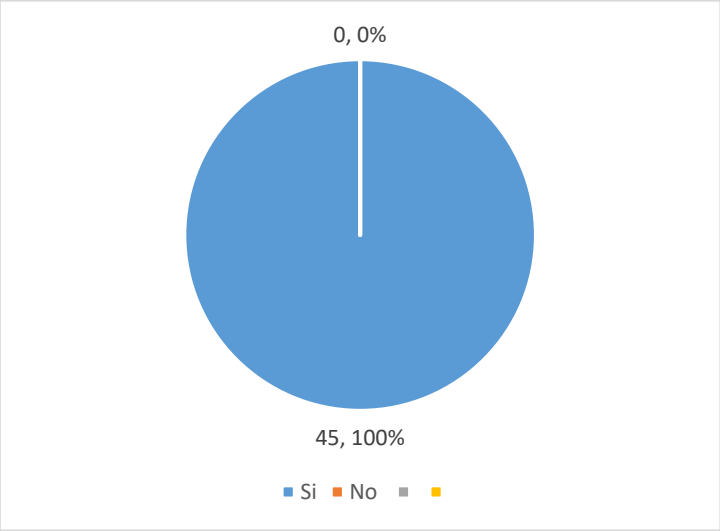



**Gráfico 5-4.** Nivel de control de seguridad de los servidores virtualizados bajo responsabilidad
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

En cuanto a que, si permitirá mejorar el nivel de control de seguridad de los servidores virtualizados bajo su responsabilidad la aplicación de las medidas de seguridad de la información a su cargo, se evidencia su necesidad cuando en la totalidad los 45 encuestados están de acuerdo.

**Tabla 6-4:** Guía metodológica de gestión riesgos de seguridad existente

| Opciones | f | % |
|---|---|---|
| Si | 6 | 13% |
| No | 27 | 87% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

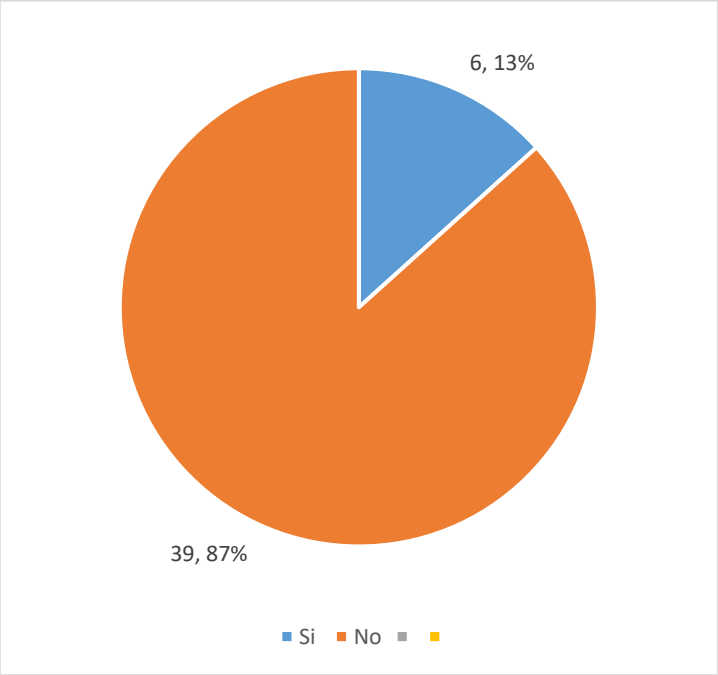



**Gráfico 6-4.** Guía metodológica de gestión riesgos de seguridad existente
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

En cuanto a la pregunta, tienen una guía metodología de gestión riesgos de seguridad de la información para la administración de servidores virtualizados a su cargo un 87% dicen que no y un 13% que si por lo que si amerita para poder lograr la seguridad de la información el que haya una conocimiento y aplicación de una guía.

Destacándose entonces la necesidad de elaboración de una guía metodológica de gestión de riesgo de la seguridad de la información en los servidores virtuales.

**Tabla 7-4:** Aplicación de las actuales normas, estándares o modelos de control de gestión de riesgos de seguridad de la información bajo su control

| Opciones | f | % |
|---|---|---|
| Si | 11 | 24% |
| No | 25 | 56% |
| No responde | 9 | 20% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

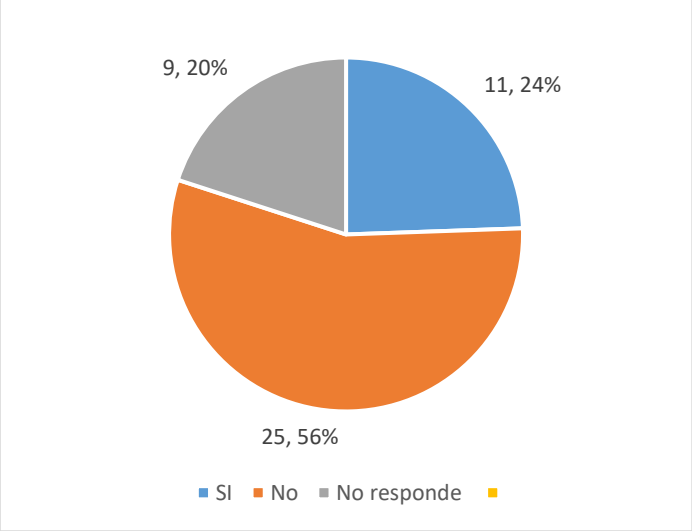



**Gráfico 7-4.** Aplicación de las actuales normas, estándares o modelos de control de gestión de riesgos de seguridad de la información bajo su control
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

En cuanto a si se aplican actuales normas, estándares o modelos de control de gestión de riesgos de seguridad de la información bajo su control, de los 45 encuestados el 24% responden afirmativamente, el 56% dicen que no, y no responden el 20%.

Significando que es bajo el número de administradores de los servidores virtuales que lo hacen y el resto no lo hace o no responden a la pregunta por desconocimiento.

**Tabla 8-4:** La aplicación de un modelo de gestión de riesgos de la seguridad de la información ayuda a mitigar los riesgos y evitar amenazas en servidores virtualizados

| Opciones | f | % |
|---|---|---|
| Si | 37 | 82% |
| No | 0 | 0% |
| No responden | 8 | 18% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

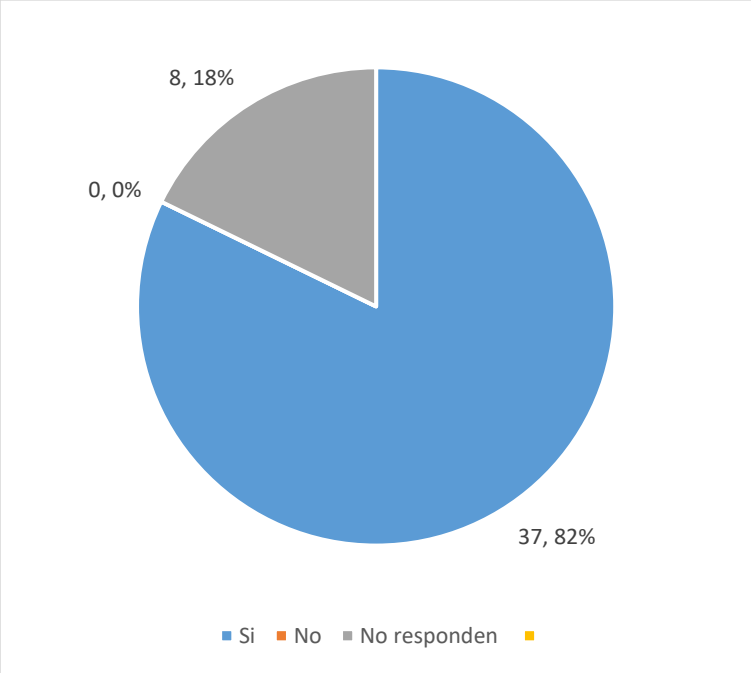



**Gráfico 8-4.** La aplicación de un modelo de gestión de riesgos de la seguridad de la información ayuda a mitigar los riesgos y evitar amenazas en servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

Respecto a que si la aplicación de un modelo de gestión de riesgos de la seguridad de la información ayuda a mitigar los riesgos y evitar amenazas en servidores virtualizados los encuestados responden en un 82% que sí y los restantes 8% no responden.

Lo que permite conocer la necesidad de un modelo de gestión de riesgos de la seguridad de la información.

**Tabla 9-4:** Metodología de gestión riesgos de seguridad de la información para controlar un problema de seguridad

| Opciones | f | % |
|---|---|---|
| Cuantitativa | 8 | 18% |
| Cualitativa | 8 | 18% |
| Mixta | 29 | 64% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

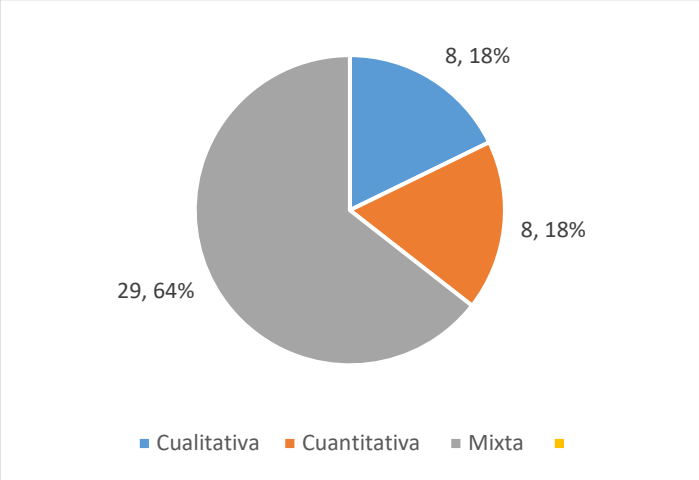



**Gráfico 9-4.** Metodología de gestión riesgos de seguridad de la información para controlar un problema de seguridad
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

Respecto a la metodología de gestión riesgos de seguridad de la información conocida para poder controlar un problema de seguridad estiman que la más adecuada es la Mixta en un 64 %, la cuantitativa en 18% y cualitativa en otro 18% de los encuestados. Lo que sugiere la necesidad de una guía metodológica más acorde con las necesidades actuales de los riesgos de la información en los servidores virtuales.

**Tabla 10-4:** Resolución de problemas en la administración de servidores virtuales mediante aplicación de una guía metodológica de gestión de riesgos de seguridad de la información

| Opciones | f | % |
|---|---|---|
| Siempre | 14 | 31 % |
| Rara vez | 3 | 7% |
| Nunca | 0 | 0% |
| No responde | 28 | 62% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

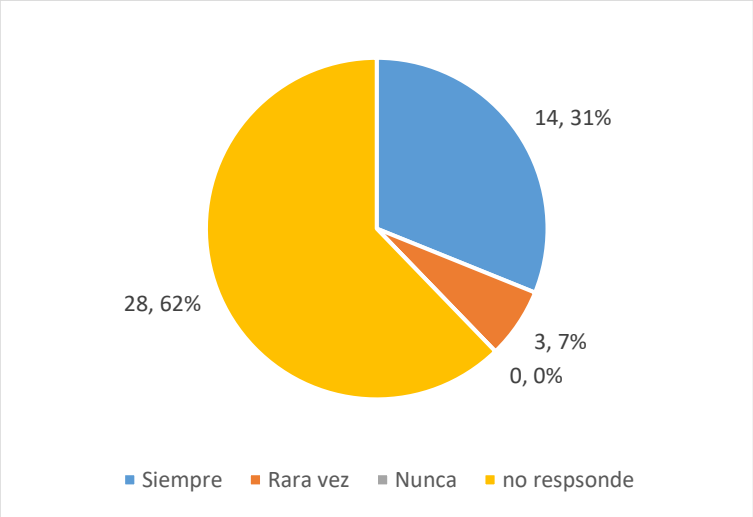



**Gráfico 10-4.** Resolución de problemas en la administración de servidores virtuales mediante aplicación de una guía metodológica de gestión de riesgos de seguridad de la información
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

En el caso de poseer una guía metodológica de gestión de riesgos de seguridad de la información, al aplicarla han resuelto los problemas presentados en la administración de servidores virtualizados, los encuestados responden que, el 31% siempre, rara vez el 7% y el 28% no responden. Se interpreta que no responden por cuanto no aplican una guía metodológica de gestión de riesgos de seguridad de la información y los restantes administradores si lo hacen.

**Tabla 11-4:** Decisiones para solucionar los problemas de riesgo de la información para la administración de los servicios virtuales a su cargo

| Opciones | f | % |
|---|---|---|
| Reducir | 29 | 64% |
| Aceptar | 3 | 7% |
| Evitar | 10 | 22% |
| Transferir | 3 | 7% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

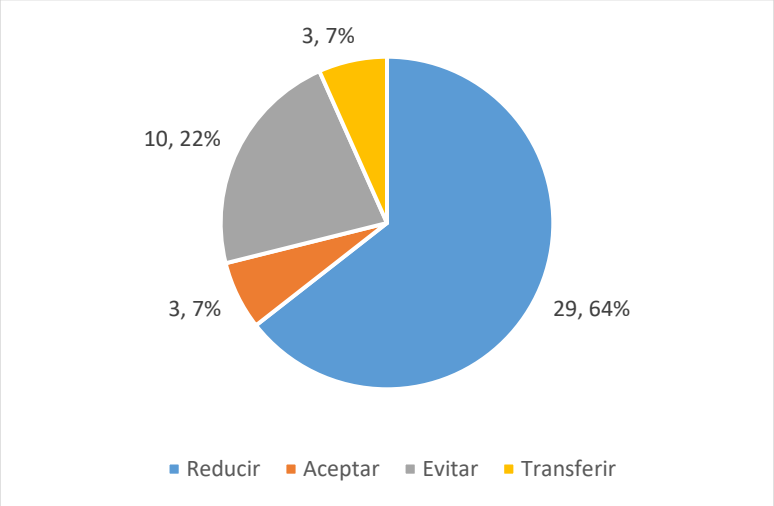



**Gráfico 11-4.** Decisiones para solucionar los problemas de riesgo de la información para la administración de los servicios virtuales a su cargo
**Realizado por:** Jiménez Fabricio, 2022

### Análisis e Interpretación

En cuanto a la pregunta sobre la decisión que han tomado para solucionar los problemas de riesgo de la información para la administración de los servicios virtuales a su cargo, las respuestas se orientan a reducir, evitar, aceptar y transferir para solventar los problemas de riesgos presentados.

**Tabla 12-4:** Mejorar el control de posibles eventos que afecten el nivel de seguridad de los servidores virtualizados a su cargo

| Opciones | f | % |
|---|---|---|
| Si | 45 | 100% |
| No | 0 | 0% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

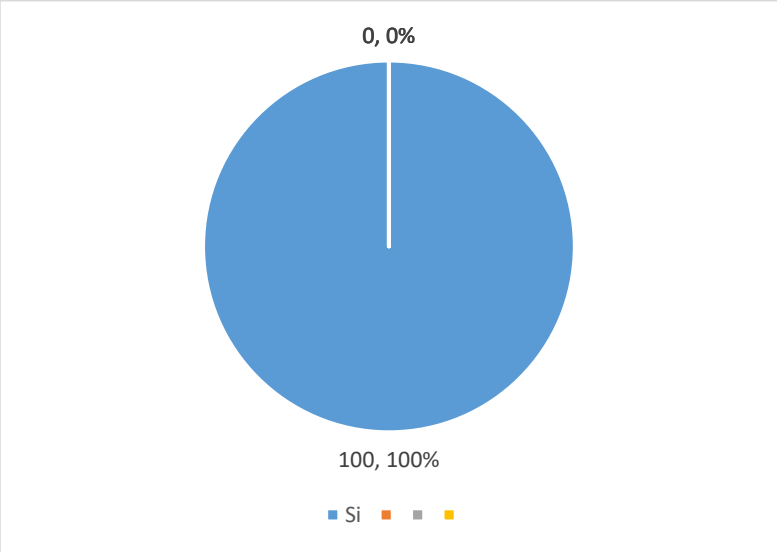



**Gráfico 12-4.** Pregunta 12
**Realizado por:** Jiménez Fabricio, 2022

### Análisis e Interpretación

Acerca de la interrogante, si estiman necesario mejorar el control de posibles eventos que afecten el nivel de seguridad de los servidores virtualizados a su cargo, el 100% de administradores de servidores virtualizados estiman que si necesario mejorarlo.

**Tabla 13-4:** Desarrollo de una nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la Información (GRSI)

| Opciones | f | % |
|---|---|---|
| Si | 45 | 100% |
| No | 0 | 0% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

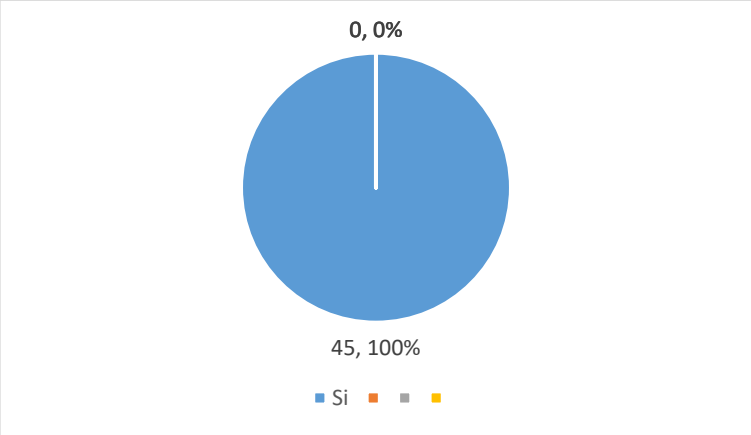



**Gráfico 13-4.** Desarrollo de una nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la Información (GRSI)
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

Al ser consultados a través de esta encuesta sobre la necesidad de desarrollar una nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la Información (GRSI) en la administración de servidores virtualizados para mejorar el control de posibles eventos que afecten el nivel de seguridad el 100% de encuestados consideran que si se hace necesario disponer de una que solucione los eventuales problemas.

**Tabla 14-4:** Aplicación de nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la información en la administración de servidores virtualizados

| Opciones | f | % |
|---|---|---|
| Si | 45 | 100% |
| No | 0 | 0% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

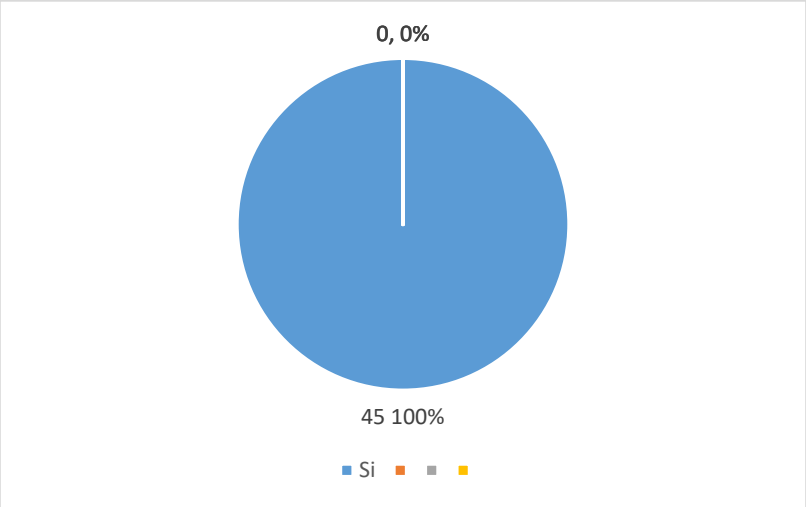



**Gráfico 14-4.** Aplicación de nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Análisis e Interpretación:**

En cuanto a, si estaría de acuerdo en que se implemente y ponga en práctica esta nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la información en la administración de servidores virtualizados a su cargo, los 45 administradores consultados están de acuerdo en que sí es necesario una nueva guía apegada a las normas establecidas

## 4.2. Estadística inferencial

### *4.2.1. Prueba T Student*

Las hipótesis de investigación o científicas para su validación son sometidas a prueba para determinar si son apoyadas o refutadas de acuerdo con los resultados obtenidos en la investigación de campo argumentando que fue apoyada o no puesto que científicamente no podemos probar que una hipótesis sea verdadera o falsa.

Son varias las pruebas estadísticas que permiten establecer algunos límites de confianza, una de estas es la prueba T de Student que es cualquier prueba en la que el estadístico utilizado tiene una distribución T de Student si la hipótesis nula es cierta.

Se aplica especialmente cuando la población estudiada sigue una distribución normal pero el tamaño de la muestra es demasiado pequeño como para que el estadístico en el que está basada la inferencia esté normalmente distribuido, utilizándose una estimación de la desviación típica en lugar del valor real, como en la presente investigación.

### *4.2.2. Hipótesis de investigación (Hi):*

El desarrollo de una guía metodológica para la gestión de riesgos en seguridad de la información, permitirá mejorar el nivel de control de seguridad de los servidores virtualizados.

### *4.2.3. Hipótesis de Nula (H0):*

El desarrollo de una guía metodológica para la gestión de riesgos en seguridad de la información, no permitirá mejorar el nivel de control de seguridad de los servidores virtualizados.

$$Ho: \mu_d = 0$$

### *4.2.4. Hipótesis Alternativa (H1):*

El desarrollo de una guía metodológica para la gestión de riesgos en seguridad de la información, permitirá mejorar el nivel de control de seguridad de los servidores virtualizados.

$$H1: \mu_d \neq 0$$

Donde $\mu_d$ es la media de las medidas.

### *4.2.5. Nivel de significancia*

Necesariamente se debe elegir un nivel de significancia para la prueba que permite juzgar si los resultados de la prueba son estadísticamente significativos y también determina la probabilidad de error que es inherente a la prueba.

Para la presente investigación se establece un nivel de significancia (denotado como α o alfa) de 0.05. Un nivel de significancia de 0.05 indica un riesgo de 5% de concluir que existe una diferencia cuando no hay una diferencia real.

$$\alpha = 0.05$$

### *4.2.6. Definir estadístico de prueba*

En función de los datos obtenidos durante la investigación se define que utilizamos la distribución T de Student para muestras pareadas, donde se establece que:

$$t_c = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}$$

$$S_d = \sqrt{\frac{\sum_{i=1}^{n}(d - \bar{d})^2}{n-1}}$$

Donde:

$t_c$ = valor estadístico del procedimiento calculado.

$\bar{d}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después.

$S_d$ = desviación estándar de las diferencias entre los momentos antes y después.

n = tamaño de la muestra.

### *4.2.7. Regla de decisión*

Caso 1.

$$t_c > t_\alpha, rechaza\ la\ hipotesis\ nula\ H_0$$

Caso 2.

$$Valor\ p < \alpha, se\ rechaza\ la\ hipotesis\ nula\ H_0$$

## 4.3. Discusión

Los datos obtenidos en la investigación fueron evaluados en el software SPSS que permite de forma automática ejecutar las fórmulas antes descritas, obteniendo los siguientes resultados:

### Normalidad

Para la prueba de normalidad en la que se debe aceptar la hipótesis nula y se consideran todas las categorías de riesgos ponderadas según la siguiente tabla:

**Tabla 15-4:** Datos de respuestas Probabilidad de necesidad de una guía Guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados identificados Post-Implementación

| Items | Inicial | Post |
|---|---|---|
| Importancia el conocimiento gestión de riesgos de seguridad de la información. | 2,73 | 0,55 |
| Gestión de riesgo aplicado en el sistema a su cargo | 3,42 | 0,58 |
| Necesario conocer los fundamentos metodológicos de gestión de riesgos de seguridad. | 3,18 | 0,68 |
| La gestión de riesgos incluye todas las medidas adoptadas para controlar los riesgos de la información. | 2,32 | 0,45 |
| La aplicación de los fundamentos metodológicos de gestión de riesgos de seguridad de la información permitirá mejorar el nivel de control de seguridad de los servidores virtualizados. | 0,18 | 0,06 |
| Tiene una guía metodología de gestión riesgos de seguridad de la información para la administración de servidores virtualizados. | 0,41 | 0,24 |
| De las actuales normas, estándares o modelos de control de gestión de riesgos de seguridad de información bajo su control las aplica o no. | 1,97 | 0,33 |
| La aplicación de un modelo de gestión de riesgos de la seguridad de la información ayuda a mitigar los riesgos y evitar amenazas | 3,05 | 0,45 |

| | | |
|---|---|---|
| De la metodología de gestión riesgos de seguridad de la información conocida cuál cree usted es la más adecuada para poder controlar un problema de seguridad | 1,50 | 0,17 |
| De poseer una guía metodológica de gestión de riesgos de seguridad de la información, al aplicarla han resuelto los problemas presentados. | 2,93 | 0,68 |
| Decisiones ha tomado para solucionar los problemas de riesgo de la información para la administración de los servicios virtuales | 2,25 | 0,55 |
| Es necesario mejorar el control de posibles eventos que afecten el nivel de seguridad de los servidores virtualizados. | 1,75 | 4,25 |
| Se hace necesario desarrollar una nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la Información. | 1,50 | 4,75 |
| Es necesario que se implemente y ponga en práctica esta nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la información en la administración de servidores virtualizados. | 5,5 | 5,5 |

**Realizado por:** Jiménez Fabricio, 2022

Para complementar este proceso de comprobación de la hipótesis y en base a los resultados de la segunda encuesta aplicada a los administradores de servidores virtualizados luego de que conocieran y aplicaran en su entorno la Guía Metodológica de Gestión de Riesgos de Seguridad de la Información en la administración de servidores virtualizados para mejorar el control de posibles eventos que afecten el nivel de seguridad se obtiene lo siguiente:

**Pregunta.** ¿La aplicación de la Guía Metodológica de Gestión de Riesgos de Seguridad de la Información en la administración de servidores virtualizados como modelo de gestión para mitigar los riesgos y evitar amenazas en servidores virtualizados se resolvieron los problemas presentados?

Si ( )  No ( )

**Tabla 16-4:** Pregunta post implementación de GMGSI-FJ

| **Opciones** | **f** | **%** |
|---|---|---|
| Si | 42 | 93% |
| No | 3 | 7% |
| **Total** | **45** | **100%** |

**Fuente:** Encuesta aplicada al personal encargado de la administración de los servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

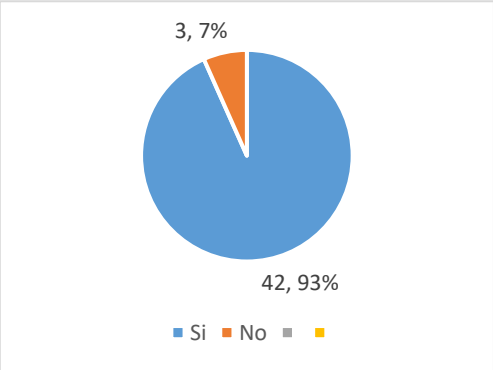



**Gráfico 15-4.** Pregunta post implementación de GMGSI-FJ
**Realizado por:** Jiménez Fabricio, 2022

**Análisis.** De los 45 administradores de servicios virtualizados que aplicaron la Guía Metodológica de Gestión de Riesgos de Seguridad de la Información como modelo de gestión para mitigar los riesgos y evitar amenazas en servidores virtualizados, en un 93% respondieron afirmativamente lo que significa que la investigación realizada y la hipótesis planteada tiene resultados favorables para remediar el problema planteado.

# CAPÍTULO V

## 5. PROPUESTA

## GUÍA METODOLÓGICA DE GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA ADMINISTRACIÓN DE SERVIDORES VIRTUALIZADOS

### Introducción

La información es el activo principal que se debe considerar dentro de una empresa o entidad pública o privada ya que es fundamental para su correcto desempeño en el cumplimiento de sus objetivos y el normal desarrollo de las operaciones.

A través de esta guía metodológica de gestión del riesgo de la seguridad de la información para la administración de servidores virtualizados se busca orientar a las entidades a gestionar los riesgos de seguridad de la información en sus servidores virtualizados, basado en los criterios de confidencialidad, integridad y disponibilidad.

Se ha definido un enfoque sistemático para la gestión del riesgo en la seguridad de la información para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información.

El abordar los riesgos a través de los esfuerzos de seguridad deben ser eficaces y oportunos justificando el dónde y cuándo sean necesarios. El proceso de la gestión del riesgo de la seguridad de la información debe ser una parte integral de todas las actividades de la gestión de la seguridad de la información.

Para alcanzar los objetivos de la gestión del riesgo de la seguridad de la información debe ser un proceso continuo, necesariamente ha de establecerse el contexto, evaluar los riesgos, y en su momento tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones que superen los problemas de dichos sistemas.

**Objetivo**

Proporcionar una Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados para mejorar el control de posibles eventos que afecten el nivel de seguridad de la empresa e instituciones públicas o privadas como resultado de esta tesis de maestría.

**Proceso para la gestión del riesgo de la seguridad de la información de servidores virtualizados.**

Para poder llevar adelante la gestión del riesgo de la seguridad de la información para la administración de servidores virtualizados se recomienda de manera general las siguientes actividades dirigidas a suministrar un buen equilibrio entre la reducción del tiempo y el esfuerzo necesario para ser identificados los controles, garantizando que los riesgos de mayor impacto sean valorados oportunamente.

- Establecer el contexto
- Valorar el riesgo latente
- Establecer la forma de tratar ese riesgo
- Admisión del riesgo
- Notificación del riesgo
- Dar el correspondiente monitoreo y revisión del riesgo

Los pasos o actividades de este proceso de gestión del riesgo quedan establecidos en el siguiente orden:

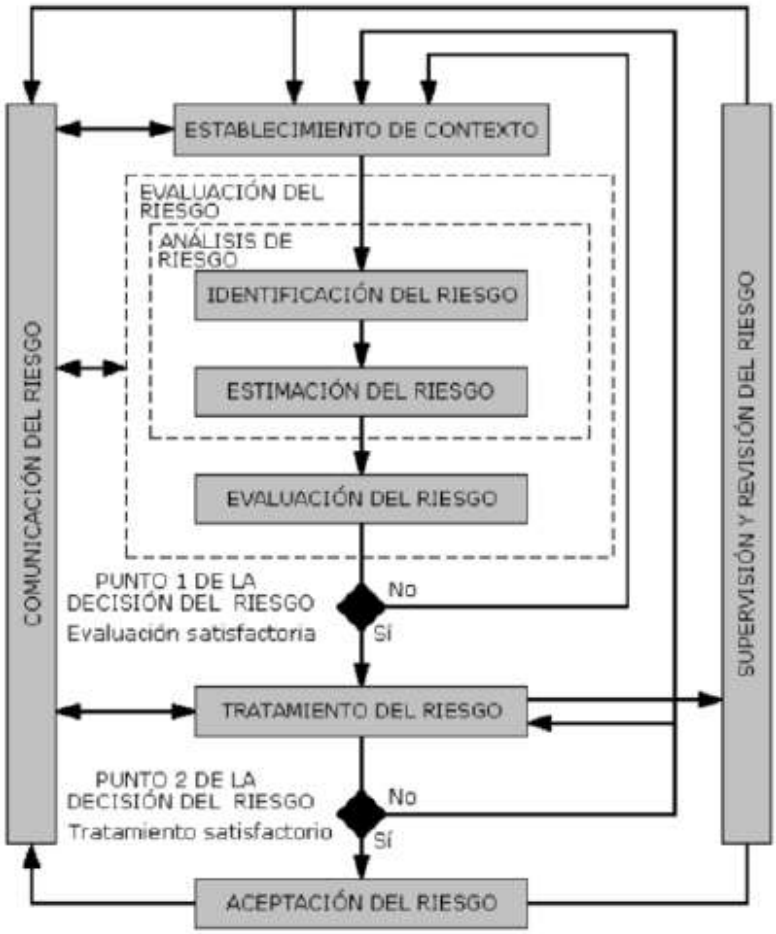



**Figura 1-5:** Proceso de gestión del riesgo en la seguridad de la información
**Fuente:** ISO27005

ISO 27001, define como 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 proceso de aplicación de seguridad en entornos virtuales.

Para llegar a la evaluación de riesgos en los entornos de servidores virtualizados seleccionado para la elaboración de esta guía.es necesario desarrollar criterios previos con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales

- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

De igual modo, los criterios de evaluación de impacto del riesgo y se pueden utilizar para especificar las prioridades del tratamiento del riesgo de la seguridad de la información. (Ardenghi, 2020)

Por lo que es recomendable desarrollar criterios de impacto del riesgo de la seguridad de la información y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información del proceso
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

Para llegar a los criterios de aceptación del riesgo de la seguridad de la información es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas. (Ambit, 2020)

Que habrá de regirse de conformidad el siguiente esquema:

**Tabla 1-5:** Proceso para la gestión de riesgo de la seguridad de la información

| **PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN** | |
|---|---|
| **ACTIVIDAD** | **PASOS** |
| | 1. Consideraciones Generales - Levantamiento de información inicial |

| | |
|---|---|
| **Establecimiento del contexto** | 2. Establecer criterios básicos para la Gestión del Riesgo<br>3. Definir alcance y límites de la Gestión del Riesgo<br>4. Establecer una organización para la operación del SGRSI |
| **Valoración del riesgo** | 5. Identificar Activos de Información<br>6. Identificar las amenazas y las vulnerabilidades<br>7. Identificar los controles existentes<br>8. Identificar consecuencias<br>9. Determinar el nivel de estimación del riesgo<br>10. Evaluar el riesgo |
| **Tratamiento del riesgo** | 11. Seleccionar controles |
| **Aceptación del riesgo** | 12. Aceptar el riesgo |
| **Comunicación del riesgo** | 13. Comunicar el riesgo |
| **Monitoreo y Revisión del Riesgo** | 14. Monitorear y revisar los riesgos |

**Fuente:** ISO27005
**Realizado por:** Jiménez Fabricio, 2022

# 1. ESTABLECIMIENTO DEL CONTEXTO

## 1.1. Condiciones Generales y levantamiento de información inicial

Es necesario tener claro el entorno donde se aplicará esta guía, precisando cual será el contexto en el que se desenvolverá, que procesos se involucran, cual es el flujo de dichos procesos para lograr identificar los riesgos de la seguridad.

La guía señala estrategias para hacer el levantamiento del contexto:

- Inventario de eventos
- Análisis de flujos de procesos
- Preparación de un plan de respuesta a incidentes
- Descripción de los requisitos de seguridad de la información para un producto o servicio
- Evidencias de la debida diligencia

## 1.2. Criterios básicos

Obedeciendo al alcance y los objetivos de la gestión del riesgo establecido previamente, se aplican diferentes enfoques técnicos que varían de acuerdo a cada repetición.

Se aconseja seleccionar o desplegar un enfoque adecuado para la gestión del riesgo que aborde los criterios básicos, entre los más importantes se incluyen: criterios de identificación, evaluación, de impacto y de aceptación del riesgo.

### 1.2.1. Criterios de identificación del riesgo

La identificación del riesgo se basa en causas identificadas para los procesos, estos pueden ser internos o externos; se debe considerar los activos de información con el valor de impacto alto a fin de determinar el riesgo de la seguridad de la información del usuario o de la institución en servidores virtualizados.

### 1.2.2. Criterios de evaluación del riesgo

Se recomienda establecer criterios para determinar la evaluación del riesgo, teniendo en cuenta algunos aspectos, como puede ser los que se detallan a continuación:

- La criticidad de los activos de información que se involucran en el proceso.
- La importancia de los pilares de la seguridad de la información para las operaciones.
- Las consecuencias negativas que afectan la reputación de la institución.
- El valor estratégico del proceso de información para la empresa.

### 1.2.3. Criterios de impacto del riesgo

Los criterios de impacto del riesgo se deben especificar según el grado de daño o de costos para la entidad, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de la información.
- Brechas (pérdidas) en la seguridad de la información.
- Operaciones deterioradas.
- Pérdida de la entidad y del valor financiero.
- Consecuencias en cuanto a la reputación.
- No cumplimiento de los requisitos legales.
- Alteración de cronogramas y fechas.

### 1.2.4. Criterios de la aceptación del riesgo

En cuanto a los criterios de aceptación del riesgo, dependen de las políticas, metas, objetivos del usuario o de la institución y de las partes interesadas en este proceso.
Cada institución puede definir sus propias escalas para los niveles de aceptación del riesgo, donde se pueden considerar algunos elementos, como los siguientes:

- Factores sociales y humanitarios
- Finanzas
- Tecnología
- Operaciones
- Aspectos legales

## 1.3. Alcance y límites

Ha de definirse el alcance del proceso de gestión del riesgo de la seguridad de la información, con el objetivo de poder garantizar que todos los activos relevantes sean tomados en cuenta en la valoración de ese riesgo, identificando los límites para abordar todos los riesgos que se pueden presentar. La organización debe considerar lo siguiente:

- Enfoque global de la organización
- Procesos de negocios
- Objetivos del negocio
- Funciones y estructura de la organización
- Entorno sociocultural

## 1.4. Organización para la gestión del riesgo de la seguridad de la información

Se debe establecer y mantener la organización y las responsabilidades en el proceso de gestión del riesgo y la seguridad de la información definidas en el correspondiente acuerdo ministerial, tratándose ya sea de instituciones privadas o del Estado.

Este proceso de organización para la ejecución de la gestión del riesgo, deberá ser aprobado por la máxima autoridad o representante de cada institución.

## 2. VALORACIÓN DEL RIESGO

Se dice que un riesgo es una combinación de los resultados que se presentarían después de la ocurrencia de un evento indeseado y de su posibilidad de ocurrencia. Se cuantifica o describe cualitativamente el riesgo al realizar la valoración respectiva que permite a los propietarios de los activos priorizar los riesgos de conformidad con la gravedad valorada y otros criterios establecidos sobre el funcionamiento dichos activos.

**Análisis del riesgo**

**Identificación del riesgo**

Este proceso consiste en determinar qué puede provocar pérdidas al usuario o la institución el mismo que consta de las siguientes actividades:

- Identificación de los activos del usuario o institución
- Identificación de las amenazas presumibles
- Identificación de vulnerabilidades encontradas
- Identificación de la existencia de controles de dichos activos.

### 2.1. Identificación de los activos

Teóricamente un activo es todo aquello que tiene valor para el usuario o la organización y que, por lo tanto, requiere de una protección adecuada. Es recomendable que para la identificación la entidad debe tener un inventario de los mismos y cada uno de ellos debe tener asignado un propietario.

Como resultado de este proceso se crea una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia a fin de poder continuar con el proceso de aseguramiento.

A fin de poder efectuar la valoración de los activos, es indispensable que el usuario o que la institución identifique primero sus activos (con un grado adecuado y mínimo de detalles). Como resultado de lo cual de manera general se pueden diferenciar dos clases de activos:

- Primarios: son actividades, procesos del negocio y la información.

- De soporte: dependen de los elementos primarios y pueden ser, hardware, software, redes, personal, ubicación y estructura de la organización.

Dentro de la entidad el inventario de activos de información tiene que estar especificado de la siguiente manera:

- Datos básicos del activo como nombre, proceso, observación
- Nivel de clasificación de la información
- Información de la ubicación electrónica y física
- Identificación del propietario
- Derechos de acceso

**Ejemplo de identificación de activos:**

De acuerdo a las necesidades del usuario o institución ha de aplicarse el siguiente ejemplo de cuadro de identificación de activos

**Tabla 2-5:** Ejemplos identificación de activos de la información

| IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN | | | | | | |
|---|---|---|---|---|---|---|
| **Nro. Activo** | **Proceso Macro** | **Subproceso** | **Tipo de Activo** | **Nombre de Activo** | **Descripción del activo** | **Ubicación** |
| **A1** | TICS | Infraestructura | Hardware | Servidores físicos | Servidor que contiene las máquinas virtuales | Data Center |
| **A2** | | Redes y comunicaciones | Redes | Switch Routers | Procesamiento de trafico de red para distribución en la red interna e Internet | Data Center |
| **A3** | | Aplicaciones informáticas | Software | Servicio de correo institucional | Información de buzones de correo electrónico | Data Center |
| **A4** | | Instalaciones | Localidad | Datacenter | Centro de Datos | Edificio Matriz |
| **A5** | | Talento Humano | Personal | Personal de soporte | Funcionarios de Soporte Técnico Nivel 1 | Edificio Matriz |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

### 2.1.1. Valoración de los activos/ponderación de la criticidad de activos

La siguiente etapa en este proceso es la ponderación de activos y en la que participan las unidades del negocio involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos.

Para este efecto la ponderación ha de realizarse en términos de "alto, medio o bajo" donde se asigna un valor cuantitativo a cada valor cualitativo.

- **Valoración del impacto en términos de la pérdida de la confidencialidad:**

**Tabla 3-5:** Valoración del impacto en términos de la pérdida de la confidencialidad

| CONFIDENCIALIDAD | CRITERIO |
|---|---|
| **Alto (3)** | La divulgación no autorizada de la información tiene un efecto crítico para la institución |
| **Medio (2)** | La divulgación no autorizada de la información tiene un efecto limitado para la institución |
| **Bajo (1)** | La divulgación de la información no tiene ningún efecto para la institución |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

- **Valoración del impacto en términos de la perdida de la integridad del activo:**

**Tabla 4-5:** Valoración del impacto en términos de la pérdida de la integridad del activo

| INTEGRIDAD | CRITERIO |
|---|---|
| **Alto (3)** | La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución |
| **Medio (2)** | La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución |
| **Bajo (1)** | La destrucción o modificación de la información tiene un efecto leve para la institución |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

- **Valoración del impacto en términos de la pérdida de la disponibilidad**

**Tabla 5-5:** Valoración del impacto en términos de la pérdida de la disponibilidad

| DISPONIBILIDAD | CRITERIO |
|---|---|
| **Alto (3)** | La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución |
| **Medio (2)** | La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución |
| **Bajo (1)** | interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

Con referencia a las tablas mencionadas, la valoración se la realiza respecto a la confidencialidad, integridad y disponibilidad ya que estas son las dimensiones en que se basa la seguridad de la información.

La valoración del impacto de un activo (VA), es el promedio de los valores de las tres dimensiones de la Gestión de la Seguridad de la Información:

$$\boldsymbol{VA}=(\boldsymbol{C}+\mathbf{I}+\mathbf{D})/\mathbf{3}$$

**Tabla 6-5:** Valoración de los activos de la información

**VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

| Nro. Activo | Nombre de Activo | Ubicación | Valoración de Impacto (pérdida)<br>C: Confidencialidad<br>I: Integridad<br>D: Disponibilidad | | | |
|---|---|---|---|---|---|---|
| | | | C | D | I | VA |
| **A 1** | Servidores físicos | Centro de Datos | 3 | 3 | 3 | 3 |
| **A 2** | Switch<br>Routers | Centro de Datos | 1 | 1 | 3 | 1.67 |
| **A 3** | Servicio de correo institucional | Centro de Datos | 2 | 2 | 2 | 2 |
| **A 4** | Datacenter | Edificio matriz | 3 | 3 | 3 | 3 |
| **A 5** | Personal de soporte | Edificio matriz | 2 | 2 | 2 | 2 |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

Todas las ponderaciones de los cuadros anteriores se aplicarán de conformidad a los activos particulares o institucionales en que se aplica esta Guía de Gestión de riesgo de la Seguridad de la Información.

## 2.2. Identificación de Amenazas

Continuando con este proceso de aplicación a la presente guía ha de identificarse las amenazas y sus orígenes. Entendiendo que una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, al usuario o a las organizaciones.

Ciertas amenazas pueden afectar a más de un activo lo que pueden causar diferentes impactos dependiendo los activos que se vean afectados por la misma.

A continuación, se describe una serie de amenazas más comunes:

**Tabla 7-5:** Ejemplos amenazas comunes

| TIPO | AMENAZA |
|---|---|
| **Daño físico** | Fuego<br>Agua<br>Accidente<br>Destrucción del equipo |

| | |
|---|---|
| | Congelamiento |
| **Eventos naturales** | Fenómenos sísmicos<br>Fenómenos volcánicos<br>Fenómenos climáticos |
| **Pérdida de servicios esenciales** | Fallas en el sistema de aire acondicionado<br>Pérdida de suministros de energía<br>Falla en equipo de telecomunicaciones |
| **Perturbación debido a la radiación** | Radiación electromagnética |
| **Compromiso de la información** | Espionaje remoto<br>Escucha encubierta<br>Hurto de documentos<br>Hurto de equipos<br>Divulgación<br>Manipulación con software |
| **Fallas técnicas** | Fallas de equipo<br>Malfuncionamiento del equipo<br>Saturación del sistema de información<br>Malfuncionamiento de software<br>Incumplimiento en el mantenimiento del sistema de información |
| **Acciones no autorizadas** | Uso no autorizado del equipo<br>Copia fraudulenta del software<br>Uso de software pirata |
| **Compromiso de las funciones** | Error en el uso<br>Abuso de derechos<br>Falsificación de derechos<br>Incumplimiento en la disponibilidad del personal |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

Se recomienda tener en cuenta las amenazas humanas, pueden ser las siguientes:

**Tabla 8-5:** Amenazas humanas

| FUENTE DE AMENAZA | MOTIVACIÓN | ACCIONES AMENAZANTES |
|---|---|---|
| **Intruso ilegal o pirata informático** | Reto<br>Ego<br>Rebelión<br>Dinero | Piratería<br>Acceso no autorizado |
| **Criminal de computación** | Destrucción de la información<br>Divulgación ilegal de la información<br>Ganancia monetaria<br>Alteración no autorizada de los datos | Soborno de la información<br>Suplantación de la identidad<br>Intrusión en el sistema |
| **Terrorismo** | Chantaje<br>Destrucción<br>Venganza | Ataques contra el sistema DDoS<br>Penetración al sistema |
| **Espionaje (empresas, gobiernos, otros intereses)** | Ventaja competitiva<br>Espionaje | Ventaja de defensa<br>Hurto de información<br>Acceso no autorizado |
| **Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos** | Curiosidad<br>Inteligencia<br>Ganancia monetaria<br>Venganza<br>Errores y omisiones no intencionales | Chantaje<br>Robo a un empleado<br>Observar información reservada<br>Uso inadecuado del computador<br>Fraude<br>Código malicioso<br>Venta de información personal |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

## 2.3. Identificación de Vulnerabilidades

Paso seguido han de identificarse las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos personales o a la institución.

Ha de recordarse que la sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Igualmente, una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, recomendándose eso sí reconocerla y monitorearla para determinar los cambios que puede ocasionar. Es importante tomar nota que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad y que es lo que se debe evitar.

**Tabla 9-5:** Identificación de vulnerabilidades

| TIPO DE ACTIVO | EJEMPLO DE VULNERABILIDADES | EJEMPLO DE AMENAZAS |
|---|---|---|
| **Hardware** | Mantenimiento insuficiente o instalación fallida de los medios de almacenamiento | Incumplimiento en el mantenimiento del sistema de información |
| | Susceptibilidad a variaciones de voltaje | Pérdida de suministro de energía |
| | Copia no controlada | Hurtos de medios o documentos |
| **Software** | Ausencia de terminación de sesión cuando se abandona la estación de trabajo | Abusos de los derechos |
| | Disposición de utilización de medios de almacenamiento sin borrado adecuado | |
| | Asignación errada de derechos de acceso | |
| | Insuficiencia de pruebas de software | |
| | Configuración incorrecta de parámetros | Error en el uso |
| | Ausencia de mecanismos de identificación y autentificación | Falsificación de derechos |
| | Gestión deficiente de contraseñas | |
| | Ausencia de protección física | |
| | | Hurto |
| **Red** | Transferencia de contraseñas en plano | Espionaje |

| | | |
|---|---|---|
| | Conexiones de red públicas sin protección | Uso no autorizado del equipo |
| | Tráfico sensible sin protección | Escucha encubierta |
| | Arquitectura insegura de red | Espionaje |
| | Ausencia de identificación y autentificación del emisor y receptor | Espionaje |
| **Personal** | Ausencia del personal | Incumplimiento en la disponibilidad del personal |
| | Entrenamiento insuficiente en seguridad | Error en el uso |
| | Falta de conciencia de seguridad | Error en el uso |
| | Trabajo no supervisado del personal externo | Hurto |
| | Ausencia de políticas para el uso correcto de los medios de telecomunicaciones | Uso no autorizado del equipo |
| **Lugar** | Ubicación susceptible en área de inundación | Destrucción |
| | Ausencia de protección | Hurto |
| **Organización** | Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso de derechos |
| | Ausencia de auditorias | Abuso de derechos |
| | Ausencia de procedimientos de identificación y valoración de riesgos | Abuso de derechos |
| | Ausencia de procedimientos de control de cambios | |
| | Ausencia de revisiones regulares por parte de la gerencia | Incumplimiento en el mantenimiento del sistema de información |
| | Ausencia de política formal sobre la utilización de computadoras portátiles | Uso no autorizado del equipo |
| | | Hurto |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

## 2.4. Identificación de los controles existentes

Corresponde necesariamente realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, como la duplicación de los controles. También, mientras se

identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente.

Existen dos tipos de controles:

- Preventivos: aquellos que actúan para eliminar las causas de riesgo para prevenir su ocurrencia o materialización.
- Correctivos: permiten restablecer la actividad después de detectar eventos no deseados.

Se utiliza una tabla de estructura de controles para realizar un trabajo ordenado y documentado.

**Tabla 10-5:** Identificación de controles existentes

| ANÁLISIS DE RIESGOS | | | | | EVALUACIÓN DE RIESGOS | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Impacto | Probabilidad | | Controles implementados existentes | Cálculo de Evaluación R |
| **Subprocesos** | **Nro. Activo** | **Nombre Activo** | **Amenaza** | **Vulnerabilidad** | **CID** | **Nivel de amenaza** | **Nivel de vulnerabilidad** | | |
| **Infraestructura** | A1 | Servidores físicos (hipervisor) | Pérdida de suministro de energía | Susceptibilidad a variaciones de voltaje | 3 | 1 | 1 | Baterías y generadores | **3** |
| **Aplicaciones informáticas** | A2 | Servicio de correo institucional (máquina virtual) | Abuso de derechos | Utilización de medios de almacenamiento sin borrado adecuado | 2 | 2 | 2 | Políticas sobre el uso de correo electrónico | 8 |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

## 2.5. Identificación de consecuencias

Una consecuencia podría ser la pérdida de la eficacia, condiciones adversas de operación, pérdidas de negocio, daños, reputación, entre otros.

Para identificar las consecuencias es necesario que la entidad tenga la lista de activos y su relación con cada proceso, la lista de amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

Estas consecuencias se pueden identificar en los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Costo financiero
- Imagen, reputación y buen nombre

## 2.6. Determinar el nivel de estimación del riesgo

Para la estimación del análisis del riesgo ha de utilizarse métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, tomando en cuenta los activos, las amenazas y las políticas del usuario o de la institución.

Identificados los riesgos, el marco de trabajo debe considerar una metodología de análisis de riesgo. Es recomendable que el análisis de riesgo cualitativo use una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo, baja, media y alta) y la probabilidad de esas consecuencias.

## 2.7. Evaluación del riesgo

Actividad de este proceso que consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Se impone el proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del riesgo. Para los efectos de esta Guía el grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad ya determinados.

### 2.7.1. Criterios de probabilidad de ocurrencia de amenazas

En la siguiente tabla se detallan los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explotar alguna vulnerabilidad existente.

**Tabla 11-5:** Criterios de probabilidad de ocurrencia de amenazas

| NIVEL DE AMENAZAS | CRITERIO POR PROBABILIDAD | CRITERIO POR CONDICIÓN DE OCURRENCIA | CRITERIO POR ATRACTIVO | EJEMPLO |
|---|---|---|---|---|
| **Alto (3)** | La ocurrencia es muy probable (probabilidad > 50%) | Bajo circunstancias normales | El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad esfácilmente explotable | **Código malicioso** |
| **Medio (2)** | La ocurrencia es probable (probabilidad =50%) | Por errores descuidos | El atacante se beneficia dealguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable | **Falla de hardware** |
| **Bajo (1)** | La ocurrencia es menos probable (probabilidad >0 y <50%) | En rara ocasión | El atacante no se beneficia del ataque | **Desastres naturales** |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

### 2.7.2. Criterios de probabilidad de ocurrencia de vulnerabilidades

**Tabla 12-5:** Criterios de probabilidad de ocurrencia de vulnerabilidades

| NIVEL DE VULNERABILIDAD | CRITERIO | EJEMPLO |
|---|---|---|
| **Alto (3)** | No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza | No se utilizan contraseñas para que los usuarios ingresen a los sistemas |
| **Medio (2)** | Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza aun nivel aceptable | Existen normas para la utilización de contraseñas, pero no se implementa |
| **Bajo (1)** | La medida de seguridad es adecuada | Existen normas para la utilización de contraseñas y es aplicada |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

### 2.7.3. Criterio de la Evaluación de Riesgos

Se impone aplicar el siguiente criterio:

El producto de la probabilidad de ocurrencia de una amenaza, la probabilidad de ocurrencia de vulnerabilidades y el valor del impacto del activo de la información (CID), tenemos como resultado el nivel de riesgo de cada activo.

$$\boldsymbol{Nivel\ de\ riesgo} = \mathbf{VA(CID)} * \mathbf{Nivel\ de\ amenaza} * \mathbf{Nivel\ de\ vulnerabilidad}$$

**Tabla 13-5:** Nivel de riesgo

| Nivel de Riesgo | |
|---|---|
| **1 - 3** | **El riesgo es BAJO** |
| **4 - 8** | **El riesgo es MEDIO** |
| **9 - 27** | **El riesgo es ALTO** |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Tabla 14-5:** Ejemplo de cálculo de evaluación de riesgo

| | | | | Evaluación de Riesgos | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Impacto | Probabilidad | | Controles implementados existentes | Cálculo de Evaluación Riesgo | Nivel de Riesgo |
| Nro. Activo | Nombre Activo | Amenaza | Vulnerabilidad | CID | Nivel de amenaza | Nivel de vulnerabilidad | | | |
| A1 | Servidores físicos (hipervisor) | Pérdida de suministro de energía | Susceptibilidad a variaciones de voltaje | 3 | 1 | 1 | Baterías y generadores | 3 | BAJO |
| A2 | Servicio de correo institucional | Abuso de derechos | Utilización de medios de almacenamiento de borrado adecuado | 2 | 2 | 2 | Políticas sobre el uso de correo electrónico | 8,00 | MEDIO |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

## 3. TRATAMIENTO DEL RIESGO DE LA SEGURIDAD DE LAINFORMACIÓN

Ha de tenerse presente que el tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la institución. Para este efecto se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo de manera adecuada.

Se recomienda la aplicación de una de las cuatro opciones existentes disponibles para el tratamiento del riesgo:

- Reducción del riesgo
- Aceptación del riesgo
- Evitación del riesgo
- Transferencia del riesgo

A continuación, se ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información:

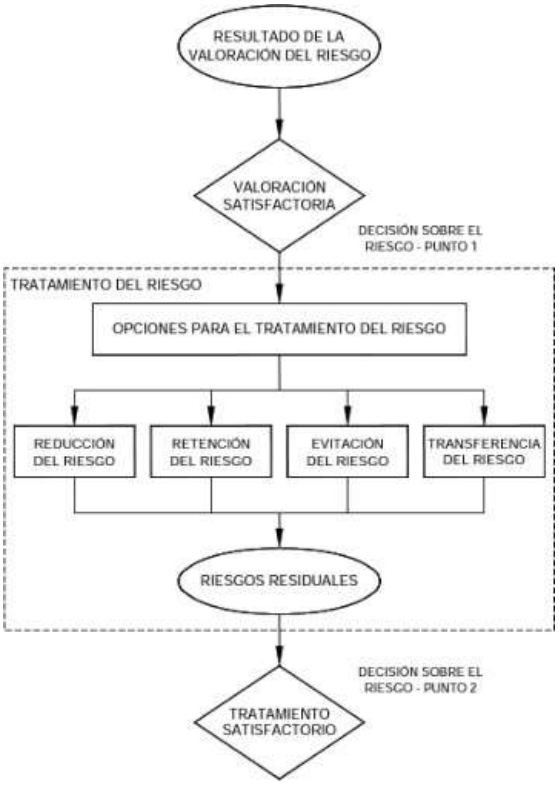



**Figura 2-5:** Actividades para el tratamiento de los riesgos

**Fuente:** ISO27005

Las expectativas para el tratamiento del riesgo deberán seleccionarse con base al resultado de la valoración del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Recomendándose que cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, deben implementar esas opciones. Las adicionales para implementar las mejoras pueden no ser siempre económicas por lo que hay que estudiarlas para determinar si se justifica o no tal inversión.

Las consecuencias adversas de los riesgos, en general, deberían ser tan bajas como sea razonablemente viable e independientemente de cualquier criterio absoluto a considerar. Por lo que habrá de ser necesario implementar controles que no son justificables en términos estrictamente económicos como, por ejemplo, los controles para la continuidad del negocio considerados para cumplir riesgos altos específicos no contemplados en esta guía.

### 3.1. Reducción del riesgo

El tratamiento del riesgo de la seguridad de información tiene por objetivo reducir el nivel del riesgo para a su vez reducir el impacto y la probabilidad de ocurrencia de daños sobre los activos de información del usuario o de la organización.

Se deberían tener en cuenta para esta selección los criterios de aceptación del riesgo, así como requisitos legales, reglamentarios y contractuales aceptados por el usuario o la institución propietaria de los activos de información. Considerar los costos y el tiempo para la implementación de los controles y los aspectos técnicos, ambientales y culturales. Es posible, frecuentemente, disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados y que se ajusten al presupuesto correspondiente.

### 3.2. Evitación del riesgo

Es aconsejable evitar la actividad o la acción que da origen al riesgo particular en vista de que cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, debe tomarse una decisión para evitar por completo el riesgo, a través del retiro de una actividad o un conjunto de actividades planificadas o existentes.

Así, al tratarse de riesgos causados por la naturaleza, puede ser unaalternativa más eficaz en términos de costo, trasladar físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control cualquier fenómeno natural.

### 3.3. Transferencia del riesgo

Dependiendo de la evaluación del riesgo, éste se debe transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular y tener un adecuado tratamiento del riesgo de la seguridad de la información dependiendo de los criterios mutuos que se viertan al respecto.

### 3.4. Retención/aceptación del riesgo

La evaluación del riesgo determinará la decisión sobre la retención del riesgo sin acción posterior.

Es recomendable aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios del usuario o de la institución para la aceptación de los riesgos.

Ejemplo del tratamiento de los riesgos:

**Tabla 15-5**: ejemplo del tratamiento de los riesgos

| Evaluación de Riesgos | | | | | | Tratamiento de Riesgos | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Impacto** | **Probabilidad** | | **Controles implementados existentes** | **Cálculo de Evaluación Riesgo** | **Nivel de Riesgo** | **Método o tratamiento del riesgo** | **Tipo de control** | **Control a implementar** | **Nivel de amenaza** | **Nivel de vulnerabilidad** | **Cálculo de evaluación de riesgo con el control implementado** | **Nivel de riesgo con el control implementado** | **Riesgo residual** |
| **CID** | **Nivel de amenaza** | **Nivel de vulnerabilidad** | | | | | | | | | | | |
| **3** | 1 | 1 | Baterías y generadores | 3 | **BAJO** | Aceptar | Preventivo | Levantar generador | 1 | 1 | 1 | **BAJO** | **ACEPTABLE** |
| **2** | 2 | 2 | Políticas sobre el uso de correo electrónico | 8,00 | **MEDIO** | Mitigar/evitar/transferir | Correctivo | Herramienta que permita el registro y monitoreo del acceso de los usuarios | 1 | 1 | 1 | BAJO | **ACEPTABLE** |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

## 4. ACEPTACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

De forma bilateral se deber tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, registrándola de manera formal.

Para lo cual esta opción se toma cuando los costos de implementación de un control de seguridad sobrepasan el valor del activo de información que se desea proteger o cuando el nivel del riesgo es muy bajo, en ambos casos la organización asume los daños provocados por la materialización del riesgo.

La organización encargada del tratamiento del riesgo de la seguridad de la información deberá definir sus propias escalas para los niveles de aceptación del riesgo por parte del usuario o de la institución.

Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgosi existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

## 5. COMUNICACIÓN DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información acerca de los riesgos. La información incluye, pero no se limita a la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

Entre las partes involucradas es importante la comunicación eficaz, dado que puede tener un impacto significativo en las decisiones que se deben tomar entre las partes, la comunicación es bidireccional, necesariamente.

La comunicación del riesgo se debería realizar con el fin de lograr objetivos como los siguientes:

- Proporcionar seguridad del resultado de la gestión del riesgo de la institución.
- Recolectar información del riesgo.
- Compartir los resultados de la valoración del riesgo y presentar el plan para el tratamiento del riesgo.

- Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas de seguridad de la información debido a la falta de entendimiento entre quienes toman las decisiones y las partes involucradas.
- Brindar soporte para la toma de decisiones.
- Obtener conocimientos nuevos sobre la seguridad de la información.
- Coordinar con otras partes y planificar las respuestas para reducirlas consecuencias de cualquier incidente.
- Dar a quienes toman las decisiones y a las partes involucradas unsentido de responsabilidad acerca de los riesgos.
- Mejorar la toma de conciencia.

## 6. MONITOREO Y REVISIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

### Monitoreo y revisión de los factores de riesgo

En conocimiento que los riesgos no son estáticos por lo que las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación, es imprescindible el monitoreo constante para detectar estos cambios; la misma que puede estar soportada por servicios externos que brinden información con respecto a nuevas amenazas o vulnerabilidades de manera oportuna.

## 5.1. CASO DE ESTUDIO: IMPLEMENTACIÓN DE LA GUÍA GMGSI-FJ

Uno de los objetivos de esta investigación es aplicar la Guía Metodológica de Gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados (GMGSI-FJ) ya diseñada en un caso de estudio.

El caso de estudio es dentro de servidores virtualizados de una infraestructura de un proveedor de servicios de internet local (ISP-FIBRATELECOM)

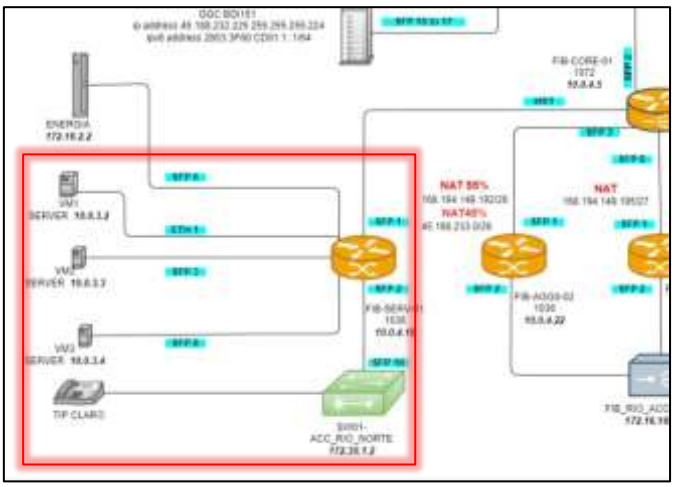


**Figura 3-5:** Infraestructura de red virtual
**Fuente:** ISP-FIBRATELECOM, 2021

El servidor físico que se utiliza es un Dell Server modelo Power Edge R710 potente para la aceleración de cargas de trabajo dentro del centro de datos (data center).

**Figura 4-5:** Servidor físico Dell Server modelo Power Edge R710 que contiene máquinas virtuales
**Fuente:** Dell.com, 2021

Para la operatividad de la empresa el servidor físico contiene varios servidores virtuales como los siguientes:

- PBX o central telefónica para comunicarse de manera interna entre los operadores de cada departamento y a su vez como call center para el soporte del requerimiento de los clientes del ISP-FIBRATELECOM.

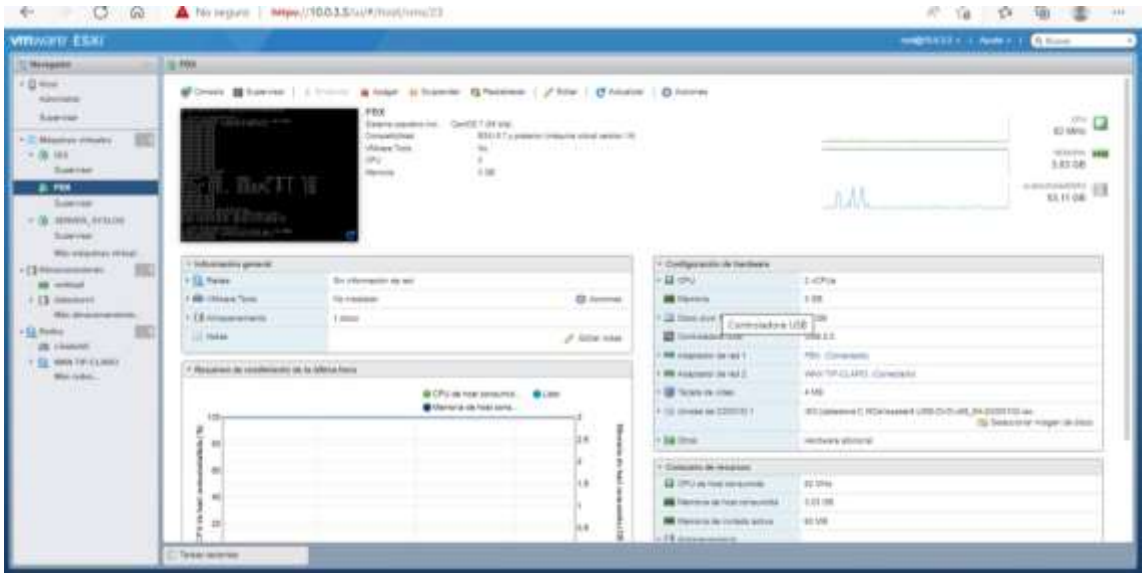


**Figura 5-5:** Servidor virtual PBX
**Fuente:** ISP-FIBRATELECOM, 2021

- GIS, es un sistema de información geográfica que utiliza visualizaciones en mapas, brindando información sobre la red y cobertura desplegada.

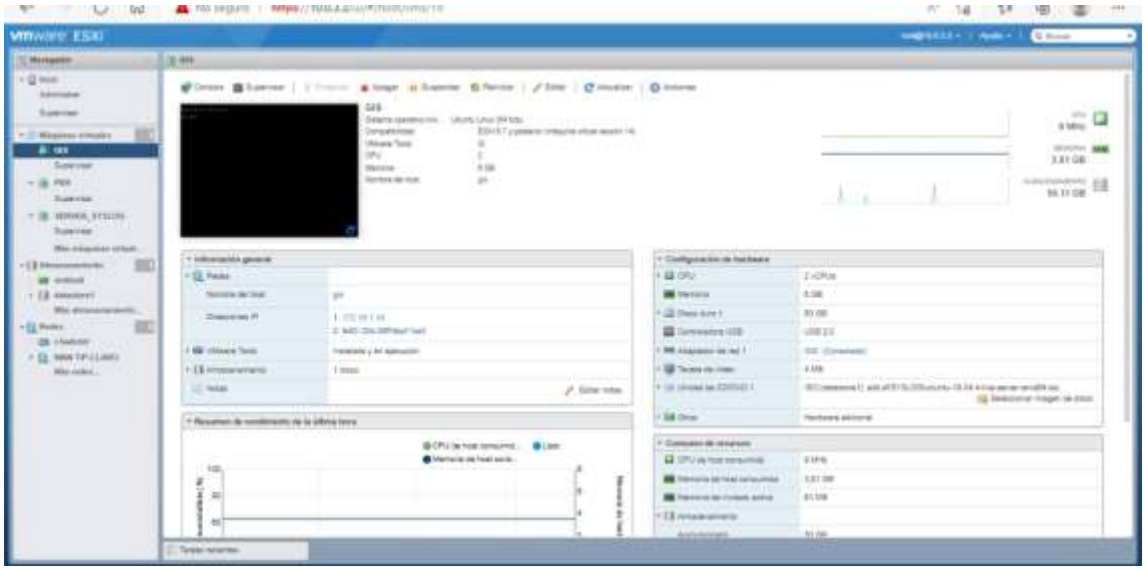


**Figura 6-5:** Servidor virtual GIS
**Fuente:** ISP-FIBRATELECOM, 2021


**Figura 7-5:** Cobertura del servidor virtual GIS
**Fuente:** ISP-FIBRATELECOM, 2021

- Servidor virtual de correo institucional, es uno de los métodos de comunicación más usados entre los usuarios de la empresa para la funcionalidad de los procesos.

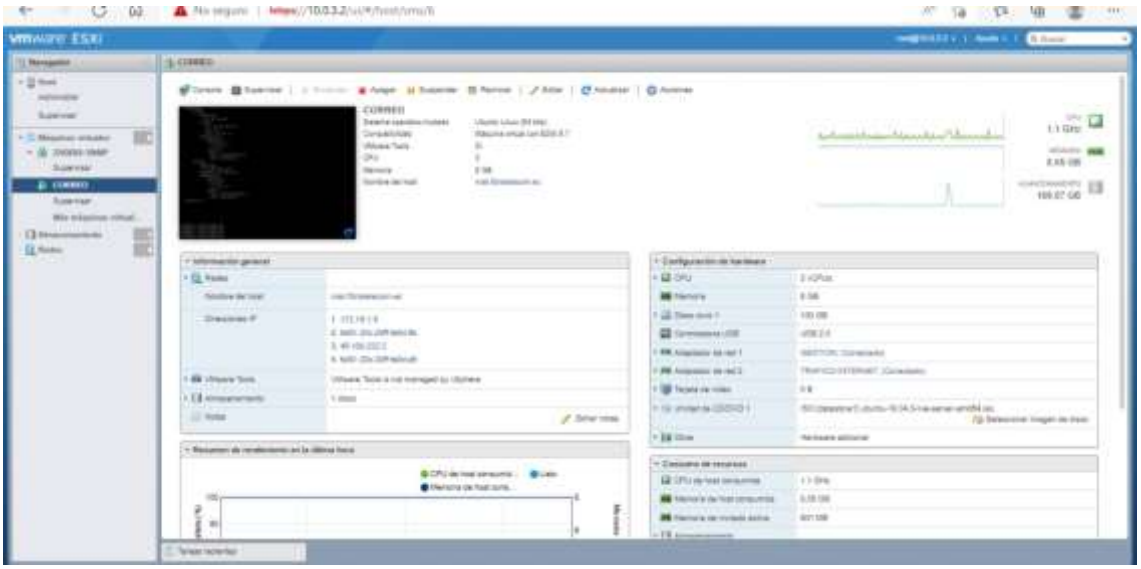


**Figura 8-5:** Servidor virtual correo institucional
**Fuente:** ISP-FIBRATELECOM, 2021

- Servidor Syslog, es un protocolo de registro de sistema (system logging protocol), en donde se puede configurar él envió de mensajes de ciertos dispositivos de la red para su análisis y monitoreo.

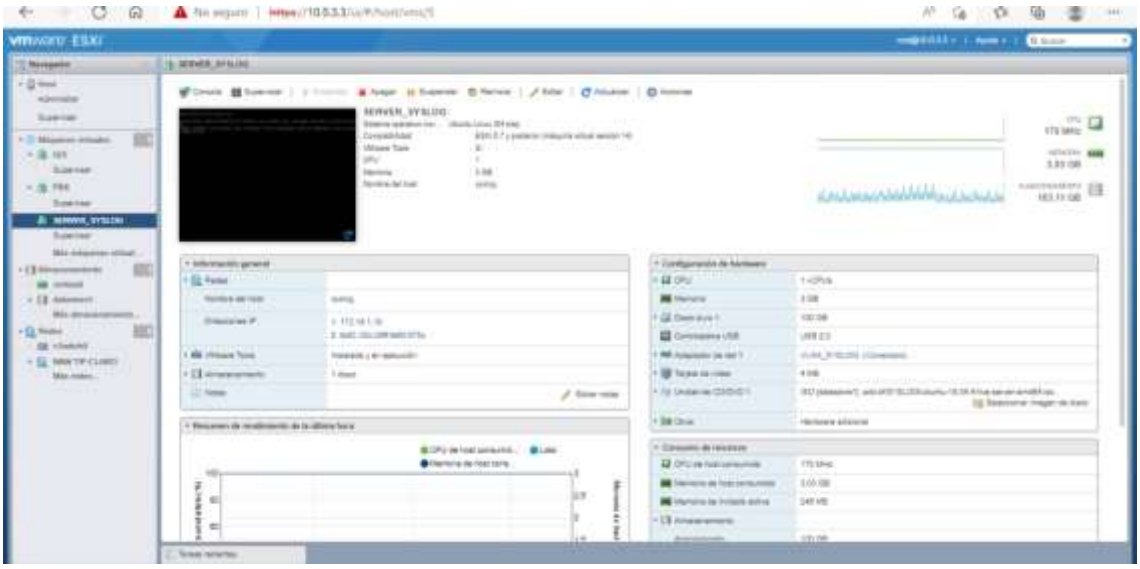


**Figura 9-5:** Servidor virtual syslog
**Fuente:** ISP-FIBRATELECOM, 2021

- Grafana, es una herramienta de interfaz de usuario que permite la visualización de cuadros y gráficos a partir de múltiples fuentes.

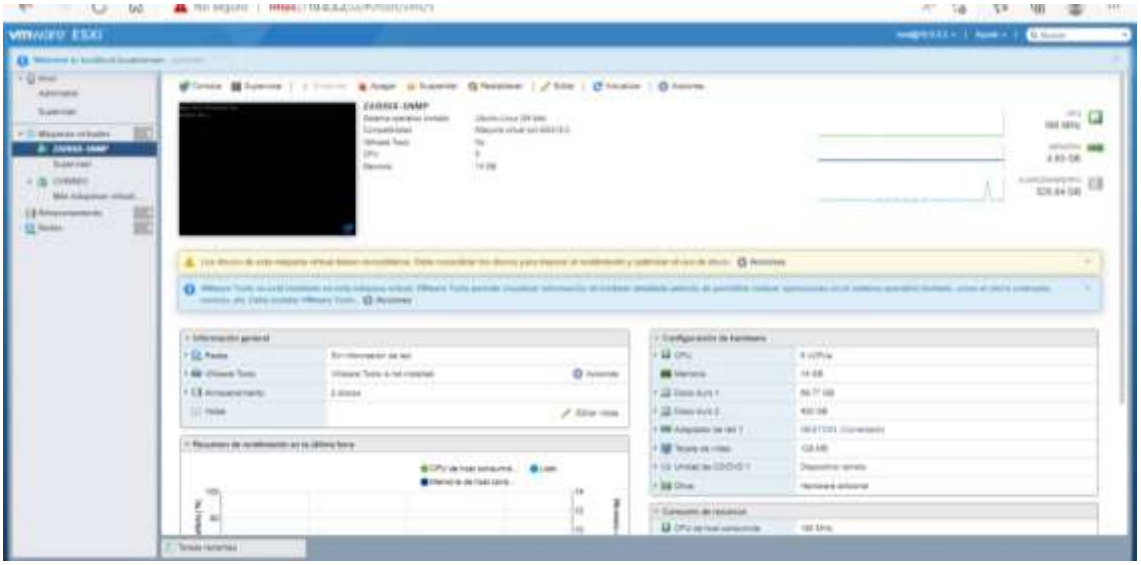


**Figura 10-5:** Servidor virtual grafana
**Fuente:** ISP-FIBRATELECOM, 2021

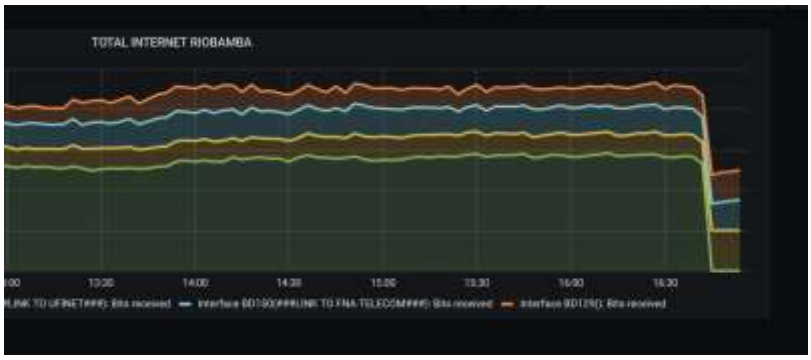


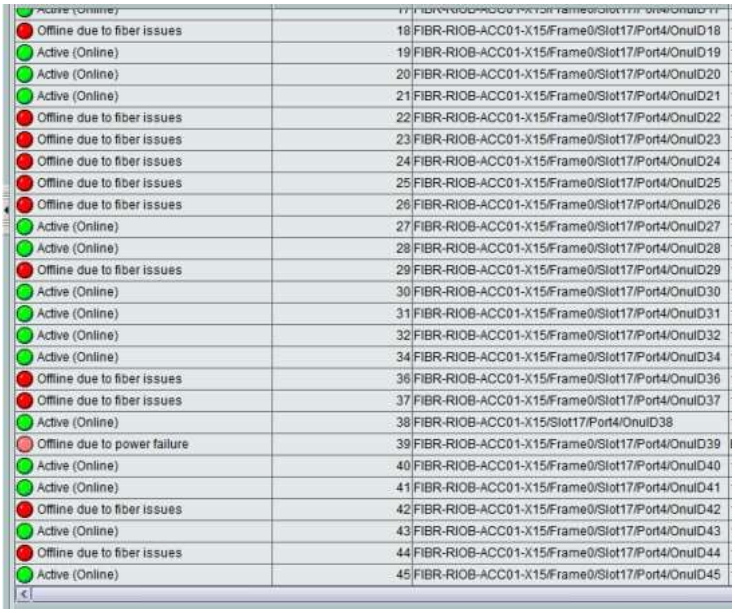

**Figura 11-5:** Tráfico de red en servidor virtual grafana
**Fuente:** ISP-FIBRATELECOM, 2021

- Speedtest, se utiliza para alojar el servidor de prueba de velocidad en tu propio sitio.


**Figura 12-5:** Test de velocidad servidor virtual speedtest
**Fuente:** ISP-FIBRATELECOM, 2021

- OLT IManager u2000 que permite centralizar y administrar mediante una interfaz graficas las líneas terminales ópticas de la red GPON.


**Figura 13-5:** Interfaz gráfica servidor virtual OLT IManager u2000
**Fuente:** ISP-FIBRATELECOM, 2021



| | | |
|---|---|---|
| Offline due to fiber issues | 18 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID18 |
| Active (Online) | 19 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID19 |
| Active (Online) | 20 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID20 |
| Active (Online) | 21 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID21 |
| Offline due to fiber issues | 22 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID22 |
| Offline due to fiber issues | 23 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID23 |
| Offline due to fiber issues | 24 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID24 |
| Offline due to fiber issues | 25 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID25 |
| Offline due to fiber issues | 26 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID26 |
| Active (Online) | 27 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID27 |
| Active (Online) | 28 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID28 |
| Offline due to fiber issues | 29 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID29 |
| Active (Online) | 30 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID30 |
| Active (Online) | 31 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID31 |
| Active (Online) | 32 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID32 |
| Active (Online) | 34 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID34 |
| Offline due to fiber issues | 36 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID36 |
| Offline due to fiber issues | 37 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID37 |
| Active (Online) | 38 | FIBR-RIOB-ACC01-X15/Slot17/Port4/OnuID38 |
| Offline due to power failure | 39 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID39 |
| Active (Online) | 40 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID40 |
| Active (Online) | 41 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID41 |
| Offline due to fiber issues | 42 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID42 |
| Active (Online) | 43 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID43 |
| Offline due to fiber issues | 44 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID44 |
| Active (Online) | 45 | FIBR-RIOB-ACC01-X15/Frame0/Slot17/Port4/OnuID45 |

**Figura 14-5:** Interfaz gráfica servidor virtual OLT IManager u2000
**Fuente:** ISP-FIBRATELECOM, 2021

Para la creación de estos servidores virtualizados se usó el hipervisor VMware ESXi que permite acceder directamente a los recursos subyacentes y controlarlos, puede realizar particiones de hardware con eficacia para consolidar las aplicaciones y reducir los costos. por su eficiente arquitectura, fiabilidad, rendimiento y soporte.


**Figura 15-5:** Interfaz gráfica hipervisor VMware
**Fuente:** ISP-FIBRATELECOM, 2021


**Figura 16-5:** Arquitectura servidor virtual VMware
**Fuente:** VMware.com, 2021

Teniendo en cuenta que se puede vulnerar uno o varios de los pilares de la seguridad de la información, que son la disponibilidad, confidencialidad e integralidad para la empresa es muy importante documentar cada una de las etapas.

Anteriormente se mencionó que algunas de las ventajas de la virtualización son: la facilidad y velocidad de implementación de servidores virtuales, la encapsulación de las máquinas virtuales y actualizaciones de parches de seguridad, lo que también supone una preocupación ya que, si no existen políticas de acceso no autorizados o hay ausencia de procedimientos formales, se convierte en un riesgo.

Posterior a haber levantado toda la información de la arquitectura de la entidad del caso de estudio, se hizo un proceso de gestión de riesgo de seguridad de la información a los servidores virtuales implementados para recomendar buenas prácticas de planificación e implementación de controles.

Con base en la guía ya elaborada los pasos a seguir en el caso de estudio se detallan de la siguiente forma:

## 1. Identificación y valoración de activos

**Tabla 16-5:** Identificación de los activos, caso de estudio

| IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nro. Activo** | | **Proceso Macro** | **Subproceso** | **Tipo de Activo** | **Nombre de Activo** | **Descripción del activo** | **Ubicación** |
| **A1** | TICS | Aplicaciones informáticas | | Software | Servidor virtual GIS (cobertura) | Información geográfica que utiliza visualizaciones en mapas, brindando | Data Center |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | información sobre la red y cobertura desplegada | |
| **A2** | TICS | Aplicaciones informáticas | Software | Servidor virtual Syslog | Información que contiene el registro de errores del sistema de los dispositivos principales de la red. | Data Center |
| **A3** | TICS | Aplicaciones informáticas | Software | Servidor virtual OLT Imanager 2000 | Información del estado (active/off line) de las terminales ópticas. | Data Center |
| **A4** | TICS | Aplicaciones informáticas | Redes y comunicación | Servidor virtual PBX | Call center, soporte y operadores de cada departamento. | Data Center |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Tabla 17-5:** Valoración de los activos, caso de estudio

**VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

| **Nro. Activo** | **Nombre de Activo** | **Ubicación** | **Valoración de Impacto (pérdida)**<br>**C: Confidencialidad**<br>**I: Integridad**<br>**D: Disponibilidad** | | | |
|---|---|---|---|---|---|---|
| | | | **C** | **I** | **D** | **VA** |
| **A1** | Servidor virtual GIS (cobertura) | Data Center | 3 | 3 | 3 | 3 |
| **A2** | Servidor virtual Syslog | Data Center | 1 | 1 | 3 | 1,66 |
| **A3** | Servidor virtual OLT Imanager 2000 | Data Center | 3 | 3 | 3 | 3 |
| **A4** | Servidor virtual PBX | Data Center | 2 | 2 | 3 | 2,33 |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

Basándose en la fórmula $\boldsymbol{VA}=(\boldsymbol{C}+\mathbf{I}+\mathbf{D})/\boldsymbol{3}$ para calcular la valoración del impacto de un activo se obtiene como resultado 3.

## 2. Identificación de amenazas y vulnerabilidades

**Tabla 18-5:** Identificación de amenazas, caso de estudio

| **TIPO** | **AMENAZA** |
|---|---|
| **Acciones no autorizadas** | Copia fraudulenta<br>Uso no autorizado del equipo<br>Abuso de derechos |
| **Pérdidas de servicios esenciales** | Pérdida de suministros de energía<br>Falla en el equipo de telecomunicaciones<br>Falla en el sistema acondicionado |
| **Fallas técnicas** | Fallas de equipo<br>Hurto de equipos |

| | | |
|---|---|---|
| | Divulgación | |
| | Manipulación con software | |
| **Compromiso de funciones** | Incumplimiento en el mantenimiento del sistema | |
| | Falsificación de derechos | |
| | Incumplimiento en la disponibilidad del personal | |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Tabla 19-5:** Amenazas, caso de estudio

| FUENTE DE AMENAZA | MOTIVACIÓN | ACCIONES AMENAZANTES |
|---|---|---|
| **Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos** | Curiosidad | Chantaje |
| | Ganancia monetaria | Robo a un empleado |
| | Venganza | Observar información reservada |
| | | Fraude |
| | | Venta de información |
| **Terrorismo** | Destrucción | Ataque contra el sistema |
| | Venganza | DDoS |
| **Espionaje de empresas** | Ventaja competitiva | Hurto de información |
| | Espionaje | Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos |
| **Empleados con entrenamiento deficiente y negligentes** | Inteligencia | Uso inadecuado |
| | Errores | Código malicioso |
| | Omisiones no intensionales | Observar información reservada |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

**Tabla 20-5:** Identificación de amenazas y vulnerabilidades, caso de estudio

| TIPO DE ACTIVO | VULNERABILIDADES | AMENAZAS |
|---|---|---|
| **Software** | Ausencia de mecanismos de identificación y autenticación | Copia fraudulenta |
| | Disposición de utilización de medios de almacenamiento | Uso no autorizado del equipo |
| | Gestión deficiente de contraseñas | Abuso de derechos |
| | | Hurto |
| **Software** | Ubicación susceptible | Destrucción |
| | Ausencia de protección física | Pérdida de suministros de energía |
| | Susceptibilidad a variaciones de voltaje | Incumplimiento de mantenimiento del sistema |
| **Software** | Ausencia de procedimientos de identificación y valoración de riesgos | Hurto |
| | Ausencia de revisiones regulares | Destrucción |
| **Redes y comunicación** | Ausencia de identificación y autentificación | Abuso de derechos |

| | | |
|---|---|---|
| | Entrenamiento insuficiente de seguridad | Error en el uso |
| | Ausencia de personal | Incumplimiento en la disponibilidad del personal |
| | Trabajo no supervisado | Escucha encubierta |
| | Ausencia de auditorias | |
| | Ausencia de procedimiento formal para el registro y retiro de usuarios | |
| | Ausencia de políticas para el uso correcto de medios de telecomunicaciones | |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

### 3. Identificación de los controles existentes

En este caso de estudio se verificará los controles existentes que la entidad tiene implementado, ya que, al realizar la valoración del impacto, esta guía metodológica de gestión de riesgos ayudará a recomendar buenas prácticas de planificación e implementación de nuevos controles preventivos o correctivos.

### 4. Análisis de riesgo

| ANÁLISIS DE RIESGOS | | | | | EVALUACIÓN DE RIESGOS | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Impacto | Probabilidad | | Controles implementadosexistentes | Cálculo de Evaluación Riesgo |
| **Subprocesos** | **Nro. Activo** | **Nombre Activo** | **Amenaza** | **Vulnerabilidad** | **CID** | **Nivel de amenaza** | **Nivel de vulnerabilidad** | | |
| **Software** | A1 | Servidor virtual GIS (cobertura) | Copia fraudulenta | Ausencia de mecanismos de identificación y autenticación | 3 | 3 | 3 | No existen | **27** |
| | | | Abuso de derechos | Disposición de utilización de medios de almacenamiento | 3 | 2 | 2 | No existen | **12** |
| | | | Uso no autorizado del equipo | Gestión deficiente de contraseñas | 3 | 1 | 1 | Contraseñas robustas | **3** |
| **Software** | A2 | Servidor virtual Syslog | Destrucción | Ubicación susceptible | 1,66 | 1 | 1 | Ubicación segura | **1,66** |
| | | | Pérdida de suministros de energía | Susceptibilidad a variaciones de voltaje | 1,66 | 3 | 1 | Baterías y generador | **4,98** |
| | | | Incumplimiento de mantenimiento del sistema | Ausencia de protección física | 1,66 | 1 | 1 | Mantenimiento | **1,66** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Software** | A3 | Servidor virtual OLT IManager 2000 | Hurto | Ausencia de procedimientos de identificación y valoración de riesgos | 3 | 2 | 2 | No existen | **12** |
| | | | | Ausencia de revisiones regulares | 3 | 1 | 1 | Revisión regular por parte de gerencia | **3** |
| **Redes y comunicación** | A4 | Servidor virtual PBX | Abuso de derechos | Ausencia de políticas para el uso correcto de medios de telecomunicaciones | 2,33 | 2 | 1 | Auditorías | **9,32** |
| | | | Error en el uso | Trabajo no supervisado | 2,33 | 1 | 1 | Revisión regular por parte de gerencia | **2,33** |
| | | | Incumplimiento en la disponibilidad del personal | Ausencia de personal | 2,33 | 3 | 1 | Control de cambio | **6,99** |
| | | | Escucha encubierta | Ausencia de procedimiento formal para el registro y retiro de usuarios | 2,33 | 1 | 1 | Autentificación | **2,33** |

**Tabla 21-5:** Análisis de riesgos, caso de estudio
**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

En el caso del servidor virtual GIS, se suscitó un problema, ya que, cualquier persona sea interna o ajena a la empresa que tenga el link o conocimiento de esta vulnerabilidad, podía acceder a información confidencial, siendo una brecha de inseguridad de la empresa. Por el momento se recomendó a la empresa deshabilitar el acceso al link público de todos los usuarios.

### 5. Identificación de las consecuencias

Dentro de las consecuencias que se puede identificar en este escenario tenemos:

- Divulgación de información sensible de la empresa a la competencia.
- Soporte ineficiente hacia los usuarios afectados.
- Robo de cajas dentro de la cobertura divulgada.
- Pérdida de tiempo operacional del personal de ventas al momento de confirmar la cobertura de un cliente nuevo interesado.
- Pérdida de tiempo operacional de las cuadrillas de instaladores para las instalaciones planificadas, ya que no tienen acceso a información de la ubicación de las cajas más cercanas de los nuevos clientes.
- Pérdida de tiempo en identificación de cajas alarmadas.
- Call center saturado.
- Costo financiero hacia la empresa por el material y el tiempo de ausencia de servicio.
- El tiempo de reparación al sufrir un robo de cajas en dependencia de los hilos de fibra a fusionar aproximadamente es de 3 a 6 horas.
- Clientes molestos, lo que afecta a la imagen o reputación de la empresa.

## 6. Cálculo de la evaluación del riesgo

**Tabla 22-5:** Cálculo de la evaluación del riesgo, caso de estudio

| ANÁLISIS DE RIESGOS | | | | EVALUACIÓN DE RIESGOS | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | **Impacto** | **Probabilidad** | | **Controles implementados existentes** | **Cálculo de Evaluación Riesgo** | **Nivel de riesgo** |
| **Nro. Activo** | **Nombre Activo** | **Amenaza** | **Vulnerabilidad** | **CID** | **Nivel de amenaza** | **Nivel de vulnerabilidad** | | | |
| **A1** | Servidor virtual GIS (cobertura) | Copia fraudulenta | Ausencia de mecanismos de identificación y autenticación | 3 | 3 | 3 | No existen | 27 | **ALTO** |
| | | Abuso de derechos | Disposición de utilización de medios de almacenamiento | 3 | 2 | 2 | No existen | 12 | **ALTO** |
| | | Uso no autorizado del equipo | Gestión deficiente de contraseñas | 3 | 1 | 1 | Contraseñas robustas | 3 | **BAJO** |
| **A2** | Servidor virtual Syslog | Destrucción | Ubicación susceptible | 1,66 | 1 | 1 | Ubicación segura | 1,66 | **BAJO** |
| | | Pérdida de suministros de energía | Susceptibilidad a variaciones de voltaje | 1,66 | 3 | 1 | Baterías y generador | 4,98 | **MEDIO** |
| | | Incumplimiento de mantenimiento del sistema | Ausencia de protección física | 1,66 | 1 | 1 | Mantenimiento | 1,66 | **BAJO** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **A3** | Servidor virtual OLT IManage r 2000 | Hurto | Ausencia de procedimientos de identificación y valoración de riesgos | 3 | 2 | 2 | No existen | 12 | **ALTO** |
| | | | Ausencia de revisiones regulares | 3 | 1 | 1 | Revisión regular por parte de gerencia | 3 | **BAJO** |
| **A4** | Servidor virtual PBX | Abuso de derechos | Ausencia de políticas para el uso correcto de medios de telecomunicaciones | 2,33 | 2 | 1 | Auditorías | 4,66 | **MEDIO** |
| | | Error en el uso | Trabajo no supervisado | 2,33 | 1 | 1 | Revisión regular por parte de gerencia | 2,33 | **BAJO** |
| | | Incumplimiento en la disponibilidad del personal | Ausencia de personal | 2,33 | 3 | 1 | Control de cambio | 6,99 | **MEDIO** |
| | | Escucha encubierta | Ausencia de procedimiento formal para el registro y retiro de usuarios | 2,33 | 1 | 1 | Autentificación | 2,33 | **BAJO** |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

El cálculo del nivel de riesgo se realiza con base en la siguiente formula: $\boldsymbol{Nivel\ de\ riesgo} = (\mathbf{CID}) * \mathbf{Nivel\ de\ amenaza} * \mathbf{Nivel\ de\ vulnerabilidad}$, obteniendo como resultado el nivel de riesgo.

Al momento de tener como resultado un nivel de riesgo alto, hay que priorizar en comparación a los riesgos medios y bajos para su respectivo tratamiento.

## 7. Tratamiento del riesgo


**Figura 17-5:** Control de autenticación servidor virtual GIS
**Fuente:** ISP-FIBRATELECOM, 2021

En el caso del servidor virtual GIS se identifican dos riesgos con ponderación ALTO, para el control correctivo el tratamiento del riesgo fue la reducción del mismo, implementando mecanismos de identificación y autenticación de los usuarios autorizados mediante credenciales para poder acceder a la información contenida en el servidor.

**Tabla 23-5:** Tratamiento del riesgo, caso de estudio

| Evaluación de Riesgos | | | | | | Tratamiento de Riesgos | | | | | | | Riesgo residual |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Impacto | Probabilidad | | Controles implementados existentes | Cálculo de Evaluación Riesgo | Nivel de Riesgo | Método o tratamiento del riesgo | Tipo de control | Control a implementar | Nivel de amenaza | Nivel de vulnerabilidad | Cálculo de evaluación de riesgo con el control implementado | Nivel de riesgo con el control implementado | |
| CID | Nivel de amenaza | Nivel de vulnerabilidad | | | | | | | | | | | |
| 3 | 3 | 3 | No existen | 27 | **ALTO** | Aceptar | Correctivo | Implementación de mecanismos de identificación y autenticación | 1 | 1 | 1 | **BAJO** | **ACEPTABLE** |

**Fuente:** Guía metodológica de gestión de riesgos de seguridad de la información en la administración de servidores virtualizados
**Realizado por:** Jiménez Fabricio, 2022

## 8. Monitoreo y revisión del riesgo

Hacer un seguimiento constante del riesgo y analizar consecuencias o posibles brechas de seguridad de la información que se puedan presentar en los servidores virtualizados.

## CONCLUSIONES

Se han estudiado los fundamentos metodológicos teóricos del campo de la gestión de riesgos de seguridad fundamentados en la información existente para adaptarlos a la administración de servidores virtualizados tomando como referencia en base a la consulta de importantes autores expertos en el área estudiada, constituyendo el fundamento teórico trascendente de esta investigación como elementos específicos para la concreción de los objetivos planteados y a efecto de contextualizar lo teórico con la realidad de la tesis se realizó la investigación de campo aplicando una encuesta a los administradores de servidores virtuales de instituciones y empresas privadas y públicas del entorno en un número de 45 administradores; cuyos aportes han sido valiosos para la ratificación de lo propuesto y el cumplimiento de los objetivos respectivos, quienes a cada una de las preguntas han respondido con criterios personales valiosos y que se detallan en la parte respetiva de este trabajo investigativo.

Se ha diseñado la guía metodología de gestión de riesgos de seguridad de la información para la administración de servidores virtualizados tomando como referencia en modelos técnicos confiables y actualizados que se basan en el modelo ISO 27005 que se estimó era el apropiado para cumplir con el objetivo de esta tesis de maestría.

La Guía Metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados producto de esta tesis ha sido aplicada en un caso de estudio que consta en esta tesis y que ha permitido ratificar los objetivos propuestos en cuanto a la utilidad que tiene una guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados para solventar los problemas de seguridad que pueden presentarse en dichos servidores.

**RECOMENDACIONES**

Se hace indispensable el estudio de los fundamentos teóricos del campo de la metodología de gestión de riesgos de seguridad de la información existente para los administradores de servidores virtualizados tomando a fin de que puedan tomar como referencia a la información de importantes autores expertos en esta área, y de allí con este fundamento teórico puedan aplicar estos elementos específicos para la remediación de los problemas que tengan que afrontar en su desempeño, ha sido de enorme utilidad a efecto de contextualizar lo teórico con la realidad de este trabajo la investigación de campo aplicando una encuesta a los administradores de servidores virtuales de instituciones y empresas privadas y públicas del entorno en un número de 45 administradores, con resultados valiosos para la ratificación de lo propuesto y el cumplimiento de los objetivos respectivos, quienes a cada una de las preguntas han respondido con criterios personales.

El diseño de la guía metodología de gestión de riesgos de seguridad de la información para la administración de servidores virtualizados tomando como referencia en modelos técnicos confiables y actualizados que se basa en el modelo ISO 27005 se recomienda como la más apropiada para lograr el aseguramiento de los datos de estos sistemas informáticos y se logrado cumplir con el objetivo de trabajo investigativo.

La aplicación de la guía metodología de gestión de riesgos de seguridad de la información para la administración de servidores virtualizados fundamentada en modelos técnicos y confiables tomando como referencia el modelo ISO 27005 dará la cobertura ante la proliferación de problemas con estos sistemas informáticos. Destacándose que al haber sido aplicada en un caso de estudio que consta en esta tesis permitió ratificar los objetivos propuestos en cuanto a la utilidad que tiene una guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados para solventar los problemas de seguridad que pueden presentarse en dichos servidores.

# GLOSARIO

**Acción correctiva**

Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

**Acción preventiva**

Medida de tipo pro activa orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001, 2005.

**Aceptación del riesgo**

Decisión informada de asumir un riesgo concreto, la aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo y revisión (Guía ISO 73, 2009).

**Activo**

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

**Alcance**

Ámbito de la organización que queda sometido al SGSI.

**Amenaza**

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

**Análisis de riesgos**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo, el análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos (Guía ISO 73, 2009)

**Análisis de riesgos cualitativo**

Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

**Análisis de riesgos cuantitativo**

Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

**Ataque**

Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

**Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

**Autenticación**

Provisión de una garantía de que una característica afirmada por una entidad es correcta.

**Autenticidad**

Propiedad de que una entidad es lo que afirma ser.

**Confidencialidad**

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Consecuencia**

Resultado de un evento que afecta los objetivos.
Un evento puede llevar a una serie de consecuencias. Una consecuencia puede ser segura o incierta y, en el contexto de la seguridad de la información, suele ser negativa. Las consecuencias pueden expresarse cualitativa o cuantitativamente. Las consecuencias iniciales pueden incrementarse a través de los efectos secundarios.

**Control**

Medida por la que se modifica el riesgo, los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto.

**Control correctivo**

Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

**Control detectivo**

Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

**Control de acceso**

Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

**Criterio del riesgo**

Términos de referencia contra los cuales se estima la importancia del riesgo (Guía ISO 73, 2009).

**Desastre**

Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

**Disponibilidad**

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

**Eficacia**

Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

**Estimación de riesgos**

Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. La estimación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.

**Evaluación de riesgos**

Proceso global de identificación, análisis y estimación de riesgos.

**Evento**

Ocurrencia o cambio de un conjunto particular de circunstancias.

Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente".

**Evento de seguridad de la información**

Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

**Fiabilidad**

Propiedad del comportamiento y de unos resultados consistentes previstos.

**Gestión de claves**

Controles referidos a la gestión de claves criptográficas.

**Gestión de incidentes de seguridad de la información**

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

**Gestión de riesgos**

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

**Identificación de riesgos**

Proceso de encontrar, reconocer y describir riesgos. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.

**Impacto**

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

**Inventario de activos**

Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

**ISO**

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

**ISO/IEC 27001**

Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

**Medida**

Variable a la que se asigna un valor como resultado de la medición.

**Necesidad de información**

Conocimiento requerido para gestionar objetivos, metas, riesgos y problemas.

**Nivel de riesgo**

Magnitud de un riesgo expresado en relación a la combinación de consecuencias y su probabilidad.

**Objetivo**

Un objetivo puede ser estratégico, táctico u operativo. Los objetivos pueden relacionarse con diferentes disciplinas (como las metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, proyecto, producto y proceso). Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, propósito, meta o hito).

**Objetivo de control**

Declaración que describe lo que se debe lograr como resultado de la implementación de los controles.

**Objetivo de la revisión**

Declaración que describe lo que se debe lograr como resultado de una revisión.

**Organización**

Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

El concepto de organización incluye, pero no se limita a un comerciante individual, compañía, corporación, agencia, empresa, autoridad, sociedad, organización benéfica o institución, o parte o combinación de las anteriores, ya sea sociedad anónima o no, pública o privada.

**Plan de tratamiento de riesgos**

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

**Proceso de gestión del riesgo**

Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consultoría, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos.

**Recursos de tratamiento de información**

Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

**Revisión**

Actividad realizada para determinar la idoneidad, adecuación y efectividad del objeto de estudio para lograr los objetivos establecidos.

**Riesgo**

El riesgo a menudo se caracteriza por la referencia a posibles eventos y o una combinación de estos. El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad asociada de ocurrencia.

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información.

El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización. (Guía ISO 73, 2009)

**Seguridad de la información**

Preservación de la confidencialidad, integridad y disponibilidad de la información.

**Sistema de Gestión**

Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos.

Un sistema de gestión puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.

**Sistema de Gestión de la Seguridad de la Información**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

**Vulnerabilidad**

Debilidad de un activo o control que puede ser explotada por una o más amenazas.

## BIBLIOGRAFÍA


AREITIO JAVIER (2008) *Seguridad de la Información, Redes, Informática y Sistemas de información* Madrid Impulso

BEZERRA, FLÁVIA ESTÉLIA SILVA COELHO LUIZ GERALDO SEGADAS DE ARAÚJO EDSON KOWASK (2016) versión adaptada al Ecuador a partir de la versión de esr renata – Colombia

CASCALZO FABIÁN, (2014) Riesgos actuales en entornos virtualizados http://www.cybsec.com

CAPACITY (2012) ¿Qué es la virtualización y cuáles son sus beneficios? Recuperado de https//blogcapacityacademy.com/2012-08-07.com/es-s/magazine/hh3954480.aspx

CIBERNÉTICA, INSTITUTO NACIONAL (2018) de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian https://www.incibe.es/protege-tu-empresa

CONSULTING, JMG VIRTUAL Los 5 mayores problemas de la virtualización de servidores 2015 https://www.jmgvirtualconsulting.com/servicios-virtuales

CONSUSLTING, VIRTUAL Ventajas y desventajas de la virtualización de servidores VMware 2017 https://www.jmgvirtualconsulting.com/vmware-vsphere/ventajas-desventajas-virtualizacion-servidores-vmware/

*Check Point.* Recuperado de: http://www.etek-reycom.com.ar/tecno/proveedor/check_point.htm

*Microsoft Virtualization.* Recuperado de: http://www.microsoft.com/spain/virtualizacion/solutions/technology/defau...

NETEC (2018). ¿Qué es virtualización? https://www.netec.com/que-es-virtualizacion

POLZE, A. AND TRÖGER, P. (2012), *Trends and challenges in operating systems—from parallel computing to cloud computing.* Concurrency Computat.:Pract. Exper., 24: 676–686. doi: 10.1002/cpe.1903

PLATZI (2017)¿Cómo aprovechar la nube? SaaS, PaaS y IaaS https://platzi.com/tutoriales/1183-bd/3076-como-aprovechar-la-nube-saas-paas-

REDHAT (2019) Qué es la gestión de riesgo https://www.redhat.com/es/topics/management/what-is-risk-management

SABNIS, S., VERBRUGGEN, M., Hickey, J. and McBride, A. J. (2012), *Intrinsically Secure Next-Generation Networks.* Bell Labs Tech. J., 17: 17–36. doi: 10.1002/bltj.21556

SÁNCHEZ G., ENRIQUE (2019) *Seguridad en los entornos virtuales* https://revista.seguridad.unam.mx/numero-20/seguridad-inform%C3%A1tica-en-entornos-virtuales

*Seguridad y cumplimiento normativo.* Recuperado de: http://www.vmware.com/latam/cloud-security-compliance/cloud-security#sth...

*SERVER virtualization security best practices.* Recuperado de: http://searchservervirtualization.techtarget.com/tutorial/Server-virtual...

*SYMANTEC BACKUP EXEC 12.5 for Windows Servers.* Recuperado de: http://ftpandina.atv.com.pe/ManualesIT/ManualLTo.pdf

*Shavlik Technologies.* Recuperado de: http://totemguard.com/soporte/files/Shavlik_NetChk_Configure.pdf

TECNO XXI (2016) Seguridad en entornos virtualeshttps://www.tecnoxxi.com/blog/negocios/seguridad-en-entornos-virtuales/

# ANEXOS

## ANEXO A. ENCUESTA APLICADA INICIAL

### ENCUESTA APLICADA AL PERSONAL ENCARGADO DE LA ADMINISTRACIÓN DE LOS SERVIDORES VIRTUALIZADOS SELECCIONADOS PARA ESTA INVESTIGACIÓN

**TEMA: Guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados.**

**Estimados administradores de servidores virtualizados:**

Mucho les agradezco se sirvan responder con un visto o una cruz en la opción que estimen conveniente en cada una de las preguntas de la presente encuesta que es con fines investigados de conclusión de maestría.

**Pregunta 1.** ¿Estima que es de importancia el conocimiento sobre gestión de riesgos de seguridad de la información en la administración de servidores virtualizados a su cargo?

SI ( ) NO ( )

**Pregunta 2.** De la gestión de riesgo aplicado en el sistema a su cargo cuál de estos factores considera de mayor trascendencia para lograr la seguridad de la información:

Tecnologías ( ) Procesos ( ) Talento humano ( )

**Pregunta 3.** ¿En la administración de los servidores virtualizados a su cargo considera necesario conocer los fundamentos metodológicos de gestión de riesgos de seguridad de la información existente?

SI ( ) NO ( )

**Pregunta 4.** Si la gestión de riesgos incluye todas las medidas adoptadas para controlar los riesgos de la información en su organización, como las que se enumeran, cuál o cuáles estiman se concretan en su trabajo

Análisis ( ) Evaluación ( ) El tratamiento ( )

La aceptación (  )  Comunicación (  )

**Pregunta 5.** La aplicación de los fundamentos metodológicos de gestión de riesgos de seguridad de la información permitirá mejorar el nivel de control de seguridad de los servidores virtualizados bajo su responsabilidad

SI  (  )  NO  (  )

**Pregunta 6.** ¿Actualmente tienen una guía metodología de gestión riesgos de seguridad de la información para la administración de servidores virtualizados a su cargo?

SI  (  )  NO  (  )

**Pregunta 7.** ¿De las actuales normas, estándares o modelos de control de gestión de riesgos de seguridad de la información bajo su control las aplica o no?

SI  (  )  NO  (  )  No responde (  )

**Pregunta 8.** ¿La aplicación de un modelo de gestión de riesgos de la seguridad de la información ayuda a mitigar los riesgos y evitar amenazas en servidores virtualizados?

Si (  )  No  (  )

**Pregunta 9**. ¿De la metodología de gestión riesgos de seguridad de la información conocida cuál cree usted es la más adecuada para poder controlar un problema de seguridad?

Cuantitativa (  )  Cualitativa  (  )  Mixta  (  )

**Pregunta 10.** ¿En el caso de poseer una guía metodológica de gestión de riesgos de seguridad de la información, al aplicarla han resuelto los problemas presentados en la administración de servidores virtualizados?

Siempre (  )  Rara vez  (  )  Nunca  (  ) No responde  (  )

**Pregunta 11.** ¿Cuáles de estas decisiones ha tomado para solucionar los problemas de riesgo de la Información para la administración de los servicios virtuales a su cargo

Reducir  (  )  Aceptar (  )  Evitar (  )  Transferir  (  )

**Pregunta 12.** ¿Consideran necesario mejorar el control de posibles eventos que afecten el nivel de seguridad de los servidores virtualizados a su cargo?

SI (  )  NO (  )

**Pregunta 13.** ¿Se hace necesario desarrollar una nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la Información (GRSI) en la administración de servidores virtualizados para mejorar el control de posibles eventos que afecten el nivel de seguridad?

SI (  )  NO (  )

**Pregunta 14.** ¿Estaría de acuerdo en que se implemente y ponga en práctica esta nueva Guía Metodológica de Gestión de Riesgos de Seguridad de la información en la administración de servidores virtualizados a su cargo?

SI (  )  NO (  )

**GRACIAS POR SU COLABORACIÓN**

## ANEXO B. ENCUESTA APLICADA POST IMPLEMENTACIÓN DE LA GUÍA

### ENCUESTA APLICADA AL PERSONAL ENCARGADO DE LA ADMINISTRACIÓN DE LOS SERVIDORES VIRTUALIZADOS SELECCIONADOS PARA ESTA INVESTIGACIÓN

**TEMA: Guía metodológica de gestión de riesgos de seguridad de la información para la administración de los servidores virtualizados.**

**Estimados administradores de servidores virtualizados:**

**Mucho les agradezco se sirvan responder con un visto o una cruz en la opción que estimen conveniente en cada una de las preguntas de la presente encuesta que es con fines investigados de conclusión de maestría.**

**Pregunta.** ¿La aplicación de la Guía Metodológica de Gestión de Riesgos de Seguridad de la Información en la administración de servidores virtualizados como modelo de gestión para mitigar los riesgos y evitar amenazas en servidores virtualizados se resolvieron los problemas presentados?

Si ( )  No ( )

**GRACIAS POR SU COLABORACIÓN**

espoch | Dirección de Bibliotecas y Recursos del Aprendizaje

**UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL**

**REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA**

**Fecha de entrega:** 18 / 11 / 2022

| **INFORMACIÓN DEL AUTOR/A (S)** |
|---|
| **Nombres – Apellidos*:*** *Fabricio Alfredo Jiménez Caicedo* |
| **INFORMACIÓN INSTITUCIONAL** |
| *Instituto de Posgrado y Educación Continua* |
| **Título a optar:** *Magíster en Seguridad Telemática* |
| **f. Analista de Biblioteca responsable:** Lic. Luis Caminos Vargas Mgs. |

Firmado electrónicamente por:
LUIS ALBERTO CAMINOS VARGAS

UNIDAD DE PROCESOS TÉCNICOS DBRA DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE ESPOCH