**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

**FACULTAD DE INGENIERÍA**

**ESCUELA INGENIERÍA DE TELECOMUNICACIONES**

# Implementación de un Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Aeronáutica Civil (INAC)

**TRABAJO ESPECIAL DE GRADO**

presentado ante la

**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

**como parte de los requisitos para optar al título**

## INGENIERO EN TELECOMUNICACIONES

REALIZADO POR: Marichal Borges, Xavier Alejandro

Nieto Barrios, Jinead Jessabel

TUTOR: Ing. Guillen González, Jhoan

FECHA: Caracas, Julio 2014

**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

**FACULTAD DE INGENIERÍA**

**ESCUELA INGENIERÍA DE TELECOMUNICACIONES**

# Implementación de un Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Aeronáutica Civil (INAC)

**TRABAJO ESPECIAL DE GRADO**

presentado ante la

**UNIVERSIDAD CATÓLICA ANDRÉS BELLO**

**como parte de los requisitos para optar al título**

## INGENIERO EN TELECOMUNICACIONES

REALIZADO POR: Marichal Borges, Xavier Alejandro

Nieto Barrios, Jinead Jessabel

TUTOR: Ing. Guillen González, Jhoan

FECHA: Caracas, Julio 2014

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA INGENIERÍA DE TELECOMUNICACIONES

# Implementación de un Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Aeronáutica Civil (INAC)

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: _____

| | | |
|---|---|---|
| Firma: | Firma: | Firma: |
| Nombre: _____ | Nombre: _____ | Nombre: _____ |

REALIZADO POR: Marichal Borges, Xavier Alejandro

Nieto Barrios, Jinead Jessabel

TUTOR: Ing. Guillen González, Jhoan

FECHA: Caracas, Julio 2014

# Resumen

**Implementación de un Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Aeronáutica Civil (INAC)**

Autor:
Marichal Borges, Xavier Alejandro
Nieto Barrios, Jinead Jessabel

Tutor:
Ing. Guillen González, Jhoan

Caracas, Julio 2014

La información es un activo muy importante para las organizaciones y en consecuencia necesita estar protegida adecuadamente. A medida que las organizaciones se desarrollan, la información se enfrenta a una gran cantidad de amenazas que pueden materializarse y causar impactos negativos sobre sus procesos administrativos y operacionales. Para prevenir o minimizar la ocurrencia de las amenazas, es necesario desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI), que mejore la disponibilidad, integridad y confidencialidad de la información en las empresas. Una de las normas más utilizadas a nivel internacional en materia de seguridad de la información, es la norma ISO/IEC 27001, que establece un ciclo estructurado en cuatro fases para asegurar los activos de información dentro de la organización. La implementación del SGSI en el Instituto Nacional de Aeronáutica Civil (INAC) se iniciará con una fase de investigación teórica, estrechamente relacionada con el estándar ISO/IEC 27000, la metodología para el análisis de riesgo (MAGERIT v3), entre otras normas internacionales y fuentes bibliográficas. La segunda fase está basada en la planificación, en la cual se organizó el proceso de implementación del SGSI, así como también un diagnóstico de la situación actual. La tercera parte consta del desarrollo del inventario de activos, el análisis de riesgos y la implementación de políticas y controles de seguridad. La cuarta fase comprende todas las pruebas que se realizaran para verificar el correcto funcionamiento del SGSI. Para finalizar, la quinta fase se utilizará para realizar mejoras necesarias al SGSI.

**Palabras Claves:** Activos, políticas, controles, amenazas, riesgos.

# Dedicatoria

*Este proyecto representa una gran meta que he logrado culminar con éxito, por esto quiero dedicárselo a mis padres Rufino Nieto e Hilda Barrios, que con su ejemplo, esfuerzo y dedicación me han inculcado valores que he podido aplicar en mi carrera y en mi vida.*

*A Christofer,*

*Por siempre apoyarme y estar ahí en los bueno y malos momentos.*

*A toda mi familia, abuelos, hermanos, tíos, primos y a mi ahijado Sebastián, los amo, porque siempre han estado ahí cuando los necesito.*

***Jessabel Nieto***

*Dedico este trabajo a todas las personas que siempre han estado ahí y que me han ayudado a crecer y a enriquecerme como persona.*

*A mi madre Xiomara Borges y a mi abuela Nelly Mayorgas , quienes siempre tuvieron la fortaleza para criarme con amor y cariño, educarme y estar presente siempre en todo momento y por ayudarme a ser el hombre que soy hoy en día.*

*A mi abuelo, por haberme enseñado a apoyar a mi familia y por haberme inculcado los valores que me formaron como hombre y como persona.*

*A José Borges, Carlos Borges, Yamiray Troconis y Fabiana Borges, quienes siempre me alentaron y me apoyaron en los buenos y malos momentos.*

***Xavier Marichal***

# Agradecimientos

Queremos agradecerle a Dios por permitirnos culminar nuestra meta, guiándonos siempre por el mejor camino.

Agradecemos a nuestros familiares, por tanto apoyo, para ayudarnos a tomar las mejores decisiones en el ámbito personal y profesional siendo ejemplos a seguir para nosotros, con valores y educación.

Al Ing. Jhoan Guillen, por haber depositado toda su confianza en nosotros y permitirnos ser parte de su equipo de trabajo, gracias por compartir tus conocimientos, por tu dedicación, atención y esfuerzos

# Índice General

# Índice de Figuras

# Índice de Tablas

# Índice de Apéndices

# Introducción

En la actualidad, la información se ha convertido en un activo muy importante para las empresas ya que diariamente estas deben procesar grandes cantidades de datos que frecuentemente están expuestos a un conjunto de amenazas que pueden materializarse y perjudicar de forma significativa a la organización, dañando su imagen, sus intereses, activos y en muchos casos su reputación.

Para proteger los activos de información, muchas organizaciones como la ISO, han desarrollado una serie de estándares internacionales como las normas ISO 27001 e ISO 27002, que poseen los requerimientos y las directrices necesarias para diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

Mediante la implementación de un SGSI en una organización, se pueden establecer controles de seguridad como políticas y mecanismos para mitigar y reducir los niveles de riesgo a los cuales se ven enfrentados los activos de información de la empresa diariamente.

Este Trabajo Especial de Grado busca implementar los controles de seguridad necesarios para mitigar las amenazas existentes en la Oficina de Tecnología de la Información (OTI) del Instituto Nacional de Aeronáutica Civil (INAC), y de esta manera proteger los activos de la organización basándose en tres parámetros principales como lo son la confidencialidad, la integridad y la disponibilidad de la información.

La información de este Trabajo Especial de Grado se estructura en seis capítulos, detallados en el Índice General, que se describen a continuación:

El primer capítulo se titula **Planteamiento del Proyecto**, en el que se expone la problemática existente en el Instituto Nacional de Aeronáutica Civil, la definición del proyecto a través de sus objetivos, justificación para llevarlo a cabo, alcance y limitaciones.

El segundo capítulo corresponde al **Marco Teórico**, en el cual se definen e incluyen todos los conceptos relacionados a un Sistema de Gestión de Seguridad de la Información, así como también la descripción de las funcionalidades del mismo y los procedimientos necesarios para la implementación.

El tercer capítulo corresponde a la **Metodología**, en donde se exponen los niveles de investigación correspondientes a este Trabajo Especial de Grado, tipo de proyecto y el procedimiento dividido en fases necesarias para una implementación exitosa del SGSI.

El cuarto capítulo abarca el **Desarrollo**, explicando cada una de las actividades necesarias en las diferentes fases de la implementación del SGSI para cumplir con los objetivos planteados en el proyecto.

El quinto capítulo de este Trabajo Especial de Grado, se titula **Resultados**, y expone los productos generados de cada una de las actividades explicadas en el capítulo anterior.

Finalmente, el sexto capítulo, contiene las **Conclusiones** y **Recomendaciones** realizadas.

La implementación de un Sistema de Gestión de Seguridad de la Información representa un tema de vital importancia para todas las organizaciones debido al creciente desarrollo tecnológico a nivel global, por lo que siempre es necesario para las empresas tomar medidas preventivas para protegerse de virus, hackers, Ataques de Penetración a la red, Denegación de Servicios (DoS), Robo, Espionaje, Alteración o Destrucción de la información, entre otros, por lo que se invita a leer y profundizar sobre este importante tema que actualmente forma parte del día a día de las organizaciones a nivel mundial.

# Capítulo I. Planteamiento del Proyecto

## I.1 Planteamiento del Problema

La información es un activo muy importante para las organizaciones y en consecuencia necesita estar protegida de manera adecuada. A medida que las organizaciones aumentan su desarrollo a nivel tecnológico y de interconectividad, la información en sus distintas formas, se enfrenta a una gran variedad de amenazas y vulnerabilidades.

Para prevenir o minimizar los riesgos a los que se somete la información en las organizaciones e incrementar el retorno de inversiones y oportunidades de crecimiento, es necesario implementar medidas y políticas de seguridad de la información, que permitan proteger el conjunto de datos en todas sus formas.

El Instituto Nacional de Aeronáutica Civil (INAC), es el organismo gubernamental, encargado de garantizar la seguridad y el desarrollo de la aeronáutica civil venezolana. En los últimos años, el mismo ha potenciado su plataforma tecnológica, con el objetivo de simplificar los trámites de los servicios que éste provee.

Todo ente rector de la aeronáutica, debe contar con un Sistema de Gestión para la Seguridad de la Información (SGSI), que garantice confidencialidad, integridad y disponibilidad de la información. Asimismo, deberá permitir el cumplimiento de las Normas Vigentes del estado y a las recomendaciones realizadas por la Organización de Aviación Civil Internacional (OACI), la cual hace mención a la protección de la aviación civil internacional contra los actos de interferencia ilícita.

Actualmente, el INAC no cuenta con un área específica que se encargue de la seguridad de los activos de información, la falta de sistemas de redundancia en los equipos informáticos del instituto, así como también de la documentación, procesos y registros relacionados a mantenimientos preventivos y correctivos, comprometen la seguridad de los activos de información y la mantienen vulnerable a incidentes de seguridad y deficiencias en algunas unidades administrativas y operativas de la organización afectando directamente la transparencia de la gestión pública de la institución.

Como solución, la Oficina de Tecnología de la información (OTI) ha iniciado la creación de una Oficina de Seguridad de la Información, que permita la adopción de un enfoque basado en seguridad, el cual pretende resolver la problemática existente, a través del desarrollo e implementación de un SGSI.

La implementación del SGSI, le aportará al INAC las bases necesarias para optimizar sus niveles de seguridad de información, lo cual ofrece numerosas ventajas tales como la posibilidad de obtener una certificación internacional reconocida, en este caso bajo el estándar ISO/IEC 27001 y además le aportará valores a la institución como mejora de la competitividad, mejora de la imagen corporativa, protección y continuidad del negocio, cumplimiento legal y reglamentario, optimización de recursos, inversión de tecnología y reducción de costos. Aunque no es posible eliminar las amenazas en su totalidad, se reducen significativamente, controlando el riesgo para generar seguridad y confianza, aportando veracidad y calidad de la información que se está tratando.

## I.2 Objetivos del proyecto

Se establecen los siguientes objetivos a cumplir con el presente Trabajo Especial de Grado.

## I.2.1 Objetivo General

Implementar un Sistema de Gestión de la Seguridad de Información en el Instituto Nacional de Aeronáutica Civil (INAC), que garantice confiabilidad, integridad y disponibilidad de la información.

## I.2.2 Objetivos Específicos

- Conceptualizar temas relacionados a un Sistema de Gestión de Seguridad de la Información.
- Describir las funcionalidades del SGSI.
- Diagnosticar la situación actual.
- Analizar los riesgos y vulnerabilidades que enfrenta la información en la organización.
- Identificar los controles necesarios para la implementación del SGSI en la Oficina de Tecnología de la Información.
- Aplicar políticas de seguridad a los equipos y ejecutar mejoras necesarias.
- Desarrollar los controles identificados bajo el estándar ISO 27002.
- Aplicar pruebas de la implementación del SGSI.

## I.3 Justificación

Los Sistemas de Gestión de la Seguridad de la Información (SGSI) representan un conjunto de políticas, controles y mecanismos que aportan soluciones en materia de Seguridad a los diferentes grupos de activos de información dentro de una organización, estos se representan de diversas formas según su naturaleza, tales como: Servicios, Datos, Software y Aplicaciones, Equipos Informáticos, Redes de Comunicaciones, Instalaciones e incluso el personal, que representa uno de los activos más importantes de cualquier organización.

La realización de este Trabajo Especial de Grado, constituye la implementación de un SGSI que generará un conjunto de políticas y controles de seguridad de la información especificados en la norma ISO/IEC 27002, que no solo reducirán significativamente los niveles de riesgo y la probabilidad de ocurrencia de las posibles amenazas a las que se enfrenta la información de la Oficina de Tecnología de la Información (OTI) en el INAC, sino además le permitirá aplicar un conjunto de procedimientos o mecanismos basados en medidas preventivas y correctivas, para minimizar los posibles impactos generados por dichas amenazas y vulnerabilidades a sus diferentes activos de información, garantizando de esta manera la integridad, confidencialidad y disponibilidad de la información.

## I.4 Alcances y Limitaciones

### I.4.1 Alcances

- Este Trabajo Especial de Grado comprende la implementación de un Sistema de Gestión de Seguridad de la Información para la Oficina de Tecnología de la Información (OTI) del Instituto Nacional de Aeronáutica Civil.
- Incluirá un diagnóstico de la situación actual, enfocado en las fortalezas y vulnerabilidades presentes en cada unidad de la OTI.
- Incluirá un Análisis de Riesgos, para medir el impacto y la probabilidad de ocurrencia de las posibles amenazas y vulnerabilidades.
- Durante el desarrollo de este Trabajo Especial de Grado no se contemplará un estudio de factibilidad económica, ni presupuestos para la adquisición de equipos, software, o cualquier otra inversión durante la implementación del SGSI.

## I.4.2 Limitaciones

- La implementación de un SGSI comprende un período de 12 meses aproximadamente, por lo tanto este Trabajo Especial de Grado está limitado en tiempo, necesario para la ejecución de todos los controles y políticas de seguridad de la información que se especifican en la norma ISO 27002. En consecuencia, no se implementarán todas las políticas sino un conjunto de ellas.
- La aprobación de los procesos y políticas desarrolladas en el proyecto para su implementación no solo depende de la OTI, sino también de la Oficina de Planificación, el cual es el área encargada de aprobar toda la documentación legal del Instituto Nacional de Aeronáutica Civil

# Capítulo II. Marco Teórico

## II.1 Instituto Nacional de Aeronáutica Civil (INAC)

El INAC es un Ente de seguridad de Estado, el cual le compete regular, fiscalizar y supervisar las actividades de la aeronáutica civil, lo cual comprende velar por cumplimiento de los derechos y deberes de los usuarios del servicio público de transporte aéreo, ejercer la vigilancia de la seguridad operacional y protección de la aviación civil incluyendo los servicios a la navegación aérea, y desarrollar las políticas aerocomerciales del espacio aéreo (INAC, 2013).

### II.1.1 Misión

"Garantizar la seguridad y el desarrollo de la aeronáutica civil venezolana para contribuir al desarrollo integral de la nación" (INAC, 2013).

### II.1.2 Visión

> Ser una organización efectiva en lo que respecta a la seguridad y servicio aeronáutico, creando una cultura de calidad y un desarrollo sustentable que permita alcanzar los más altos estándares en función de las necesidades del sector de la aviación civil nacional e internacional (INAC, 2013).

## II.2 La información

Es un activo muy importante y esencial para las organizaciones y por lo tanto necesita estar protegido de forma adecuada y más aún en ambientes en los cuales se

tienen gran interconexión entre diferentes empresas y corporaciones. (ISO/IEC 27002, 2007)

La información adopta diferentes formas. Puede ser de tipo oral, impresa, escrita en papel o incluso estar digitalizada o almacenada electrónicamente, transmitida por correo o por medios electrónicos (celulares, computadoras, aplicaciones web, entre otras) (ISO/IEC 27002, 2007).

## II.3 Seguridad de la Información

Motivado a la expansión de las Tecnologías de Información y Comunicaciones (TIC), se han reducido las barreras de tiempo y espacio para el acceso a la información, razón principal por la que deben aplicarse los mecanismos necesarios para protegerla del acceso no autorizado. Por lo tanto, es fundamental el concepto de seguridad de la información, la cual se entiende como la protección de la información, y para lograrlo, se debe preservar las siguientes características: Confidencialidad, Integridad, Disponibilidad (Areitio, 2008).

### II.3.1 Confidencialidad

La información solo debe ser accesible para aquellos que tienen la autorización necesaria para acceder a ella, bien sea para lectura, escritura, modificación o eliminación de la misma (ISO/IEC 27001, 2005).

### II.3.2 Integridad

Se debe garantizar la exactitud y la totalidad de la información, es un aspecto que también está ligado a los diferentes métodos de procesamiento del conjunto de datos, ya que estos juegan un papel importante con respecto al hecho de que la información este completa o no (ISO/IEC 27001, 2005).

### II.3.3 Disponibilidad

La información debe estar disponible para aquellos que tienen la autorización necesaria en cualquier momento que ellos lo requieran (ISO/IEC 27001, 2005)

## II.4 Sistemas de Información

Según Alarcón (2006), "Es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común: satisfacer las necesidades de información de una organización" (p. 11).

### II.4.1 Ataques a los Sistemas de Información

En la actualidad existe una serie de técnicas y ataques desde el punto de vista telemático que constituyen riesgos potenciales para la seguridad de la información, debido a esto, es preciso conocer los diferentes tipos de ataques e incidentes telemáticos, con el fin de saber el tipo de medidas que se pueden implementar para mejorar la seguridad de la información que maneja un organismo específico.

### II.4.2 Ataques de Denegación de Servicio (DoS)

Es uno de los tipos de ataques más utilizados en la actualidad, según Areitio (2008), "es una técnica que tiene como objetivo dejar fuera de servicio a la(s) máquina(s) de la víctima, provocando de este modo, que deje de ofrecer los servicios que antes ofrecía" (p. 164).

En una red de comunicaciones, un intruso puede realizar un ataque de DoS y evitar que un equipo ofrezca algún tipo de servicio o incluso generar la caída total del sistema operativo remoto. Con este tipo de ataques se pueden denegar servicios como DHCP, FTP, DNS, alterar configuración o incluso dañar equipos como servidores, switches, routers, computadoras, entre otros que son propios de la organización.

Este tipo de ataques poseen ciertas características entre las cuales se pueden destacar la facilidad para realizarlos, la posibilidad de generar pérdidas económicas y de información a la organización víctima del ataque

### II.4.3 Ataques de Inundación

Son ataques que genera un usuario malintencionado o inconsciente, para evitar que los usuarios legítimos del sistema tengan acceso a un recurso, normalmente de red, causando de esta manera gran congestión en las conexiones de la red de la organización.

### II.4.4 Ataques de Denegación de Servicio Distribuido (DDoS)

Existen ataques que son mucho más sofisticados, entre los cuales uno de los más importantes es el ataque DDoS, en este tipo de ataques, según Areitio (2008), "El atacante utiliza distintos agentes ubicados en varios servidores de la red sobre los que actúa, para realizar un ataque sincronizado contra la máquina víctima" (p. 171).

Al manejar atacar desde diferentes nodos de la red, se genera un incremento significativo en el nivel de congestión de la red, a causa del constante flujo de información que envían cada uno de los nodos manejados por el atacante.

Como defensa ante este tipo de ataques, se puede realizar un seguimiento desde el punto en el que se originó, examinando los posibles rastros o huellas que el atacante pudiera haber dejado de forma inconsciente en los agentes que utilizó para realizar el ataque de DDoS.

### II.4.5 Código Malicioso *(Malware)*

Es un tipo de software que tiene la capacidad para infiltrarse dentro del Sistema Operativo de una computadora o incluso dentro de un Sistema de Información y causar daños al mismo.

Entre los diferentes tipos de Malware, se pueden mencionar virus, troyanos, gusanos, software maligno para espiar (spyware), phishing, entre otros, cada uno de ellos afecta directamente no solo a los equipos de la organización, sino más importante aún, amenazan directamente la seguridad de la información que se encuentre almacenada dentro de dichos equipos.

## II.5 Sistemas de Gestión de la Seguridad de la Información (SGSI)

Para entender el concepto de un Sistema de Gestión de Seguridad de la Información (SGSI), se debe entender el concepto general de un sistema de gestión. Según Areitio (2008), Un Sistema de Gestión "abarca una estructura, unos recursos, unos proyectos y unos procedimientos que tienden a poner en práctica los objetivos y políticas de una organización" (p. 200).

Para Areitio (2008), El SGSI "es parte del sistema de gestión global, basado en el enfoque en los riesgos del negocio y que establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información" (p. 200).

El SGSI, se puede definir entonces como un conjunto de políticas de administración de la seguridad de la información dentro de una empresa, con el paso del tiempo se han desarrollado diferentes estándares que definen y establecen todos los elementos, requisitos y procedimientos para el diseño e implementación de un SGSI, tales como la norma ISO/IEC 27001, el BS-7799-2: 2001, entre otros.

Estos sistemas se encargan de analizar en detalle y ordenar la estructura de los sistemas de información, definir procesos, procedimientos y normativas de trabajo, utilizar controles para garantizar la seguridad de la información, así como también revisar y evaluar la efectividad y cumplimiento del mismo. Además, como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

## II.5.1 Norma ISO 27001

La ISO 27001, se define como un estándar o norma para la seguridad de la información, mediante el cual es posible afirmar que esta norma constituye la base para la gestión de la seguridad en cualquier tipo de organización, con o sin fines de lucro, pública o privada.

## II.5.1.1 Ciclo Deming o PDCA

El ciclo Deming, se define como una de las principales herramientas para lograr la mejora continua de la calidad en la administración en las organizaciones o empresas. Este consiste, en una secuencia lógica de cuatro etapas, que se deben ejecutar secuencialmente, Planear, Hacer, Verificar y Actuar; pasos por los cuales son definidos también en las siglas PDCA (Plan- Do- Check- Act). Como resultados al ejecutar este ciclo, permite a las empresas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo costos y precios, optimizando la productividad e incrementando la participación del mercado, logrando de esta forma aumentar la rentabilidad de la empresa u organización.

## II.5.1.1.1 Planificar (Plan)

Según la norma ISO/IEC 27001:2005, la fase de planificación consiste en "Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización" (p. 7).

Es la Fase de diseño del SGSI, el cual realiza la evaluación de riesgos de seguridad de la información y la selección de controles adecuados, planifica los cambios a grandes rasgos, identifica los objetivos que constituyen el objeto de la

mejora, determinar los métodos y recursos para alcanzarlos, definir los indicadores que permitirán establecer el punto de partida y cuantificar los objetivos.

#### II.5.1.1.2 Hacer *(Do)*

La norma ISO/IEC 27001: 2005, especifica que durante esta fase se debe "Implementar y operar la política, los controles, procesos y procedimientos SGSI" (p. 7).

Realiza los cambios para implementar la mejora propuesta y una vez esté definido asigna una fecha en la cual se llevará a cabo lo planeado. Generalmente, conviene realizar una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.

#### II.5.1.1.3 Controlar o Verificar *(Check)*

Esta fase tiene como objetivo revisar y evaluar el desempeño del SGSI. Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados.

#### II.5.1.1.4 Actuar *(Act)*

Una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desechar. En otras palabras, en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

Una vez culminado el paso 4 (Act), se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implementar.

## II.5.2 Norma ISO 27002

La ISO 27002 anteriormente denominada 17799:2005, se define como un estándar o norma el cual desarrolla y recomienda códigos de buenas prácticas para la implementación de un sistema de gestión de seguridad de la información.

### II.5.2.1 Dominios

Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información (Instituto Nacional de Tecnologías de la Comunicación, 2014).

La norma ISO/IEC 27002 se encuentra estructurada por 11 Dominios, los cuales emanan 39 Objetivos de Control que conforman 133 controles en total, cada uno tiene asociado una guía de implantación y cada organización deberá realizar los estudios necesarios para saber los controles que aplican y cuáles no.

### II.5.2.2 Controles de Seguridad

Son las medidas o salvaguardas que deben ser aplicadas dentro de la organización para garantizar la seguridad de los activos de información, los controles de seguridad se encuentran clasificados por dominios en la norma ISO 27002, y su función principal se basa en minimizar la probabilidad de ocurrencia de las amenazas y reducir el impacto producido por la materialización de los riesgos.

## II.5.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

En el libro I – Método de MAGERIT (2012) "responde a lo que se denomina 'Proceso de Gestión de los Riesgos', dentro del 'Marco de Gestión de Riesgos'. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un

marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información" (p.7).

Siendo esta una de las metodologías de análisis y gestión de riesgos más reconocidas a nivel mundial y fue desarrollada en España por el Consejo Superior de Administración Electrónica, con la finalidad de generar un modelo capacitado para identificar todas las amenazas y vulnerabilidades a las que se ven expuestos todos los activos de información que pertenecen a una organización pública o privada. Gracias a esta metodología, se hace mucho más sencillo determinar las medidas, controles o salvaguardas necesarias para garantizar la seguridad de la información.

## II.5.4 Activos

"Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos" (UNE 71504, 2008).

### II.5.4.1 Tipos de Activos

Los Activos de información de una organización se clasifican de acuerdo a las siguientes categorías.

- **Servicios:** Función que satisface una necesidad de los usuarios. Algunos ejemplos de servicios típicos son: Correo electrónico, DNS, DHCP, FTP, Telnet, SSH, Carpetas compartidas, Directorios Telefónicos, entre otros.
- **Datos e Información:** Elementos que representan los conocimientos relacionados al área. Los datos son el corazón que permite a una organización prestar sus servicios, como memorándum, actas, informes, códigos fuente,

datos de interés administrativo, de carácter personal y registro de actividades (log) por mencionar algunos.

- **Aplicaciones y Software:** Es referido a tareas que han sido automatizadas para su desempeño por un equipo informático, por ejemplo, sitios web, navegadores web, monitores transaccionales, ofimática, sistemas operativos, gestores de base de datos, etc.
- **Equipos Informáticos:** Son los bienes materiales, físicos destinados a soportar directa o indirectamente los servicios que presta la organización, tales como computadoras, servidores, routers, switches, impresoras, teléfonos, antenas, entre otros.
- **Personal:** Es el activo principal, son personas que manejan la información de valor para la organización, por ejemplo interno, subcontratado, externos.
- **Redes de Comunicaciones:** Medios de transporte que llevan datos de un sitio a otro como las redes LAN, WAN, WLAN, VPN, MAN, punto a punto, frame relay, etc.
- **Instalaciones:** Toda aquella infraestructura que sustenta los equipos, aplicaciones y software, personal y demás activos de la organización, por ejemplo las oficinas, edificios y vehículos.
- **Activos Intangibles:** Son aquellos que están relacionados con la imagen y la reputación de la institución.

## II.5.4.2 Dependencias entre Activos

Para El libro I – Método de MAGERIT (2012):

Se dice que un ‘activo superior’ depende de otro ‘activo inferior’ cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre

el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores (p.23).

### II.5.4.3 Valoración de Activos

"La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes" (MAGERIT, 2012, p.24).

En la Oficina de Tecnología de la Información (OTI) del Instituto Nacional de Aeronáutica Civil se valorarán cada uno de los activos de forma cuantitativa en una escala del uno al cinco según los tres parámetros principales en un SGSI, los cuales son: integridad, confidencialidad y disponibilidad de los activos.

## II.5.5 Gestión de Riesgos

El libro I – Método de MAGERIT (2012) señala el riesgo como:

> Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema (p.9).

Para identificar los peligros a los que se enfrenta la información dentro de una organización, es necesario realizar la gestión de riesgos. Según Areitio (2008), la gestión de riesgos se define como "el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado" (p. 7).

### II.5.5.1 Análisis de Riesgos

En el libro I – Método de MAGERIT (2012) definen el Análisis de riesgos como un "proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización" (p.9).

El libro I – Método de MAGERIT (2012) señala que:

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

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza (p.22).

### II.5.5.1.2 Amenazas y Vulnerabilidades

Areitio (2008) señala que:

Una vulnerabilidad puede entenderse como la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Las vulnerabilidades asociadas a los activos, incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, administración, equipos, software o la información (p.23)

Una amenaza, es una "causa potencial de un incidente que puede causar daños a un sistema de información o a una Organización" (UNE 71504, 2008). Para que una amenaza se materialice es necesario que esta explote una vulnerabilidad del activo o un grupo de ellos para producir un daño (Areitio, 2008).

Se debe tener en consideración que "cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía" (MAGERIT, 2012, p.28).

Durante el desarrollo del Análisis de Riesgo del SGSI para la Oficina de Tecnología de la Información se tomarán en consideración las siguientes amenazas y vulnerabilidades mostradas a continuación:

| Amenazas | Vulnerabilidades |
|---|---|
| Fuego | Sistema contra incendio insuficiente |
| | Vulnerabilidades colocadas deliberadamente |
| | Falta de mantenimiento de sistemas contra incendios |
| | Inexistencia de políticas |
| | Inexistencia de planes de recuperación de desastre |
| | Falta de procedimientos de emergencia contra incendios |
| | Condiciones inadecuadas de temperatura y humedad |
| Líquidos | Falta de mantenimiento de las tuberías de agua |
| | Vulnerabilidades colocadas deliberadamente |
| | Ausencia de procedimientos |
| | Inexistencia de planes de recuperación de desastre |
| | Condiciones inadecuadas de temperatura y humedad |

| | |
|---|---|
| | Inexistencia de políticas |
| **Amenazas** | **Vulnerabilidades** |
| Avería de origen Físico | Falta de mantenimiento del activo |
| | Inexistencia de políticas de uso adecuado del activo |
| | Sistema No supervisado |
| | Ausencia de procedimientos para instalación y mantenimiento del activo |
| | Vulnerabilidades colocadas deliberadamente |
| | Control de cambios deficientes |
| Avería de origen lógico | Falta de mantenimiento |
| | Vulnerabilidades colocadas deliberadamente |
| | Errores de configuración |
| | Desbordamientos de búfer |
| | Ausencia de procedimientos |
| | Inexistencia de políticas |
| | Control de cambios deficientes |
| Fallo de servicios de comunicaciones | Falta de mantenimiento |
| | Ausencia de procedimientos |
| | Inexistencia de políticas |
| | Falta de validaciones |
| | Vulnerabilidades colocadas deliberadamente |
| | Control de cambios deficientes |
| | Mal manejo de los recursos |

| Amenazas | Vulnerabilidades |
|---|---|
| Degradación de los soportes de almacenamiento de la información | Falta de mantenimiento |
| | Vulnerabilidades colocadas deliberadamente |
| | Ausencia de procedimientos |
| | Inexistencia de políticas |
| Difusión de Software dañino | Falta de actualizaciones |
| | Vulnerabilidades colocadas deliberadamente |
| | Errores de configuración |
| | Se permiten protocolos innecesarios |
| | Sin filtrado entre segmento de red |
| | Inexistencia de políticas |
| | Controles no aplicados |
| | Sistemas no supervisados |
| Errores de enrutamiento | Vulnerabilidades colocadas deliberadamente |
| | Errores de configuración |
| | Falta de supervisión |
| Alteración de la información | Vulnerabilidades colocadas deliberadamente |
| | Credenciales robadas |
| | Control de cambios deficiente |
| | Ausencia de procedimientos |
| | Falta de supervisión |
| | Error de definición de privilegios |

| Amenazas | Vulnerabilidades |
|---|---|
| Destrucción de la información | Ausencia de procedimientos |
| | Inexistencia de políticas |
| | Software antivirus obsoleto |
| | Vulnerabilidades colocadas deliberadamente |
| | Credenciales robadas |
| | Error de definición de privilegios |
| Divulgación de Información | Inexistencia de Políticas |
| | Falta de controles |
| | Error de definición de privilegios |
| Caída del Sistema | Falta de Redundancia lógica y física |
| | Falta de mantenimiento |
| | Control de cambios deficiente |
| | Vulnerabilidades colocadas deliberadamente |
| | Agotamiento de recursos |
| Indisponibilidad del personal | Inexistencia de políticas |
| | Sobrecarga de trabajo |
| | Condiciones inadecuadas de temperatura y humedad |
| Suplantación de identidad del usuario | falta de monitoreo de los accesos |
| | Falta de políticas de acceso(Contraseñas) |
| Intercepción de información (escucha) | Vulnerabilidades colocadas deliberadamente |

| Amenazas | Vulnerabilidades |
|---|---|
| Intercepción de información (escucha) | Falta de filtrado de los parámetros de entrada |
| | Se permiten protocolos innecesarios |
| | Ausencia de procedimientos |
| | Sistemas no supervisados |
| Introducción de falsa información | Vulnerabilidades colocadas deliberadamente |
| | Falta de supervisión |
| | Errores de configuración |
| | Inexistencia de políticas |
| Denegación de Servicio | Vulnerabilidades colocadas deliberadamente |
| | Errores de configuración |
| | Ausencia de procedimientos |
| | Ausencia de monitoreo del Trafico de la Red |
| | Falta de configuraciones de seguridad |
| Robo | Inexistencia de políticas de control de activos |
| | Contraseñas que contengan pocos caracteres |
| | Inexistencia de políticas de control de Acceso |
| | Falta de supervisión |
| | Error de definición de privilegios |
| Extorsión | Incumplimiento del procedimiento |
| | Incumplimiento de las políticas |

**Tabla 1. Amenazas y Vulnerabilidades a tomar en consideración en el análisis de riesgos.**

**(Elaboración Propia)**

### II.5.5.1.3 Impacto Acumulado

En el libro I – Método de MAGERIT (2012) señala que:

> El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo y es tanto mayor cuanto mayor sea la degradación del activo atacado (p.28).

### II.5.5.1.4 Impacto de Amenazas

El libro I – Método de MAGERIT (2012):

> Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema (p.28).

### II.5.5.1.5 Nivel de Riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia (MAGEIRT, 2012, p.29).

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

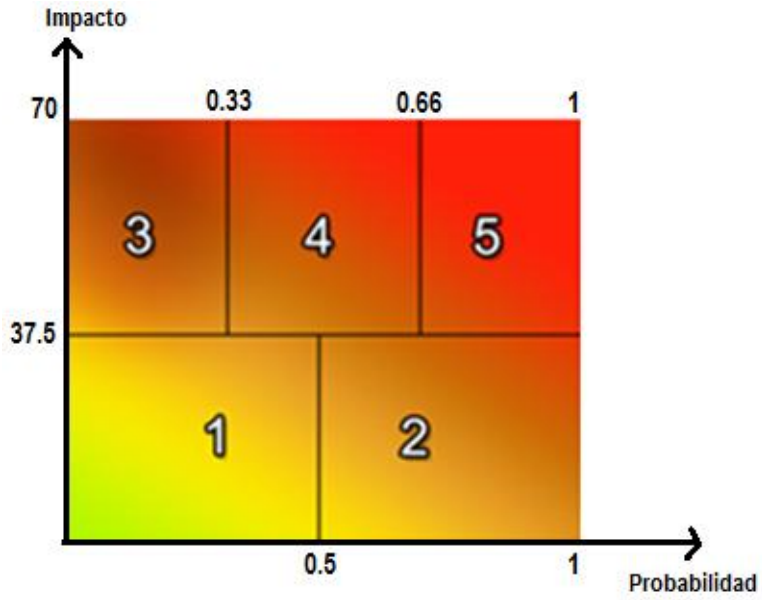



**Figura 1. El riesgo en función del impacto y la probabilidad**

**(Elaboración Propia)**

| Escala de Zonas de Riesgo | Criterio | Nivel de Riesgo |
|---|---|---|
| 0 ≤ Probabilidad de Ocurrencia ≤ 0.5<br>0 ≤ Impacto Acumulado < 37.5 | Muy Bajo | 1 |
| 0.5 < Probabilidad de Ocurrencia ≤ 1<br>0 ≤ Impacto Acumulado < 37.5 | Bajo | 2 |
| 0 ≤ Probabilidad de Ocurrencia ≤ 0.33<br>37.5 ≤ Impacto Acumulado ≤ 75 | Moderado | 3 |
| 0.33 < Probabilidad de Ocurrencia ≤ 0.66<br>37.5 ≤ Impacto Acumulado ≤ 75 | Alto | 4 |
| 0.66 < Probabilidad de Ocurrencia ≤ 1<br>37.5 ≤ Impacto Acumulado ≤ 75 | Muy Alto | 5 |

**Tabla 2. Escala y criterio para evaluar el nivel de riesgo**

**(Elaboración Propia)**

## II.5.5.2 Tratamiento de Riesgos

El libro I – Método de MAGERIT (2012) señala:

> Permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume (p.19).

## II.5.5.2.1 Documento de la Declaración de Aplicabilidad

Para Flores (2007), la declaración de aplicabilidad es un **"**documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamientos de riesgos, justificando inclusiones y exclusiones" (p.45).

La declaración de aplicabilidad es importante ya que define cómo se implementará el sistema de gestión de seguridad de la información, definiendo cuáles de los 133 controles sugeridos en la norma ISO 27002 son los que se implementarán y, para los controles que correspondan, cómo se realizará su implementación, ya sea mediante un mecanismo o cualquier tipo de documentación necearía.

## II.5.5.2.2 Documentación del SGSI

Los controles de seguridad de un Sistema de Gestión de la Seguridad de la Información basado en el estándar ISO 27000 pueden implementarse mediante diferentes tipos de documentación como políticas, normativas, registros o bitácoras, cheklists, formularios, entre otros.

### II.5.5.2.2.1 Política de Seguridad

Cao (2007) define la política de seguridad como:

Un documento de política de seguridad tiene como misión servir para dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los objetivos establecidos, la legislación y regulaciones existentes. La Política de Seguridad debe establecer los requisitos y criterios de protección en el ámbito de la organización y servir de guía para la creación de normas de seguridad. Formalmente describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son sus objetivos de cara a la seguridad (p.4).

### II.5.5.2.2.2 Normativas de seguridad

Cao (2007) señala que:

> Una norma de seguridad establece unos requisitos que se sustentan en la política y que regulan determinados aspectos de seguridad. Son por tanto, declaraciones a satisfacer. Una norma debe ser clara, concisa y no ambigua en su interpretación. En cuanto a la estructura de un documento normativo, se recomienda estructurarlo en los siguientes apartados:
>
> - Objetivo: declaración del propósito o intención de la redacción del documento y de los objetivos de seguridad relacionados con la política que se intentan satisfacer.
> - Definiciones: Se indican las definiciones de aquellos términos que aparezcan en la norma y que pudieran ofrecer dificultad para su comprensión.
> - Responsables del cumplimiento: se define dentro de la Organización qué departamento o responsable velará por el cumplimiento de la norma y revisará su correcta implantación o cumplimiento.

- Incumplimiento: se establecen las consecuencias que se derivarán del incumplimiento de la norma cuando éste sea detectado o las acciones disciplinarias que ocasionarán.
- Normas a aplicar: debe contener los requisitos de seguridad que se declaran de obligado cumplimiento.
- Documentos relacionados: Se indican otros documentos del marco normativo que pudieran estar relacionados con el cumplimiento de la norma. (p.5)

## II.5.5.2.2.3 Procedimientos

Flores (2007) define los procedimientos como "documentos que aseguran se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen como medir la efectividad de los controles" (p.44).

Cao (2007) señala que:

> Un procedimiento determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad. Son por tanto, la especificación de una serie de pasos en relación la ejecución de un proceso o actividad. Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución.
>
> En cuanto a la estructura de un procedimiento, se recomienda estructurarlo en los siguientes apartados:
>
> - Propósito u Objetivo: Declaración del propósito o intención de la redacción del documento y de los requisitos de seguridad que se intentan satisfacer.

- Definiciones: Deben especificarse las definiciones de aquellos términos que aparezcan en el procedimiento y que pudieran ofrecer dificultad para su comprensión.
- Alcance: Aplicabilidad y límites de la organización donde este procedimiento es vinculante.
- Desarrollo del proceso: Se debe determinar el conjunto de actividades y tareas a realizar en la ejecución del proceso. (p.7)

### II.5.5.2.2.4 Políticas de uso

Según Cao (2007):

> Una política de uso es un documento destinado a usuarios finales con la intención de establecer una regulación específica sobre la utilización de un sistema, tecnología o recurso. En este caso, deben documentarse las normas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información o los aspectos generales que se desean regular así como los usos que son considerados autorizados y los usos no aceptables (p.9).

### II.5.5.2.3 Mecanismos de Seguridad

"Los mecanismos de seguridad existen para proporcionar y dar soporte a los servicios de seguridad" (Areitio Bertolín, 2008, pág. 31)

### II.5.5.2.3.1 Respaldo de los Datos

Según Aguilera (2010) el Respaldo de Datos consiste en "Guardar copias de seguridad de la información del sistema en un lugar seguro" (p. 18). Es un mecanismo que permite almacenar o guardar copias de seguridad del sistema en un lugar o dispositivo seguro, para ello se utiliza una combinación entre software y hardware.

### II.5.5.2.3.2 Control de Acceso

Es un mecanismo que emplea técnicas de seguridad mediante la utilización de nombres de usuarios y contraseñas, permitiendo el acceso a la información únicamente a los usuarios legítimos y registrados.

### II.5.5.2.3.3 Encriptación

Para Aguilera (2010), en la encriptación "Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Emisor y receptor son conocedores de la clave y a la llegada del mensaje se produce el descifrado" (p. 17). Es un método de seguridad en el que la información es cifrada con una clave especial generada mediante un algoritmo de encriptación. Antes de transmitir la información, el emisor la cifra con la clave antes mencionada y lo envía por el medio de transmisión, una vez que le llega la información al receptor, se procede a desencriptarla con la misma clave para obtener el mensaje en claro.

### II.5.5.2.3.4 Antivirus

Es un software de seguridad que detecta e impide la entrada de virus y otros malware al Sistema Operativo de un equipo.

### II.5.5.2.3.5 Cortafuegos *(Firewall)*

Constituyen un conjunto de dispositivos de software, hardware o una combinación de ambos que se encarga de restringir ciertos accesos al sistema, protegiendo de esta manera la integridad de la información.

### II.5.5.2.3.6 Certificados Digitales

Para Aguilera (2010), los certificados digitales son "documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es

quien dice ser, avalada por la verificación de su clave pública" (p. 17). Este tipo de documentos garantizan la integridad y confidencialidad de la información y representan uno de los mecanismos de seguridad más utilizados en las redes de datos.

## II.5.6 Funcionalidades del SGSI

El SGSI posee un conjunto de características o funcionalidades que están relacionadas al modelo de ejecución PDCA, las cuales son:

- Definición de Alcance y límites del SGSI en función de los requerimientos y características de la organización.
- Definición de la Política de Seguridad del SGSI que debe incluir un marco referencial para establecer sus objetivos y un conjunto de principios para la acción relacionados a la seguridad de la información.
- Aplicación de una Metodología de Gestión y Análisis de Riesgos como MAGERIT versión 3 para determinar, cuantificar y medir los niveles de riesgo de cada una de las amenazas existentes.
- Formulación de un Plan de Tratamiento de Riesgos.
- Implementación de un Conjunto de Controles de Seguridad basados en la norma ISO/IEC 27002 o incluso pueden ser diseñados por la misma organización tomando en cuenta sus necesidades y requerimientos para proteger a sus activos de información, reduciendo los niveles de riesgo de las amenazas previamente determinadas.
- Monitoreo y Revisión del SGSI, mediante la detección de eventos de seguridad y la determinación de la efectividad de los controles implementados.
- Mantenimiento y Mejoras al SGSI tomando las acciones correctivas necesarias identificadas en el proceso de monitoreo y revisión.

# CAPÍTULO III. Metodología

Este Trabajo Especial de Grado fue desarrollado bajo la modalidad de Proyecto Factible, utilizando una combinación de 2 niveles de investigación, los cuales son Investigación Documental e Investigación de Campo. En este capítulo se realiza el estudio de la modalidad definida para la metodología del proyecto y los niveles de investigación necesarios para la implementación del SGSI.

Del mismo modo, también se hace referencia a los procedimientos que se seguirán para llevar a cabo la investigación y el desarrollo de las políticas de seguridad que van a ser implementadas, los instrumentos y la descripción de las técnicas que permitirán analizar la información relacionada a los conceptos teóricos y prácticos necesarios para la implementación de un SGSI con la finalidad de cumplir con los objetivos específicos del proyecto.

## III.1 Nivel de Investigación

Este proyecto presenta una combinación de dos métodos de investigación:

### III.1.1 Investigación Documental

Representa el estudio y el análisis de información y datos provenientes de materiales impresos, bibliografías, publicaciones y cualquier otro tipo de documentación válida o legal, que se realiza sobre un tema específico.

La implementación de un SGSI, requiere de una fase de investigación bibliográfica que aportará los conceptos necesarios relacionados al proyecto además de reflexiones, criterios, conclusiones, recomendaciones y en general el pensamiento

de los diferentes autores de las obras o textos consultados, por lo que es adecuado adoptar este tipo de nivel de investigación.

### III.1.2 Investigación de Campo

Consiste en la recolección de datos relacionados a una situación, tema o hecho específico directamente desde un contexto de estudio, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos.

El desarrollo e implementación de un SGSI requiere de un conjunto de fases y procedimientos entre los cuales se realizan diferentes procesos de levantamiento de información en el contexto en el cuál se realizará la implementación del Sistema de Gestión de Seguridad de la Información, con el objetivo de determinar las amenazas y vulnerabilidades a los cuales se encuentran sometidos los activos de información de la organización. Con los resultados obtenidos se realiza un Análisis de Riesgos, en el cuál se determina mediante la utilización de una Metodología de Análisis y Gestión de Riesgos como MAGERIT, la probabilidad de ocurrencia de cada una de las amenazas, así como también sus valoraciones, niveles de riesgos y posibles impactos a la organización.

Mediante el análisis de riesgos en la Oficina de Tecnología de Información (OTI) del INAC, es posible determinar los controles de seguridad necesarios para proteger los activos de información que son vulnerables a cualquier tipo de amenazas previamente identificadas, estos controles se desarrollan en forma de mecanismos, políticas o procedimientos específicos que ayudan a reducir los impactos y la probabilidad de ocurrencia de las amenazas.

### III.1.3 Proyecto Factible

Este Trabajo Especial de Grado estará enmarcado dentro de la modalidad de Proyecto Factible, según La Universidad Pedagógica Experimental Libertador, el

proyecto Factible consiste en la "Investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos" (UPEL, 2012, pág. 21).

La implementación de un SGSI se logra mediante el desarrollo de una serie de políticas y mecanismos de seguridad de la información que ayudan a mitigar las amenazas existentes a los cuales se ven sometidos los activos de información de la organización.

Estas políticas y mecanismos se desarrollan siguiendo las directrices de los controles establecidos en la norma ISO/IEC 27002 pero tomando en cuenta los resultados obtenidos en el Diagnóstico de la Situación Actual y el Análisis de Riesgos, que indican cuales son las amenazas que pueden generar mayor impacto en los activos de información, sin embargo es importante mencionar que la implementación de un SGSI comprende la ejecución de las fases de Planificación, Hacer, Seguimiento y Acción, de forma cíclica según lo establece la norma ISO/IEC 27001, por lo que constantemente se monitorean los resultados de los controles aplicados en la Organización y de acuerdo a esto se toman las medidas necesarias para el mejoramiento continuo, por lo que es posible que las políticas y mecanismos implementados cambien a lo largo del tiempo.

En este sentido, es factible la implementación de un SGSI, ya que comprende las fases de formulación de políticas, programas, tecnologías y procesos para dar solución a los requerimientos de seguridad actuales de la Oficina de Tecnología de la Información del INAC.

## III.2 Procedimiento

A continuación se presenta el estudio de cada una de las fases que comprende este Trabajo Especial de Grado:

### III.2.1 Fase I: Investigación Teórica

Como primer paso para el desarrollo de este Trabajo Especial de Grado, es necesario realizar una búsqueda o localización de la documentación, los conceptos y las normas involucradas en este proyecto, con la finalidad de conocer el funcionamiento y los procedimientos necesarios para implementar un SGSI.

Para reforzar y ampliar nuestros conocimientos, se examinarán de manera conceptual, diferentes fuentes bibliográficas tales como libros de texto, artículos, publicaciones, normas internacionales y otras fuentes en Internet, los conceptos relacionados a las políticas de seguridad, tipos de amenazas y vulnerabilidades de la información, tecnologías utilizadas en la implementación de un SGSI y las fases para la gestión de la seguridad de información bajo la norma ISO/IEC 27001 así como también la gestión de controles bajo la norma ISO/IEC 27002.

Para obtener la información necesaria relacionada a los niveles de riesgos y los posibles impactos que puedan generar las amenazas existentes en la Oficina de Tecnología de la Información (OTI) del INAC, se realizará el estudio de una de las Metodologías de Gestión y Análisis de Riesgos más reconocidas a nivel mundial, conocida como MAGERIT versión 3. Esta metodología es la que mejor se adapta a las necesidades y a los requerimientos de seguridad de información en la OTI, por lo que se considera como la Metodología de Análisis de Riesgos ideal para la implementación del SGSI.

### III.2.2 Fase II: Planificación *(Plan)*

De acuerdo a los conceptos estudiados en la fase anterior, se aplicará el ciclo de vida del Proyecto, comenzando con la fase de Planificación. Según la norma ISO/IEC 27001, durante esta fase, se establece como paso inicial la definición de los Objetivos y el alcance del SGSI, por lo que fue necesario desarrollar el objetivo general de este Trabajo Especial de Grado, en el cual se implementará un SGSI en la Oficina de

Tecnología de la Información (OTI) del INAC garantizando confiabilidad, integridad y disponibilidad de los activos de información. En cuanto al alcance, es importante destacar que la implementación del SGSI se realizará únicamente en la OTI del INAC, incluyendo el Centro de Datos (Datacenter) y los Cuartos de Cableado.

Una vez definido los objetivos y el alcance del proyecto, es necesario conocer la situación actual de los activos de información que maneja cada una de las Unidades de la OTI, por lo que se realizará un proceso de levantamiento de información en el cuál se harán entrevistas a los empleados de cada una de las unidades y se estudiaran las condiciones y la infraestructura de los equipos, los servidores, el Datacenter, los cuartos de cableado, los niveles de seguridad de los servicios como DNS, DHCP, Correo Electrónico, Carpetas Compartidas, Controles de Acceso Físico a la infraestructura de la OTI y lógicos relacionados a las redes LAN, WAN y WLAN, entre otros.

Con los resultados obtenidos en el proceso de levantamiento de información, se desarrollarán Arboles de Dependencia entre los Activos, en el cual se visualizan de forma clara los activos superiores (Activos Padres) que generan altos niveles de dependencia sobre los activos inferiores (Activos Hijos). Estos Árboles de Dependencia son muy útiles ya que aportan una idea concreta de cuáles son los activos más importantes que deben ser protegidos en la OTI.

Otro aspecto importante durante la fase de levantamiento de información es el registro de todos los activos de información de cada una de las unidades, esta información es de vital importancia para desarrollar un Inventario de Activos de la OTI, el cuál es un documento que contiene información detallada de cada uno de los activos de información, su ubicación, el tipo de Activo, responsable del activo, así como también otras características físicas o lógicas de dicho activo.

## II.2.3 Fase III: Hacer *(Do)*

### III.2.3.1 Realización de Inventario y Valoración de Activos

Durante esta fase se desarrollará el Inventario de Activos, el cual es un documento que contiene un registro detallado de cada uno de los activos de información, los cuales son clasificados de acuerdo a la Unidad a la que pertenecen y al tipo de Activo (Datos o Información, Servicios, Equipos Informáticos, Instalaciones, Software y Aplicaciones, Redes de Comunicaciones y Personal). Cada activo posee su nombre, descripción, Ubicación, Unidad Responsable, Custodio y otras características específicas de dicho activo.

Una vez registrados todos los activos de información de la OTI, se procederá a valorar a cada uno de ellos, utilizando un esquema de valoración basado en el modelo de valoración cuantitativa de activos definidos en MAGERIT versión 3. Bajo este esquema, a cada activo se le da una valoración del 1 al 5, en donde 1 representa un valor muy bajo y 5 un valor muy alto de acuerdo a 3 parámetros fundamentales de seguridad: confidencialidad, integridad y disponibilidad.

Para valorar la propiedad de disponibilidad del activo, se debe responder a la siguiente pregunta: ***¿Cuál sería la importancia que tendría el que el activo no estuviera disponible?*** A continuación se muestra la escala y los criterios a emplear para cuantificar la disponibilidad.

| Valor | Criterio |
|---|---|
| 1 | Afectaría un proceso administrativo del instituto |
| 2 | Afectaría más de un proceso administrativo del instituto |
| 3 | Afectaría un proceso operacional del instituto |
| 4 | Afectaría más de un proceso operacional del instituto |
| 5 | Afectaría todos los procesos operacionales y administrativos del instituto |

**Tabla 3. Valoración y criterios para cuantificar la disponibilidad de los activos**

Para valorar la integridad del activo, la pregunta a responder será ***¿Qué importancia tendría que el activo fuese alterado sin autorización ni control?*** A continuación se muestra la escala y los criterios a emplear para cuantificar la integridad del activo.

| Valor | Criterio |
|---|---|
| 1 | No aplica / No es relevante |
| 2 | Los errores que hay o la información que falta no afecta el resultado del proceso |
| 3 | Tiene que estar correcto y completo al menos en un 50%para no afectar el resultado del proceso |
| 4 | Tiene que estar correcto y completo al menos en un 75% para no afectar el resultado del proceso |
| 5 | Tiene que estar correcto y completo al menos en un 99% para no afectar el resultado del proceso |

**Tabla 4. Valoración y criterios para cuantificar la integridad de los activos**

Para ponderar adecuadamente la propiedad de confidencialidad del activo, se debe responder la siguiente pregunta ***¿Cuál es la importancia que tendría acceder al activo de manera no autorizada?*** A continuación se muestra la escala y los criterios a emplear para cuantificar la confidencialidad del activo.

| Valor | Criterio |
|---|---|
| 1 | No aplica / No es relevante |
| 2 | Daños muy bajos, el incidente no trasciende del área afectada |
| 3 | Daños altos, el incidente no trasciende el área afectada |
| 4 | Serían relevantes, el incidente implica a otras áreas |
| 5 | Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas |

**Tabla 5. Valoración y criterios para cuantificar la confidencialidad de los activos**

De esta manera, el valor total del activo será la suma de cada una de las valoraciones asignadas a cada parámetro, tal y como se muestra en la siguiente figura:

| Nombre del Activo | Confidencialidad | Integridad | Disponibilidad | Valor del Activo |
|---|---|---|---|---|
| Servidores | 5 | 4 | 5 | 14 |

**Tabla 6. Esquema de Valoración de Activos**

**Fuente: Elaboración propia.**

El Inventario de Activos y La valoración de los activos serán desarrollados en 2 Documento específicos, uno de ellos llamado Inventario de Activos de la Oficina de Tecnología de La Información del INAC y el otro denominado Valoración de Activos de Información, ambos deben ser entregados a la Gerencia de Infraestructura Tecnológica de la OTI en el INAC.

## III.2.3.2 Análisis de Riesgos

Con las amenazas y vulnerabilidades identificadas en el proceso de levantamiento de información y el Documento de Diagnóstico de la Situación Actual, se desarrollará una lista de Amenazas y Vulnerabilidades, en el cual se agrupan las Amenazas de acuerdo a un conjunto de vulnerabilidades observadas que podrían generarlos. Estas Vulnerabilidades deben ser valoradas del 1 al 5, de acuerdo a cada Unidad de la OTI, usando el mismo criterio de valoración cuantitativa definida en MAGERIT, en el que un valor de 1 representa una vulnerabilidad baja y 5 un valor muy alto de vulnerabilidad. Al final para cada Unidad, se calculará un promedio con las valoraciones de las vulnerabilidades y el resultado de dicha operación es lo que se

conoce como el Valor de la Amenaza. El valor de la amenaza se calcula mediante la siguiente fórmula:

$$Valor\ de\ Amenaza = \frac{\sum Valoracion\ de\ cada\ Vulnerabilidad}{Nº\ de\ Vulnerabilidades}$$

**Figura 2. Fórmula para calcular el Valor de la Amenaza.**

**Fuente: Elaboración propia.**

Con este valor de Amenaza, el siguiente paso es calcular la Probabilidad de Ocurrencia, el cual se obtiene dividiendo el valor de la Amenaza, entre el valor máximo que puede tomar la amenaza. Una vez conocido el valor de la Amenaza y su Probabilidad de Ocurrencia, se calculará para cada uno de los activos de información de cada unidad, el impacto acumulado, usando la siguiente relación matemática:

$$Impacto\ Acumulado = ValorAmenaza\ x\ ValorActivo$$

**Figura 3. Fórmula para calcular impacto acumulado sobre un activo**

**Fuente: Elaboración Propia**

Posteriormente, se procederá a valorar el nivel del impacto de la amenaza sobre el activo, de acuerdo al siguiente esquema:

| Impacto Acumulado (I) | Impacto de la Amenaza |
|---|---|
| $1 \leq I \leq 15$ | 1 |
| $15 < I \leq 30$ | 2 |

| | |
|---|---|
| $30 < I \leq 45$ | 3 |
| $45 < I \leq 60$ | 4 |
| $60 < I \leq 75$ | 5 |

**Tabla 7. Esquema de Valoración de Impacto de la Amenaza**

**Fuente: Elaboración propia.**

Finalmente es necesario determinar el nivel de riesgo de cada amenaza sobre cada activo, y esto se logra utilizando nuevamente un esquema de valoración de riesgos definido en MAGERIT versión 3, este esquema fue adaptado tomando en cuenta el Valor del Impacto Acumulado y la Probabilidad de Riesgo de la Amenaza, de acuerdo a la distribución mostrada en la Figura 1.

### III.2.3.3 Selección de Controles

Con los resultados obtenidos en el Análisis de Riesgos, se determinará el conjunto de controles de seguridad de información especificados en la norma ISO/IEC 27002 que deben ser implementados en la OTI. Sin embargo, cada control tiene una serie de directrices y especificaciones por lo que es necesario desarrollar los documentos (normativas o procedimientos) y mecanismos (Técnicas de Seguridad de la Información) de cada uno de los controles.

La presentación de los controles seleccionados para el SGSI constituye un documento llamado Declaración de Aplicabilidad, el cuál será presentado en el capítulo IV de este Trabajo Especial de Grado.

### III.2.3.4 Implementación de Controles para el SGSI

Con la lista de controles seleccionados, se procederá a desarrollar la documentación y los mecanismos necesarios para cada control, esto implica un trabajo extenso, por lo que se contará con el apoyo del Gerentes de Infraestructura Tecnológica y la Gerente de Sistemas, así como también con el apoyo de los encargados de las diferentes unidades de la OTI, entre los cuales se pueden mencionar Soporte Técnico, Seguridad de Datos, Servidores, Redes LAN, Redes WAN, Redes WLAN, Telefonía IP, Telefonía Móvil, Desarrollo, Requerimientos y Base de Datos.

Entre los documentos más relevantes que forman parte de los controles del SGSI se pueden mencionar La Política de Seguridad de la OTI, La Política de Gestión de Activos, el inventario de Activos, Normativas de Perímetro de Seguridad Física para el Datacenter y los Cuartos de Cableado, la Política de Control de Acceso, Normativa para Protección contra Amenazas Externas, entre otras.

En cuanto a los mecanismos implementados se pueden mencionar algunos como Listas de Acceso (ACL's), Bloqueo de Puertos vulnerables a ataques de virus troyanos, gusanos, entre otros, los resultados de estos mecanismos serán presentados en el Capítulo IV de este Trabajo Especial de Grado.

## III.2.4 Fase IV: Seguimiento *(Check)*

Durante esta fase, se realiza un proceso de gestión y monitoreo de los controles implementados en la OTI, se medirá la eficiencia de los controles realizando Pruebas de Seguridad antes y después de la Implementación de los Controles y realizando una comparación de los resultados obtenidos. Entre las Pruebas de Seguridad realizadas, se pueden mencionar Ataques de Penetración a la Red, Escaneo de Tráfico en las redes LAN, WAN y WLAN, Escaneo de Puertos Abiertos en la Red, Ataque a las contraseñas de Acceso de la red WLAN para verificar su resistencia, entre otros. En

base a los resultados obtenidos, se modificarán los valores en el Documento de Análisis de Riesgos.

### III.2.5 Fase V: Actuar *(Act)*

Esta fase comprende las diferentes sugerencias, mejoras y actualizaciones que se le aplicarán al SGSI, de tal manera que se puedan optimizar las acciones preventivas y correctivas relacionadas a las vulnerabilidades y amenazas que puedan afectar la seguridad de la información. Estas mejoras se realizarán de acuerdo a los resultados obtenidos en las Pruebas de Seguridad, sin embargo es importante que el proceso de implementación del SGSI se mantenga constante en el tiempo y que vaya evolucionando de acuerdo a nuevas amenazas y vulnerabilidades que puedan aparecer o fortalecerse con el tiempo.

# CAPÍTULO IV. Desarrollo

El desarrollo de este trabajo especial de grado se basó en diferentes fases diseñadas en la metodología, que permitieron la organización de la Implementación del Sistema de Gestión de Seguridad de la Información de una manera óptima y sistemática. Es por esto que la presentación de este capítulo está estructurada en las siguientes fases que se cumplieron secuencialmente.

## IV.1 Fase I: Investigación Teórica

| Fase | Objetivos | Actividades |
|---|---|---|
| **Investigación Teórica** | ✓ Conceptualizar temas relacionados a un Sistema de Gestión de Seguridad de la Información.<br>✓ Describir las funcionalidades del SGSI. | 1. Estudiar las normas ISO 27001 y 27002.<br>2. Investigar en diferentes fuentes bibliográficas (Libros, Tesis, Normas y Metodologías Internacionales como MAGERIT). |

**Tabla 8. Esquema para el Desarrollo de la Fase Investigación Teórica del Proyecto.**

En esta etapa se creó toda la base bibliográfica, necesaria para el entendimiento de un Sistema de Gestión de Seguridad de la Información como documentación en línea, libros de texto, trabajos de grado, normas internacionales y metodologías relacionadas, con la finalidad de conocer el funcionamiento y los procedimientos necesarios para implementar un SGSI.

Dentro de la documentación bibliográfica se destaca el estándar ISO/IEC 27000, específicamente las normas ISO/IEC 27001, con la cual se ampliaron los conocimientos relacionados a los conceptos y políticas de seguridad, tipos de amenazas y vulnerabilidades de la información, tecnologías utilizadas en la

implementación de un SGSI y las fases para la gestión de la seguridad, así como también la gestión de controles bajo la norma ISO/IEC 27002.

La principal dificultad encontrada durante el desarrollo de la investigación teórica es que las Normas ISO/IEC 27001 e ISO/IEC 27002 son sumamente generales, dejando a libre criterio del diseñador las formas en la que se realizarán las diferentes actividades previas antes de implementar los controles necesarios, por ejemplo el análisis de riesgos.

Por lo que la información pertinente para la realización del análisis de riesgos se tomó como referencia una metodología reconocida a nivel mundial denominada MAGERIT versión 3, en ella se obtuvo la información relacionada a los niveles de riesgos y los posibles impactos que generaría el que se materializara un grupo de vulnerabilidades y en consecuencia una amenaza. Otra dificultad encontrada durante la realización de esta fase fueron los ajustes que se debían realizar en la metodología de análisis de riesgos para adaptarla de la mejor manera a las necesidades y a los requerimientos de la OTI, para lo cual se realizaron reuniones periódicas con el tutor del proyecto y consultas con especialistas del estándar ISO/IEC 27000 en Venezuela.

Es importante destacar que la fase de investigación teórica es la única etapa atemporal, ya que a medida que se avanza secuencialmente en el trabajo especial de grado se ha documentado en profundidad y se han obtenido los mejores resultados en las posteriores fases hasta el cumplimiento de todos los objetivos planteados.

## IV.2 Fase II: Planificación *(Plan)*

| Fase | Objetivos | Actividades |
|---|---|---|
| **Planificación *(Plan)*** | ✓ Diagnosticar la situación actual. | 1. Estudiar las normas ISO 27001 y 27002.<br>2. Reunirse con el Tutor.<br>3. Entrevistar a cada una de las unidades de la OTI. |

| | |
|---|---|
| | 4. Estudiar la situación actual del Datacenter.<br>5. Estudiar la situación actual de los Cuartos de Cableado. |

**Tabla 9. Esquema para el Desarrollo de la Fase Planificación *(Plan)* del Proyecto.**

Al cumplir con la fase de investigación teórica y de acuerdo al ciclo de implementación de un SGSI *(Plan- Do- Check- Act)*, se comenzó con la fase de Planificación, en donde se establece como paso inicial la definición de los Objetivos, cronograma de actividades a cumplir y alcance del SGSI, siendo este último una implementación del SGSI únicamente para la Oficina de Tecnología de la Información (OTI) del INAC. En cuanto al cronograma se planificó de acuerdo a los entregables de cada objetivo y las cinco fases de las cuales consta el proyecto.

Una vez estudiado y analizado toda la documentación teórica y haber definido objetivos y alcances se realizó el levantamiento de información de todos los activos entrevistando a cada uno de los empleados de las unidades de la OTI (Ver Figura 2), con preguntas orientadas a cada área con el fin de establecer un diagnóstico de la situación actual, con el fin de identificar las vulnerabilidades y fortalezas de toda la oficina en cuanto a seguridad de la información de los activos se refiere.

Seguidamente, se procedió a realizar los levantamientos de información uno para el Datacenter, y otro para los cuartos de cableado logrando observar la situación actual de sus infraestructuras, y las vulnerabilidades a los cuales se ven expuestos, así como también los niveles de seguridad de los servicios como DNS, DHCP, Correo Electrónico, Carpetas Compartidas, Controles de Acceso Físico a la infraestructura de la OTI y lógicos relacionados a las redes LAN, WAN y WLAN, entre otros.

Al culminar todos los levantamientos de información en la OTI y haber recopilado y analizado su información se desarrollaron árboles de dependencias por cada área, ofreciendo una amplia visión en cuanto a la jerarquía de los activos, visualizando

aquellos que dependen de otros, es decir los activos superiores (Activos Padres) que generan altos niveles de dependencia sobre los activos inferiores (Activos Hijos). Estos Árboles de Dependencia son muy útiles ya que permiten observar las relaciones y dependencias que existen entre ellos, por esta razón, al materializarse una amenaza que afecte directamente a un activo, todos aquellos que dependen de él también se verán afectados y aporta una idea clara de cuáles son los activos más importantes que deben ser protegidos en la OTI.

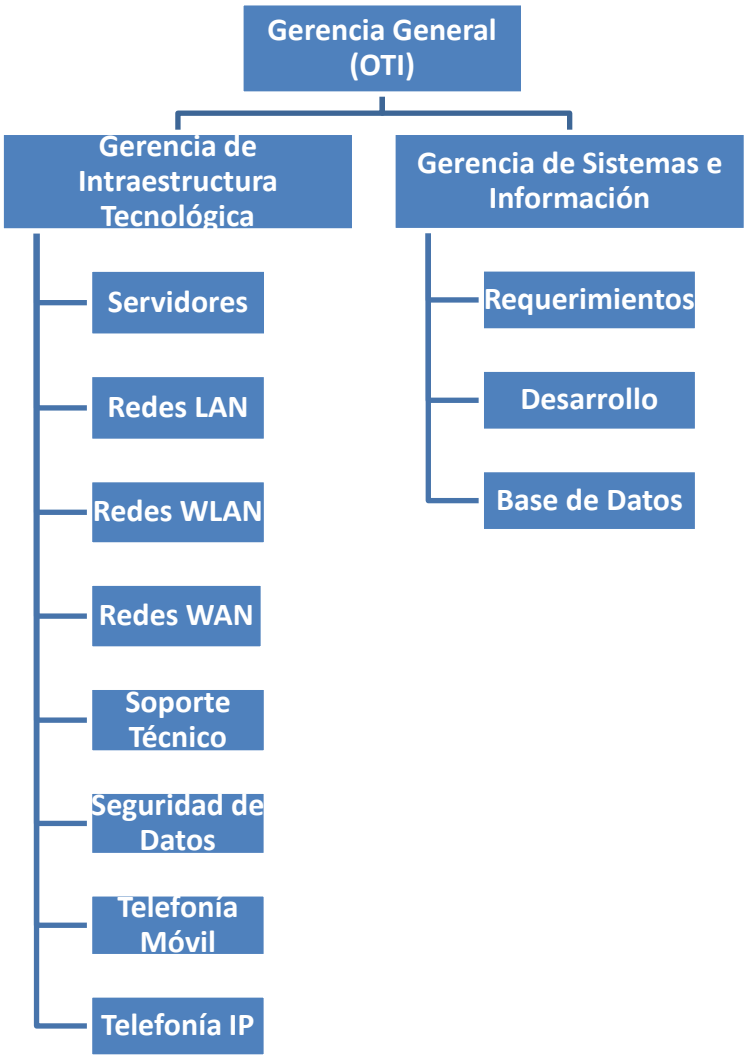



**Figura 4. Estructura organizacional de la Oficina de Tecnología de la Información (OTI) del INAC.**

## IV.3 Fase III: Hacer *(Do)*

| Fase | Objetivos | Actividades |
|---|---|---|
| **Hacer *(Do)*** | ✓ Analizar los riesgos y vulnerabilidades que enfrenta la información en la organización.<br>✓ Identificar los controles necesarios para la implementación del SGSI en la Oficina de Tecnología de la Información.<br>✓ Aplicar políticas de seguridad a los equipos y ejecutar mejoras necesarias.<br>✓ Desarrollar los controles identificados bajo el estándar ISO 27002. | 1. Estudiar resultados de las entrevistas y el Diagnóstico de la Situación Actual.<br>2. Estudiar los resultados del Análisis de Riesgos.<br>3. Seleccionar los Controles aplicables para la OTI en el INAC.<br>4. Desarrollar la documentación y los mecanismos necesarios para los controles seleccionados.<br>5. Implementar los controles. |

**Tabla 10. Esquema para el Desarrollo de la Fase Hacer *(Do)* en el Proyecto.**

En esta etapa del proyecto, se realizó el Análisis de Riesgo, la selección de controles de seguridad de la información especificados en la norma ISO 27002, y el desarrollo de la documentación y los mecanismos necesarios para la implementación de dichos controles.

El Análisis de Riesgos, permitió determinar el valor, la probabilidad de ocurrencia, los impactos y nivel de riesgo de cada una de las amenazas existentes en la Oficina de Tecnología de la Información del INAC. El cálculo del valor de la amenaza se determinó mediante el promedio de los valores de cada una de las vulnerabilidades relacionadas a dicha amenaza (Ver Figura #2), la probabilidad de ocurrencia se calculó dividiendo dicho valor entre 5, ya que cada amenaza puede tener una valoración entre 1 y 5.

Posteriormente, se procedió a calcular el impacto acumulado de cada amenaza con respecto a todos los activos de información de las diferentes unidades de la OTI, multiplicando el valor de la Amenaza por el Valor del Activo (Ver Figura #3).

De acuerdo al valor obtenido de Impacto Acumulado, se calcula el Impacto Total de la Amenaza sobre dicho activo, asignando el valor correspondiente de acuerdo a la tabla de Impacto de Amenaza especificada en la Metodología de Análisis de Riesgo (Ver Tabla #7).

Con el valor del Impacto de la Amenaza sobre el activo y su probabilidad de Ocurrencia, se calcula el Nivel de Riesgo, de acuerdo a la región correspondiente mostrada en la siguiente figura:

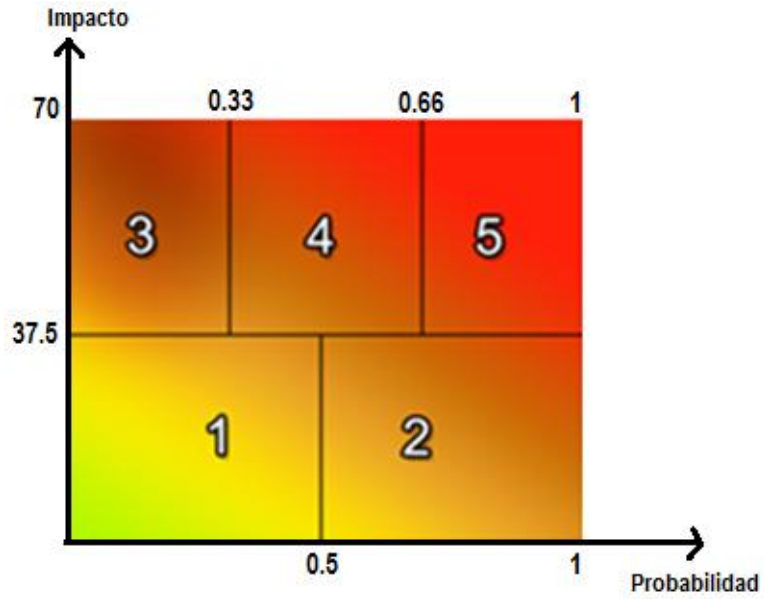



**Figura 5. El riesgo en función del impacto y la probabilidad**

**(Elaboración Propia)**

Para facilitar el Análisis de los niveles de riesgo y los impactos que producen las amenazas sobre los activos de información en la OTI, se construyó una Matriz de Riesgo por Unidad de la OTI, tal y como se muestra en el Apéndice E.

Tomando en cuenta que la información que suministra la Matriz de Riesgo es extensa y difícil de interpretar, se desarrolló un Diagrama Gráfico que contiene un resumen de las amenazas que poseen mayor impacto en los activos de cada una de las unidades de la OTI. En el diagrama se visualizan los niveles de riesgo de cada amenaza de acuerdo al siguiente esquema:


**Figura 6. Niveles de Riesgo de Amenaza para Diagrama Gráfico de Análisis de Riesgo.**

Haciendo una analogía con el esquema de valoración de Nivel de Riesgo antes mencionado, un color Rojo (Muy Alto) representa un Nivel de Riesgo de 5, Naranja (Alto), un nivel de Riesgo de 4 y Amarillo (Moderado), un nivel de riesgo de 3.

Este resumen ofrece un esquema que permite visualizar de forma gráfica y sencilla las amenazas cuyos niveles de riesgo son moderados, altos o muy altos, ya que el resto de las amenazas que poseen impactos y probabilidad de ocurrencia bajos o muy bajos se aceptaron, decisión tomada en conjunto con la gerencia, ya que no tienen la capacidad de afectar de manera perjudicial a los activos de información. El diagrama Gráfico del Análisis de Riesgo se puede visualizar en el Apéndice F. Con los resultados obtenidos de este proceso se desarrolló posteriormente un documento de Análisis de Riesgo que contiene los resultados y la descripción detallada del estudio realizado, dicho documento será presentado en el Capítulo V de este Trabajo Especial de Grado.

Una vez finalizado el proceso de Análisis de Riesgo y conociendo las amenazas potenciales en la OTI, se procedió a seleccionar los controles especificados en la norma ISO 27002. Es importante mencionar, que la norma ISO 27002 posee un total de 133 controles de seguridad, sin embargo, de acuerdo a los resultados obtenidos en el Análisis de Riesgo, se determinó que para mitigar las amenazas existentes en la Oficina de Tecnología de la Información del INAC, son aplicables 53 controles, de los cuales, se tomó la decisión junto con la Gerencia de la OTI de priorizar la

implementación de 15 de ellos. La totalidad de los controles definidos, fueron especificados en un documento denominado Declaración de Aplicabilidad.

La Declaración de Aplicabilidad mostrada en el Apéndice H de este Trabajo Especial de Grado, será la referente a los controles ya implementados por razones de seguridad y confidencialidad de la organización.

Con el Documento de Aplicabilidad se determina cual es la documentación y los mecanismos necesarios para llevar a cabo la implementación de los controles de seguridad seleccionados. Entre los documentos se pueden mencionar políticas, normativas, formularios, planillas, registros, entre otros.

Los mecanismos que conforman a los controles de seguridad de la información, son Listas de Acceso (ACL'S), Bloqueo de Puertos vulnerables en la red LAN de la OTI, funcionalidades de los equipos de telecomunicaciones como Port Security, protocolos de autenticación como LDAP e IPSec, entre otros.

Al finalizar la documentación y el diseño de los mecanismos de cada control, se procedió a informar a la Oficina de Planificación para formalizarlos y consecutivamente a la Gerencia de Infraestructura tecnológica para que se ejecutarán las operaciones necesarias e implementar los controles de seguridad de la información.

## IV.4 Fase IV: Seguimiento *(Check)*

| Fase | Objetivos | Actividades |
|---|---|---|
| **Seguimiento *(Check)*** | ✓ Aplicar pruebas de la implementación del SGSI. | 1. Revisar el Documento de Análisis de Riesgos.<br>2. Verificar el nivel complejidad de las contraseñas de acceso a la red WLAN y a los equipos de Telecomunicaciones.<br>3. Realizar intento de conexión a la red LAN con una PC no autorizada.<br>4. Realizar monitoreo de Puertos Abiertos en la red LAN de la OTI.<br>5. Realizar Ataque de Descubrimiento de los servicios y los equipos que conforman la red LAN de la OTI. |

**Tabla 11. Esquema para el Desarrollo de la Fase Seguimiento *(Check)* del Proyecto.**

Esta fase del proyecto corresponde a la etapa de Monitoreo y Control del SGSI, una vez implementados los controles de seguridad, se procedió a revisar el Documento de Análisis de Riesgos para aplicarle las actualizaciones respectivas. (Ver Apéndice G).

Asimismo, se realizaron diferentes pruebas de seguridad de la información para verificar el funcionamiento de los controles que conforman al SGSI, la primera prueba consistió en verificar el nivel de complejidad de las contraseñas de acceso a la red WLAN y a los equipos de Telecomunicaciones para determinar en cuanto tiempo se pueden descubrir dichas claves de acceso, esta prueba se realizó con la ayuda de una aplicación web llamada *How Secure is my Password*.

La siguiente prueba consistió en conectar una PC portátil intrusa a un punto de red de la OTI, antes de implementar el control de Gestión de Redes, el servidor DHCP le asignaba una dirección IP dinámica a cualquier equipo que se conectara a la red LAN,

sin importar si es un equipo legítimo de la oficina o si se trata del equipo de un usuario no autorizado ajeno al INAC. Mediante esta prueba se busca verificar que la asignación de direcciones IP dinámicas y el acceso a la red LAN se le otorga únicamente a los auténticos usuarios de la OTI, y para lograrlo, se verificaron los puntos de red de todos los usuarios de cada área en los equipos de telecomunicaciones ubicados en el Datacenter, posteriormente se realizó un filtrado por direcciones MAC para brindarle conexión a los empleados respectivos de cada punto de red y apagando el puerto de forma automática en caso de ser usado por una PC con una dirección física distinta perteneciente a un usuario no autorizado.

La siguiente prueba consistió en verificar los puertos y los protocolos estrictamente necesarios para la OTI, mediante un levantamiento de información y un escaneo de la red LAN, con el uso de un software de monitoreo llamado Wireshark para identificar los protocolos y puertos que están abiertos y operativos, como resultado se obtuvo una lista de puertos vulnerables que fueron bloqueados para evitar ataques de penetración, descubrimiento de la topología de la red y denegación de servicios.

Por último, se utilizó un software de monitoreo y gestión conocido como The Dude, para realizar un ataque de Descubrimiento de la red y los equipos que conforman a la Oficina de Tecnología de la Información del INAC, antes de realizar el bloqueo de puertos vulnerables, se utilizó este programa para descubrir toda la topología de la red LAN y los equipos de la OTI que se encuentran en el Datacenter, por lo que no existía protección contra este tipo de ataques, sin embargo, al aplicar las políticas y los controles respectivos, se ha logrado mitigar y prevenir este tipo de ataques.

Los resultados de cada una de las pruebas de seguridad realizadas serán mostrados en el Capítulo V de este Trabajo Especial de Grado.

## IV.5 Fase V: Actuar *(Act)*

| Fase | Objetivos | Actividades |
|---|---|---|
| **Actuar *(Act)*** | ✓ Aplicar pruebas de la implementación del SGSI. | 6. Medir la eficiencia de los Controles Implementados. |

**Tabla 12. Esquema para el Desarrollo de la Fase Actuar *(Act)* del Proyecto.**

Una vez realizadas las pruebas de seguridad y con los resultados obtenidos, fue necesario medir la eficiencia de cada uno de los controles implementados en la OTI, con el objetivo de mantener los niveles de seguridad de los activos de información, verificar el funcionamiento de los controles y aplicar las mejoras necesarias.

Las mejoras al SGSI serán presentadas en el Capítulo V de este Trabajo Especial de Grado.

Es importante mencionar que la implementación de este SGSI debe ser un proceso cíclico, en donde la Gerencia de la OTI debe estar en constante monitoreo y planificación, verificando el funcionamiento de los controles existentes, implementado nuevos controles y aplicando las mejoras necesarias.

# CAPÍTULO V. Resultados

Los resultados obtenidos con la realización de este Trabajo Especial de Grado se presentan a continuación de acuerdo a cada uno de los objetivos específicos planteados en el Capítulo I y conforme a la tabla de productos presentada a continuación.

| Fase | Objetivos | Actividades | Productos |
|---|---|---|---|
| **Investigación Teórica** | ✓ Conceptualizar temas relacionados a un Sistema de Gestión de Seguridad de la Información.<br>✓ Describir las funcionalidades del SGSI. | 1. Estudiar las normas ISO 27001 y 27002.<br>2. Investigar en diferentes fuentes bibliográficas (Libros, Tesis, Normas y Metodologías Internacionales como MAGERIT). | Marco Teórico |
| **Planificación *(Plan)*** | ✓ Diagnosticar la situación actual. | 1. Estudiar las normas ISO 27001 y 27002.<br>2. Reunirse con el Tutor.<br>3. Entrevistar a cada una de las unidades de la OTI.<br>4. Estudiar la situación actual del Datacenter.<br>5. Estudiar la situación actual de los Cuartos de Cableado. | Marco Teórico<br>Documento de Diagnóstico de Situación Actual (Apéndice B)<br>Política de Seguridad de la Información (Apéndice I) |
| **Hacer *(Do)*** | ✓ Analizar los riesgos y vulnerabilidades que enfrenta la información en la organización.<br>✓ Identificar los controles necesarios para la implementación del SGSI en la Oficina de | 1. Estudiar resultados de las entrevistas y el Diagnóstico de la Situación Actual.<br>2. Estudiar los resultados del Análisis de Riesgos.<br>3. Seleccionar los Controles aplicables para la OTI en el | Documento de Análisis de Riesgos (Apéndice G)<br>Declaración de Aplicabilidad (Apéndice H) |

| | | | |
|---|---|---|---|
| | Tecnología de la Información.<br>✓ Aplicar políticas de seguridad a los equipos y ejecutar mejoras necesarias.<br>✓ Desarrollar los controles identificados bajo el estándar ISO 27002. | INAC.<br>4. Desarrollar la documentación y los mecanismos necesarios para los controles seleccionados.<br>5. Implementar los controles. | Conjunto de Controles Implementados (Apéndice H) |
| **Seguimiento *(Check)*** | ✓ Aplicar pruebas de la implementación del SGSI. | 1. Revisar el Documento de Análisis de Riesgos.<br>2. Verificar el nivel complejidad de las contraseñas de acceso a la red WLAN y a los equipos de Telecomunicaciones.<br>3. Realizar un intento de conexión a la red LAN con una PC no autorizada.<br>4. Realizar un monitoreo de Puertos Abiertos en la red LAN de la OTI.<br>5. Realizar un Ataque de Descubrimiento de los servicios y los equipos que conforman la red LAN de la OTI. | Documento de Análisis de Riesgos Actualizado |
| **Actuar *(Act)*** | ✓ Aplicar pruebas de la implementación del SGSI. | 1. Medir la eficiencia de los Controles Implementados. | Mejoras al SGSI. (Apéndice O) |

**Tabla 13. Productos y actividades para cada fase y objetivos del proyecto.**

## V.1 Referente al primer y segundo objetivo específico

Objetivos Específicos:

Número 1: Conceptualizar temas relacionados a un Sistema de Gestión de Seguridad de la Información.

Número 2: Describir las funcionalidades del SGSI.

Conceptualizar temas relacionados a un Sistema de Gestión de Seguridad de la Información y Describir las funcionalidades del SGSI respectivamente corresponden al primer y segundo objetivos específicos respectivamente.

La investigación realizada referente al tema de la implementación de un sistema de gestión de seguridad de la información, se expone en el Marco Teórico (Capítulo II). El estudio realizado nos permite tener la base teórica necesaria para el desarrollo de este trabajo especial de grado.

## V.2 Referente al tercer objetivo específico: Diagnosticar la situación actual

Como producto de este objetivo se obtienen los documentos Diagnóstico de la Situación Actual (Ver apéndice B), en donde se refleja las vulnerabilidades y fortalezas de todas las unidades de la OTI, en el inicio del proyecto y la Política de Seguridad (Ver apéndice I) de la Información que contiene información relacionada los controles implementados en la OTI.

## V.3 Referente al cuarto objetivo específico: Analizar los riesgos y vulnerabilidades que enfrenta la información en la organización.

El análisis de los riesgos, amenazas y vulnerabilidades se muestran mediante las matrices de análisis de riesgos para cada área de la OTI (Ver apéndice E) y finalmente el Documento de Análisis de Riesgos como producto de este objetivo (Ver apéndice G).

Es importante destacar que ambas documentaciones no podrán ser mostradas en su totalidad, por motivos de seguridad y confidencialidad de la información.

## V.4 Referente al quinto objetivo específico: Identificar los controles necesarios para la implementación del SGSI en la Oficina de Tecnología de la Información

Como producto de este objetivo, se obtuvo un Documento denominado Declaración de Aplicabilidad, en el cual solo se muestran los controles implementados en el INAC junto con una breve descripción, un estado inicial del control y la documentación y mecanismos necesarios para su implementación.

Este documento fue de utilidad para organizar la implementación de cada uno de los controles en la OTI. (Apéndice H).

## V.5 Referente a los objetivos específicos seis y siete

Objetivos Específicos:

Número 6: Aplicar políticas de seguridad a los equipos y ejecutar mejoras necesarias.

Número 7: Desarrollar los controles identificados bajo el estándar ISO 27002.

Para estos objetivos, se obtuvo como producto la documentación y los mecanismos de los controles implementados. Con respecto a la documentación, se pueden mencionar la Política de Seguridad de la Información, Política de Gestión de Activos, Política de Control de Acceso y la Normativa de Control de Redes. (Apéndices I, J, K y L respectivamente).

En cuanto a los mecanismos se realizó un bloqueo de puertos vulnerables y un filtrado de protocolos estrictamente necesario y se aplicaron funcionalidades como Port Security a los switches de la red LAN de la OTI, también se desarrolló una Base de Datos y un Sistema de Gestión de Activos.

La aplicación de estas políticas y mecanismos generó ciertos resultados que se utilizaron para actualizar el Documento de Análisis de Riesgo. (Ver Apéndice G).

## V.6 Referente al Octavo objetivo específico: Aplicar pruebas de la implementación del SGSI

Durante la fase de Seguimiento se realizaron diferentes pruebas para verificar el funcionamiento del SGSI. De acuerdo a los resultados obtenidos en el Análisis de Riesgo y a los controles seleccionados en la Declaración de Aplicabilidad, se decidió realizar las siguientes pruebas:

### V.6.1 Verificar el nivel de Seguridad de las Contraseñas

Para esta prueba, se utilizó una aplicación Web gratuita online, dicha herramienta cuenta con una interfaz que contiene un campo para ingresar la contraseña a ser verificada y que en fracciones de segundos calcula el tiempo en el que la contraseña podría ser descifrada por un hacker o por un software que utilice código malicioso.

Inicialmente se ingresaron 2 contraseñas utilizadas en la OTI, una para el acceso a uno de los equipos de telecomunicaciones de la red LAN y otra referente a una contraseña de usuario para el acceso a la PC del funcionario respectivo, los resultados fueron los siguientes:

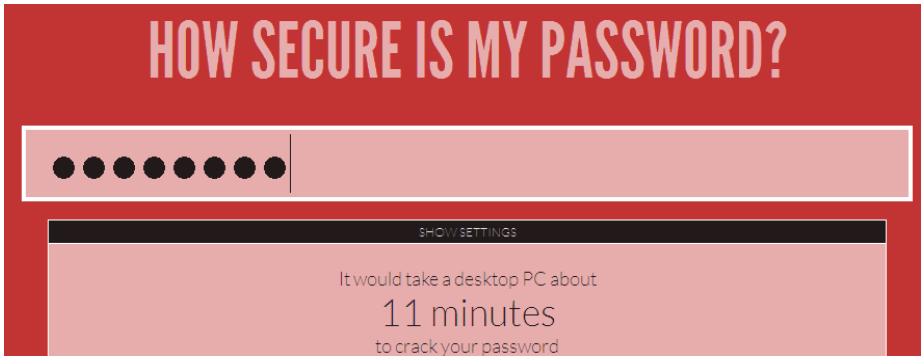



**Figura 7. Prueba de Verificación de Seguridad de Contraseña de Acceso de Usuario.**


**Figura 8. Prueba de Verificación de Seguridad de Contraseña de Acceso a equipos de Telecomunicaciones.**

De acuerdo a los resultados obtenidos, se determinó que el nivel de seguridad de las contraseñas era débil, por lo que se desarrolló una Normativa para la Gestión de Contraseñas en donde se especifica que las claves de acceso a los equipos informáticos deben ser largas y contener combinaciones de letras, números y caracteres especiales. Al cumplir con esta normativa, se realizó nuevamente la prueba de seguridad y esta vez se obtuvieron resultados efectivos, tal y como se muestra en la siguiente figura:

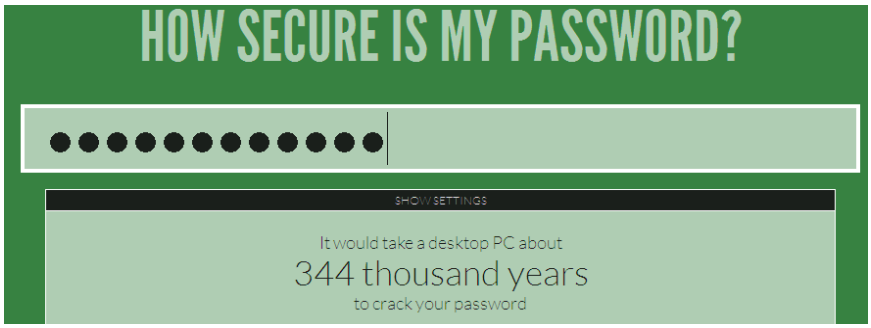



**Figura 9. Prueba de Verificación de Seguridad de Contraseña de Acceso aplicando la Normativa para la Gestión de Contraseñas.**

Se puede observar que las contraseñas de acceso a los equipos informáticos, son robustas y difíciles de descifrar, estos resultados generaron un aporte para reducir las amenazas de Destrucción de la Información, Suplantación de Identidad, Introducción

de Falsa Información, Avería de Origen Lógico y Fallo en el Servicio de Comunicaciones, entre otras, esto se puede visualizar en el control de gestión de contraseña de usuarios ubicado en la Lista de Controles Implementados y Valoración de Amenazas Mitigadas (Ver Apéndice H, página 104).

## V.6.2 Realizar un Ataque de Penetración y Descubrimiento a la red LAN de la OTI

Para esta prueba se utilizó un software de monitoreo llamado The Dude que tiene la capacidad de descubrir toda la topología de la red por la cual se conecte la PC del intruso identificando el nombre de los dispositivos que pertenecen a la red, su dirección IP e incluso, monitoreando el estado del envío y recepción de tráfico de todos los usuarios que conforman la red. Al principio esta prueba se realizó sin aplicar ningún tipo de mecanismo de seguridad y fue fácil descubrir la red, tal y como se muestra en la siguiente figura:

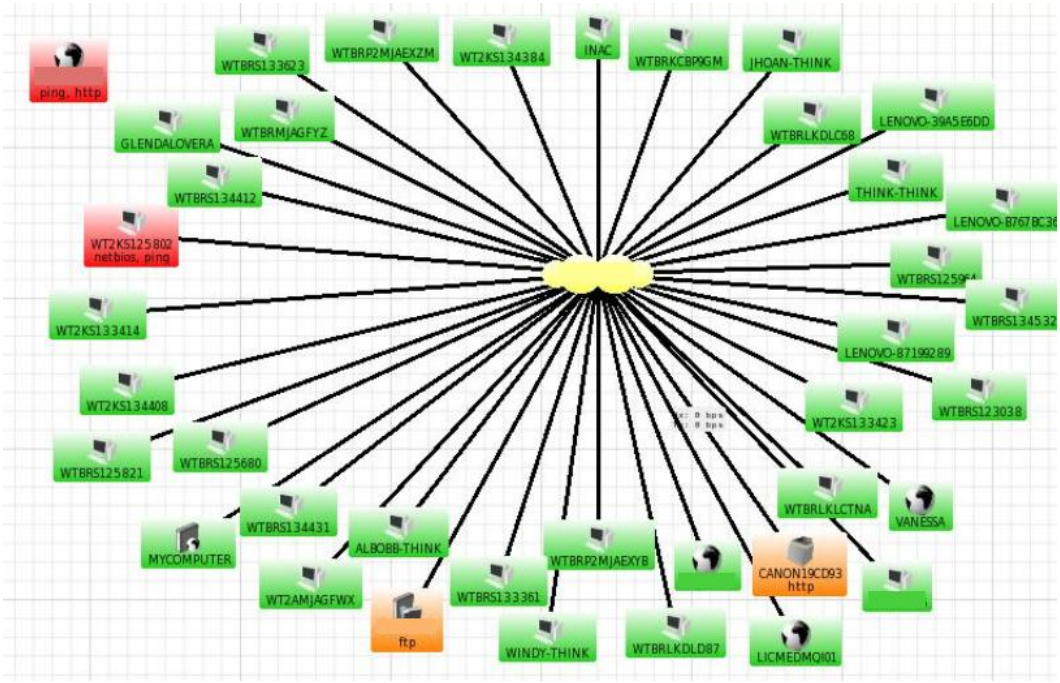



**Figura 10. Ataque de Descubrimiento a la red LAN de la OTI.**

## V.6.3 Realizar un monitoreo de puertos abiertos en la red LAN de la OTI

En esta prueba se utilizó el software de Monitoreo de Redes Wireshark para escanear el tráfico, los puertos y protocolos abiertos a través de la red LAN, a continuación se muestran los resultados obtenidos:

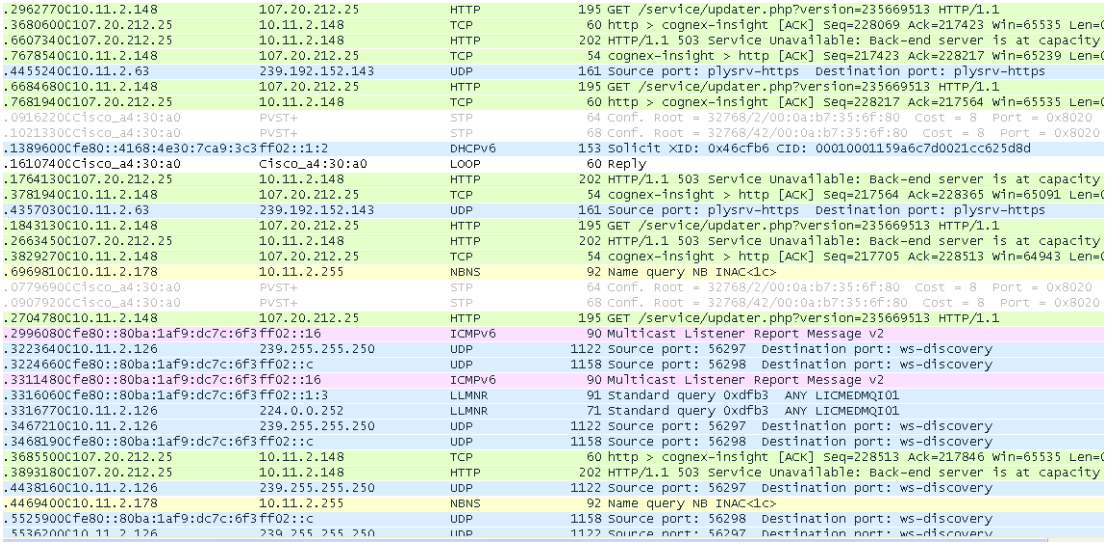



**Figura 11. Escaneo de Puertos y Protocolos en la red LAN de la OTI.**

En base a los resultados obtenidos, se pudo construir un documento que contenía una lista de puertos y protocolos necesarios que son aquellos con los que trabajan las diferentes unidades de la OTI y se requieren para brindar los servicios de voz y datos y una lista de puertos vulnerables e innecesarios que representan una amenaza para la OTI. Con la ayuda de esta lista, se realizó un proceso de bloqueo de los puertos innecesarios para proteger la red contra ataques de virus, hackers y software malicioso con la ayuda de un Firewall Cisco Modelo ASA 5500 manejado a través de un software de gestión por el Área de Seguridad de Datos. (Ver Apéndice Q).

## V.6.4 Prueba de Bloqueo del acceso de una PC no autorizada a la red LAN de la OTI

Inicialmente se conectó una PC ajena al INAC a un punto de red para verificar si el servidor DHCP le brindaba una IP de forma dinámica al equipo, tal y como se muestra en la siguiente figura:

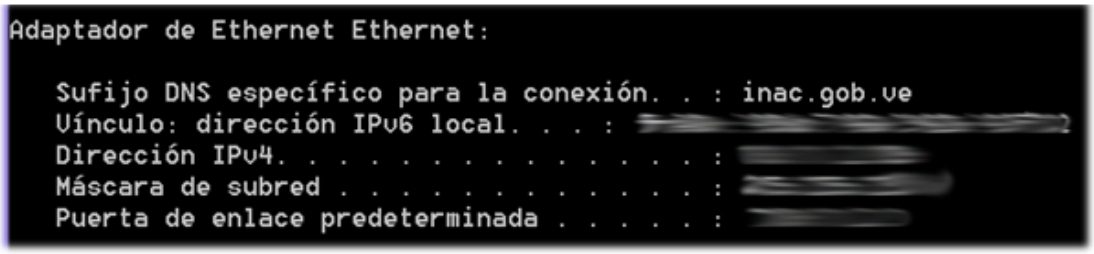



**Figura 12. Conexión de una PC intrusa a la red LAN de la OTI.**

El resultado de esta prueba, permite visualizar la existencia de una vulnerabilidad que puede incurrir en una amenaza para la OTI, ya que cualquier intruso puede accesar de forma no autorizada y perjudicar a la integridad, confidencialidad y disponibilidad de los activos de información en el INAC.

Debido a esto, fue necesario implementar mecanismos de seguridad como Port Security, en el cual a cada puerto del switch se le asigna una dirección MAC específica admisible, si el usuario usa cualquier otro dispositivo con una dirección física diferente a la que tiene registrado el equipo, el puerto se apaga por un lapso de tiempo determinado para evitar Ataques de Penetración, Denegación de Servicios y para proteger la información que viaja a través de la red LAN de la OTI, al implementar Port Security, se obtuvo el siguiente resultado:

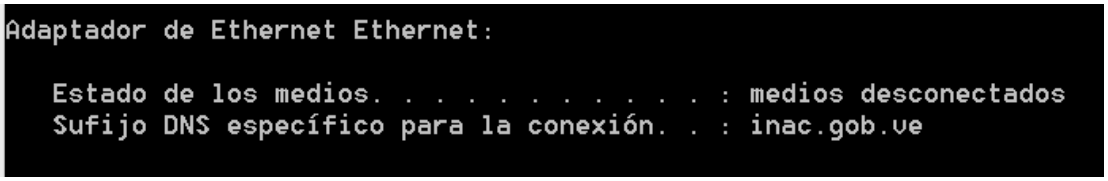


**Figura 13. Intento fallido de conexión a la red LAN gracias a Port Security.**

Con esto se puede observar que como la MAC del equipo no es la misma que tiene registrado el switch, el puerto se apaga y por lo tanto, el intruso no tiene acceso a la red LAN.

Una vez aplicadas las pruebas de Seguridad mencionadas en el Capítulo IV de este Trabajo Especial de Grado, se obtuvo como producto otra actualización en el Documento de Análisis de Riesgo y al mismo tiempo se ejecutaron las siguientes mejoras necesarias al SGSI:

- ✓ Agregar el Campo de Cédula de los empleados a las Tablas de Activo del Sistema de Gestión de Activos.
- ✓ Bloquear puertos 2210 y 2211 en la red LAN de la OTI para impedir descubrimiento de la red con el software The Dude.
- ✓ Fortalecer las contraseñas de acceso a los equipos de conmutación y enrutamiento de la OTI.

# CAPÍTULO VI. Conclusiones y Recomendaciones

Gracias a este Trabajo Especial de Grado y en base a los conocimientos y experiencias adquiridas durante su elaboración se procede a señalar lo siguiente:

## VI.1 Conclusiones

### Conceptualizaciones y funcionalidades relacionadas a un Sistema de Gestión de Seguridad de la Información (SGSI)

Los activos de una organización en sus distintas formas se enfrentan a una gran cantidad de amenazas y vulnerabilidades, por lo que necesitan estar protegidos de la mejor manera en cuanto a confidencialidad, integridad y disponibilidad de los mismos.

Para prevenir o minimizar los riesgos a los que se somete la información en las organizaciones, fue necesario aplicar medidas y políticas de seguridad mediante la Implementación de un Sistema de Gestión de Seguridad de la Información, ya que este se encarga de analizar en detalle la situación actual de los activos en la institución y los riesgos a los que se ven sometidos, del mismo modo define procesos, procedimientos y normativas de trabajo, así como también revisan y evalúan la efectividad y cumplimiento del mismo. Además, como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

### Diagnóstico de la Situación Actual

Para implementar un SGSI, es importante definir los objetivos y alcance que tomara el sistema con el fin de implementarlo de una manera efectiva y dentro del

tiempo estimado, una vez definido esto, es primordial conocer el trabajo que se realiza en todas las áreas dentro del alcance y diagnosticar la situación actual que presentan los activos, esto con el fin de tener una idea global en cuanto a sus condiciones referente a seguridad de la información y la infraestructura que presentan dentro de la organización.

**Analizar los riesgos y vulnerabilidades que enfrenta la información en la organización.**

Diagnosticar la situación actual no es suficiente para seleccionar los controles de seguridad a implementar de una manera efectiva, por lo que es necesario la elaboración de un análisis de riesgos, evaluando el nivel de riesgo, la probabilidad de ocurrencia de que se materialice una amenaza y el impacto que tendría esto sobre los activos, pudiendo visualizar las amenazas más fuertes y débiles a las que se someten los activos dentro de la organización.

En cuanto a la selección de controles es importante conjugar los resultados obtenidos del análisis de riesgos y la experiencia de la gerencia o los funcionarios implicados, con el fin de aceptar aquellas amenazas con el menor nivel de riesgo e impacto sobre los activos y de tal forma, seleccionar los controles más efectivos que mitiguen las amenazas más peligrosas que en el caso de materializarse afecte severamente a la institución.

**Identificación de controles necesarios para la implementación del SGSI en la OTI.**

La Declaración de Aplicabilidad, es un documento que quedará en el INAC para la Gerencia de la OTI, y que servirá como guía para el monitoreo de los controles que ya han sido implementados y al mismo tiempo ayudará a organizar las políticas y mecanismos que se vayan a implantar en un futuro, bien sea dentro de la OTI o en cualquiera de los otros departamentos de la organización.

**Aplicación de Políticas de Seguridad en la OTI**

En la OTI, se implementaron diferentes políticas de seguridad, entre las cuales se pueden mencionar la Política de Seguridad de la Información, la Política de Gestión de Activos y la Política de Control de Accesos.

Cada una de estas políticas es un documento independiente que forma parte del SGSI y que quedará en el INAC para brindar las especificaciones necesarias para garantizar la seguridad y la protección de la información.

**Desarrollo de los controles identificados bajo el estándar ISO 27002.**

Entre los mecanismos que se desarrollaron en la práctica, se puede mencionar el Sistema de Gestión de Activos, que permite almacenar toda la información referente a los activos y al personal del INAC en una Base de Datos, con la cual se puede generar el Inventario de Activos de Información y al mismo tiempo mostrar informes o consultas relacionados a los mismos.

En materia de control de accesos, se aplicó la función de Port Security en los switches Cisco que controlan el acceso de los usuarios a la red LAN y se implementó la asignación direcciones IP específicas en el servidor DHCP de acuerdo a una lista que contiene todas las direcciones MAC de cada funcionario de la OTI y también se realizó un bloqueo de puertos vulnerables utilizados por virus y software malicioso. Todos estos mecanismos ayudan a mitigar amenazas de Ataques de Penetración de la red, descubrimiento, divulgación o destrucción de la Información y ataques DoS.

**Pruebas de implementación del SGSI**

Entre las pruebas realizadas se pueden mencionar el acceso a la red LAN con una PC no autorizada, el escaneo de puertos vulnerables, la verificación del tiempo de descifrado de las contraseñas de acceso a la red y los equipos informáticos, y el Ataque de Penetración a la red LAN.

Las pruebas de seguridad aportaron resultados importantes, que ayudaron a verificar el funcionamiento de los controles implementados y al mismo tiempo a conocer nuevas vulnerabilidades que pueden ser tratados mediante el proceso de mejoramiento continuo o la implementación futura de nuevos controles de seguridad en el INAC.

Es importante destacar que mediante la implementación de un sistema de gestión de seguridad de la información, no es posible eliminar las amenazas en su totalidad, sin embargo, se reducen significativamente controlando el riesgo, para generar seguridad, confianza, aportando veracidad y calidad de la información que se está tratando.

## VI.2 Recomendaciones

Con relación a la implementación de un SGSI, los resultados obtenidos en cada una de las fases de este Trabajo Especial de Grado y a las directrices y especificaciones contenidas en la norma ISO 27002 y en la Metodología de Gestión de Riesgos MAGERIT versión 3, se hacen las siguientes recomendaciones:

- Ampliar el entorno en donde se ejecutarán los controles de seguridad de la información, dependiendo de los requerimientos de la organización, MAGERIT versión 3 recomienda que se vaya ampliando paulatinamente el SGSI hacia los demás Departamento de la empresa.
- Realizar de forma periódica el proceso de Análisis de Riesgos a fin de determinar las modificaciones en las valoraciones e impactos de las amenazas existentes y al mismo tiempo identificar nuevas vulnerabilidades que hayan surgido con el tiempo.
- Se recomienda mejorar algunos aspectos de la infraestructura de los cuartos de cableado, tales como refrigeración, ubicación y control de acceso, garantizando únicamente el ingreso de personal autorizado a través de Tarjetas de Proximidad o Sistemas Biométricos.

- Se recomienda implementar el resto de los controles aplicables para la Oficina de Tecnología de la Información en el INAC, ya que esto permitirá incrementar los niveles de seguridad de la información.

# Bibliografía

Alarcón Fernández, V. (2006). *Desarrollo de Sistemas de Información.* Barcelona, España.

Areitio Bertolín, J. (2008). *Seguridad de la Información: Redes, Informática y Sistemas de Información.* Madrid, España: Paraninfo.

Areitio, J. (2008). *Seguridad de la Información: Redes, Informática y Sistemas de Información.* Madrid, España: Paraninfo.

Cao, J. (2007). *Guía para la elaboración del marco normativo de un sistema de gestión de seguridad de la información (SGSI).*

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

INAC. (2013). *Instituto Nacional de Aeronáutica Civil*. Obtenido de www.inac.gob.ve

Instituto Nacional de Tecnologías de la Comunicación. (29 de Mayo de 2014). Obtenido de www.inteco.es

ISO/IEC 13335-1. (2004). *Information technology - Security techniques - Management of information and communications technology secutiry - Part 1: Concepts and models for information and communications.*

ISO/IEC 27001. (2005). *Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de seguridad de la información.*

ISO/IEC 27002. (2007). *Tecnología de la información. Técnicas de seguridad. Código de prácticas para la gestión de la seguridad de la información.*

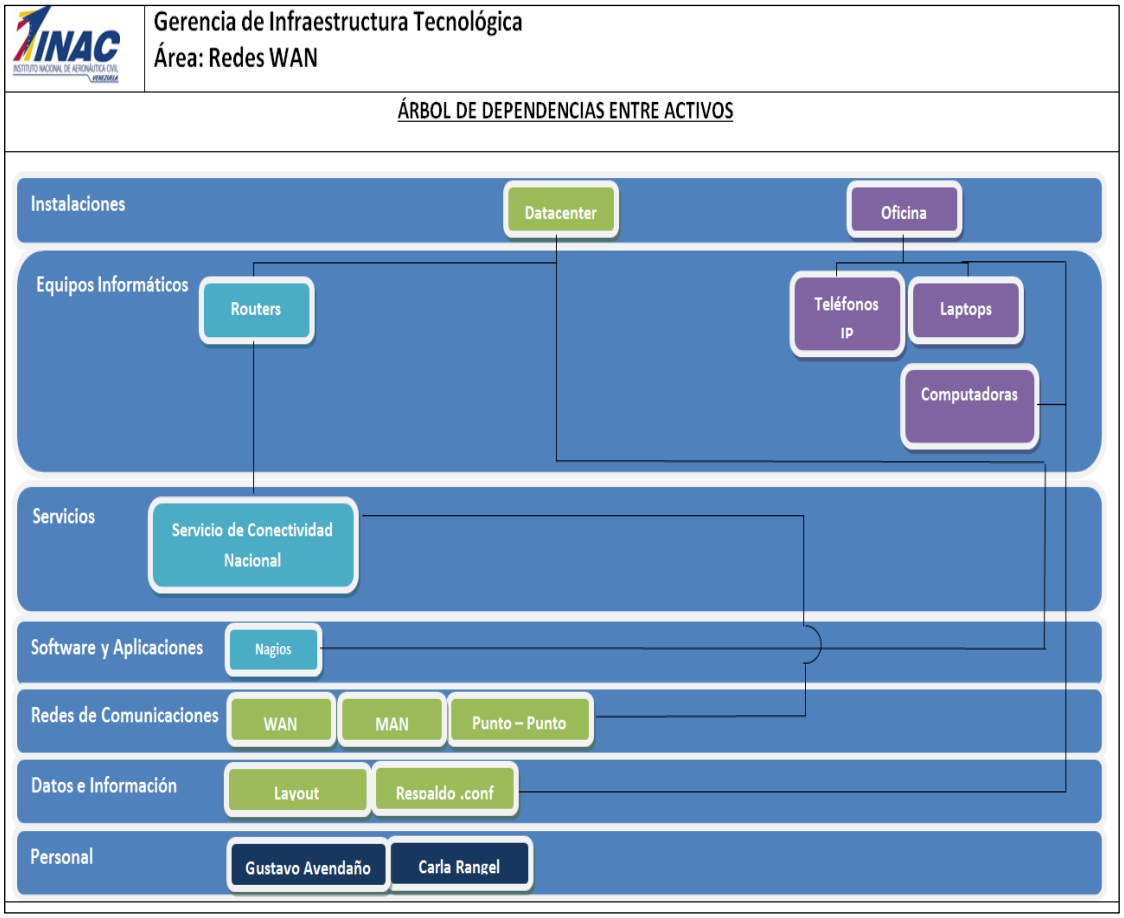
UNE 71504. (2008). *Metodología de análisis y gestión de riesgos para los sistemas de información.* Madrid: AENOR.

.

# APÉNDICES

## Apéndice A

### Árbol de Dependencias




**Nota: Por razones de seguridad y confidencialidad de la información, la institución se reserva el contenido de este documento.**

# Apéndice B

## Documento del Diagnóstico de la Situación Actual

**Instituto Nacional de Aeronáutica Civil**

**Oficina de Tecnología de la Información**

# Implementación de un Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Aeronáutica Civil (INAC)

# Diagnóstico de Situación Actual en la Oficina de Tecnología de la Información

**Realizado por:**

Marichal Xavier

Nieto Jinead

**Tutor Empresarial:**

Ing. Jhoan Guillen

**FEBRERO, 2014**

# INTRODUCCIÓN

La información es un activo muy importante para cualquier organización y en consecuencia debe estar protegida de la mejor manera, a medida que una institución se desarrolla la información se enfrenta a grandes cantidades de amenazas y vulnerabilidades que si llegan a materializarse causarían impactos negativos, afectando los procesos operacionales y administrativos de la organización, en prevención a ello es importante implementar un sistema que garantice la confidencialidad, integridad y disponibilidad de la información.

La Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) establece un completo plan de acciones que ayudará al Instituto, específicamente a la Oficina de Tecnología de la Información (OTI) a solucionar problemas de seguridad, técnicos, organizativos y legislativos que enfrenta la organización. Para realizar dicha implementación se adoptó el modelo PDCA (Planificar, Hacer, Verificar y Actuar), en donde a la planificación se refiere, se deben estructurar los objetivos y alcance del proyecto siendo este último la OTI de la Torre Británica, además de diagnosticar la situación que actualmente presentan todas las unidades de la oficina.

En función de formalizar un diagnóstico se realizó un levantamiento de información entrevistando a los trabajadores de cada unidad, respondiendo a un cuestionario orientado al área. Una vez culminado esta recolección de información se hicieron visibles las vulnerabilidades que presentan los activos en todas sus formas con respecto a la seguridad de la información. En definitiva este documento pretende evidenciar la situación actual de la Oficina de Tecnología de la Información en cuanto a seguridad se refiere.

**Nota: Por confidencialidad de la información, la institución se reserva el contenido de este documento.**

# Apéndice C

## Documento Valoración de Activos

| ACTIVOS | DISPONIBILIDAD | INTEGRIDAD | CONFIDENCIALIDAD | TASACIÓN |
|---|---|---|---|---|
| **INSTALACIONES** | | | | |
| Oficina | 2 | 2 | 2 | 6 |
| Depósito | 3 | 3 | 2 | 8 |
| **EQUIPOS INFORMÁTICOS** | | | | |
| Antenas WiFi | 3 | 4 | 4 | 11 |
| Switches | 4 | 5 | 5 | 14 |
| Antenas Almacenadas | 2 | 2 | 2 | 6 |
| Antenas Punto - Punto | 2 | 2 | 4 | 8 |
| Laptops | 2 | 2 | 4 | 8 |
| Computadoras | 2 | 2 | 4 | 8 |
| Teléfonos IP | 2 | 2 | 2 | 6 |
| Kit de Herramientas | 4 | 3 | 1 | 8 |
| **SERVICIOS** | | | | |
| Conectividad Inalámbrica | 4 | 4 | 5 | 13 |
| Conexión a Red Remota | 5 | 5 | 5 | 15 |
| Red Punto - Punto | 5 | 5 | 5 | 15 |
| **SOFTWARE Y APLICACIONES** | | | | |
| Nagios | 4 | 4 | 5 | 13 |
| **REDES DE COMUNICACIONES** | | | | |
| Red Inalámbrica (WiFi) | 4 | 4 | 5 | 13 |
| Enlaces Punto - Punto | 5 | 5 | 5 | 15 |
| **DATOS E INFORMACIÓN** | | | | |
| Datos técnicos de Antenas | 3 | 4 | 2 | 9 |
| Hoja de servicios | 2 | 3 | 2 | 7 |
| **PERSONAL** | | | | |
| Richard Mora, Maikel Espinoza, Ernesto Chávez | 4 | 4 | 5 | 13 |

**Nota: Por razones de seguridad y confidencialidad de la información, la institución se reserva el resto del contenido de este documento.**

# Apéndice D

## Matriz Valoración de Amenazas y Vulnerabilidades

| GERENCIA | INFRAESTRUCTURA TECNOLÓGICA | | | | | | | | SISTEMAS DE INFORMACIÓN | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **VULNERABILIDADES** | **Servidores** | **Redes LAN** | **Redes WAN** | **Redes WLAN** | **Telefonía Móvil** | **Telefonía IP** | **Seguridad de Datos** | **Soporte Técnico** | **Requerimientos** | **Base de Datos** | **Desarrollo** | **AMENAZAS** |
| Falta de mantenimiento de los activos | 2 | 4 | 4 | 3 | 2 | 2 | 3 | 2 | 1 | 3 | 2 | **AVERÍA DE ORIGEN FÍSICO** |
| Inexistencia de políticas de uso adecuado del activo | 5 | 5 | 5 | 4 | 2 | 1 | 4 | 4 | 3 | 4 | 4 | |
| Sistema No supervisado | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 2 | 2 | 1 | |
| Ausencia de procedimientos para instalación y mantenimiento del activo | 4 | 4 | 4 | 3 | 2 | 1 | 3 | 3 | 2 | 3 | 3 | |
| Vulnerabilidades colocadas deliberadamente | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | |
| Control de cambios deficientes | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
| **Valor de la Amenaza por Unidad** | **2,50** | **2,83** | **2,83** | **2,50** | **1,67** | **1,33** | **2,33** | **2,50** | **1,83** | **2,50** | **2,17** | |
| **Probabilidad de Ocurrencia** | **0,5** | **0,57** | **0,57** | **0,5** | **0,33** | **0,27** | **0,47** | **0,5** | **0,37** | **0,5** | **0,43** | |

**Nota: Por razones de seguridad y confidencialidad de la información, la institución se reserva el resto del contenido de este documento.**

# Apéndice E

## Matriz Análisis de Riesgos

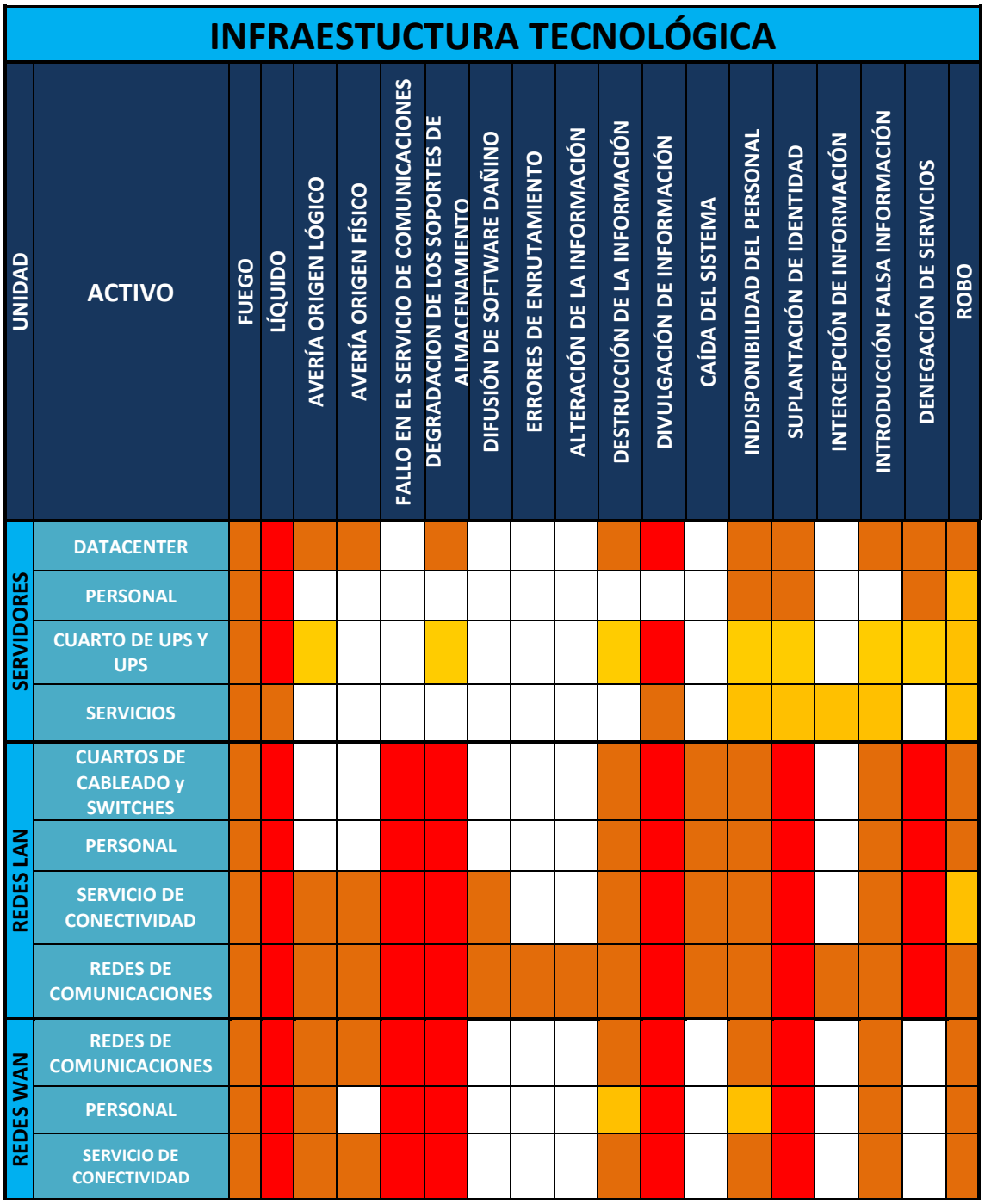
IMPACTO Y NIVEL DE RIESGO DE AMENAZAS SOBRE ACTIVOS EN SERVIDORES

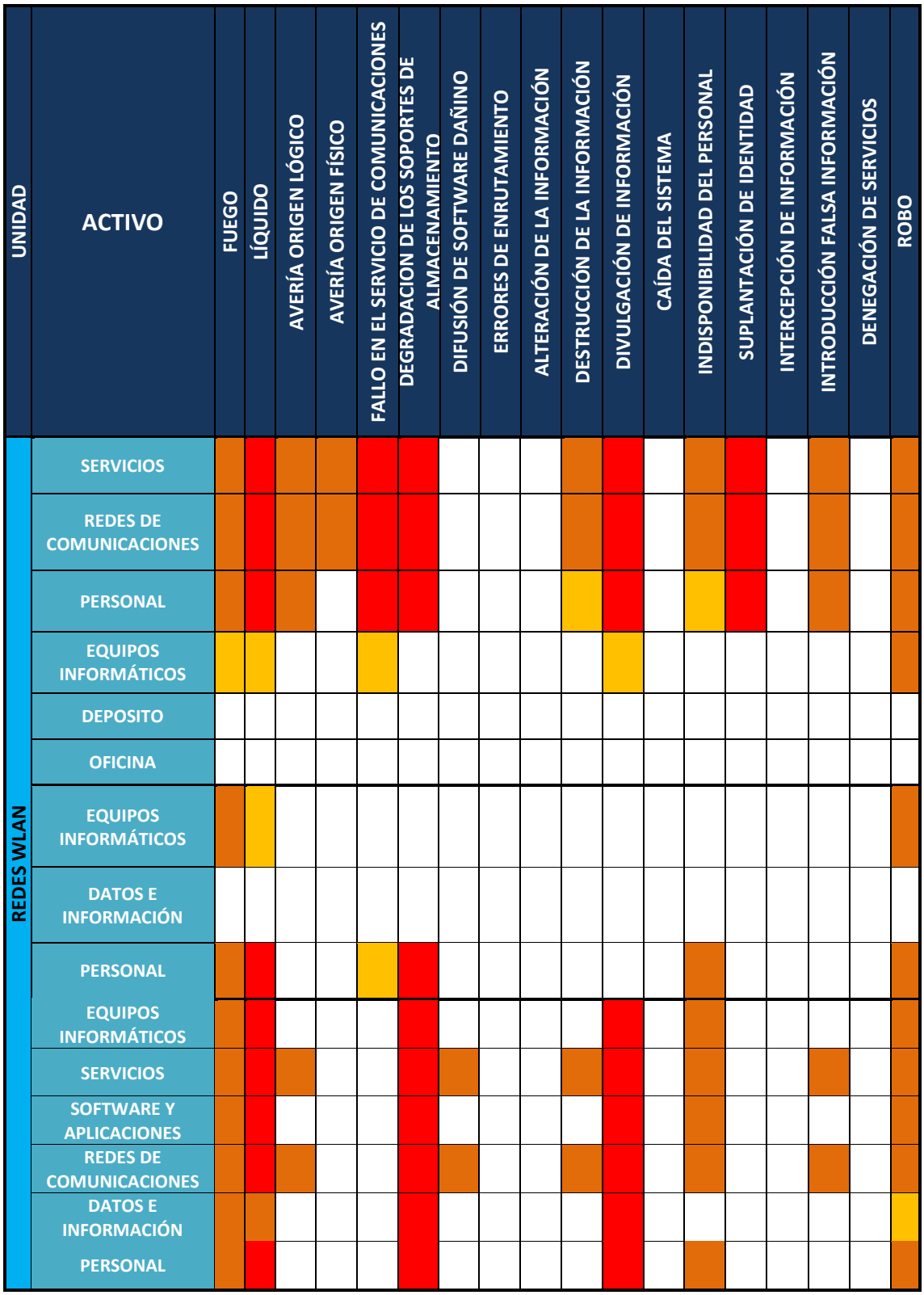
| ACTIVOS | TASACIÓN | FUEGO | LÍQUIDOS | AVERÍA DE ORIGEN FÍSICO | AVERÍA DE ORIGEN LÓGICO | FALLO DE SERVICIOS DE COMUNICACIONES | DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE LA INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE INDENTIDAD DEL USUARIO | INTERCEPCIÓN DE INFORMACIÓN (ESCUCHA) | INTRODUCCIÓN DE FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIO | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Probabilidad de Ocurrencia** | | 0,63 | 0,67 | 0,5 | 0,6 | 0,4 | 0,55 | 0,48 | 0,4 | 0,46 | 0,5 | 0,7 | 0,43 | 1 | 0,6 | 0,4 | 0,6 | 0,6 | 0,6 |
| **INSTALACIONES** | | | | | | | | | | | | | | | | | | | |
| Datacenter | 15 | 3,14 | 3,33 | 2,5 | 2,9 | 2,1 | 2,75 | 2,38 | 1,8 | 2,29 | 2,7 | 3,3 | 2,43 | 3 | 3 | 2 | 2,8 | 3 | 2,8 |
| **Impacto** | | 47,1 | 50 | 38 | 43 | 32 | 41,25 | 35,7 | 27 | 34,4 | 40 | 50 | 36,5 | 45 | 45 | 30 | 42 | 45 | 42 |
| **Impacto de** | | **4** | **4** | **3** | **3** | **3** | **3** | **3** | **2** | **3** | **3** | **4** | **3** | **3** | **3** | **2** | **3** | **3** | **3** |
| **Nivel de Riesgo** | | **4** | **5** | **4** | **4** | **1** | **4** | **1** | **1** | **1** | **4** | **5** | **1** | **4** | **4** | **1** | **4** | **4** | **4** |
| Oficina | 6 | 3,14 | 3,33 | 2,5 | 2,9 | 2,1 | 2,75 | 2,38 | 1,8 | 2,29 | 2,7 | 3,3 | 2,43 | 3 | 3 | 2 | 2,8 | 3 | 2,8 |
| **Impacto** | | 18,8 | 20 | 15 | 17 | 13 | 16,5 | 14,3 | 11 | 13,7 | 16 | 20 | 14,6 | 18 | 18 | 12 | 17 | 18 | 17 |
| **Impacto de** | | **2** | **2** | **2** | **2** | **1** | **2** | **1** | **1** | **1** | **2** | **2** | **1** | **2** | **2** | **1** | **2** | **2** | **2** |
| **Nivel de Riesgo** | | **2** | **2** | **1** | **2** | **1** | **2** | **1** | **1** | **1** | **2** | **2** | **1** | **2** | **2** | **1** | **2** | **2** | **2** |
| Cuarto de UPS | 12 | 3,14 | 3,33 | 2,5 | 2,9 | 2,1 | 2,75 | 2,38 | 1,8 | 2,29 | 2,7 | 3,3 | 2,43 | 3 | 3 | 2 | 2,8 | 3 | 2,8 |
| **Impacto** | | 37,7 | 40 | 30 | 34 | 26 | 33 | 28,6 | 22 | 27,5 | 32 | 40 | 29,2 | 36 | 36 | 24 | 34 | 36 | 34 |
| **Impacto de** | | **3** | **3** | **2** | **3** | **2** | **3** | **2** | **2** | **2** | **3** | **3** | **2** | **3** | **3** | **2** | **3** | **3** | **3** |
| **Nivel de Riesgo** | | **4** | **5** | **1** | **2** | **1** | **2** | **1** | **1** | **1** | **2** | **5** | **1** | **2** | **2** | **1** | **2** | **2** | **2** |
| **EQUIPOS INFORMÁTICOS** | | | | | | | | | | | | | | | | | | | |
| UPS | 12 | 3,14 | 3,33 | 2,5 | 2,9 | 2,1 | 2,75 | 2,38 | 1,8 | 2,29 | 2,7 | 3,3 | 2,43 | 3 | 3 | 2 | 2,8 | 3 | 2,8 |
| **Impacto** | | 37,7 | 40 | 30 | 34 | 26 | 33 | 28,6 | 22 | 27,5 | 32 | 40 | 29,2 | 36 | 36 | 24 | 34 | 36 | 34 |
| **Impacto de** | | **3** | **3** | **2** | **3** | **2** | **3** | **2** | **2** | **2** | **3** | **3** | **2** | **3** | **3** | **2** | **3** | **3** | **3** |
| **Nivel de Riesgo** | | **4** | **5** | **1** | **2** | **1** | **2** | **1** | **1** | **1** | **2** | **5** | **1** | **2** | **2** | **1** | **2** | **2** | **2** |
| NetApp | 13 | 3,14 | 3,33 | 2,5 | 2,9 | 2,1 | 2,75 | 2,38 | 1,8 | 2,29 | 2,7 | 3,3 | 2,43 | 3 | 3 | 2 | 2,8 | 3 | 2,8 |
| **Impacto** | | 40,8 | 43,3 | 33 | 37 | 28 | 35,75 | 30,9 | 23 | 29,8 | 35 | 43 | 31,6 | 39 | 39 | 26 | 36 | 39 | 36 |
| **Impacto de** | | **3** | **3** | **3** | **3** | **2** | **3** | **3** | **2** | **2** | **3** | **3** | **3** | **3** | **3** | **2** | **3** | **3** | **3** |
| **Nivel de Riesgo** | | **4** | **5** | **1** | **2** | **1** | **2** | **1** | **1** | **1** | **2** | **5** | **1** | **4** | **4** | **1** | **2** | **4** | **2** |
| Overland | 11 | 3,14 | 3,33 | 2,5 | 2,9 | 2,1 | 2,75 | 2,38 | 1,8 | 2,29 | 2,7 | 3,3 | 2,43 | 3 | 3 | 2 | 2,8 | 3 | 2,8 |
| **Impacto** | | 34,5 | 36,6 | 28 | 31 | 24 | 30,25 | 26,2 | 20 | 25,2 | 29 | 37 | 26,7 | 33 | 33 | 22 | 31 | 33 | 31 |
| **Impacto de** | | **3** | **3** | **2** | **3** | **2** | **3** | **2** | **2** | **2** | **2** | **3** | **2** | **3** | **3** | **2** | **3** | **3** | **3** |
| **Nivel de Riesgo** | | **2** | **2** | **1** | **2** | **1** | **2** | **1** | **1** | **1** | **2** | **2** | **1** | **2** | **2** | **1** | **2** | **2** | **2** |

**Nota: Por razones de seguridad y confidencialidad de la información, la institución se reserva el resto del contenido de este documento.**

# Apéndice F

## Resumen del Análisis de Riesgos




UNIDAD
ACTIVO
FUEGO
LÍQUIDO
AVERÍA ORIGEN LÓGICO
AVERÍA ORIGEN FÍSICO
FALLO EN EL SERVICIO DE COMUNICACIONES
DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO
DIFUSIÓN DE SOFTWARE DAÑINO
ERRORES DE ENRUTAMIENTO
ALTERACIÓN DE LA INFORMACIÓN
DESTRUCCIÓN DE LA INFORMACIÓN
DIVULGACIÓN DE INFORMACIÓN
CAÍDA DEL SISTEMA
INDISPONIBILIDAD DEL PERSONAL
SUPLANTACIÓN DE IDENTIDAD
INTERCEPCIÓN DE INFORMACIÓN
INTRODUCCIÓN FALSA INFORMACIÓN
DENEGACIÓN DE SERVICIOS
ROBO
REDES WLAN
SERVICIOS
REDES DE COMUNICACIONES
PERSONAL
EQUIPOS INFORMÁTICOS
DEPOSITO
OFICINA
EQUIPOS INFORMÁTICOS
DATOS E INFORMACIÓN
PERSONAL
EQUIPOS INFORMÁTICOS
SERVICIOS
SOFTWARE Y APLICACIONES
REDES DE COMUNICACIONES
DATOS E INFORMACIÓN
PERSONAL

| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SOPORTE TÉCNICO | OFICINA | | | | | | | | | | | | | | | | | | |
| | COMPUTADORAS , LAPTOPS | | | | | | | | | | | | | | | | | | |
| | SERVICIOS | | | | | | | | | | | | | | | | | | |
| | SOFTWARE Y APLICACIONES | | | | | | | | | | | | | | | | | | |
| | DATOS E INFORMACIÓN | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |

| SISTEMAS DE INFORMACIÓN | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
| REQUERIMIENTOS | OFICINA | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE RESTABLECIMIENTO DE CLAVES | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE GESTIÓN ADMINISTRATIVA | | | | | | | | | | | | | | | | | | |
| | SIGESP Y LOTUS | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |
| BASE DE DATOS | OFICINA | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE PRIVILEGIOS Y SOPORTE DE USUARIOS | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE GESTIÓN | | | | | | | | | | | | | | | | | | |
| | SOFTWARE Y APLICACIONES | | | | | | | | | | | | | | | | | | |
| | BASES DE DATOS | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |

| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DESARROLLO | OFICINA | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE INTRANET | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE SOPORTES DEL SISTEMA | | | | | | | | | | | | | | | | | | |
| | JOOMLA Y APACHE | | | | | | | | | | | | | | | | | | |
| | CÓDIGOS FUENTES | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |

# Apéndice G

## Documento del Análisis de Riesgos

**Instituto Nacional de Aeronáutica Civil**

**Oficina de Tecnología de la Información**

# Implementación de un Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Aeronáutica Civil (INAC)

# Documento de Análisis de Riesgos

**Realizado por:**

Marichal Xavier

Nieto Jinead

**Tutor Empresarial:**

Ing. Jhoan Guillen

**ABRIL, 2014**

# INTRODUCCIÓN

La información es un activo muy importante para cualquier organización y en consecuencia debe estar protegida de la mejor manera, a medida que una institución se desarrolla la información se enfrenta a grandes cantidades de amenazas y vulnerabilidades que si llegan a materializarse causarían impactos negativos, afectando los procesos operacionales y administrativos de la organización, en prevención a ello es importante implementar un sistema tomando tres parámetros fundamentales, la confidencialidad, integridad y disponibilidad de la información.

La Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) establece un completo plan de acciones que ayudará al Instituto, específicamente a la Oficina de Tecnología de la Información (OTI) a solucionar problemas de seguridad, técnicos, organizativos y legislativos que enfrenta la organización. Para realizar dicha implementación se adoptó el modelo PDCA (Planificar, Hacer, Verificar y Actuar), en donde a la planificación se refiere, se deben estructurar los objetivos y alcance del proyecto siendo este último la OTI de la Torre Británica, además de diagnosticar la situación que actualmente presentan todas las unidades de la oficina.

El Análisis de Riesgo corresponde a una de las actividades de la Fase de Hacer en la implementación del SGSI y constituye un proceso en el cual se realiza un estudio a cada una de las amenazas y vulnerabilidades existentes en la organización para determinar sus niveles de riesgo y los posibles impactos que pueden generarse sobre los activos de información.

**Nota: Por razones de seguridad y confidencialidad de la información, la institución se reserva el contenido de este documento.**

# Apéndice H

## Declaración de Aplicabilidad

| Control | Descripción | Control Actual | Implementación |
|---|---|---|---|
| 5.1.1 Documento de Política de Seguridad de la Información. | Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. | Política de Seguridad de la Información. | **Documentación**<br>• Mejoras en la Política de Seguridad de l**a** Información. |
| 5.1.2 Revisión de la política de Seguridad de la Información. | La política de seguridad de la información debe revisarse a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y eficacia continúa. | Política de Seguridad de la Información | **Documentación**<br>• Se describirá dentro del Documento de la Política de Seguridad de la Información la revisión y evaluación de oportunidades para la mejora de la política. |
| 7.1.1 Inventario de Activos | Se deben identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes. | Inexistente | **Documentación**<br>• Política de Gestión de Activos<br>• Inventario de activos<br>• Procedimiento para la Gestión de Activos<br>**Mecanismos**<br>• Sistema para la gestión de activos en Access<br>• Formulario para el registro de activos |
| 7.1.2 Propiedad de los Activos | Toda información y activos asociados con los recursos de procesamiento de la información deben tener un propietario, responsable y *custodio por parte designada de la organización.* | Inexistente | **Documentación**<br>• Política de Gestión de Activos<br>**Mecanismos**<br>• Sistema para la gestión de activos en Access<br>• Formulario para el registro de activos |

| Control | Descripción | Control Actual | Implementación |
|---|---|---|---|
| 7.1.3 Utilización Aceptable de los Activos | Deben identificarse, documentarse e implementarse las reglas para la utilización aceptable de la información y de los activos asociados con los recursos de procesamiento de la información. | Inexistente | **Documentación**<br>• Política de Gestión de Activos |
| 8.3.2 Devolución de los Activo. | Todos los usuarios empleados, contratistas y terceras personas debieran devolver todos los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo. | Inexistente | **Documentación**<br>• Debe reflejarse en la política de gestión de activos, la devolución de todos los software, documentos corporativos, dispositivos móviles, tarjetas de acceso, manuales y la información almacenada en otros medios electrónicos ya sean de la organización o equipos personales, de igual forma se debe devolver a la institución en la terminación de un empleo.<br>**Mecanismos**<br>• Sistema de Gestión de Activos<br>• Compromiso de cumplimiento de la Política y Normativa de Seguridad de la Información |
| 8.3.3 Retiro de los derechos de Acceso | Los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información debieran ser retirados a la terminación de su empleo, contrato o acuerdo, o debieran ser reajustados de acuerdo al cambio. | Inexistente | **Documentación**<br>• Debe reflejarse en la Política de Control de Accesos, la cancelación de todos sus accesos o si son nuevos derechos de acceso ya sean físicos o lógicos, claves, tarjetas de proximidad, suscripciones entre otros, al culminar o cambiar un empleo.<br>**Mecanismos**<br>• Retirar los accesos que no fueron aprobados para el nuevo empleo |

| Control | Descripción | Control Actual | Implementación |
|---|---|---|---|
| 9.1.1 Perímetros de Seguridad Física | Los perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) deberían utilizarse para proteger las áreas que contienen información y medios de procesamiento de información. | Tarjeta de Proximidad | **Documentación**<br>• Normativa de Perímetro de Seguridad Física para el Datacenter.<br>• Normativa de Perímetro de Seguridad Física para Cuartos de Cableado<br>**Mecanismos**<br>• Norma ANSI/TIA/EIA-570-A (Infraestructura de Cuartos de Cableado de Telecomunicaciones)<br>• Norma ANSI/EIA/TIA- 942 (Infraestructura de Telecomunicaciones para Data Center) |
| 9.1.2 Controles Físicos de Entrada | Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado. | 1. Tarjeta de Proximidad<br>2. Circuito Cerrado de Cámaras | **Documentación**<br>• Política de Control de Accesos<br>**Mecanismos**<br>• Tarjeta de Proximidad<br>• Vigilancia por parte de Seguridad<br>• Monitoreo mediante circuito cerrado de cámaras |
| 9.1.3 Seguridad de Oficinas, Habitaciones e Instalaciones. | Debería diseñare y aplicarse la seguridad física para las oficinas, habitaciones e instalaciones. | Inexistente | **Documentación**<br>• Procedimiento de acuerdo a las normas de salud y seguridad pertinentes. |
| 9.2.3 Seguridad del Cableado | El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño. | Inexistente | **Documentación**<br>• Normativa para la Seguridad del Cableado en cuanto a las Líneas de Energía y de Telecomunicaciones, la Intercepción No Autorizada.<br>• Una Lista de las conexiones y Etiquetados de Cables y Equipos para reducir errores.<br>**Mecanismos**<br>• TIA/EIA 568-B1<br>• ANSI/TIA/EIA-570-A<br>• ANSI/TIA/EIA-607<br>• ANSI/TIA/EIA-606-A |
| 10.1.2 Gestión de Cambio | Se debieran controlar los cambios en los medios y sistemas de procesamiento de la información. | Inexistente | **Documentación:**<br>• Procedimiento para el Control de Cambios<br>**Mecanismos**<br>• Planilla para la Gestión de Cambios |

| Control | Descripción | Control Actual | Implementación |
|---|---|---|---|
| 10.6.2 Seguridad de Servicios de Red | En todo contrato de redes se debieran identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente. | Inexistente | **Documentación**<br>• Normativa de Seguridad de Servicios de Red<br>**Mecanismos**<br>• Port Security<br>• Cifrado de la Información de Configuración de los equipos (Switches, Routers, Servidores).<br>• Firewalls<br>• Cifrado de la Información que viaja a través de la red.<br>• Bloqueo de Puertos Innecesarios |
| 11.1.1 Política Control de Accesos | Se debiera establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso. | Inexistente | **Documentación**<br>• Política de Control de Accesos<br>• Normativa de Control de Acceso Físico<br>**Mecanismos**<br>• Tarjeta de Proximidad<br>• Vigilancia por parte de Seguridad<br>• Monitoreo mediante circuito cerrado de cámaras |
| 11.2.2 Gestión de Privilegios | Se debiera restringir y controlar la asignación y uso de privilegios. | Se deben realizar mejoras | **Documentación**<br>• Política de Control de Accesos (11.1.1) |
| 11.2.3 Gestión de Contraseñas de Usuarios | Debería controlarse la asignación de contraseñas a través de un proceso de gestión formal | Se deben realizar mejoras | **Documentación**<br>• Política de Control de Accesos (11.1.1) |
| 11.3.3 Políticas de Escritorios y Pantallas Limpias. | Para los recursos de procesamiento de la información, debería adoptarse una política de escritorios limpios de papel y de dispositivos de almacenamiento removibles y una política de pantallas limpias. | Inexistente | **Mecanismos**<br>• Compromiso de cumplimiento de la Política y Normativa de Seguridad de la Información. |

| Control | Descripción | Control Actual | Implementación |
|---|---|---|---|
| 11.4.4 Protección del Diagnóstico Remoto y de la Configuración del Puerto. | Se debiera controlar el acceso físico y lógico a los puertos de diagnóstico y configuración. | Inexistente | **Documentación**<br>• Debe reflejarse en la Política de Control de Accesos, para la gestión, diagnóstico y configuración de Puertos.<br>**Mecanismos**<br>• Port Security<br>• Bloqueo de Puertos Lógicos |
| 11.6.1 Restricción de Acceso a la Información | El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debiera limitarse en concordancia con la política de control de acceso definida. | Se deben realizar mejoras | **Documentación**<br>• Política de Control de Acceso Normativa para la restricción de acceso a la información.<br>**Mecanismos**<br>• Gestión de Privilegios<br>• Bloqueo de Contenido Web<br>• Bloqueo de Descargas de Software Potencialmente dañino. |

# Apéndice I

## Política de Seguridad de la Información

## 1. Introducción

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge y la masiva utilización de recursos informáticos (Computadores, impresoras, redes de datos, etc.) como medio para almacenar, transferir y procesar información, se ha incrementado desmesuradamente, al grado de convertirse en un elemento esencial para el funcionamiento de las diferentes instituciones, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Ante este esquema las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales, es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, lo que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

De esta manera, las políticas de seguridad en informática emergen como el instrumento para concientizar a los miembros de las instituciones acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la institución cumplir con su misión.

El proponer estas políticas de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dichas políticas en función del ambiente dinámico que nos rodea.

## 2. Objetivo

Proporcionar a los usuarios un medio de consulta para conocer las normas de seguridad de la información, que deben ser observadas en forma permanente.

## 3. Términos y Definiciones

**Acceso Remoto:** Es una tecnología de redes que permite a los usuarios distantes/externos tener acceso a redes empresariales a través de Internet o servidores de acceso remoto.

**Activo de Información:** Es la información misma en cualquiera de sus formas y modalidades; es decir, impresa, manuscrita, oral, electrónica y visual a la cual la Institución, según sus intereses, le ha atribuido un valor determinado en función a la trascendencia de dicha información

**Administrador del Sistema:** Persona natural o jurídica que configura y mantiene en correcto funcionamiento un sistema.

**Clasificación:** Son diferentes niveles de confidencialidad o criticidad que se asignan a los Activos de Información de acuerdo a su contenido estratégico, valor comercial, valor de reposición, repercusiones legales y su importancia para la continuidad operacional y/o reanudación de las operaciones y que tiene la finalidad determinar el grado de protección requerida.

**Confidencialidad:** Es el compromiso de discreción, que la Institución exige a sus empleados, contratados, terceros y/o relacionados, sobre los conocimientos, procedimientos y documentos que comprenden los activos de información de su propiedad o bajo su custodia.

**Contraseña (Password):** Secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización, expedida a un usuario, para acceder a la data o a la información contenida en un sistema.

**Control**: Mecanismo de seguridad que verifica lo que un usuario puede hacer, una vez que tenga acceso a los datos o recursos del sistema, en base a un determinado perfil.

**Control de Acceso:** Proceso que autoriza y controla quién y cómo se tiene acceso a los datos y a los recursos de un sistema.

**Custodio:** Es la persona designada por el propietario de la información para proteger y almacenar la información de los sistemas y redes de la Institución, según las especificaciones dadas.

**Data (datos):** Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por personas o por medios automáticos.

**Disponibilidad:** Valor que mide el nivel de operatividad de los sistemas informáticos para los usuarios, en un periodo específico.

**Dispositivos Móviles:** Son todos aquellos equipos de computación de uso individual de una persona, tanto en posesión como en operación, suficientemente pequeños para ser transportados y utilizados durante su transporte.

**Información:** significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

**Integridad:** Atributo que garantiza que la información recibida sea exactamente igual a la información transmitida. También garantiza que la información recuperada de un medio de almacenamiento o archivo sea exactamente igual a la información

**Intranet:** Es una infraestructura bien definida y limitada, basada en los estándares y tecnologías de Internet, que soporta el intercambio de información dentro de una organización.

**Políticas de Seguridad:** Es una declaración de intenciones emanadas de la alta dirección de la Institución, que cubre la seguridad de los activos de información y que proporciona las bases para definir y delimitar las responsabilidades que se requieran en las diversas actuaciones técnicas y organizativas.

**Pruebas de Penetración:** Es un conjunto de actividades sistemáticas cuyo objetivo es detectar y alertar sobre posibles fallas de seguridad, que podrían ser utilizadas, por personal interno o externo, para atacar y/o penetrar en un sistema.

**Riesgo:** Es la probabilidad de que ocurra un evento o posible incidente que pudiera ocasionar pérdida o daño al patrimonio de la institución.

**Seguridad:** Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad, que no permitan influencias o actos hostiles específicos, que pudieran propiciar el acceso a la data, de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema.

**Usuario:** Toda persona autorizada para utilizar los activos y servicios de información en base al conocimiento requerido, atendiendo el cargo ejercido dentro de la organización.

## 4 Política de Seguridad

### 4.1 Política de seguridad de la información

#### 4.1.1 Documento de la política de seguridad de la información

Un documento de política de seguridad de la información deberá aprobarse por la dirección, ser publicado y comunicado a todos los empleados y partes externas pertinentes.

#### 4.1.2 Revisión de la política de seguridad de la información

Las actividades de seguridad de la información deberán coordinarse por los representantes de diferentes partes de la organización, con roles y funciones de trabajo pertinentes.

## 5. Gestión de activos

### 5.1 Responsabilidad por los activos

#### 5.1.1 Inventario de activos

Todos los activos deberán identificarse claramente, y elaborarse y mantenerse el inventario de activos.

#### 5.1.2 Propiedad de los activos

Toda información y activos asociados con los recursos de procesamiento de la información deberán tener un responsable, propietario y custodio dentro de la organización.

#### 5.1.3 Utilización aceptable de los activos

Deberán identificarse, documentarse, e implementarse las reglas para la utilización aceptable de la información y de los activos asociados con los recursos de procesamiento de la información.

## 6 Seguridad física y ambiental

### 6.1 Áreas seguras

#### 6.1.1 Perímetro de seguridad física

Los perímetros de seguridad física (barreras tales como paredes, puertas de entrada controladas por tarjetas o puestos de recepción manual) deberán utilizarse para

proteger las áreas que contienen la información y las instalaciones de procesamiento de la información.

### 6.1.2 Controles físicos de entrada

Las áreas de seguridad deberán estar protegidas por controles de entrada apropiados que aseguren el permiso de acceso solo al personal autorizado.

### 6.1.3 Seguridad de Oficinas, Habitaciones e Instalaciones

Se debe diseñar y aplicar la seguridad física para las oficinas y habitaciones, esto incluye la correcta localización de los medios claves para evitar el acceso del público no autorizado.

## 7. Gestión de las comunicaciones y operaciones

### 7.1 Procedimientos y responsabilidades de operación

### 7.1.1 Gestión de cambios

Se debe controlar los cambios en los medios y sistemas de procesamiento de la información mediante un procedimiento formal de Gestión de Cambios de Hardware o Software.

### 7.2 Gestión de seguridad de la red

### 7.2.1 Seguridad de los servicios de la red

En todo contrato de redes se debieran identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas, redes de valor agregado y soluciones de seguridad de red manejadas como

firewalls y sistemas de detección de intrusiones. Estos servicios pueden ir desde una simple banda ancha manejada u ofertas complejas de valor agregado.

## 8. Control de Acceso

### 8.1 Requisitos del negocio para el control de accesos

#### 8.1.1 Política de Control de Acceso

Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

### 8.2 Gestión de accesos de usuarios

#### 8.2.1 Gestión de Privilegios

Los sistemas multi-usuario que requieren protección contra el acceso no autorizado deben controlar la asignación de privilegios a través de un proceso de autorización formal.

#### 8.2.3 Gestión de Contraseñas de Usuarios

La asignación de claves secretas se debiera controlar a través de un proceso de gestión formal.

### 8.3 Control de acceso a las aplicaciones e información

#### 8.3.1 Restricción de Acceso a la Información

El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debe limitarse en concordancia con la política de control de acceso definida.

# Apéndice J

## Política de Gestión de Activos

## 5. Políticas

### 5.1 Inventario de Activos

La Gerencia de Seguridad de la Información deberá crear documentación y mecanismos que permitan mantener un inventario vigente de los activos de información bajo su responsabilidad. Todos los activos deberían identificarse claramente mediante la utilización de un inventario de activos. El inventario debe incluir información relacionada al nombre del activo, descripción, propietario, responsable, custodio, documentación, ubicación, codificación y cualquier otro tipo de información relevante del activo.

La Gerencia de Seguridad de la Información debe revisar el contenido del Inventario de Activos cada cierto tiempo (Se recomienda un lapso de tiempo no mayor a 6 meses) y cumplir con la normativa para el ingreso o salidas de activos de información.

### 5.2 Asignación de Propiedad de los Activos de Información

Toda información y activos asociados al Instituto Nacional de Aeronáutica Civil, deberá tener un propietario, un responsable y un custodio.

- El propietario es el dueño del activo, puede ser un Gerente, encargado o incluso un área o unidad específica.

- El responsable es el encargado o superior inmediato del custodio o la persona que tiene relación directa con el activo. Es el encargado de definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

- El custodio es el funcionario que mantiene el activo en su poder, es responsable de mantener la integridad, disponibilidad y confidencialidad del activo.

## 5.3 Utilización aceptable de los activos

Todo Activo de Información deberá ser protegido, custodiado y resguardado de conformidad con los niveles de clasificación que le fueron asignados, utilizando para ello los métodos y técnicas de seguridad aprobados por el Instituto Nacional de Aeronáutica Civil. Deberían identificarse, documentarse e implementarse las reglas para la utilización aceptable de la información y de los activos asociados con los recursos de procesamiento de la información.

### 5.3.1 Normativa para la Utilización aceptable de los activos

Los activos de información deben ser utilizados, manejados y gestionados de acuerdo a las siguientes normas:

- Cada activo de información debe ser manejado únicamente por el propietario, responsable, custodio o por aquellas personas que tengan autorización para ello.
- Todo activo debe poseer un propietario, un responsable y un custodio.
- Los activos de información no deben ser retirados de las instalaciones del INAC sin previa autorización por parte del propietario o funcionario responsable de dicho activo.
- Los activos correspondientes a equipos informáticos, deben ser manejados y gestionados de acuerdo a los requerimientos y a la normativa para el manejo y mantenimiento de equipos.
- Los activos correspondientes a datos e información, deben ser tratados de acuerdo a la normativa de la clasificación de activos y solo debe compartirse aquella información que sea de uso público, resguardando todos aquellos datos e información confidenciales y de vital importancia para el INAC.
- Las contraseñas, llaves de seguridad, códigos fuentes de software y aplicaciones deben mantenerse bajo estrictos niveles de confidencialidad, evitando materializar amenazas por divulgación de información, robo o destrucción de la misma.

- Los activos relacionados a redes de comunicaciones, deben ser manejados, configurados y gestionados según la Normativa y el procedimiento para el control de las redes, así como también la Política de Seguridad de Servicios de Red.
- Las instalaciones deben seguir las normas relacionados al Perímetro de Seguridad Física.
- El personal debe seguir los reglamentos del instituto en cuanto al manejo de la información, así como velar por el cumplimiento de todas las políticas, normativas y procedimientos descritos anteriormente.

### 5.4 Clasificación de los Activos

Todo Activo de Información perteneciente a, o bajo la custodia, del Instituto Nacional de Aeronáutica Civil, deberá ser clasificado de acuerdo a la normativa de clasificación vigente en materia de Protección de Activos de Información del Instituto.

La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.

### 5.5 Política de Ingresos y Salidas de Activos

Los nuevos activos que ingresen a una unidad específica perteneciente a una Gerencia del INAC o en su defecto los activos de información que estén de salida por motivos de daños físicos o cambios por movilización de activos, deben ser inmediatamente registrados o eliminados respectivamente del Inventario de Activos por la Gerencia de Seguridad de la Información, previo a la aprobación de la Gerencia asociada a dicha unidad, es decir, no se debe esperar el tiempo estimado para la realización del levantamiento de información del inventario de activos.

# Apéndice K

## Inventario de Activos

### Inventario de Activos

| CodigoActivo | Nombre | Clasificacion | Descripcion | Tipo | Gerencia | Unidad | Propietario | Responsable | Custodio | Documentacion | Ubicación_Física |
|---|---|---|---|---|---|---|---|---|---|---|---|
| OTISE001 | Carpetas Compartidas | Confidencial | Permite compartir servicios, información, impresores. | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Victor Fuentes | Check-List | DataCenter, Torre Británica/ Piso 2 |
| OTISE002 | Web | Uso Interno | Permite brindar el servicio de acceso web. | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Jesús Liendo | Inexistente | DataCenter, Torre Británica/ Piso 2 |
| OTISE003 | DHCP | Uso Interno | Permite brindar direccionamiento web de forma dinámica. | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Robert Rangel | Inexistente | DataCenter, Torre Británica/ Piso 2 |
| OTISE004 | DNS | Uso Interno | Brinda resolución de nombre de dominio para direcciones IP asociadas a contenido web o alojado en servidores. | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Robert Rangel | Inexistente | DataCenter, Torre Británica/ Piso 2 |
| OTISE005 | NTP | Estrictamente Confidencial | Protocolo necesario para la sincronización de los relojes | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Robert Rangel | Inexistente | DataCenter, Torre Británica/ Piso 2 |
| OTISE006 | Correo | Uso Interno | Servicio de Mensajería Electrónica | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Victor Fuentes | Inexistente | DataCenter, Torre Británica/ Piso 2 |
| OTISE007 | Dominio | Uso Interno | Red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet. | Servicios | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Victor Fuentes | Inexistente | DataCenter, Torre Británica/ Piso 2 |
| OTISE008 | UPS | Estrictamente Confidencial | Equipo para el respaldo de energía eléctrica. | Equipos Informáticos | Infraestructura Tecnológica | Servidores | OTI - Torre Britanica | Jhoan Gulllen | Robert Rangel | Inexistente | DataCenter, Torre Británica/ Piso 2 |

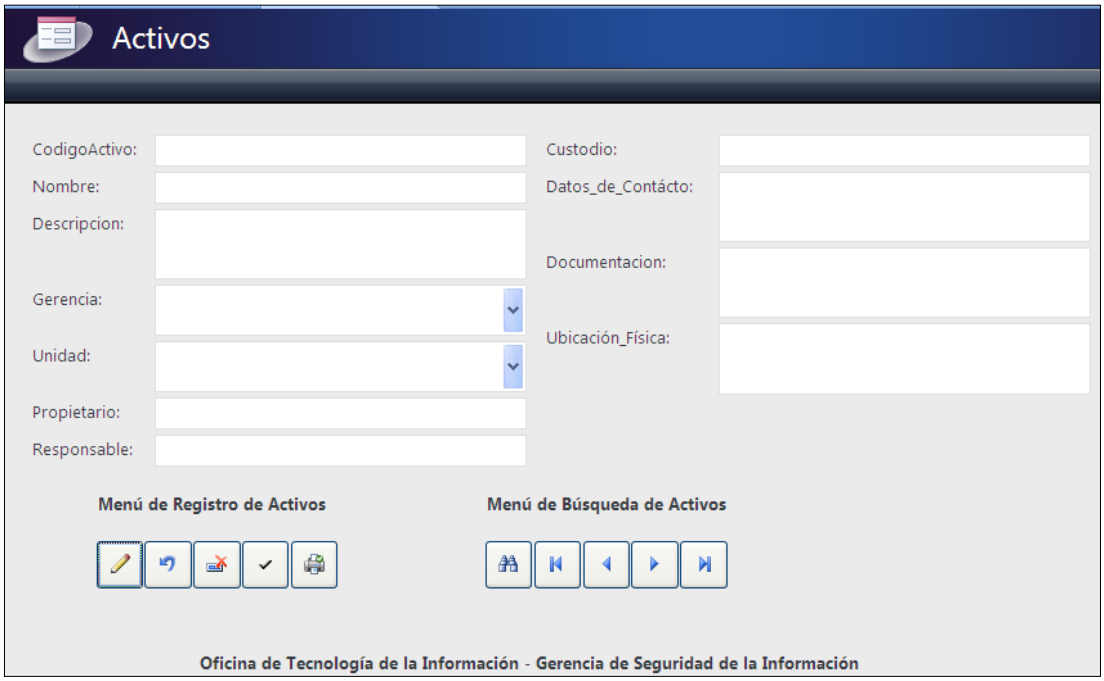
viernes, 04 de julio de 2014 Página 1

Para contactar a un Propietario, Responsable o Custodio de un Activo, ubicar sus datos en el Anexo a este Inventario

**Nota: Por razones de seguridad y confidencialidad de la información, la institución se reserva el contenido de este documento.**

# Apéndice L

## Sistema de Gestión de Activos




# Apéndice M

## Política de Control de Acceso

# 4. Políticas

## 4.1 Política de Perímetro de seguridad física

Todas las áreas que contienen información e instalaciones de procesamiento de la información deben estar protegidas mediante perímetros de seguridad necesarios tales como barreras, paredes, puertas de entrada controladas por tarjeta, o puesto de recepción manual, adicionalmente la seguridad de áreas como Datacenter y los cuartos de cableado deben guiarse mediante las siguientes normas.

### 4.1.1 Normativa de Perímetro de Seguridad Física para el Datacenter

La sala de informática es un espacio de ambiente controlado que tiene como único propósito alojar equipos y el cableado directamente relacionados con los sistemas informáticos y otros sistemas de telecomunicaciones.

La distribución de la planta debe ser coherente con las necesidades de equipo y de las instalaciones de los proveedores, tales como:

- Requisitos de carga del suelo, incluyendo equipos, cables, cables de conexión, y de los medios de comunicación (carga estática concentrada, carga baja uniforme estática, carga de laminación dinámica).

- Requisitos de espacio libre servicio (requisitos de liquidación a cada lado de los equipos necesarios para el mantenimiento adecuado de los equipos).

- Los requisitos de flujo de aire.

- Los requisitos de alimentación de CC y restricciones de longitud del circuito.

#### 4.1.1.1 Diseño arquitectónico

- **Tamaño:** La sala de informática tendrá las dimensiones necesarias para cumplir los requisitos conocidos de equipos específicos incluyendo permisos adecuados, esta información puede obtenerse de los proveedores de los equipos. El tamaño del Centro de Datos debe dimensionarse de tal forma de permitir la escalabilidad y la ocupación de nuevos equipos que ingresen en el futuro.
- **Directrices para otros equipos:** Los equipos eléctricos de control, tales como los sistemas de distribución de energía o acondicionadores, y los UPS hasta 100 kVA se permitirán en el aula de informática, con la excepción de las baterías de celdas húmedas.

  Los UPS de más de 100 kVA y cualquier otro tipo de UPS que contenga baterías de celdas húmedas deben estar ubicados en una habitación separada con excepción de lo requerido por el AHJ. El equipo no relacionado con el apoyo de la sala de informática (por ejemplo, tuberías, conductos, neumática, entre otros) no se instalará, transitará o insertará en la sala de ordenadores.
- **Altura del techo:** La altura mínima en la sala de ordenadores será de 2,6 m (8,5 pies) desde el piso terminado a cualquier obstrucción como rociadores, dispositivos de iluminación o cámaras. En cuanto a los requisitos de altura para las salas de refrigeración, racks o gabinetes, se debe cumplir que la altura sea al menos de 2.13 m (7 pies). Un mínimo de 460 mm (18 pulgadas) de espacio libre deberá mantenerse como espacio para las cabeceras de aspersores de agua.
- **Tratamiento:** Los pisos, paredes y techos deberán estar sellados, pintados o construidos de un material específico para minimizar el polvo y evitar el daño de los equipos. Los acabados deben ser de color claro para mejorar la iluminación ambiente. Los pisos deben tener propiedades anti-estáticas de conformidad con la norma IEC 61000-4-2.
- **Iluminación:** La iluminación del Centro de Datos será de un mínimo de 500 lux (50 bujías-pie) en el plano horizontal y 200 lux (20 bujías-pie) en el plano vertical, medido a 1 m (3 pies) por encima del piso terminado en medio de todos los pasillos entre las empresas. Los accesorios de iluminación no deben ser alimentados desde el mismo panel de distribución eléctrica en el equipo de

telecomunicaciones en la sala de ordenadores. El alumbrado de emergencia y señalización, se deben ubicar correctamente en la Sala de Datos.

- **Puertas:** Las puertas del Centro de Datos serán de un mínimo de 1 m (3 pies) de ancho y 2,13 m (7 pies) de alto, sin umbrales de las puertas con bisagras para abrir hacia el exterior, deslices de lado a lado, o con facilidades para ser extraíble. Se recomienda tener diferentes niveles de puertas y accesos al Datacenter para mayor seguridad y que las puertas sean lo más sólidas y blindadas posibles, cuyos accesos deberán estar protegidas con Sistemas de Tarjetas de Proximidad, Sistemas Biométricos y de ser posible con llave.
- **Suelo de carga:** La capacidad de carga sobre el suelo en la sala de informática deberá ser suficiente para soportar tanto la carga distribuida y concentrada de los equipos instalados con el cableado y los medios asociados. La distribución de la capacidad mínima de suelo de carga serán 7,2 kPa (150 lbf / ft2) La capacidad de carga del piso distribuido recomendada es de 12 kPa (250 lbf / ft2). El suelo, no aussi - tener un mínimo de 1,2 kPa (25 lbf / ft2) Capacidad para colgar de apoyo que las cargas están suspendidas desde el fondo de la planta (por ejemplo, las escalas de cables que cuelgan del techo de la planta más abajo). La capacidad recomendada de colgar el suelo es de 2,4 kPa (50 lbf / ft2).
- **Señalización:** La señalización, si se usa, debe ser desarrollada en el nivel de seguridad del edificio. La Señalización adecuada de salida se colocará de conformidad con la AHJ.
- **Consideraciones Sísmicas:** Especificaciones para las instalaciones conexas tendrá en cuenta los requisitos de zona sísmica aplicable. Consulte la especificación Telcordia GR-63-CORE para más información sobre consideraciones sísmicas.

### 4.1.2 Normativa de Perímetro de Seguridad Física para los cuartos de cableados

El diseño y la infraestructura de los cuartos de cableado deben cumplir con las siguientes normas para la Seguridad de la Información y de los equipos:

- Los cuartos de cableado o de telecomunicaciones deben cumplir con las especificaciones del estándar ANSI/EIA/TIA570-A.
- La infraestructura debe estar protegida al acceso de personal no autorizado de acuerdo a la Política de control de acceso físico de entrada.
- Todo cuarto de cableado debe estar resguardado por un perímetro conformado por paredes resistentes y de difícil acceso al público.
- Está prohibida la colocación de objetos ajenos a los equipos de telecomunicaciones dentro de los cuartos de cableado.
- Los niveles de refrigeración deben ser adecuados y deben mantenerse bajo estricto control de temperatura para evitar sobrecalentamiento y daños físicos a los equipos de telecomunicaciones.
- El acceso a los cuartos de cableado debe estar restringido únicamente al personal autorizado, los cuales deben acceder mediante tarjetas de proximidad o sistema biométrico.
- Los niveles de iluminación debe ser adecuados para facilitar la visualización, instalación, configuración y mantenimiento de los equipos.
- El aterramiento de los equipos en los rack es obligatorio para proteger los equipos en caso de fallas eléctricas.

## 4.2 Política para el control físico de entrada

Las áreas de seguridad deben estar protegidas mediante controles de entrada apropiados que aseguren el acceso físico solo al personal autorizado.

Todos los empleados, contratistas, usuarios de terceras partes y visitantes que deseen ingresar a las instalaciones del Instituto Nacional de Aeronáutica Civil deberán contar con una tarjeta de proximidad, la cual le suministre acceso únicamente a los privilegios que se requieran.

### 4.2.1 Normativa para el control físico de entrada

Todo acceso físico de entrada de empleados, contratistas, usuarios de terceras partes y visitantes deben regirse bajo las siguientes normas:

- Todos los visitantes deberán suministrar información personal como nombres, apellidos y número de identificación (cédula, pasaporte), para el control de registros de acceso.
- Todo visitante deberá adquirir una tarjeta de proximidad teniendo acceso estrictamente al área por la cual se haya registrado para acceder, dejando como garantía su documento de identificación (Cédula de Identidad o Pasaporte en caso de ser extranjero), la cual será devuelta una vez haya concluido sus actividades y regresado la tarjeta de proximidad al departamento respectivo.
- Cada usuario de terceras partes debe adquirir una tarjeta de proximidad de carácter "Pase Especial" de acceso a las áreas que estén estrictamente relacionadas con las actividades que deba desempeñar en la institución. Durante la adquisición de un Pase Especial se debe suministrar información personal a más detalle como nombres, apellidos, número de identificación (cédula o pasaporte), dirección personal, teléfonos de ubicación, fotografía, carta de aceptación del instituto en la que se incluye el cargo a desempeñar y el tiempo estimado en que se realizaran las actividades pertinentes, estos datos serán únicamente utilizados para el registro y afiliarlo con un número único de tarjeta de proximidad
- Todo empleado o contratista debe adquirir una tarjeta de proximidad de acuerdo a los privilegios que requiera el cargo a desempeñar por el que fue empleado o contratado. La información más relevante suministrada para la adquisición de dicha tarjeta como nombres y apellidos, cargo, fotografía, número de identificación será mostrada en la impresión de la tarjeta para control de seguridad en la institución.
- Todo derecho de acceso adquirido deberá ser revocado al culminar la fecha de vencimiento por la cual fue registrada la tarjeta de proximidad. En caso de un

tiempo de extensión, cambio de status, o privilegios deberá ser informado a las autoridades pertinentes y realizar nuevamente la solicitud.

### 4.3 Política para la seguridad de oficinas, habitaciones e instalaciones.

Toda infraestructura de la institución sean oficinas, habitaciones o instalaciones deben localizarse de forma estratégica para evitar el acceso de personal no autorizado, cumpliendo con la política para el control físico de entrada y la política de perímetros de seguridad física.

### 4.4 Política de gestión de privilegios

Todas las unidades pertenecientes al INAC deben definir los roles o permisos para la administración y control de acceso de los usuarios a los diferentes sistemas y equipos informáticos.

#### 4.4.1 Normativa para la Gestión de Privilegios

La gestión de privilegios para el control de acceso de los usuarios a los sistemas y los equipos electrónicos del INAC debe seguir la siguiente normativa:

- Todo sistema debe tener como mínimo 2 niveles de privilegios (Administrador y Usuarios).
- Todos los usuarios deben contar con un nivel de privilegio a los sistemas autorizado por la Gerencia del área respectiva.
- La Gerencia debe comunicar al administrador del sistema el nivel de privilegio que se le fue autorizado a cada funcionario del área respectiva.
- El administrador del sistema es el encargado de brindar los privilegios respectivos, previamente autorizados por la Gerencia.
- Es responsabilidad del Gerente del área respectiva, comunicar a la Gerencia de Seguridad de la Información sobre los privilegios otorgados y seguir el procedimiento para la Gestión de Activos.

## 4.5 Política de gestión de contraseñas de usuarios

El acceso a todo sistema o equipo electrónico que maneje información debe estar protegido mediante la autenticación de un nombre de usuario y una contraseña para validar la identidad de los usuarios.

### 4.5.1 Normativa para la gestión de contraseñas de usuarios

La asignación de contraseñas debe asignarse de acuerdo a la siguiente normativa:

- Todo usuario deberá firmar un Acta de Confidencialidad en donde se comprometerá a mantener las contraseñas personales de manera confidencial y las de grupo solo dentro de los miembros del mismo.
- Se deberán asignar contraseñas temporales seguras a todos aquellos usuarios que ingresen por primera vez al sistema, es responsabilidad de los usuarios enviar un acuse de recibo de la contraseña y de cambiarla inmediatamente.
- En caso de pérdida u olvido de la contraseña, es responsabilidad del usuario responder a las preguntas de seguridad respectiva para el restablecimiento de la misma. De haberse olvidado las respuestas de seguridad, el usuario deberá comunicar al Gerente o Superior inmediato a fin de reestablecer la contraseña.
- En caso de no contar con un sistema de restablecimiento de contraseñas, es responsabilidad del usuario comunicarse con el gerente del área, superior inmediato o en su defecto comunicar a la Gerencia de seguridad de la información.
- Es responsabilidad del usuario, cambiar la contraseña o en su defecto comunicar a la Gerencia de Seguridad de la Información o a su superior inmediato, cuando se tenga sospecha de que la contraseña ha sido vulnerada o descubierta.
- Se deberá verificar la identidad del usuario antes de proporcionar una contraseña nueva, temporal o reemplazarla.
- Está prohibido el envío y almacenamiento de contraseñas por medios electrónicos no cifrados, de terceras partes o no protegidos.

- Está prohibida la utilización de contraseñas de fábrica que vengan por defecto con los softwares utilizados en la institución.
- Toda contraseña debe ser lo más robusta posible, siguiendo los siguientes requerimientos mínimos: 10 caracteres, de los cuales al menos 3 deben ser letras, 3 números y debe contener caracteres especiales.

### 4.6 Política para la restricción de acceso a la información

Todas las unidades deben cumplir con las políticas de gestión de privilegios definida y restringir el acceso a todos los usuarios que no pertenezcan al área pertinente a fin de proteger los datos y la información de los equipos y sistemas respectivos.

# Apéndice N

## Normativa para el Control de Redes

## 1. Normativas para la seguridad de servicios de red.

Todo el equipo tecnológico (computadoras, estaciones de trabajo, supercomputadoras, y equipo accesorio), que esté o sea conectado a la red del Instituto Nacional de Aeronáutica Civil (INAC), o aquel que en forma autónoma se tenga y que sea propiedad de la institución, debe sujetarse a las normas que emita la Gerencia de Seguridad de la Información.

- Los usuarios y/o contratistas no deberán instalar líneas telefónicas, proxy, servicios DHCP, FTP canales de transmisión de datos, módems, sin la debida autorización de la Gerencia de Seguridad de la Información y de la Gerencia Encargada de la Plataforma Tecnológica.
- Se deberá establecer la utilización de una fuente de energía interrumpible (UPS), para apoyar ordenadamente el apagado o el funcionamiento continuo del equipo que apoya las operaciones críticas de la Institución.
- Un generador de reserva debería considerarse si es requerido que el procesamiento continúe en el caso de una falla prolongada de energía.
- El equipo UPS y los generadores deberían verificarse con regularidad para asegurar que tiene la capacidad adecuada y son probados de acuerdo con las recomendaciones del fabricante.
- El suministro de agua debería ser estable y adecuado para abastecer los equipos de aire acondicionado, de humidificación y los sistemas de extinción de fuego (cuando sea utilizado).
- El equipo de telecomunicaciones debería estar conectado al proveedor del servicio por al menos dos rutas diferentes para prevenir la falla en un camino de la conexión que interrumpa los servicios de voz y datos.
- Todos los equipos deben ser objeto de mantenimiento preventivo, de conformidad con un cronograma preestablecido (se recomienda que sea cada tres meses).

- Las estaciones de trabajo, redes y otros medios que pueden ser afectados por virus informáticos, deben contar con software antivirus, el cual debe ser actualizado periódicamente.
- Los requerimientos para la instalación y actualización de redes deben ser formalizados y controlados adecuadamente, asegurando que su ejecución no interfiera con la operación normal de los servicios.
- El usuario es responsable del cuidado y uso adecuado de los recursos informáticos (Computador personal, impresora, CD, entre otros), que se le asignen para el desarrollo normal de sus funciones.
- Los usuarios no podrán trasladar o reubicar los equipos de redes sin previa autorización de la Gerencia Encargada de la Plataforma Tecnológica. Para efectos de retiro de equipos de las instalaciones del Instituto Nacional de Aeronáutica Civil (INAC), éstos deberán contar con autorización escrita.
- A Todos los equipos de redes se les debe realizar copias de respaldo de la información sensible y configuración de los mismos.
- Las informaciones sensibles y confidenciales que se encuentren almacenadas en los servidores y equipos de redes deben ser protegidas mediante herramientas de cifrado.
- El daño o robo de cualquier equipo de red debe ser notificado inmediatamente a la Gerencia Encargada de la Plataforma Tecnológica y a la Gerencia de Seguridad de la Información.
- Las líneas de energía y de telecomunicaciones en los lugares de procesamiento de la información deberían estar bajo tierra, donde sea posible, o sujeto a una protección alternativa adecuada.
- El cableado de redes debería protegerse de la intercepción no autorizada o el daño, por ejemplo, utilizar un conducto o evitar rutas por áreas públicas.
- Los cables de energía deberían separarse de los cables de comunicaciones para prevenir la interferencia.

- Deberían utilizarse marcas claramente identificables en los cables y los equipos para minimizar los errores de manipulación, tales como, conexión accidental incorrecta de cables de red.
- La lista de conexiones deberá estar documentada para reducir la posibilidad de errores.
- Para los sistemas sensibles o críticos, se deben considerar controles adicionales como la instalación de conducto blindado y habitaciones o cajas cerradas en puntos de inspección y terminación, la utilización de rutas alternativas y/o medios de transmisión que proporcionen la seguridad apropiada, la utilización de escudo electromagnético para proteger los cables, la iniciación de barridos técnicos e inspecciones físicas para los dispositivos no autorizados que son adjuntados a los cables y el acceso controlado a paneles de conexión y cuartos de cableado.

**2. Uso Aceptable**

Los usuarios de la Red de datos del INAC utilizarán la infraestructura de la red de esta institución para el intercambio de información cuyo contenido sea de investigación, académico o necesario para el desempeño de la función administrativa.

Los usuarios de la Red de datos del INAC deberán utilizar eficientemente la red con el fin de evitar, en la medida de lo posible, la congestión de la misma.

**3. Uso No Aceptable**

La infraestructura y servicios ofrecidos por la Red de Datos del INAC no deben usarse para:

- Cualquier transmisión de información o acto que viole la legislación vigente en el Estado Venezolano.
- Fines privados, personales o lúdicos.

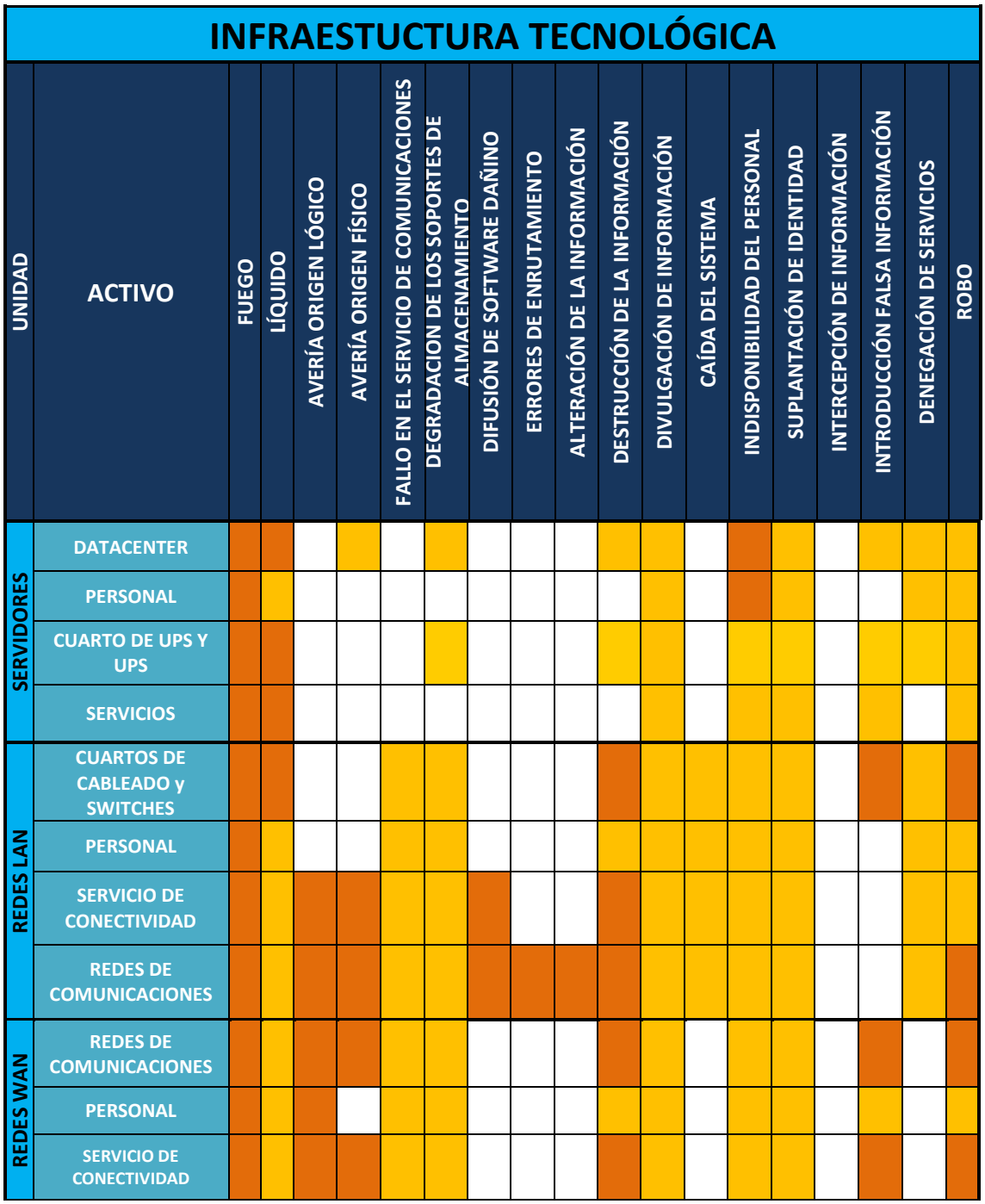
- La circulación de información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Desarrollo de actividades que produzcan:
  - La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
  - La destrucción o modificación premeditada de la información de otros usuarios.
  - La violación de la privacidad e intimidad de otros usuarios.
  - El deterioro del trabajo de otros usuarios.
- Destrucción, manipulación o apropiación indebida de la información que circula por la red.
- La conexión o instalación indebida de equipos de red activos (hubs, switches, routers, modems, firewalls, puntos de acceso inalámbricos, etc.) que previsiblemente perturbe el correcto funcionamiento de la misma o comprometa su seguridad, salvo expresa autorización de la Gerencia de Infraestructura Tecnológica.
- Conexión, desconexión o reubicación de equipos sin la autorización expresa de la Gerencia de Infraestructura Tecnológica.

## 8. Incumplimiento

En caso de no cumplir con las normas establecidas en este documento, los funcionarios responsables se verán sometidos a las sanciones establecidas en la Ley de Delitos Informáticos.

# Apéndice O

## Eficiencia de Controles y Reducción de Valor de Amenazas



| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| REDES WAN | SERVICIOS | | | | | | | | | | | | | | | | | | |
| | REDES DE COMUNICACIONES | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |
| | EQUIPOS INFORMÁTICOS | | | | | | | | | | | | | | | | | | |
| | DEPOSITO | | | | | | | | | | | | | | | | | | |
| REDES WLAN | OFICINA | | | | | | | | | | | | | | | | | | |
| | EQUIPOS INFORMÁTICOS | | | | | | | | | | | | | | | | | | |
| | DATOS E INFORMACIÓN | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |
| | EQUIPOS INFORMÁTICOS | | | | | | | | | | | | | | | | | | |
| REDES WLAN | SERVICIOS | | | | | | | | | | | | | | | | | | |
| | SOFTWARE Y APLICACIONES | | | | | | | | | | | | | | | | | | |
| | REDES DE COMUNICACIONES | | | | | | | | | | | | | | | | | | |
| | DATOS E INFORMACIÓN | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |

| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SOPORTE TÉCNICO | OFICINA | | | | | | | | | | | | | | | | | | |
| | COMPUTADORAS , LAPTOPS | | | | | | | | | | | | | | | | | | |
| | SERVICIOS | | | | | | | | | | | | | | | | | | |
| | SOFTWARE Y APLICACIONES | | | | | | | | | | | | | | | | | | |
| | DATOS E INFORMACIÓN | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |

| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| REQUERIMIENTOS | OFICINA | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE RESTABLECIMIENTO DE CLAVES | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE GESTIÓN ADMINISTRATIVA | | | | | | | | | | | | | | | | | | |
| | SIGESP Y LOTUS | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |
| BASE DE DATOS | OFICINA | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE PRIVILEGIOS Y SOPORTE DE USUARIOS | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE GESTIÓN | | | | | | | | | | | | | | | | | | |
| | SOFTWARE Y APLICACIONES | | | | | | | | | | | | | | | | | | |
| | BASES DE DATOS | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |

| UNIDAD | ACTIVO | FUEGO | LÍQUIDO | AVERÍA ORIGEN LÓGICO | AVERÍA ORIGEN FÍSICO | FALLO EN EL SERVICIO DE COMUNICACIONES | DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO | DIFUSIÓN DE SOFTWARE DAÑINO | ERRORES DE ENRUTAMIENTO | ALTERACIÓN DE LA INFORMACIÓN | DESTRUCCIÓN DE LA INFORMACIÓN | DIVULGACIÓN DE INFORMACIÓN | CAÍDA DEL SISTEMA | INDISPONIBILIDAD DEL PERSONAL | SUPLANTACIÓN DE IDENTIDAD | INTERCEPCIÓN DE INFORMACIÓN | INTRODUCCIÓN FALSA INFORMACIÓN | DENEGACIÓN DE SERVICIOS | ROBO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DESARROLLO | OFICINA | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE INTRANET | | | | | | | | | | | | | | | | | | |
| | SERVICIO DE SOPORTES DEL SISTEMA | | | | | | | | | | | | | | | | | | |
| | JOOMLA Y APACHE | | | | | | | | | | | | | | | | | | |
| | CÓDIGOS FUENTES | | | | | | | | | | | | | | | | | | |
| | PERSONAL | | | | | | | | | | | | | | | | | | |

# Apéndice P

## Compromiso de Cumplimiento de la Política y Normativa de Seguridad de la Información

Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para Transporte Acuático y Aéreo

INAC

**COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA Y NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN**

**Cédula:** _____ **Nombre y Apellido:** _____

Por medio de la presente, se hace de su conocimiento que las Autoridades del Instituto Nacional de Aeronáutica Civil reconoce como activos de información todos aquellos elementos como equipos informáticos, datos e información en formato digital, físico o cualquier otro medio, software o aplicaciones, redes de comunicaciones, instalaciones o servicios. En base a esto, la Gerencia de Seguridad de la Información manifiesta su determinación de cumplir con los parámetros y requerimientos de seguridad de la información que garantice la integridad, confidencialidad y disponibilidad de los activos.

Deberá almacenar por tiempo indefinido todos los datos e información a la que haya tenido acceso de la empresa durante y después de su relación laboral, no pudiendo divulgarlos ni utilizarlos de forma directa o indirecta, esta obligación se mantendrá vigente tras la culminación de la relación laboral.

Es responsabilidad del funcionario proteger los activos de información y la reputación de la institución bajo el cumplimiento de las siguientes normas:

- El funcionario responsable no debe dejar información confidencial expuesta en escritorios, impresoras o áreas comunes.
- Mantener su lugar de trabajo despejado y libre de información confidencial.
- Guardar bajo llave la información sensible.
- Ser prudente con las conversaciones para evitar divulgación de la información.
- Acceder sólo a la información y recursos a los que tenga autorización.
- El carnet de acceso a las instalaciones es personal, intransferible y no debe brindar acceso a terceras personas, por lo que debe portarse siempre en un lugar visible.

Las contraseñas o credenciales de acceso a sistemas son intransferibles y confidenciales, asegúrese de cambiarla periódicamente siendo lo suficientemente robusta y no la deje expuesta, ya que será su responsabilidad cualquier uso indebido que pueda hacerse a través de su clave, en caso de sospechas de que la misma haya sido vulnerada cámbiela inmediatamente y notifíquelo a la Gerencia de Seguridad de la Información.

En caso de irregularidades que puedan afectar a los activos de información o reputación del INAC, notifique inmediatamente a la Gerencia de Seguridad de la Información ya que, la violación de la Política y Normativa de Seguridad de la Información, será considerada como una omisión o imprudencia que afecta gravemente la seguridad del trabajo, siendo ésta causal de despido justificado de conformidad con la Ley Orgánica de Trabajo. Adicionalmente, puede incluso generar sanciones penales contemplados en la Ley sobre Delitos Informáticos vigente.

De esta manera, usted declara que se responsabiliza de poner en práctica la Política y Normativa de Seguridad de la Información del INAC y devolver todos los bienes asignados durante la relación laboral, con el fin de garantizar la imagen del instituto y la protección de la información.

_____

**Firma del Funcionario Conforme**

A los Días____ del mes____ del año____

# Apéndice Q

## Software de Gestión Cisco ASA para Bloqueo de Puertos