DISEÑO DE LA ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA EMPRESA FESNEPONAL

JOSÉ WILSON CASTRO PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA DC
2023
DISEÑO DE LA ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA EMPRESA FESNEPONAL

JOSÉ WILSON CASTRO PADILLA

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Msc. KATERINE MARCELES VILLALBA
Directora de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA DC
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá DC., Septiembre de 2023

DEDICATORIA

Queridos familiares, amigos y seres queridos,

Hoy quiero compartir con ustedes un momento muy especial en mi vida. Después de mucho esfuerzo, dedicación y perseverancia, he completado mi especialización en seguridad informática en la Universidad Nacional Abierta y a Distancia (UNAD).
Este logro no habría sido posible sin el apoyo incondicional de mi familia, amigos y seres queridos. Ustedes me han brindado su amor, aliento y motivación durante todo este proceso. Cada palabra de aliento, cada llamada telefónica y cada mensaje de texto han sido vitales para mi éxito.
En particular, quisiera agradecer a mis padres por creer en mí y apoyarme en cada paso de mi camino. También agradezco a mis hermanos y hermanas, amigos cercanos y colegas por su apoyo constante y por motivarme a seguir adelante cuando las cosas se pusieron difíciles.
Agradezco a los profesores de la UNAD por compartir su conocimiento y experiencia conmigo y por ayudarme a crecer tanto a nivel personal como profesional. También agradezco a mis compañeros de clase por su amistad, colaboración y motivación mutua.
Finalmente, dedico mi logro a todos aquellos que han luchado y siguen luchando por alcanzar sus sueños. Espero que mi éxito pueda inspirarlos a seguir adelante y nunca rendirse ante los obstáculos.
Gracias de nuevo a todos por su amor y apoyo. Este logro no habría sido posible sin ustedes.

AGRADECIMIENTOS

Agradecer a mis amigos y colegas por su colaboración, discusiones interesantes y por compartir sus conocimientos y experiencias conmigo. Agradezco especialmente a mis profesores, cuya dedicación y profesionalismo me inspiraron y motivaron en cada etapa de mi aprendizaje.

A la Universidad por brindarme la oportunidad de adquirir conocimientos y habilidades en la especialización. Estoy muy agradecido por la calidad de la educación que recibí y por la dedicación del cuerpo docente y administrativo de la universidad.

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE ILUSTRACIONES

Pág.

GLOSARIO

ACCESIBILIDAD: La capacidad de acceder a los datos y recursos de la información de manera segura y autorizada.

AMENAZA: Un evento o acción que tiene el potencial de causar daño o violar la seguridad de la información.

ANÁLISIS DE RIESGOS: El proceso de identificación, evaluación y tratamiento de los riesgos de seguridad de la información.

AUTENTICACIÓN: La verificación de la identidad de un usuario antes de permitir el acceso a los datos y recursos de la información.

BACKUP: La copia de los datos y recursos de la información para su almacenamiento seguro y para la recuperación en caso de pérdida o daño.

CONFIDENCIALIDAD: La protección de la información contra el acceso o divulgación no autorizada.

CRIPTOGRAFÍA: La técnica de protección de la información mediante el cifrado y la decodificación de datos.

FIREWALL: Una barrera de seguridad diseñada para proteger la red y los sistemas de información de accesos no autorizados.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: El proceso de gestión de los riesgos de seguridad de la información mediante la aplicación de controles de seguridad.

INTEGRIDAD: La protección de la información contra la modificación no autorizada o la corrupción.

ISO/IEC 27001: La norma internacional para la gestión de la seguridad de la información.

MALWARE: Software malicioso diseñado para dañar o interferir con el funcionamiento de los sistemas de información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Un documento que establece las normas, prácticas y procedimientos para la gestión de la seguridad de la información.

PRIVACIDAD: La protección de la información personal y sensible contra la divulgación no autorizada.

PROTECCIÓN CONTRA VIRUS: La protección de los sistemas de información contra los virus y otras amenazas maliciosas.

REDES PRIVADAS VIRTUALES (VPN): Una tecnología de red que permite el acceso seguro a los recursos de la información a través de Internet.

RESPALDO: Una medida de control de seguridad que garantiza la recuperación de los datos y recursos de la información en caso de pérdida o daño.

SEGURIDAD FÍSICA: La protección de los recursos de la información contra el acceso no autorizado y el daño físico.

SEGURIDAD DE LA INFORMACIÓN: La protección de la información contra las amenazas y los riesgos de seguridad.

USUARIO: Una persona o entidad que accede a los datos y recursos de la información.

RESUMEN

La seguridad de la información es vital para las organizaciones, ya que deben proteger sus datos y recursos contra amenazas y riesgos de seguridad. La norma ISO/IEC 27001:2013 establece los requisitos para la gestión de la seguridad de la información en las organizaciones, lo que implica la identificación, evaluación y tratamiento de los riesgos de seguridad mediante la aplicación de controles de seguridad. Los tres pilares de la seguridad de la información son la confidencialidad, la integridad y la disponibilidad. Las medidas de control de seguridad incluyen la gestión de contraseñas, la autenticación, la autorización, la encriptación, la seguridad física, los backups, la gestión de incidentes de seguridad y la concientización de los usuarios. La política de seguridad de la información es un documento que establece las normas, prácticas y procedimientos para la gestión de la seguridad de la información en una organización. La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 ayuda a las organizaciones a proteger sus datos y recursos contra las amenazas y riesgos de seguridad, y a cumplir con los requisitos legales y reglamentarios.

Palabras claves: Análisis, Controles, Integridad, Riesgo, Seguridad.

ABSTRACT

Information security is critical for organizations as they need to protect their data and resources against security threats and risks. The ISO 27001 standard establishes the requirements for managing information security in organizations, which involves identifying, assessing, and treating security risks through the implementation of security controls. The three pillars of information security are confidentiality, integrity, and availability. Security control measures include password management, authentication, authorization, encryption, physical security, backups, security incident management, and user awareness. The information security policy is a document that sets out the rules, practices, and procedures for managing information security in an organization. Implementing an information security management system based on the ISO 27001 standard helps organizations to protect their data and resources against security threats and risks, and to comply with legal and regulatory requirements.

Keywords: Analysis, Controls, Integrity, Risk, Security

INTRODUCCIÓN

En la actualidad, es muy usual escuchar el concepto de transformación digital, económica y social, esto se da como consecuencia del avance de las Tecnologías de la Información y las Comunicaciones y el uso de Internet por millones de usuarios en todo el mundo. Esta posibilidad de conexión a nivel global ha permitido que la información esté tipificada como uno de los activos más valiosos e importantes para cualquier tipo de entidad; sin embargo, muchas organizaciones no la tienen asegurada.

Con el pasar del tiempo y el avance de la tecnología, la seguridad de los datos se ha vuelto un tema de suma importancia, por lo tanto, cualquier organización independientemente de que sea publica ó privada, debe ser consciente que están expuestas a un número de amenazas y riesgos que existen hoy en día, y aprovechan cualquier tipo de vulnerabilidad para someter a los activos críticos de información a ataques y espionajes, etc. Es por ello que para salvaguardar la información se deben utilizar herramientas de gestión a través de procesos automatizados, documentados que garanticen la confidencialidad, integridad y disponibilidad de la misma.

El presente trabajo plantea el diseño de un sistema de gestión de seguridad de la información SGSI, para el Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional FESNEPONAL, siguiendo los lineamientos contemplados en la norma ISO/IEC 27001:2013, logrando con esto minimizar el riesgo de su infraestructura tecnológica y de los procesos asociados.

Es importante mencionar que este proyecto surgió basado en las necesidades que se observaron en esta organización en particular y buscando una contribución para ésta. La utilización de la norma ISO/IEC 27001, como modelo metodológico para el diseño del sistema de gestión de seguridad de la información SGSI, pretende asegurar un correcto diseño de la solución, aprovechando la amplia difusión, documentación y desarrollo de la norma,

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El desarrollo de las tecnologías de la información y las comunicaciones permite que cada vez más las organizaciones en todos los ámbitos, optimicen sus procesos, aumentando las posibilidades de crecimiento y expansión, sin embargo, la dependencia cada vez mayor de las tecnologías de la información plantean grandes riesgos para la seguridad de la información, estos riesgos en la mayoría de los casos no reciben el tratamiento adecuado, debido a que no existe la suficiente concientización por parte de las organizaciones de la importancia de proteger sus activos de información, como es el caso de FESNEPONAL Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional. En este contexto el sistema de gestión de seguridad de la información basado en el estándar ISO/IEC 27001:2013, provee una valiosa herramienta para que organizaciones de todos los sectores y tamaños den un tratamiento adecuado al riesgo inherente al manejo de la información, para este caso específico los riesgos asociados al manejo de información por medios tecnológicos.
FESNEPONAL en Agosto de 2021 debido a influencias de desastres naturales conto con un siniestro en donde debido a fuertes lluvias y devastadores vientos en la ciudad de Bogotá lograron el debilitamiento de la infraestructura física donde se encontraba un tanque de agua de aproximadamente 1000 litros de agua, desencadenando que toda esta agua callerá directamente al centro de datos e inundara todo el sitio ocasionando la pérdida de todos los dispositivos que alli se encontraban, la organización en su momento no tiene disponible un plan de continuidad de negocio, las copias de seguridad se hacían en un dispositivo externo pero dentro del mismo centro de datos, el daño en el hardware fue transferido a la aseguradora quien aseguro el siniestro en cierta proporción, la información y los servicios de red logro recuperarse, pero tomo su tiempo. incidentes como estos se pretenden mitigar con la implementación de un sistema gestión de la información basado en la norma ISO/IEC 27001:2013.

FESNEPONAL Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional, es una organización sin ánimo de lucro, dedicada a servir con calidad a los asociados y sus familias, razón por la cual el sistema de gestión de seguridad de la información se ve como parte fundamental para alcanzar los objetivos propuestos por la organización, protegiendo la disponibilidad, integridad y confidencialidad de la información como activo fundamental de la compañía,

brindando confianza a sus socios de negocios y a sus colaboradores internos y cumpliendo con la normatividad vigente.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo puede llegar a gestionar los riesgos de seguridad de la información FESNEPONAL Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional con el fin de contribuir a la mejora continua de la organización?

2 JUSTIFICACIÓN

FESNEPONAL Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional ha experimentado un crecimiento constante en sus operaciones comerciales, expansión de sucursales y un aumento en su portafolio de productos y servicios. A medida que la organización se expande, la tecnología también ha crecido para satisfacer las necesidades del negocio. Sin embargo, gran parte de este crecimiento ha sido poco planificado y ha expuesto a la organización a una serie de riesgos en términos de seguridad de la información.

La falta de planificación y gestión en el área de seguridad de la información ha dejado a la empresa vulnerable ante los incidentes de seguridad, lo que ha resultado en pérdida de información, fraude y otros problemas relacionados con la seguridad de la información. Estos incidentes tienen consecuencias graves, incluyendo pérdida de negocios, clientes y colaboradores.

Es esencial que FESNEPONAL Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional implemente una política de mejora continua en todas las áreas y procesos de la organización. Para lograr esto, es necesario diseñar un sistema de gestión de seguridad de la información (SGSI) que permita la definición de políticas de seguridad apoyadas por la dirección. Además, el SGSI deberá permitir la identificación y tratamiento de los riesgos, así como la revisión y mejora continua en el área de TI de la organización.

La implementación de un SGSI permitirá que la empresa tenga un enfoque proactivo en la gestión de la seguridad de la información, en lugar de una respuesta reactiva. Esto ayudará a reducir los riesgos y a minimizar los impactos negativos de los incidentes de seguridad en el negocio y en los clientes y colaboradores de la organización. En resumen, el SGSI es un elemento clave para garantizar la seguridad de la información en la organización y proteger los activos críticos de la empresa.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar la etapa de planificación de un sistema de gestión de seguridad de la información para el área de TI de la empresa FESNEPONAL - Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional basado en la norma ISO/IEC 27001:2013, con el fin de iniciar un proceso de organización y mejora continua que permita la protección de la disponibilidad, integridad y confidencialidad de la información en la ciudad de Bogotá.

3.2 OBJETIVOS ESPECÍFICOS

Evaluar a través de un diagnóstico inicial de la organización mediante la metodología GAP alineado a la ISO/IEC 27001:2013 con el fin de analizar las brechas y conocer la situación actual.

Establecer las vulnerabilidades, amenazas y riesgo de los activos de información del área TI mediante el uso de la metodología Magerit para poder gestionar el impacto de los riesgos asociados.

Proponer un documento de aplicabilidad basado en la norma ISO/IEC 27002:2013 con el fin de establecer buenas prácticas de seguridad y mitigar el riesgo.

Elaborar una política de seguridad de la información basado en los riesgos identificados con el fin de promover un manejo seguro a la información.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Importancia de un SGSI en una organización. Actualmente, las tecnologías de la información y comunicación representan un apoyo fundamental en materia de progreso y sostenibilidad al interior de las empresas. Un sistema de gestión de seguridad de la información representa un apoyo en la aplicación y ejecución de todos los procesos relacionados con la generación, almacenamiento y disposición de información. Esto, con el propósito de identificar los lineamientos que logran un nivel de seguridad de la información aceptable, en donde las posibilidades de que se materialice alguna amenaza sean mínimas y así se preserve de la mejor manera la administración y control de la información de las organizaciones sin importar si su naturaleza es pública o privada.[1]

Un sistema de gestión de Seguridad de la Información en la organización brindará un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información, asociados a un adecuado manejo de la seguridad de la información, en primer lugar generar la concientización tanto en el área directiva de la compañía como en el resto del personal, de la importancia que tiene la información en el desarrollo de las actividades de la organización, y en el beneficio que trae desarrollar una estrategia adecuada para salvaguardar la integridad, confidencialidad y la disponibilidad de la información, en cada empresa sin importar su tamaño o el servicio que presten.

La creación de unas políticas claras de manejo seguro de la información, basada en el entorno de la empresa y alineadas con los objetivos de la compañía, permitirá minimizar el riesgo de pérdida, corrupción o indisponibilidad de la información.

La generación de confianza entre sus socios de negocios y colaboradores internos, en cuanto al manejo seguro de la información por parte de FESNEPONAL, Lo cual puede ayudar al fortalecimiento de las relaciones comerciales y laborales, contribuyendo con esto al crecimiento de la compañía.

---

[1] UNIVERSIDAD MILITAR NUEVA GRANADA. [Sitio web]. Bogotá: UMNG, Importancia del Sistema de Gestión de Seguridad de la Información (SGSI) y su incidencia en materia de control interno. [Consultado el 12 septiembre 2023]. Disponible en: https://repository.unimilitar.edu.co/handle/10654/41450

El seguir un sistema metodológico de tratamiento seguro de la información permite la generación de un ciclo de mejora continua, aumentando la seguridad, mejorando la conciencia y ayudando a construir un sistema de gestión de seguridad de la información cada vez mejor.

4.1.2 La identificación de los activos de información en la organización. La identificación de los activos de información es un proceso dentro de la gestión de la seguridad de la información que consiste en identificar los activos de información de una organización y catalogarlos para su posterior protección. Los activos de información pueden ser cualquier tipo de información valiosa para la organización, como datos de clientes, información financiera, propiedad intelectual, secretos comerciales, entre otros.

La identificación de activos de información es el primer paso para la implementación de un sistema de gestión de seguridad de la información (SGSI) y es crucial para establecer políticas y controles de seguridad adecuados. Al conocer los activos de información que posee la organización, se pueden identificar las posibles amenazas y vulnerabilidades a las que están expuestos y se pueden establecer las medidas necesarias para mitigar estos riesgos.

El proceso de identificación de activos de información puede llevarse a cabo mediante un inventario que contenga información detallada de cada activo, como su ubicación física, propiedad, valor, importancia para la organización, riesgos asociados, entre otros.

Es importante tener en cuenta que la identificación de activos de información debe ser un proceso continuo, ya que la organización puede adquirir o cambiar activos de información con el tiempo. Por lo tanto, es importante actualizar el inventario de forma periódica para asegurarse de que todos los activos relevantes se incluyan en la gestión de la seguridad de la información de la organización.[2]

4.2 MARCO CONCEPTUAL

[2] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. (2013). International Organization for Standardization.

4.2.1 Metodologías de Evaluación de Riesgos.

4.2.1.1 MAGERIT. Es una metodología de gestión de riesgos de seguridad de la información desarrollada por el Centro Criptológico Nacional (CCN) de España. El objetivo de Magerit es ayudar a las organizaciones a identificar, evaluar y tratar los riesgos de seguridad de la información a través de un proceso sistemático y estructurado.

Magerit se basa en un enfoque de ciclo de vida completo para la gestión de riesgos de seguridad de la información, que incluye la identificación de activos de información, la evaluación de amenazas y vulnerabilidades, la evaluación de riesgos, la selección de controles y la implementación, seguimiento y mejora continua del proceso.

La metodología Magerit se divide en tres fases principales: análisis de activos, análisis de riesgos y definición de controles. En la fase de análisis de activos, se identifican los activos de información de la organización y se determina su valor y criticidad. En la fase de análisis de riesgos, se evalúan las amenazas y vulnerabilidades que afectan a los activos de información y se determina el nivel de riesgo asociado. En la fase de definición de controles, se seleccionan y priorizan los controles necesarios para mitigar los riesgos identificados.

Magerit ha sido ampliamente adoptado por organizaciones públicas y privadas en España y se ha convertido en una de las metodologías de gestión de riesgos de seguridad de la información más utilizadas en el país. También ha sido reconocido por organismos internacionales como el Consejo de Europa y la Organización para la Seguridad y la Cooperación en Europa (OSCE).

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España se basa en un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones y de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos controlados y mitigados.[3]

[3] GOBIERNO DE ESPAÑA. [Sitio web]. España: administración electrónica Gobierno de España. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Consultado el 12 septiembre 2023]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

4.2.1.2 LA NORMA ISO/IEC 27005. Establece los requisitos y directrices para la gestión del riesgo de seguridad de la información. Proporciona un enfoque sistemático para la evaluación de los riesgos, la selección de controles y la implementación de medidas para la gestión de riesgos de seguridad de la información en una organización. Se basa en el ciclo de vida de la gestión del riesgo y se aplica a cualquier tipo de organización, independientemente de su tamaño, tipo o naturaleza de la información que maneje.

La norma ISO/IEC 27005 se centra en la identificación, evaluación y tratamiento de los riesgos de seguridad de la información. La identificación de los riesgos es un proceso que implica la identificación de los activos de información de una organización, la identificación de las amenazas y vulnerabilidades asociadas a esos activos, y la evaluación del impacto potencial de los riesgos en la organización. Una vez identificados los riesgos, se lleva a cabo una evaluación de riesgos para determinar la probabilidad y el impacto de cada riesgo.

Una vez evaluados los riesgos, se seleccionan y aplican los controles necesarios para mitigar los riesgos. La selección de controles debe basarse en una evaluación de la efectividad de los controles existentes y la identificación de nuevas medidas de seguridad necesarias para reducir el riesgo. Finalmente, se implementan y se revisan regularmente las medidas de seguridad y los controles seleccionados.

La norma ISO/IEC 27005 es un marco importante para la gestión de riesgos de seguridad de la información y ayuda a las organizaciones a proteger sus activos de información y minimizar el impacto de los riesgos de seguridad de la información. Su implementación puede mejorar la confianza de los clientes y partes interesadas en la capacidad de la organización para proteger la información y mitigar los riesgos de seguridad.

La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO/IEC 27001. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.[4]

[4] PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence. ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. [Consultado el 12 septiembre 2023]. Disponible en: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

4.2.1.3 LA NORMA ISO/IEC 31000. Esta norma fue publicada en noviembre del 2009 por la Organización Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades. Esta norma provee de una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.[5]

4.2.1.4 La Norma ISO 27001:2013. La norma ISO/IEC 27001:2013 establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Esta norma se enfoca en la gestión del riesgo de seguridad de la información y se aplica a cualquier tipo de organización, independientemente de su tamaño, sector o tipo de información que maneje.

La norma ISO/IEC 27001:2013 establece una metodología basada en el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar) para la implementación del SGSI. Esta metodología se enfoca en la identificación de los riesgos, la selección y aplicación de controles de seguridad adecuados, la monitorización y medición de los resultados y la mejora continua del sistema.

La norma ISO/IEC 27001:2013 es una herramienta importante para la gestión de la seguridad de la información, ya que establece un marco claro y estructurado para la implementación de un SGSI. Además, su adopción puede generar beneficios como la mejora en la gestión de riesgos, la protección de la información, el cumplimiento de las leyes y regulaciones aplicables, y el aumento de la confianza de los clientes y las partes interesadas.

Es importante destacar que la implementación de la norma ISO/IEC 27001:2013 requiere un compromiso y liderazgo de la dirección, así como una cultura de seguridad de la información en toda la organización. Además, es necesario realizar una evaluación inicial de la seguridad de la información y definir un plan de acción para la implementación del SGSI.

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

---

[5] PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence. Norma ISO 27002: El dominio político de seguridad. [Consultado el 12 septiembre 2023]. Disponible en: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

La ISO/IEC 27001:2013 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. [6]

4.2.1.5 La Norma ISO/IEC 27002:2013. El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. La norma ISO/IEC 27002:2013 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas.

La norma ISO/IEC 27002:2013 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La norma ISO/IEC 27002:2013 se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles. [7]

4.2.1.6 Seguridad de la Información. Es un conjunto de procedimientos, actividades, protocolos y políticas para proteger la confidencialidad, la integridad y la disponibilidad de la información de las organizaciones, tanto al interior como fuera de ellas, mitigando los impactos que se puedan generar de su mal uso y custodia.
La seguridad de la información en las organizaciones se refiere al conjunto de medidas y prácticas que se implementan para proteger la información y los sistemas informáticos de una organización contra amenazas, riesgos y vulnerabilidades que puedan afectar su confidencialidad, integridad y disponibilidad. La seguridad de la información es esencial para garantizar la protección de los activos de información, que incluyen datos, aplicaciones, hardware, software y recursos de red.

---

[6] PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence. Sistemas de Gestión de Riesgos y Seguridad. [Consultado el 12 septiembre 2023]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

[7] PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence. Software ISO Riesgos y Seguridad. [Consultado el 12 septiembre 2023]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

La seguridad de la información en las organizaciones implica el desarrollo de políticas, procedimientos, estándares y controles de seguridad para garantizar la protección de la información. También implica la educación y concienciación de los empleados y usuarios de la organización para que adopten prácticas seguras y responsables en el manejo de la información.
La seguridad de la información se ha vuelto cada vez más importante en la era digital, en la que los datos y la información se han convertido en uno de los activos más valiosos de las organizaciones. Las amenazas a la seguridad de la información pueden provenir de diversas fuentes, incluidos ataques cibernéticos, robo de información, errores humanos y desastres naturales. Por lo tanto, es esencial que las organizaciones adopten un enfoque proactivo para la seguridad de la información y que estén preparadas para enfrentar y mitigar las amenazas.[8]

4.3 MARCO CONTEXTUAL

4.3.1 FESNEPONAL – FONDO DE EMPLEADOS SUBOFICIALES Y NIVEL EJECUTIVO DE LA POLICIA NACIONAL

Actividades financieras de fondos de empleados y otras formas asociativas del sector solidario.
La distribución de fondos, sin ánimo de lucro, entre sus asociados, para la compra de bienes y servicios. Se incluyen las actividades de unidades tales como:
• Las cooperativas de ahorro y crédito, cuya función principal consiste en adelantar actividad financiera exclusivamente con sus asociados.
• Las cooperativas multiactivas o integrales con sección de ahorro y crédito.
• Los fondos de empleados.
• Los fondos mutuos de inversión.

El fondo de empleados de la policía nacional es de carácter privado y tiene relación con los uniformes y símbolos de dicha institución, y sus asociados son pensionados de dicha institución, esto indica que el fondo de empleados está conformado principalmente por personas que han trabajado en la policía nacional y que se han retirado de ella.

[8] PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence. ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. [Consultado el 13 septiembre 2023]. Disponible en: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/.

La Ilustración 1 muestra las insignias y uniformes de la Policía Nacional, que son vestidos sin problema por haber pertenecido a la fuerza pública.

Ilustración 1 - Uniformados PONAL

Fuente: FESNEPONAL [Sitio web]. Bogota: FESNEPONAL. acerca de nosotros. [Consultado el 29 mayo 2023]. Disponible en: https://www.fesneponal.com/wp-content/uploads/2021/10/nosotros.jpg.

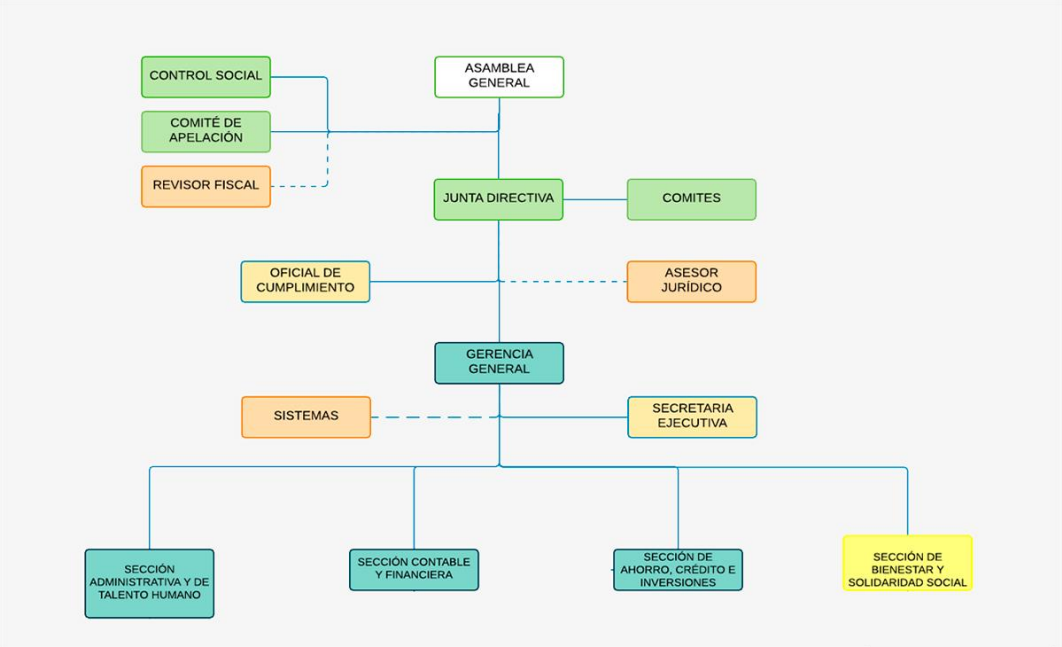
4.3.2 MISIÓN. FESNEPONAL es una organización solidaria sin ánimo de lucro, dedicada a servir con calidad a los asociados y sus familias; motivando la cultura del ahorro, generándoles créditos, educación, salud y cultura, brindando beneficios sociales para fortalecer los lazos de solidaridad y equidad, contando con personal honesto, solidario, justo, respetuoso, diligente, leal y comprometido con el mejoramiento continuo. [9]

4.3.3 VISIÓN. FESNEPONAL será reconocida por su liderazgo en el sector solidario, comercial y de servicios, con un crecimiento de la base social e inversión de proyectos de desarrollo empresarial. Comprometidos con la protección al medio ambiente, la innovación tecnológica del portafolio de servicios y dando la máxima importancia a la satisfacción de todos los asociados de la organización como de sus familias.

4.3.4 ESTRUCTURA ORGÁNICA. La organización pone a disposición un organigrama plasmando la jerarquía de su estructura orgánica, la cual se muestra a continuación:

[9] FESNEPONAL [Sitio web]. Bogota: FESNEPONAL. Nosotros. [Consultado el 29 mayo 2023]. Disponible en: https://www.fesneponal.com/index.php/nosotros/

Ilustración 2 - Estructura organizacional



Fuente: FESNEPONAL [Sitio web]. Bogota: FESNEPONAL. Estructura Organizacional. [Consultado el 29 mayo 2023]. Disponible en: https://www.fesneponal.com/wp-content/uploads/2020/02/organigrama.png.

4.3.5 Principios y valores corporativos. La organización solidaria, por naturaleza se fundamenta en los principios y valores cooperativos, los que ennoblecen la acción de la organización solidaria y la de sus integrantes, enaltece el quehacer solidario y permite extender los vínculos entre sus iguales fortaleciendo el compromiso con la comunidad, el medio ambiente y el país en general.

4.4 ANTECEDENTES O ESTADO ACTUAL

El presente documento se basó en la realización y diseño de una guía de buenas prácticas y procedimientos sistémicos, que consisten en minimizar los riesgos y salvaguardar la protección de la información, específicamente en organizaciones y entidades del estado, con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la misma, a través de una herramienta de gestión relacionada con la seguridad y privacidad de los datos. Es por ello que surgió la necesidad de desarrollar un sistema de gestión de seguridad de la información (SGSI) tomando como referencia la metodología que define la norma ISO/IEC 27001. Con el fin de ponerlo a disposición de las entidades del gobierno y que sea utilizado como guía para definir sus políticas de seguridad de la información. De esta manera el presente

documento busca proporcionar los lineamientos básicos y de forma general sobre cómo empezar a diseñar y dimensionar el alcance para realizar la implementación de un Sistema de Gestión de Seguridad de la Información en una organización del estado colombiano. [10]

Este proyecto aplicado permite conocer el contexto de la empresa Centro de Terapias Integrales Misalud S.A.S., en sus proceso y áreas con el objetivo de diseñar un SGSI que apoye en un futuro los distintos procesos y actividades allí efectuados, minimizando los riesgos de la información y controlar las vulnerabilidades que puedan estar presentes en el sistema de información, mediante el uso de políticas de seguridad documentados y que sean actualizados constantemente. [11]

Hoy en día, toda organización debe asegurar que los activos de información cuenten con un sistema aceptable de seguridad, con el fin de salvaguardar la información que se procesa y se almacena en estos, dado que, actualmente estos archivos son indispensables a nivel empresarial. En este sentido, a través de la construcción de un sistema de gestión de seguridad de la información, se aporta a la empresa Cooperativa Multiactiva de Centrales Eléctricas de Nariño con el fin de que sean parte del cambio y que por medio del diseño e implementación de un SGSI puedan asegurar la integridad, confidencialidad y disponibilidad de sus datos. Para el desarrollo del diseño del sistema de gestión de seguridad de la información se tomó en cuenta los parámetros de la norma ISO/IEC 27001:2013 y de la metodología MAGERIT, siendo esta última la que permitió identificar los activos de información, valorarlos, identificar sus amenazas y valorar su impacto y sus riesgos, a partir de esta información se realizaron algunas recomendaciones con el fin de que los funcionarios de la empresa implementen políticas frente a su sistema de gestión de seguridad lo que les permitirá tener control sobre sus activos.[12]

---

[10] De, J. C. (2019). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 para entidades del estado. [Proyecto aplicado, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/27821

[11] Márquez, H. (2021). *Diseño del Sistema De Gestión de la Seguridad De Información (SGSI) en la Institución Prestadora de Servicios de Salud Centro De Terapias Integrales Misalud S.A.S.*. [Proyecto aplicado]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/39391

[12] Zambrano, L. G. (2021). *Diseño de un sistema de seguridad de la información para la Cooperativa Multiactiva de Centrales Eléctricas de Nariño basado en la norma ISO 27001:2013.*.

El presente proyecto tiene como finalidad mejorar el tratamiento de la información, los activos y personal de la compañía ESSENSALE S.A.S ubicada en Santiago de Cali, para tener respuesta rápida a posibles desastres naturales, acciones mal intencionadas de acceso abusivo o compromiso de los sistemas de información de la compañía. Se desarrollará un sistema de gestión de seguridad de la información estableciendo diferentes políticas para proteger los activos de ESSENSALE S.A.S. [13]

Los trabajos presentados tienen en común el hecho de que todos describen la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en diferentes organizaciones. En el primer trabajo menciona la elaboración de una guía de buenas prácticas y procedimientos sistémicos para preservar la confidencialidad, integridad y disponibilidad de la información en organizaciones y entidades del estado colombiano. En el segundo trabajo hace referencia a la implementación de un SGSI en el Centro de Terapias Integrales Misalud S.A.S. con el objetivo de minimizar los riesgos de la información y controlar las vulnerabilidades del sistema de información. En el tercer trabajo destaca la importancia de que toda organización tenga un sistema de seguridad aceptable para salvaguardar la información que procesa y almacena, y se describe la implementación de un SGSI en la Cooperativa Multiactiva de Centrales Eléctricas de Nariño, con el fin de asegurar la integridad, confidencialidad y disponibilidad de sus datos. Finalmente, en el cuarto trabajo presentado describe la implementación de un SGSI en ESSENSALE S.A.S. para mejorar el tratamiento de la información, los activos y el personal de la compañía y protegerlos de posibles desastres naturales o acciones malintencionadas.

4.5 MARCO LEGAL

Ley 79/1988, Artículo 131. El Artículo 131 de la Ley 79 de 1988 se refiere a los fondos de empleados, asociaciones mutualistas y entidades similares, y establece que, en ausencia de disposiciones legales y normas estatutarias específicas, se aplicarán las disposiciones de la ley. Además, el artículo autoriza al presidente de

---

[Proyecto aplicado]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/39349

[13] Rincón, C. D. (2021). *Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la Norma Internacional ISO/IEC 27001:2013 para la Compañía Essensale S.A.S.*. [Proyecto aplicado]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/39179

la República para expedir normas reguladoras de estas entidades, incluyendo su naturaleza jurídica, requisitos para su reconocimiento, estatutos sociales, derechos y deberes de los asociados, régimen económico y financiero, órganos de representación, fusión, disolución y sanciones. El propósito de este artículo es establecer un marco legal claro y coherente para la operación de estas entidades, lo que promueve la estabilidad y el crecimiento de la economía del país. [14]

El Decreto 1481/1989. Considera los fondos de empleados como personas jurídicas que manejan ahorro. Son asociaciones de personas que tienen como vínculo común pertenecer y depender laboralmente de una misma empresa o de varias sociedades que desarrollen una actividad mancomunada. Los fondos de empleados se constituyen como una entidad privada con un número de personas y capital variable e ilimitado, sin ánimo de lucro. [15]

La Ley 454/1988. Define la economía solidaria como El sistema socioeconómico, cultural y ambiental conformado por el conjunto de fuerzas sociales organizadas en forma asociativa, identificadas por prácticas autogestionarias solidarias, democráticas y humanistas, sin ánimo de lucro, para el desarrollo integral del ser humano como sujeto, actor y fin de la economía. [16]

La Ley 1273 de 2009. Es una ley colombiana que busca establecer medidas para prevenir y sancionar los delitos informáticos, como el acceso abusivo a sistemas informáticos, la interceptación de datos, la violación de la privacidad, la difusión de virus informáticos y el hurto de información. Esta ley tipifica estos delitos y establece penas y sanciones para quienes los cometan. También establece medidas para la protección de la propiedad intelectual en el ámbito digital. El objetivo principal de esta ley es garantizar la seguridad y la confidencialidad de la información en el entorno digital, así como promover el uso responsable y ético de la tecnología de la información.

---

[14] Colombia, Congreso de la República (1988). Ley 79 del 23 de diciembre de 1988. Bogotá. Diario Oficial. Núm. 38.648.

[15] Colombia, Presidencia de la República (1989). Decreto 1481 del 7 de julio de 1989. Sitio web: Unidad Administrativa Especial de Organizaciones Solidarias. Disponible en: http://www.dansocial.gov.co/sites/default/files/pagina-basica/pdf/Decreto1481_1989.pdf

[16] Colombia, Congreso de la República (1998). Ley 454 del 4 de agosto de 1998. Bogotá. Diario Oficial. Núm. 43.357.

Ley 1581 de 2012. Esta ley regula el uso y protección de los datos personales y la información de los ciudadanos. Fue sancionada el 17 de octubre de 2012 y entró en vigencia a partir del 9 de junio de 2013. [17]

[17] CONGRESO DE LA REPÚBLICA DE COLOMBIA [Sitio web]. Bogotá: Congreso, Ley 1581 de 2012. [Consultado el 29 mayo 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5 DISEÑO METODOLÓGICO

El diseño de un sistema de gestión de seguridad de la información para el área de TI de la empresa FESNEPONAL constituyendo de esta forma a un proyecto de tipo aplicado, requiere encontrar, analizar y establecer las causas que exponen a la empresa a fallas de seguridad de la información en el área de tecnología.

Con esta información se podrá explicar qué amenazas atentan contra la seguridad de la información y en qué condiciones se dan, lo que corresponde a la investigación de tipo explicativo y experimental.

Además, el carácter de la investigación explicativa, presente en este trabajo, conlleva a la aplicación de una teoría de referencia como lo es la norma ISO/IEC 27001:2013, que nos conduce a generalizaciones que dan cuenta de los eventos e incidentes de seguridad de la información que se producen en determinadas condiciones.

5.1 METODOLOGIA DE APLICACIÓN

La utilización de una metodología práctica para abordar el problema planteado y alcanzar los objetivos del proyecto aplicado. Esta metodología se centra en realizar un análisis GAP o de brechas, lo que implica identificar las diferencias entre el estado actual y el estado deseado en términos de seguridad de la información.

Además, se hace mención al uso de la metodología Magerit para la valoración y tratamiento de los riesgos. Magerit es un enfoque reconocido en seguridad de la información que permite identificar y evaluar los riesgos, así como definir estrategias para mitigarlos.

También hace referencia a la aplicabilidad del anexo A de la norma ISO/IEC 27002:2013. El anexo A proporciona un conjunto de controles de seguridad de la información que se pueden implementar para mitigar los riesgos identificados. Su aplicación es relevante para garantizar una adecuada protección de los activos de información.

Finalmente, se menciona la aplicación de políticas de seguridad de la información. Las políticas son documentos que establecen las directrices y procedimientos para el manejo y protección de la información de FESNEPONAL. Su implementación

contribuye a establecer un marco de referencia claro y consistente en materia de seguridad de la información.

5.2 POBLACIÓN Y MUESTRA

A todas las personas involucradas, desde los diferentes cargos y roles, por su valiosa contribución en el éxito de la implementación de la norma ISO/IEC 27001:2013. La dedicación, el esfuerzo y la colaboración de todos ustedes han sido fundamentales para garantizar la implementación de la seguridad de la información en la entidad:

Gerente General: Es el responsable general de la organización y de la toma de decisiones estratégicas. Su participación en la gestión de proyectos de TI a través de la asignación de recursos financieros, humanos y técnicos, así como de la definición de los objetivos y prioridades de la organización.

Director de Proyectos de TI: Es el encargado de liderar los proyectos de TI en la organización, desde la planificación hasta la ejecución y entrega. Su participación implica la definición de los objetivos, el plan de trabajo, los recursos necesarios, la asignación de responsabilidades, la gestión de riesgos y la comunicación con los demás departamentos.

Secretaria General: Es la encargada de la gestión administrativa y de apoyo a los diferentes departamentos de la organización. Su participación en proyectos de TI puede ser a través de la coordinación de la documentación, la gestión de la agenda y la logística para reuniones y capacitaciones.

Ingeniero de Comunicaciones y Seguridad: Es el responsable del diseño, implementación y mantenimiento de las redes de comunicaciones y de la seguridad de la información en la organización. Su participación en proyectos de TI implica la definición de los requisitos de infraestructura de red y seguridad, la selección de proveedores y herramientas, y la supervisión de la implementación.

Auxiliar de Tecnología: Es el encargado de brindar soporte técnico en la organización. Su participación en proyectos de TI puede ser a través de la asistencia en la identificación de problemas y la solución de incidencias, la instalación de hardware y software, la actualización de sistemas y la realización de mantenimiento preventivo.

Técnico de Sistemas: Es el encargado de la configuración, administración y mantenimiento de los sistemas informáticos en la organización. Su participación en proyectos de TI puede ser a través de la selección y configuración de software y hardware, la identificación de problemas y la solución de incidencias, y la actualización y mejora continua de los sistemas.

5.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las fuentes de información primarias para llevar a cabo la implementación del sistema de gestión de seguridad de la información son aquellas que se obtuvieron directamente de la organización y su entorno, como:

Documentos internos de la organización, como políticas, procedimientos, manuales, informes, registros, etc.
Entrevistas con los empleados y representantes de la organización para obtener información sobre las prácticas actuales y los posibles riesgos de seguridad de la información.
Análisis de los procesos de negocio y de los flujos de información de la organización.
Análisis de los sistemas de información y de las tecnologías utilizadas por la organización.
Resultados de las evaluaciones de riesgos y de las pruebas de vulnerabilidades realizadas por la organización.
Normas y regulaciones aplicables a la organización, como la norma ISO/IEC 27001:2013, leyes de protección de datos, regulaciones sectoriales, etc.

Para recopilar información se emplean diversas técnicas, entre ellas la observación para registrar los patrones de comportamiento de los usuarios y el personal que integra el Departamento de Tecnología. Además, se lleva a cabo la entrevista no estructurada o conversación con el personal para obtener su opinión personalizada.

6 DESARROLLO DE LOS OBJETIVOS

6.1 DESARROLLO DE OBJETIVO 1: DIAGNÓSTICO INICIAL DE LA ORGANIZACIÓN MEDIANTE LA METODOLOGÍA GAP ALINEADO A LA ISO/IEC 27001:2013 CON EL FIN DE ANALIZAR LAS BRECHAS Y CONOCER LA SITUACIÓN ACTUAL.

Un análisis GAP es una herramienta que se utiliza para comparar dos estados o situaciones diferentes y determinar las diferencias entre ellas. En el ámbito de la seguridad de la información, un análisis GAP se utiliza para evaluar si los controles de seguridad implementados en una organización cumplen con los requisitos de una norma o estándar específico, como la norma ISO/IEC 27001:2013. El análisis GAP permite identificar las diferencias o brechas entre el estado actual de la seguridad de la información y el estado deseado (cumplimiento con la norma), lo que permite desarrollar un plan de acción para cerrar esas brechas y mejorar la seguridad de la información.

6.1.1 Resumen resultados del estado de los requerimientos de la ISO/IEC 27001:2013. La norma ISO/IEC 27001:2013 evalúa los sistemas de gestión de seguridad de la información en una organización a través de 7 cláusulas o dominios:

CONTEXTO DE LA ORGANIZACIÓN: se evalúa la comprensión de la organización y su entorno, y cómo esto afecta la seguridad de la información.

LIDERAZGO: se evalúa el compromiso de la alta dirección con la seguridad de la información y cómo se establecen los roles y responsabilidades en la organización.

PLANIFICACIÓN: se evalúa cómo la organización planifica y establece los objetivos de seguridad de la información y cómo se gestiona el riesgo.

SOPORTE: se evalúa cómo la organización proporciona los recursos y la formación necesaria para implementar y mantener el SGSI.

OPERACIÓN: se evalúa cómo se implementa y controla el SGSI.

EVALUACIÓN DEL DESEMPEÑO: se evalúa cómo se supervisa y mide el rendimiento del SGSI y cómo se realizan las auditorías internas y revisiones por la dirección.

MEJORA CONTINUA: se evalúa cómo se gestiona la mejora continua del SGSI y cómo se toman las acciones correctivas y preventivas.

Cada una de estas cláusulas incluye diferentes requisitos que deben cumplirse para obtener la certificación de la norma ISO/IEC 27001:2013.

Los niveles de madurez son una clasificación que se utiliza para evaluar la capacidad de una organización en términos de calidad de procesos y servicios. El modelo propuesto define siete niveles de madurez que van desde el nivel 1 hasta el nivel 7.

Nivel 1: **No Aplicable** (NA): El requerimiento o control no es aplicable a la organización.
Nivel 2: **No Implementado** (NI): El requerimiento o control no ha sido implementado en la organización.
Nivel 3: **Inicial** (IN): Se caracteriza por tener procesos poco definidos, informales y reactivos, donde la organización tiene dificultades para repetir procesos exitosos y los empleados no están capacitados para realizar su trabajo de manera efectiva.
Nivel 4: **Gestionado** (GE): La organización ha establecido procesos básicos y repetibles para gestionar sus proyectos, con roles y responsabilidades claras, lo que permite mejorar la calidad y eficiencia de los procesos.
Nivel 5: **Establecido** (ES): Los procesos están documentados y estandarizados en toda la organización, y los empleados están capacitados para cumplir con los estándares establecidos.
Nivel 6: **Predecible** (PR): La organización ha implementado un proceso de medición y análisis para monitorear y mejorar el desempeño de sus procesos.
Nivel 7: **Optimizado** (OP): La organización tiene la capacidad de mejorar continuamente sus procesos a través de la innovación y el uso de las mejores prácticas.

El objetivo final es alcanzar el nivel 7, donde la organización tiene la capacidad de mejorar continuamente y adaptarse a los cambios del entorno.
Cada nivel representa un nivel más alto de capacidad y mejora en la gestión de procesos y servicios, y cada nivel es un precursor para el siguiente.

De los 100 controles evaluados, se determinó que ninguno de ellos alcanza el nivel de madurez optimizado (OP), predecible (PR), establecido (ES), gestionado (GE) o inicial (IN). Todos los controles fueron calificados como no implementados (NI) y, por lo tanto, no se están ejecutando. Además, ninguno de los controles se considera no aplicable (NA). En resumen, la organización evaluada no ha implementado ninguno de los controles evaluados, lo que indica una falta de madurez en su sistema de gestión de seguridad de la información.

Cuadro 1 – Los niveles de Madurez

Cantidad	Descripción	Nivel de Madurez	% implementación
0	**OPTIMIZADO** El requerimiento o control se ha implementado, se ejecuta con una frecuencia establecida, responsabilidades bien definidas, se encuentra documentado, cuenta con indicadores y se busca la mejora continua	OP	0%
0	**PREDECIBLE** El requerimiento o control se ha implementado, se ejecuta con una frecuencia establecida, responsabilidades bien definidas, se encuentra documentado y cuenta con indicadores	PR	0%
0	**ESTABLECIDO** El requerimiento o control se ha implementado, se ejecuta con una frecuencia establecida, responsabilidades bien definidas y se encuentra documentado	ES	0%
0	**GESTIONADO** El requerimiento o control se ha implementado y se ejecuta con una frecuencia establecida	GE	0%
0	**INICIAL** El requerimiento o control se ha implementado y se ejecuta de manera inicial	IN	0%
100	**NO IMPLEMENTADO** El requerimiento o control no se ha implementado	NI	100%
0	**NO APLICABLE** El requerimiento o control no aplica	NA	0%
100			**100%**

Fuente: Autoría propia

6.1.2 Estado de la Seguridad de la Información. La seguridad de la información está calificada en un estado básico debido a que no cuenta actualmente con la implantación de un Sistema gestión de la Seguridad de la Información SGSI. Para esta calificación se evaluó todos los controles de los requerimientos de la norma ISO/IEC 27001:2023 dando esta como resultado de NO IMPLEMENTADO y una valoración cuantitativa de 0,0 este se promedió con el resultado del anexo A de la norma ISO/IEC 27002:2013 cuyo resultado es Básico con una valoración cuantitativa de 0,8.

Tenemos:
Estado de la seguridad de la información = Requerimientos de la ISO/IEC 27001 + (Más) El anexo A de la ISO/IEC 27002:2013 / (Dividido) en 2.

Estado de la seguridad de la información = (0,0 + 0,8) / 2 = 0,4 se realiza la clasificación de acuerdo con el cuadro 2 con el nombre de Estados, el cual incluye una valoración Básico en el rango de 0 a 2, una valoración Medio en el rango de 2 a 4, y una valoración Avanzado en el rango 4 a 5.

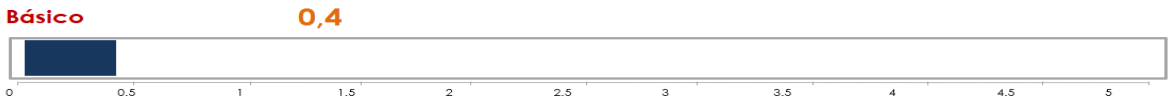
Cuadro 2 - Estados

ITEMS	ESTADO	RANGO
1	BÁSICO	0 - 2
2	MEDIO	2 - 4
3	AVANZADO	4 - 5

Fuente: Autoría propia

El estado general de la seguridad de la información se encuentra en el nivel de madurez Básico con una calificación del 0,4, a continuación se presenta gráficamente esta situación.

Ilustración 3 - Estado de la seguridad de la información



Fuente: Autoría propia

6.1.3 Requerimientos de la ISO/IEC 27001:2013. En este punto de Requerimientos de la ISO/IEC 27001:2013 se evalúan los 100 Controles y las siete (7) Clausulas o Dominios de la norma ISO/IEC 27001:2023, Se tiene en cuenta los siete (7) niveles de madurez ver Cuadro 1, en donde la mayor cantidad de controles se centran en el nivel de madurez NO IMPLEMENTADO con una valoración del 100% correspondiente a 100 controles evaluados.

Cuadro 3 - Nivel de Madurez Constante

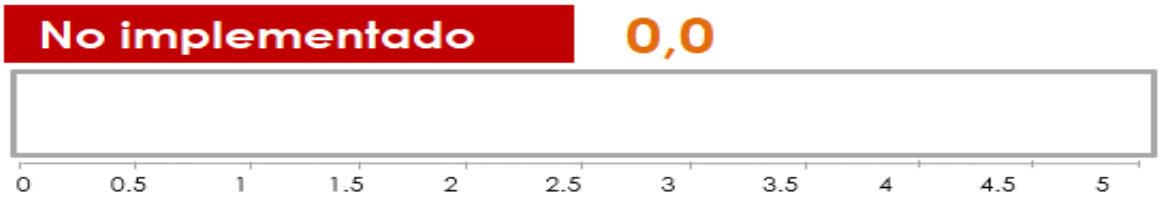
ITEMS	NIVEL DE MADUREZ	CONSTANTE
1	Optimizado	1
2	Predecible	0,8
3	Establecido	0,6
4	Gestionado	0,4
5	Inicial	0,02

Fuente: Autoría propia

Esta métrica nos indica que la entidad FESNEPONAL no reúne los requerimientos iniciales de un plan de seguridad de la información.

En la Ilustración 4 - Requerimientos de la ISO/IEC 27001:2013 se muestra el estado en que se encuentra el nivel de madurez en NO IMPLEMENTADO con una valoración del 0,0 y el resultado depende del promedio de la columna valoración de la Ilustración 1 - Resumen resultados del estado de los requerimientos de la ISO/IEC 27001:2013.

Ilustración 4 - Requerimientos de la ISO/IEC 27001:2013



Fuente: Autoría propia

6.1.4 Resumen resultados del estado de los requerimientos de la ISO/IEC 27001:2013

En la Ilustración 5 - Resumen de resultados del estado de los requerimientos de la norma ISO/IEC 27001:2013, se presenta un resumen detallado de las siete cláusulas de la norma y sus respectivos niveles de madurez. Además, se incluye una valoración de la calificación de evaluación de la norma, que revela un hecho preocupante: de los 100 controles evaluados, se evidencia que el 100% de ellos se encuentra en un estado de NO IMPLEMENTADO.

Ilustración 5 - Resumen resultados del estado de los requerimientos de la ISO/IEC 27001:2013

Requerimientos	Optimizado	Predecible	Establecido	Gestionado	Inicial	No impementada	No aplica	Constante	Valoración	Calificación
Claúsula 4 - Contexto de la organización	0	0	0	0	0	4	0	0,00	0,00	No implementado
Claúsula 5 - Liderazgo	0	0	0	0	0	17	0	0,00	0,00	No implementado
Claúsula 6 - Planificación	0	0	0	0	0	25	0	0,00	0,00	No implementado
Claúsula 7 - Soporte	0	0	0	0	0	19	0	0,00	0,00	No implementado
Claúsula 8 - Operación	0	0	0	0	0	8	0	0,00	0,00	No implementado
Claúsula 9 - Evaluación del Desempeño	0	0	0	0	0	19	0	0,00	0,00	No implementado
Claúsula 10 - Mejora del SGSI	0	0	0	0	0	8	0	0,00	0,00	No implementado
Total	0	0	0	0	0	100	0		0,0	100

Fuente: Autoría propia

6.1.5 Resumen resultados del estado de los controles del Anexo A de la ISO/IEC 27001:2013. A continuación se realiza un breve resumen de las Cláusulas del Anexo A de la norma ISO/IEC 27001:2013:

ANEXO A.5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN: Esta cláusula se centra en establecer una política de seguridad de la información que sirva como marco general para las actividades de seguridad. Incluye la definición de los objetivos de seguridad, la asignación de responsabilidades y la comunicación de la política a todos los empleados.

ANEXO A.6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Esta cláusula aborda la necesidad de establecer una estructura organizativa para gestionar la seguridad de la información. Incluye aspectos como la designación de un responsable de seguridad de la información, la definición de roles y responsabilidades, y la coordinación de actividades relacionadas con la seguridad.

ANEXO A.7 - SEGURIDAD DE LOS RECURSOS HUMANOS: Esta cláusula se refiere a las medidas necesarias para garantizar la seguridad de los recursos humanos de una organización. Incluye aspectos como la verificación de antecedentes, la gestión de los términos y condiciones de empleo, la concienciación y la formación en seguridad de la información.

ANEXO A.8 - GESTIÓN DE ACTIVOS: Esta cláusula se centra en la gestión de los activos de información de una organización. Incluye la identificación de los activos, la clasificación de la información, la gestión de la propiedad y la responsabilidad sobre los activos, así como las medidas para protegerlos adecuadamente.

ANEXO A.9 - CONTROL DE ACCESO: Esta cláusula aborda la necesidad de controlar el acceso a la información y los sistemas de información. Incluye aspectos como la gestión de contraseñas, la autenticación de usuarios, la gestión de privilegios y los controles de acceso físico y lógico.

ANEXO A.10 - CRIPTOGRAFÍA: Esta cláusula se refiere al uso de técnicas de criptografía para proteger la confidencialidad, la integridad y la autenticidad de la

información. Incluye aspectos como el uso de algoritmos criptográficos, la gestión de claves y la protección de la información en tránsito y en reposo.

ANEXO A.11 - SEGURIDAD FÍSICA Y AMBIENTAL: Esta cláusula se centra en la protección de los recursos físicos y el entorno en el que se encuentran los sistemas de información. Incluye aspectos como la protección contra amenazas físicas, el control de acceso a las instalaciones, la gestión de dispositivos móviles y la protección contra incendios y desastres naturales.

ANEXO A.12 - SEGURIDAD EN LAS OPERACIONES DE SISTEMAS: Esta cláusula aborda la necesidad de implementar controles para garantizar la seguridad en las operaciones de los sistemas de información. Incluye aspectos como la gestión de cambios, la gestión de incidentes, la copia de seguridad y la recuperación de datos, y la gestión de registros y registros de auditoría.

ANEXO A.13 - SEGURIDAD DE LAS COMUNICACIONES: Esta cláusula se refiere a la protección de las comunicaciones de la información. Incluye aspectos como la gestión de la seguridad de la red, el uso de protocolos seguros, el cifrado de datos en tránsito y la protección contra el acceso no autorizado a la información transmitida.

ANEXO A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS: Esta cláusula aborda la seguridad en el ciclo de vida de los sistemas de información. Incluye aspectos como la gestión de la seguridad en la adquisición de sistemas, el desarrollo seguro de aplicaciones, las pruebas de seguridad y la gestión de la seguridad en los sistemas heredados.

ANEXO A.15 - RELACIONES CON LOS PROVEEDORES: Esta cláusula se centra en establecer controles de seguridad para las relaciones con los proveedores de servicios y productos relacionados con la seguridad de la información. Incluye aspectos como la evaluación de proveedores, la gestión de contratos y acuerdos de servicio, y la seguridad en la cadena de suministro.

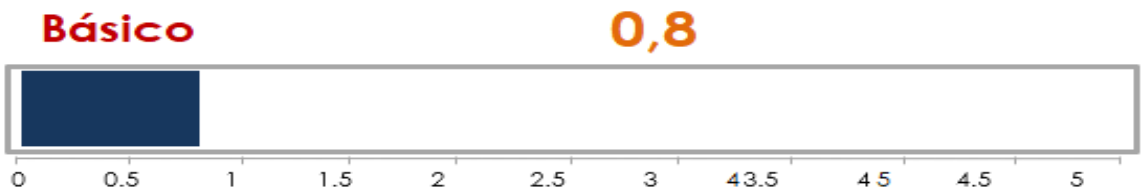
ANEXO A.16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Esta cláusula se refiere a la gestión de incidentes de seguridad de la información. Incluye aspectos como la identificación, el registro, la gestión y la resolución de incidentes de seguridad, así como el seguimiento y la mejora continua de los procesos de gestión de incidentes.

ANEXO A.17 - ASPECTOS DE SI EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO: Esta cláusula aborda la necesidad de incorporar la seguridad de la información en la gestión de la continuidad del negocio. Incluye aspectos como la planificación de la continuidad del negocio, la gestión de la respuesta a incidentes y la recuperación de desastres, y la coordinación de las actividades de seguridad durante una interrupción.

ANEXO A.18 - CUMPLIMIENTO: Esta cláusula se refiere a la necesidad de cumplir con los requisitos legales, reglamentarios y contractuales relacionados con la seguridad de la información. Incluye aspectos como la identificación y el cumplimiento de los requisitos legales, la gestión de registros, la protección de la información personal y la gestión de auditorías y revisiones de cumplimiento.

6.1.6 Controles de ANEXO A de la ISO/IEC 27001:2013. En la Ilustración 6 - Controles de ANEXO A de la ISO/IEC 27001:2013, se evidencian los resultados arrojados de la evaluación de la entidad FESNEPONAL, e incluye el Anexo A de la norma ISO/IEC 27002:2013 la cual contemplan los 114 controles de la norma, y la califica en un nivel de madurez en un estado BÁSICO con una valoración de 0,8, y el resultado depende del promedio de la columna valoración de la Ilustración 7 - Resumen resultados de los controles del ANEXO A de la ISO/IEC 27001:27001, lo cual indica que no tienen implementado controles o si los tienen no los tienen documentado según la norma lo exige.

Ilustración 6 - Controles de ANEXO A de la ISO/IEC 27001:2013



Fuente: Autoría propia

6.1.7 Resumen resultados de los controles del ANEXO A de la ISO/IEC 27001. En la Ilustración 7 - Resumen resultados de los controles del ANEXO A de la ISO/IEC 27001:27001 se presentan los 114 controles pertenecientes a los 14 Clausulas o dominios del anexo A de la norma ISO/IEC 27001:2013 la mayoría de los controles evaluados tienen una calificación "Básico", lo que indica que están en un nivel inicial o básico de madurez. Algunos controles tienen una calificación "Medio", lo que sugiere que están en un nivel intermedio de madurez. Se dejan a disposición de la gerencia las medidas a adoptar con relación a esta evaluación inicial indicando todos los riesgos posibles a no implementación de políticas de seguridad de la información.

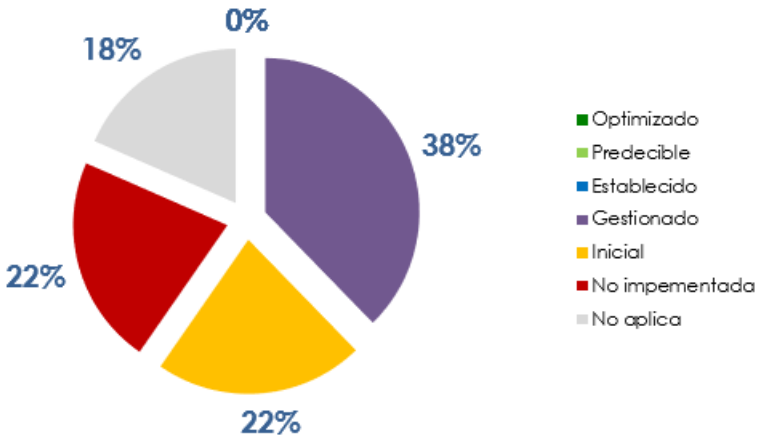
Ilustración 7 - Resumen resultados de los controles del ANEXO A de la ISO/IEC 27001

Controles	Optimizado	Predecible	Establecido	Gestionado	Inicial	No impementada	No aplica	Contante	Valoración	Calificación
Anexo A.5 - Políticas de seguridad de la información	0	0	0	0	0	2	0	0,00	0,00	No implementado
Anexo A.6 - Organización de la seguridad de la información	0	0	0	1	3	3	0	0,07	0,33	Básico
Anexo A.7 - Seguridad de los recursos humanos	0	0	0	1	1	1	3	0,14	0,70	Básico
Anexo A.8 - Gestión de activos	0	0	0	6	3	1	0	0,25	1,23	Básico
Anexo A.9 - Control de acceso	0	0	0	9	4	1	0	0,26	1,31	Básico
Anexo A.10 - Criptografía	0	0	0	0	0	2	0	0,00	0,00	No implementado
Anexo A.11 - Seguridad física y ambiental	0	0	0	6	6	1	2	0,19	0,97	Básico
Anexo A.12 - Seguridad en las operaciones de Sistemas	0	0	0	8	1	1	4	0,32	1,61	Básico
Anexo A.13 - Seguridad de las comunicaciones	0	0	0	3	0	4	0	0,17	0,86	Básico
Anexo A.14 - Adquisición, desarrollo y mantenimiento de sistemas	0	0	0	1	2	0	10	0,15	0,73	Básico
Anexo A.15 - Relaciones con los proveedores	0	0	0	2	2	1	0	0,17	0,84	Básico
Anexo A.16 - Gestión de incidentes de seguridad de la información	0	0	0	0	1	6	0	0,00	0,01	Básico
Anexo A.17 - Aspectos de SI en la gestión de continuidad del negocio	0	0	0	4	0	0	0	0,40	2,00	Medio
Anexo A.18 - Cumplimiento	0	0	0	2	2	2	2	0,14	0,70	Básico
Total	0	0	0	43	25	25	21		0,8	114

Fuente: Autoría propia

Esta evaluación contempla todos los controles del ANEXO A de la norma ISO/IEC 27002:2013, donde se relacionan los 114 controles sus 18 anexos, el 38% se centra en controles gestionados con un resultado de 43, 22% en controles iniciales con resultado de 25, el 22% en controles no implementados con un resultado de 25, en 18% en controles que no aplican a la organización con un resultado de 21, como se puede observar gráficamente en la Ilustración 8 - Resumen resultados de los controles del ANEXO A de la ISO/IEC 27001 porcentajes, se deduce una calificación del 0,8 en la cual la gerencia debería tomar medidas al respecto y agilizar la implementación del sistema gestión de seguridad de la información basado en la ISO/IEC 27001:2013, ya que en la actualidad se ha incrementado bastante los riesgos a los sistemas informáticos.

Ilustración 9 - Resumen resultados de los controles del ANEXO A de la ISO/IEC 27001 porcentajes



Fuente: Autoría propia

6.2 DESARROLLO DEL OBJETIVO 2: VULNERABILIDADES, AMENAZAS Y RIESGO DE LOS ACTIVOS DE INFORMACIÓN DEL ÁREA TI MEDIANTE EL USO DE LA METODOLOGÍA MAGERIT PARA PODER GESTIONAR EL IMPACTO DE LOS RIESGOS ASOCIADOS.

6.2.1 Identificación y valoración de activos. Para identificar los activos del área de IT de FESNEPONAL utilizaremos una metodología llamada “MAGERIT”, la cual, define activo como los “Recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección” y los identifica y divide de la siguiente manera:

- Datos / Información: Es el activo esencial de la organización, ósea los datos que se generan y procesan.
- Aplicaciones Informáticas: Es el software que permite el manejo de la información o datos.
- Equipos informáticos: Es el hardware que permite el almacenamiento de la información o datos, de las aplicaciones y servicios.
- Equipamiento Auxiliar: Todos los equipos que son apoyo para los equipos informáticos.
- Servicios: Son los activos que se pueden prestar, así como los que son necesarios para el procesamiento o gestión de la información.
- Redes de comunicaciones: Son los activos que permiten el intercambio de información o datos.
- Instalaciones: Son los activos en donde están alojados los equipos informáticos y de comunicaciones.
- Personal: Personal que administra y manipula todos los activos anteriormente citados.

Se valora el riesgo de manera cuantitativa, lo cual permite la obtención de la información a partir de la cuantificación de los datos sobre variables. Las dimensiones de seguridad sobre las cuales se realizará la valoración cuantitativa de los activos son:
Confidencialidad (C): es cuando la información no se coloca a disposición ni se revela a individuos, entidades o procesos no autorizados.
Integridad (I): es el mantenimiento de la exactitud y estado completo de la información y sus métodos de proceso.
Disponibilidad (D): es el acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

MAGERIT utiliza la escala estándar, va del 0 al 10 siendo el (0) un valor despreciable y (10) el valor más alto. Así mismo cada valor dentro de la escala representa un criterio de niveles de daño ocasionado por la ausencia de confidencialidad, disponibilidad e integridad como se ve en el cuadro 4 – Criterios de valoración de activos presenta un puntaje de 10 con un valor muy alto (MA) y corresponde a un criterio de daño muy grave, un puntaje de 7 a 9 con un valor alto (A) y corresponde a un criterio de daño grave, un puntaje de 4 a 6 con un valor medio (MA) y corresponde a un criterio de daño importante, un puntaje de 1 a 3 con un valor bajo (B) y corresponde a un criterio de daño menor y un puntaje de 0 con un valor despreciable (MB) y corresponde a un criterio de daño irrelevante:

Cuadro 4 - Criterios de valoración de activos

VALOR			CRITERIO
10	Muy Alto	MA	Daño muy grave
7-9	Alto	A	Daño grave
4-6	Medio	MA	Daño importante
1-3	Bajo	B	Daño menor
0	Despreciable	MB	Irrelevante

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, 2012.

Se puede considerar Daño muy grave [10] a:

- Daños excepcionalmente serios que pueden afectar la eficacia o la seguridad del objetivo operativo o logístico del área de IT de FESNEPONAL.
- Daños que pueden causar un incumplimiento grave en un contrato o normas ya sean externas o internas.
- Daños que puedan causar un incidente serio de seguridad y dificulte la investigación de los mismos.
- Daños que pueden causar grandes pérdidas económicas.
- Daños que pueden causar la pérdida de confidencialidad de Datos o información clasificada como secreta para el área de IT en FESNEPONAL.

Se puede considerar daño Grave [7-9] a:

- Daños que pueden causar una interrupción de las actividades del área IT con un impacto para las demás áreas de la organización.
- Daños que pueden causar una publicidad negativa del área IT a nivel general con las demás áreas de la organización.
- Daños que pueden causar la pérdida de confidencialidad de Datos o información clasificada como reservada o confidencial para FESNEPONAL.

Se puede considerar daño Importante [4-6] a:

- Daños que pueden afectar labores de un grupo de individuos del área IT o un área de FESNEPONAL.
- Daños que pueden causar la pérdida de confidencialidad de Datos o información clasificada como de difusión limitada para el área IT.
- Daños que pueden causar la interrupción de actividades propias del área IT.

Se puede considerar daño menor [1-3] a:

- Daños que probablemente causen interrupción de las actividades propias del área IT.
- Daños que probablemente afecten a un individuo del área IT.
- Daños que pueden causar mal manejo de información clasificada como sin clasificar para el área IT de FESNEPONAL.

Se puede considerar daño despreciable [0] a:

- Daños que no afectan las actividades propias del área IT.
- Daños que no afectan la eficacia o la seguridad del objetivo operativo o logístico del área.
- Daños que no afectan a los individuos del área IT.
- Daño que no causan incumplimiento de un contrato o normas, ya sean externas o internas.

La suma de la valoración de las tres variables sobre el activo determina el valor total del activo en el proceso de IT. El valor máximo de un activo es 30 y mínimo es 0. La valoración total del activo será clasificada como lo relaciona el cuadro 5 – Clasificación de valoración de activos en escala de colores con un valor de 0 a 10 tendrá una clasificación de Bajo, un valor de 10 a 20 tendrá una clasificación de Medio y un valor de 20 a 30 tendrá una clasificación de Alto.

Cuadro 5 - Clasificación de valoración de activos en escala de colores

VALOR	CLASIFICACIÓN
0-10	Bajo
10-20	Medio
20-30	Alto

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, 2012.

6.2.2 Desarrollo de la metodología para la identificación y valoración de activos en el área de IT de FESNEPONAL. El cuadro 6 – Identificación de activos de información se presenta la aplicación de la metodología MAGERIT en la entidad FESNEPONAL, con el objetivo de gestionar los riesgos de seguridad de la información de manera efectiva y garantizar la protección de los activos de la organización, la identificación de los activos de información de clasifican en ocho (8) grupos:

Grupo 1 - Datos e Información: Este grupo se centra en la clasificación de los activos relacionados con datos e información.

Grupo 2 - Aplicaciones: Aquí se incluyen los activos vinculados a las aplicaciones utilizadas en la organización.

Grupo 3 - Equipos Informáticos: Este grupo engloba los activos que comprenden los equipos de cómputo.

Grupo 4 - Equipos Auxiliares: En esta categoría se encuentran los activos auxiliares relacionados con los equipos informáticos.

Grupo 5 - Servicios Internos: Este grupo se relaciona con los activos que representan servicios internos dentro de la organización.

Grupo 6 - Redes de Comunicación: Aquí se agrupan los activos vinculados a las redes de comunicación utilizadas.

Grupo 7 - Instalaciones: Esta categoría abarca los activos que se refieren a las instalaciones físicas de la organización.

Grupo 8 - Personal: Por último, este grupo se refiere a los activos relacionados con el personal de la organización.

Cuadro 6 - Identificación de activos de Información

IDENTIFICACIÓN DE ACTIVOS IT FESNEPONAL Metodología Magerit			
Grupo	**Tipo de activo**	**Nombre del Activo**	**Descripción**
1	[D/I] Datos e información	Base de datos TREBOLSIFONE	Base de datos en donde se registra información la información contable y financiera de la entidad.
		Archivos en Dispositivo NAS	File server donde se aloja la información de todas las áreas.
		Página web	https://www.fesneponal.com/
		Diagrama general de red	Diagrama de la red de FESNEPONAL y sus instalaciones
		Inventario de equipos y direcciones IPs.	Archivo con el inventario de IPs y equipos
		Procedimientos, manuales y formatos del área	Todo lo relacionado a gestión documental

2	[SW] Aplicaciones	Correo electrónico	Correo que permite la comunicación entre las áreas y externos.
		Ofimática	Suite de office instalada en los equipos de los usuarios
		Antivirus	Sophos Endpoint
		Oficina Virtual	Software gestión de requerimientos de asociados.
		Sistema Operativo	Sistemas operativos W10 en usuarios, Windows server en servidores y Linux.
		Otros Software	HelpDesk
			Issabel
3	[HW] Equipos informáticos	Computadores	Estaciones de trabajo de los usuarios
		Servidor de dominio	Roles de directorio activo, DNS y Servicios de Red.
		Servidor de aplicaciones	MSSQLSERVER
		Servidor Oficina Virtual	SrvOVirtual
		Almacenamiento en Red - NAS	SrvNAS
		Servidor de Terminal Server	Servidor de Acceso Remoto
		Servidor Issabel	PBX (Planta Telefónica)
		Teléfonos IP	Estaciones de Voip de las oficinas
		Firewall	Dispositivo de seguridad perimetral
		Impresora	Dispositivos de impresion
4	Equipos Auxiliares	Cableado	Cableado estructurado (voz, datos y eléctrico)
		UPS	Sistema de alimentación ininterrumpida - APC
		Mobiliario	Mobiliario de oficinas
		CCTV	Circuito cerrado de televisión de las diferentes Áreas
5	[IS] Servicios Internos	[Voip] Telefonía IP	Telefonía local y comunicación entre extensiones
		Soporte técnico	Soporte técnico del área IT a los usuarios
		Internet	Servicio de Internet
6	[RCOM] Redes de comunicación	Wifi	servicio de internet inalámbrico
		LAN	Conexión de red de área local
		Switch	Dispositivo de comunicación de la red de datos
7	[I] Instalaciones	Datacenter	Centro de datos
		Oficinas de IT	Oficinas
8	[P] Personal	Director de IT	Coordinador del área
		Técnicos de IT	Técnicos

Fuente: Autoría propia

6.2.3 Valoración de activos IT- FESNEPONAL. El cuadro 7 toma la información del cuadro 6 la identificación de los activos de información donde se asigna una valoración de 0 a 10 según el cuadro 4 criterios de valoración de activos de información, donde corresponda y se presenta la valoración de los activos de TI en cuanto a los pilares de la seguridad de la información (D) Disponibilidad, (I) Integridad, (C) Confidencialidad, la columna valoración total incluye la sumatoria de los tres pilares de la información y se clasifica de acuerdo al cuadro 5 Clasificación de valoración de activos en escala de colores .

Cuadro 7 - Valoración de activos IT

VALORACIÓN DE ACTIVOS IT- FESNEPONAL Metodología Magerit					
TIPO DE ACTIVO	**NOMBRE DEL ACTIVO**	**VALORACIÓN**			**VALORACIÓN TOTAL DEL ACTIVO (C+I+D)**
		C	**I**	**D**	
[D/I] Datos e información	Base de datos TREBOLSIFONE	9	9	9	27
	Archivos en Dispositivo NAS	10	9	9	28
	Página web	6	6	4	16
	Diagrama general de red	3	3	3	9
	Inventario de equipos y direcciones Ips.	7	6	5	18
	Procedimientos, manuales y formatos del área	6	6	5	17
[SW] Aplicaciones	Correo electrónico	10	8	8	26
	Ofimática	3	6	9	18
	Antivirus	7	7	8	22
	Sistema operativo	6	5	5	16
	Issabel	4	4	5	13
[HW] Equipos informáticos	Computadores	3	3	3	9
	Servidor de dominio	4	6	8	18
	Servidor de aplicaciones	6	6	9	21
	Servidor de ERP	4	5	5	14
	Servidor NAS	8	8	7	23
	Servidor Oficina Virtual	3	6	6	15
	Firewall	3	6	6	15
	Telefonos IP	2	3	4	9
	Firewall	4	8	10	22
	workstation	4	6	6	16
	Impresoras	4	5	6	15
[AUX] Equipamiento auxiliar	Servicio eléctrico (generadores)	4	6	9	19
	Cableado	4	6	9	19
	UPS	4	6	9	19

	Mobiliario	3	3	3	9
	CCTV	8	6	9	23
[IS] Servicios Internos	[Voip] Telefonía IP	3	3	3	9
	Soporte técnico	4	6	9	19
	Internet	4	6	8	18
[RCOM] Redes de comunicación	Wifi	3	3	3	9
	LAN	4	7	8	19
	Switch	4	7	7	18
	Routers	4	7	8	19
[I] Instalaciones	Datacenter	8	7	9	24
	Oficinas de IT	3	6	6	15
[P] Personal	Director de IT	6	10	6	22
	Técnicos de IT	0	10	10	20

Fuente: Autoría Propia

6.2.4 Identificación y valoración de amenazas IT- FESNEPONAL: El siguiente paso en la metodología MAGERIT consiste en determinar las amenazas que puedan afectar a cada activo. Cuando se ha determinado si una amenaza afecta a un activo se debe realizar un estimado de que tanto es vulnerable el activo en dos aspectos:

Impacto: Que tan perjudicado resultaría el activo.

Frecuencia: Cada cuanto se materializa la amenaza.

La metodología MAGERIT determina estos dos valores tal cual lo relaciona el cuadro 8 valoración de frecuencia e impacto:

Cuadro 8 - Valoración de frecuencia e impacto

FRECUENCIA	DESCRIPCIÓN	IMPACTO	DESCRIPCIÓN
5	Muy frecuente (A diario)	5	Muy alto
4	Frecuente (Mensual)	4	Alto
3	Normal (Una vez al año)	3	Medio
2	Poco frecuente (Cada varios años)	2	Bajo
1	Nunca ocurre	1	Sin impacto

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, 2012.

En el cuadro 9 identificación y valoración de amenazas se identifican y valoran las amenazas más importantes a las que están expuestos los activos del área IT de FESNEPONAL. Se identifican las amenazas con respecto a la frecuencia e impacto.

Cuadro 9 - Identificación y valoración de amenazas IT

IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS IT- FESNEPONAL Metodología Magerit				
TIPO DE ACTIVO	**NOMBRE DEL ACTIVO**	**AMENAZAS**	**FRECUENCIA**	**IMPACTO**
[D/I] Datos e información	Base de datos SVRVMDVSDATA Archivos en Dispositivo NAS Página web Diagrama general de red Inventario de equipos y direcciones IPs. Procedimientos, manuales y formatos del área	Accesos no autorizados	2	5
		Robo de información	1	5
		Destrucción de información	1	5
		Error humano	3	4
		Pérdida de información	2	5
[SW] Aplicaciones	Correo electrónico Ofimática Antivirus Sistema operativo Issabel	Errores de configuración	3	4
		Difusión de software malicioso	2	4
		Vulnerabilidades de las aplicaciones	2	5
		Errores de mantenimiento y/o actualizaciones	3	4
		Accesos no autorizados	2	4
		Daño de software	2	5
[HW] Equipos informáticos	Computadores Servidor de dominio Servidor de aplicaciones Servidor de ERP Servidor NAS Servidor Oficina Virtual Firewall Teléfonos IP Firewall Workstation Impresoras	Daños físicos (rotura, agua, sobretensión)	2	5
		Errores de configuración	3	4
		Corte de fluido eléctrico	2	5
		Errores de mantenimiento y/o actualizaciones	3	4
		Uso indebido	4	2
		Robo / pérdida	1	5
		Accesos no autorizados	2	4
[AUX] Equipamiento auxiliar	Servicio eléctrico (generadores) Cableado UPS Mobiliario CCTV	Averías	3	5
		Contaminación	2	3
		Corte de fluido eléctrico	2	5
		Fallo servicio de videograbación	2	5
		Denegación de servicios	2	4
		Robo	1	5

[IS] Servicios Internos	[Voip] Telefonía IP Soporte técnico Internet	Errores de usuarios	3	3
		Fallo en el proveedor de servicios	2	4
		Tiempos de respuesta altos	2	4
[RCOM] Redes de comunicación	Wifi LAN Antenas de radioenlace Switch Routers	Averías	3	5
		Fallo de servicio de comunicaciones	2	4
		Error humano	3	4
		Corte de fluido eléctrico	2	5
		Mala cobertura	3	4
[I] Instalaciones	Datacenter Oficinas de IT	Averías / vandalismo	1	5
		Corte de fluido eléctrico	2	5
		Accesos no autorizados	2	5
[P] Personal	Director de IT Técnicos de IT	Indisponibilidad del personal	4	3
		Extorsión	1	5
		Deficiencias	2	4
		Ingeniería social	3	4

Fuente: Autoría Propia

6.2.5 Identificación y valoración del riesgo IT – FESNEPONAL. El riesgo es la medida del daño probable sobre un sistema, al conocer el impacto de las amenazas de los activos se puede calcular el riesgo, teniendo en cuenta la frecuencia de la ocurrencia. La siguiente fórmula permite determinar el valor del riesgo que tiene un activo de información:

Vlr.Total de activo **x** Vlr.Frecuencia de amenaza **x** Vlr. Impacto **=** Vlr.Riesgo

En el siguiente cuadro se presenta la valoración del tratamiento del riesgo, el cual es un proceso clave dentro de la gestión de riesgos. Consiste en evaluar las opciones disponibles para abordar los riesgos identificados y determinar la mejor estrategia para reducir, mitigar o transferir los riesgos.

Cuadro 10 – Escala valoración del riesgo

VLR. RIESGO	NIVEL		TRATAMIENTO
0-149	Bajo	Aceptable	Aceptar el riesgo, se debe analizar costo beneficio para decidir si asumir el riesgo.
150-299	Medio	Importante	Reducir, compartir o transferir el riesgo, se debe crear planes que mitiguen la materialización del riesgo.

300-750	Alto	Inaceptable	Evitar, reducir, o trasferir el riesgo. Se debe en lo posible eliminar la actividad que genera el riesgo en la medida que sea posible.

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, 2012.

En el siguiente cuadro se realiza la identificación y valoración de los riesgos más significativos a los que está expuesta el área de Tecnologías de la Información (IT) de FESNEPONAL. Se ha dado especial énfasis a aquellos riesgos que han sido evaluados como generadores de un valor de activo ALTO, lo que indica que su impacto potencial en los activos de la organización es considerado significativo.

Cuadro 11 - Identificación y valoración del riesgo IT

IDENTIFICACIÓN Y VALORACIÓN DEL RIESGO IT- FESNEPONAL Metodología Magerit							
TIPO DE ACTIVO	**NOMBRE DEL ACTIVO**	**VR TOTAL ACTIVO**	**AMENAZAS**	**FRECUENCIA**	**IMPACTO**	**RIESGO ASOCIADO A LA AMENAZA**	**VALOR DEL RIESGO**
[D/I] Datos e información	Base de datos TREBOLSIFONE	27	Accesos no autorizados	2	5	Pérdida de integridad y confidencialidad en las bases de datos	270
			Robo de información	1	5	No disponibilidad de las BD	135
			Error humano	3	4	Pérdida de integridad en las bases de datos	324
			Pérdida de información	2	5	Errores en la operación y la No disponibilidad de la BD	270
	Archivos en Dispositivo NAS	28	Accesos no autorizados	1	5	Pérdida de integridad y confidencialidad	140
			Robo de información	2	5	No disponibilidad de los archivos	280
			Error humano	3	4	Pérdida de integridad en los archivos	336
			Pérdida de información	1	5	Errores en la operación y la No disponibilidad	140
[SW] Aplicaciones	Correo electrónico	26	Errores de configuración	3	4	No disponibilidad del correo	312
			Difusión de software malicioso	2	4	Daño en el aplicativo del correo	208
			Vulnerabilidades de las aplicaciones	2	5	Daño en el aplicativo del correo	260
			Errores de mantenimiento y/o actualizaciones	2	5	No disponibilidad del correo	260

			Accesos no autorizados	2	4	Pérdida de confidencialidad del correo	208
	Antivirus	22	Difusión de software malicioso	2	5	Daño en el Endpoint	220
			Errores de mantenimiento y/o actualizaciones	3	5	No disponibilidad del antivirus	330
			Errores de configuración	3	5	No disponibilidad del antivirus	330
[HW] Equipos informáticos	Servidor de aplicaciones	21	Daños físicos (rotura, agua, sobretensión)	2	5	No disponibilidad en el servidor	210
			Errores de configuración	3	4	No disponibilidad e integridad en el servidor	252
			Corte de fluido eléctrico	3	5	No disponibilidad en el servidor	315
			Errores de mantenimiento y/o actualizaciones	3	4	No disponibilidad en el servidor	252
			Robo / pérdida	1	5	No disponibilidad, confidencialidad en el servidor	105
			Accesos no autorizados	2	4	No confidencialidad	168
	Servidor NAS	23	Daños físicos (rotura, agua, sobretensión)	2	5	No disponibilidad de la NAS	230
			Errores de configuración	3	4	No integridad de la NAS	276
			Corte de fluido eléctrico	2	4	No disponibilidad de la NAS	184
			Errores de mantenimiento y/o actualizaciones	3	4	No disponibilidad de la NAS	276
			Uso indebido	2	4	No Integridad, confidencialidad de la NAS	184
			Robo / pérdida	1	5	No disponibilidad de la NAS	115
	Firewall	22	Errores de configuración	4	4	No disponibilidad, integridad del firewall	352
			Corte de fluido eléctrico	2	5	No disponibilidad del firewall	220
			Errores de mantenimiento y/o actualizaciones	3	4	No disponibilidad del firewall	264
			Robo / pérdida	1	5	No disponibilidad del firewall	110
			Accesos no autorizados	2	4	No confidencialidad del firewall	176
[AUX] Equipamiento auxiliar	CCTV	23	Averías	3	5	No disponibilidad del CCTV	345
			Corte de fluido eléctrico	3	4	No disponibilidad del CCTV	276

			Fallo servicio de videograbación	2	5	No disponibilidad, integridad del CCTV	230
			Denegación de servicios	2	4	No disponibilidad del CCTV	184
			Robo	2	5	No disponibilidad y confidencialidad del CCTV	230
[I] Instalaciones	Datacenter	24	Averías / vandalismo	1	5	No disponibilidad en los servicios tecnológicos	120
			Corte de fluido eléctrico	2	5	No disponibilidad en los servicios tecnológicos	240
			Accesos no autorizados	2	5	No confidencialidad en el DC	240
[P] Personal	Director de IT	22	Indisponibilidad del personal	1	4	No disponibilidad del área IT	88
			Deficiencias	1	4	No disponibilidad del área IT	88
			Ingeniería social	2	4	No disponibilidad, integridad, confidencialidad del área IT	176

Fuente: autoría propia

El activo de la “Base de datos TREBOLSIFONE” y su evaluación en relación con la amenaza del Error humano. Esta amenaza se refiere a los errores cometidos por personas en el manejo y gestión de la base de datos, lo que podría resultar en la pérdida de integridad de los datos almacenados.

El riesgo asociado a esta amenaza se ha valorado como alto, con una puntuación de 324. La valoración del riesgo se basa en diferentes factores, como la probabilidad de que ocurra un error humano, la vulnerabilidad de la base de datos ante estos errores y el impacto potencial en la integridad de los datos.

Una valoración alta indica que existe una alta probabilidad de que ocurran errores humanos y que la base de datos es vulnerable a dichos errores. Además, el impacto de una pérdida de integridad en la base de datos se considera significativo.

Con esta información, se reconoce la importancia de implementar medidas y controles adecuados para minimizar la probabilidad de errores humanos y mitigar los posibles impactos en la integridad de la base de datos TREBOLSIFONE.

El activo "Archivos en Dispositivo NAS" y su evaluación en relación a la amenaza del Error humano. Esta amenaza implica los posibles errores cometidos por personas en la gestión y manipulación de los archivos almacenados en el dispositivo NAS.

El riesgo asociado a esta amenaza ha sido valorado como alto, con una puntuación de 336. La valoración del riesgo se basa en varios factores, como la probabilidad de

que se produzca un error humano, la vulnerabilidad del dispositivo NAS frente a estos errores y el impacto potencial en la integridad de los archivos.
Una valoración alta indica que existe una alta probabilidad de que se produzcan errores humanos y que el dispositivo NAS es vulnerable a dichos errores. Además, se considera que la pérdida de integridad de los archivos tendría un impacto significativo.

El activo "correo electrónico" y su evaluación con relación a la amenaza del Error de configuración. Esta amenaza se refiere a los posibles errores cometidos durante la configuración del sistema de correo electrónico, lo que podría resultar en la falta de disponibilidad del servicio de correo.
El riesgo asociado a esta amenaza se ha valorado como 312, lo que indica una valoración alta. La valoración del riesgo se basa en diferentes factores, como la probabilidad de que ocurra un error de configuración, la vulnerabilidad del sistema de correo ante estos errores y el impacto potencial en la disponibilidad del servicio de correo.
Una valoración alta implica que existe una alta probabilidad de que se produzcan errores de configuración y que el sistema de correo electrónico es vulnerable a dichos errores. Además, la falta de disponibilidad del servicio de correo se considera un impacto significativo.

El activo antivirus en cuanto a la amenaza de errores de mantenimiento y/o actualizaciones tiene un riesgo asociado de no disponibilidad del antivirus con una valoración de 330, Para mitigar este riesgo, es importante implementar medidas de control adecuadas. Esto puede incluir la planificación y ejecución adecuada de los procesos de mantenimiento y actualización del antivirus, la realización de pruebas y validaciones periódicas, la capacitación del personal responsable del mantenimiento, y la implementación de procedimientos de respaldo y recuperación en caso de fallas en el antivirus. Además, es fundamental seguir las recomendaciones y mejores prácticas proporcionadas por el fabricante del software antivirus.

El activo "antivirus" y su evaluación con relación a la amenaza de errores de configuración. Esta amenaza se refiere a posibles errores que puedan ocurrir durante la configuración del software antivirus, lo que podría resultar en la falta de disponibilidad del antivirus.
El riesgo asociado a esta amenaza se ha valorado como 330, lo que indica una valoración alta. La valoración del riesgo se basa en diferentes factores, como la probabilidad de que ocurran errores durante la configuración del antivirus, la

vulnerabilidad del software ante estos errores y el impacto potencial en la disponibilidad del antivirus.
Una valoración alta implica que existe una alta probabilidad de que se produzcan errores de configuración y que el antivirus sea vulnerable a dichos errores. La falta de disponibilidad del antivirus se considera un impacto significativo, ya que podría dejar al sistema expuesto a amenazas de malware y otros ataques cibernéticos.

El activo Servidor de aplicaciones en cuanto a la amenaza Corte de fluido eléctrico tiene un riesgo asociado de no disponibilidad en el servidor con una valoración de 315, Para mitigar este riesgo, es importante implementar medidas de control adecuadas. Esto puede incluir la instalación de sistemas de respaldo de energía, como generadores eléctricos o UPS (Sistemas de Alimentación Ininterrumpida), para garantizar una alimentación continua del servidor de aplicaciones en caso de un corte de fluido eléctrico. Además, es recomendable realizar pruebas regulares de los sistemas de respaldo para verificar su funcionamiento adecuado.

El activo firewall en cuanto a la amenaza Errores de configuración tiene un riesgo asociado de No disponibilidad, integridad del firewall con una valoración de 352,
Para mitigar este riesgo, es importante implementar medidas de control adecuadas. Esto incluye seguir buenas prácticas de configuración del firewall, como utilizar configuraciones estándar recomendadas, mantener actualizado el firmware del firewall y realizar auditorías periódicas para identificar posibles errores o vulnerabilidades.

6.3 DESARROLLO DEL OBJETIVO 3: APLICABILIDAD BASADO EN LA NORMA ISO/IEC 27002:2013 CON EL FIN DE ESTABLECER BUENAS PRÁCTICAS DE SEGURIDAD Y MITIGAR EL RIESGO.

La norma ISO/IEC 27002:2013 proporciona directrices y mejores prácticas para la implementación de los controles de seguridad de la información especificados en el Anexo A de la norma ISO/IEC 27001:2013. El Anexo A, también conocido como "Control Objectives and Controls" (Objetivos de Control y Controles), enumera una serie de controles de seguridad de la información que pueden aplicarse en una organización para proteger la confidencialidad, integridad y disponibilidad de la información.

La Declaración de Aplicabilidad (SOA) se utiliza en el contexto de la norma ISO/IEC 27001:2013 para identificar y justificar los controles específicos del Anexo A que serán aplicables en una organización en función de su evaluación de riesgos y contexto específico. La SOA se basa en los resultados de la evaluación de riesgos y establece qué controles se implementarán, cuáles se excluyen y cómo se justifica su aplicabilidad.

1. TIPO DE ACTIVO:	[D/I] Datos e información
NOMBRE DEL ACTIVO:	Base de datos TREBOLSIFONE
VR TOTAL ACTIVO:	27
AMENAZAS:	Error humano
FRECUENCIA:	3
IMPACTO:	4
RIESGO ASOCIADO A LA AMENAZA:	Pérdida de integridad en las bases de datos
VALOR DEL RIESGO:	324
SALVAGUARDA:	Implementar un ambiente de pruebas antes de salir a operación
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	129,6
SOA – APLICABILIDAD:	18.1.4 Protección de datos y privacidad de la información personal.

PLAN DE ACCIÓN:

- Implementar mecanismos de autenticación y autorización para garantizar que solo usuarios autorizados tengan acceso y capacidad de modificar los datos.
- Realizar copias de respaldo periódicas de las bases de datos y garantizar su almacenamiento seguro para facilitar la restauración en caso de pérdida o corrupción de datos.

- Implementar controles de detección de intrusiones y monitoreo de actividad para identificar y responder rápidamente a cambios no autorizados en los datos.
- Aplicar controles de acceso basados en roles y privilegios para limitar el acceso y los permisos de modificación solo a aquellos usuarios que lo necesiten.
- Utilizar técnicas de encriptación para proteger la integridad de los datos almacenados en las bases de datos.
- Implementar procesos de gestión de cambios controlados para garantizar que cualquier modificación en la estructura o los datos de las bases de datos se realice de manera autorizada y documentada.

2. TIPO DE ACTIVO:	[D/I] Datos e información
NOMBRE DEL ACTIVO:	Archivos en Dispositivo NAS
VR TOTAL ACTIVO:	28
AMENAZAS:	Error humano
FRECUENCIA:	3
IMPACTO:	4
RIESGO ASOCIADO A LA AMENAZA:	Pérdida de integridad en los archivos
VALOR DEL RIESGO:	336
SALVAGUARDA:	Implementar pruebas antes de pasar a producción
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	134,4
SOA – APLICABILIDAD:	10.1.1 Política de uso de los controles criptográficos. 12.3.1 Copias de seguridad de la información. 18.1.5 Regulación de los controles criptográficos.

PLAN DE ACCIÓN:

- Establecer políticas y procedimientos claros para el almacenamiento, acceso y gestión de archivos, incluyendo controles de acceso y permisos adecuados.
- Implementar mecanismos de autenticación y autorización para garantizar que solo usuarios autorizados tengan acceso a los archivos y puedan realizar modificaciones.
- Realizar copias de seguridad regulares de los archivos y verificar periódicamente su integridad para asegurar que los datos puedan ser recuperados en caso de pérdida o corrupción.
- Utilizar tecnologías de cifrado para proteger los archivos sensibles, tanto en tránsito como en reposo.
- Implementar controles de detección de intrusiones y monitoreo de actividad para identificar y responder rápidamente a cambios no autorizados en los archivos.

- Capacitar al personal en la importancia de mantener la integridad de los archivos y en las mejores prácticas de seguridad de la información.

3. TIPO DE ACTIVO:	[SW] Aplicaciones
NOMBRE DEL ACTIVO:	Correo electrónico
VR TOTAL ACTIVO:	26
AMENAZAS:	Errores de configuración
FRECUENCIA:	3
IMPACTO:	4
RIESGO ASOCIADO A LA AMENAZA:	No disponibilidad del correo
VALOR DEL RIESGO:	312
SALVAGUARDA:	Soporte por parte de Microsoft previo a cambios significativos
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	124,8
SOA – APLICABILIDAD:	12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información.

PLAN DE ACCIÓN:

- Establecer redundancia y respaldo de los sistemas de correo electrónico para garantizar la disponibilidad continua del servicio.
- Implementar medidas de seguridad, como firewalls, sistemas de detección y prevención de intrusiones, y sistemas de filtrado de correo no deseado, para proteger el sistema de correo electrónico contra ataques y amenazas cibernéticas.
- Realizar pruebas regulares de continuidad y recuperación ante desastres para asegurar que el correo electrónico pueda ser restaurado en caso de interrupciones o fallos.
- Establecer acuerdos de nivel de servicio (SLA) con proveedores de servicios de correo electrónico externos, si corresponde, para garantizar altos niveles de disponibilidad y soporte técnico.
- Capacitar al personal en el uso adecuado del correo electrónico y en la identificación de posibles amenazas, como phishing o malware, que puedan afectar su disponibilidad.

4. TIPO DE ACTIVO:	[SW] Aplicaciones
NOMBRE DEL ACTIVO:	Antivirus
VR TOTAL ACTIVO:	22
AMENAZAS:	Errores de mantenimiento y/o actualizaciones
FRECUENCIA:	3
IMPACTO:	5

RIESGO ASOCIADO A LA AMENAZA:	No disponibilidad del antivirus
VALOR DEL RIESGO:	330
SALVAGUARDA:	Soporte por parte del proveedor
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	132
SOA – APLICABILIDAD:	7.2.2 Concienciación, educación y capacitación en seguridad de la información. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información.

PLAN DE ACCIÓN:

- Realizar implementaciones adecuadas y actualizaciones regulares del software antivirus en todos los sistemas y redes de la organización.
- Establecer procesos de monitoreo y mantenimiento proactivo del antivirus para detectar posibles problemas y asegurar su correcto funcionamiento.
- Implementar mecanismos de respaldo y redundancia para garantizar la continuidad del servicio antivirus en caso de fallas.
- Establecer políticas y procedimientos claros para el uso y la administración del antivirus, incluyendo la configuración, actualización y escaneo regular de los sistemas.
- Capacitar y concientizar al personal sobre la importancia de la seguridad informática y el uso adecuado del antivirus.
- Establecer acuerdos de nivel de servicio (SLA) con proveedores de antivirus, si corresponde, para garantizar altos niveles de disponibilidad y soporte técnico.

5. TIPO DE ACTIVO:	[SW] Aplicaciones
NOMBRE DEL ACTIVO:	Antivirus
VR TOTAL ACTIVO:	22
AMENAZAS:	Errores de configuración
FRECUENCIA:	3
IMPACTO:	5
RIESGO ASOCIADO A LA AMENAZA:	No disponibilidad del antivirus
VALOR DEL RIESGO:	330
SALVAGUARDA:	Soporte por parte del proveedor. Pruebas en equipos de red de alistamiento
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	132
SOA – APLICABILIDAD:	7.2.2 Concienciación, educación y capacitación en seguridad de la información. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información.

PLAN DE ACCIÓN:

- Mantener actualizado el software antivirus y aplicar los últimos parches de seguridad.
- Realizar escaneos regulares en busca de malware y asegurarse de que los sistemas estén protegidos de manera continua.
- Configurar correctamente el antivirus, asegurándose de que todas las funcionalidades de protección estén habilitadas y ajustando las configuraciones según las necesidades de la organización.
- Realizar pruebas periódicas para verificar la efectividad del antivirus y su capacidad para detectar y eliminar amenazas conocidas y emergentes.
- Capacitar y concienciar a los usuarios sobre la importancia de utilizar el antivirus de manera adecuada y reportar cualquier anomalía o incidente de seguridad.
- Establecer políticas y procedimientos de gestión de incidentes para abordar rápidamente las situaciones en las que el antivirus falle o no esté disponible.
- Implementar medidas adicionales de seguridad, como firewalls, sistemas de detección de intrusiones y filtrado de contenido web, para complementar la protección proporcionada por el antivirus.

6. TIPO DE ACTIVO:	[HW] Equipos informáticos
NOMBRE DEL ACTIVO:	Servidor de aplicaciones
VR TOTAL ACTIVO:	21
AMENAZAS:	Corte de fluido eléctrico
FRECUENCIA:	3
IMPACTO:	5
RIESGO ASOCIADO A LA AMENAZA:	No disponibilidad en el servidor
VALOR DEL RIESGO:	315
SALVAGUARDA:	Planes BCP, DRP, BIA. Pruebas periódicas de generadores y UPS
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	127
SOA – APLICABILIDAD:	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.2.4 Mantenimiento de los equipos. 12.6.2 Restricciones en la instalación de software.

PLAN DE ACCIÓN:

- Implementar redundancia y tolerancia a fallos en la infraestructura del servidor, como sistemas de alimentación ininterrumpida (UPS), fuentes de energía alternativas y sistemas de almacenamiento en red (NAS).
- Realizar copias de seguridad regulares de los datos almacenados en el servidor y asegurarse de que los procedimientos de recuperación ante desastres estén en su lugar.

- Implementar soluciones de monitoreo y gestión de rendimiento para detectar y abordar problemas potenciales antes de que afecten la disponibilidad del servidor.
- Aplicar controles de acceso y autenticación adecuados para prevenir el acceso no autorizado y proteger la integridad del servidor.
- Mantener los sistemas operativos y software del servidor actualizados con los últimos parches de seguridad para mitigar las vulnerabilidades conocidas.
- Establecer procedimientos y políticas de respuesta a incidentes para abordar rápidamente los eventos de no disponibilidad y minimizar el tiempo de inactividad.

7. TIPO DE ACTIVO:	[HW] Equipos informáticos
NOMBRE DEL ACTIVO:	Firewall
VR TOTAL ACTIVO:	22
AMENAZAS:	Errores de configuración
FRECUENCIA:	4
IMPACTO:	4
RIESGO ASOCIADO A LA AMENAZA:	No disponibilidad, integridad del firewall
VALOR DEL RIESGO:	352
SALVAGUARDA:	Soporte por parte del proveedor o fabricante. Pruebas y backup periódicos
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	140,8
SOA – APLICABILIDAD:	9.3.1 Uso de información confidencial para la autenticación. 9.4.2 Procedimientos seguros de inicio de sesión. 11.1.1 Perímetro de seguridad física. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

PLAN DE ACCIÓN:

- Mantener el firewall actualizado con las últimas versiones de firmware y parches de seguridad.
- Configurar el firewall de acuerdo con las mejores prácticas de seguridad y las necesidades específicas de la organización.
- Realizar pruebas regulares para verificar la efectividad y la integridad del firewall.
- Implementar medidas de monitoreo y registro para detectar cualquier actividad sospechosa o intento de violación.
- Establecer políticas y procedimientos de gestión de cambios para garantizar que cualquier cambio en la configuración del firewall sea autorizado y controlado.

- Capacitar al personal responsable del firewall sobre su correcta administración y las mejores prácticas de seguridad.
- Establecer un plan de contingencia para abordar situaciones de no disponibilidad del firewall y garantizar la continuidad de los servicios.

8. TIPO DE ACTIVO:	[AUX] Equipamiento auxiliar
NOMBRE DEL ACTIVO:	CCTV
VR TOTAL ACTIVO:	23
AMENAZAS:	Averías
FRECUENCIA:	3
IMPACTO:	5
RIESGO ASOCIADO A LA AMENAZA:	No disponibilidad del CCTV
VALOR DEL RIESGO:	245
SALVAGUARDA:	Soporte por parte del proveedor. Stock de insumos
VR SALVAGUARDA:	60%
VR RIESGO RESIDUAL:	138
SOA – APLICABILIDAD:	11.1.1 Perímetro de seguridad física. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales.

PLAN DE ACCIÓN:

- Mantener el CCTV en buen estado de funcionamiento y realizar mantenimiento regular para asegurar su disponibilidad.
- Implementar un sistema de respaldo o redundancia para el CCTV, como cámaras de seguridad adicionales o sistemas de grabación alternativos, para evitar la interrupción completa en caso de fallas.
- Establecer un plan de monitoreo y mantenimiento proactivo para identificar y solucionar problemas de manera oportuna.
- Realizar pruebas regulares para verificar la calidad de las imágenes y la funcionalidad del CCTV.
- Establecer políticas y procedimientos claros para la administración y el acceso al sistema de CCTV, incluyendo la asignación de roles y responsabilidades.
- Capacitar al personal encargado del monitoreo y la gestión del CCTV sobre el uso adecuado del sistema y los protocolos de respuesta ante incidentes.
- Realizar copias de seguridad periódicas de las grabaciones del CCTV y almacenarlas de manera segura para garantizar la preservación de la evidencia en caso de necesidad.

6.4 DESARROLLO DEL OBJETIVO 4: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS RIESGOS IDENTIFICADOS CON EL FIN DE PROMOVER UN MANEJO SEGURO A LA INFORMACIÓN.

6.4.1 PROPÓSITO. Establecer lineamientos de protección y resguardo, así como de integridad y confidencialidad de la información de FESNEPONAL, como uso de los activos e infraestructura Tecnológica que soporta sus operaciones, resguardando el correcto uso de los recursos informáticos de la organización, estableciendo directrices para la protección de los recursos informáticos que soporta las operaciones diarias de FESNEPONAL, a fin de brindar calidad en sus servicios y garantizar su efectividad, eficiencia y eficacia facilitando la implementación de estrategias que garanticen el buen uso de estos recursos que la organización proporciona a sus colaboradores para la ejecución de su labor diaria.

Aplicando los estatutos y leyes estipuladas que rigen la materia y empleando las mejores prácticas de calidad, procesos, seguridad y tecnología de la información.

6.4.2 OBJETIVOS. Tienen como finalidad establecer estándares de seguridad, mitigar riesgos, promover la cultura de seguridad y garantizar el uso adecuado de los recursos informáticos en la organización.

- Definir los requisitos mínimos de seguridad para el uso de los recursos informáticos y las tecnologías críticas.
- Mitigar el riesgo de daños a la reputación, sanciones legales o pérdida de ingresos comerciales debido al compromiso de los sistemas y activos de información.
- Mejorar la cultura y el conocimiento de la Seguridad de la Información para los colaboradores y los clientes, en el uso de los recursos informáticos.
- Informar a los colaboradores del uso adecuado de los recursos informáticos y las sanciones administrativas que ocasiona su desacato.

6.4.3 ALCANCE DEL DOCUMENTO. La información contenida en el presente documento muestra las políticas de seguridad para FESNEPONAL, con el fin de proteger tanto al usuario como a la organización de situaciones que pongan en riesgos los sistemas y la información que permiten su funcionamiento administrativo, operativo y tecnológico, agilizando los procesos de las distintas unidades que conforman de FESNEPONAL, con el fin de proteger tanto al cliente interno como al externo y a la organización de situaciones que pongan en riesgos los activos tecnológicos.

Por tanto, este documento va dirigido a todos los colaboradores que forman parte de FESNEPONAL y a todas aquellas unidades externas que prestan sus servicios en la organización con los recursos informáticos que esta les brinda para ejercer su labor diaria.

El presente documento debe ser revisado y actualizado con una periodicidad anual sí y solo sí el proceso ha sufrido cambios o se requiera de aplicar nuevos controles o normativas de mejores prácticas.

6.4.4 DEFINICIONES/ ABREVIATURAS

CISO: Oficial de Seguridad de la Información (por sus siglas en ingles "Chief Information Security Officer"), es responsable de alinear la seguridad de la información con los objetivos del negocio y así garantizar la confidencialidad, integridad y disponibilidad de la información y los datos.

CREAR CUENTA: Consiste en la asignación de una identificación (usuario y una contraseña) para acceder a la red corporativa, así como a un sistema de información; por ejemplo, equipo, programas, entre otros.

DISPOSITIVOS DE INTERCEPTACIÓN DE DATOS: Son dispositivos que tienen el fin de acceder de forma ilícita a sistemas de información, interfiriendo en el funcionamiento de un sistema informático o extrayendo la información.

DYNAMIC DNS: Es un método para actualizar automáticamente un servidor de nombres en el servidor de nombres de dominio (DNS), a menudo en tiempo real, con la configuración DDNS activa de sus nombres de host, direcciones u otra información configurada.

DERECHOS DE ACCESO PRIVILEGIADO: El acceso privilegiado significa acceso a activos tecnológicos con privilegios más elevados que los de un usuario base, generalmente hace referencia a acceso de raíz, acceso de

administrador o acceso a cuentas de servicio. Una cuenta con privilegios es una cuenta de usuario que tiene privilegios más altos que otras cuentas.

ID: Es la abreviatura del vocablo inglés “Identificación”, que traducido al idioma español significa “identificación”. La “id” sirve para dar un nombre de usuario.

JAIL BREAK: Proceso de suprimir algunas de las limitaciones impuestas por Apple en dispositivos que utilicen el sistema operativo iOS mediante el uso de núcleos modificados. Su equivalente en Android es el Root.

MALWARE: Es la abreviatura de “Malicious software”, término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

MDM: MOBILE DEVICE MANAGEMENT (GESTIÓN DE DISPOSITIVOS MÓVILES): Es una herramienta tecnológica utilizada para el resguardo, cuidado y monitoreo de información corporativa. Es un conjunto de software que permite monitorizar, controlar y asegurar dispositivos móviles.

POLITÉCNICAS: BLOQUEO FÍSICO DE COMPUTADORES: Por encima del sistema operativo y el software, existen diversas tecnologías y eficaces mecanismos diseñados para impedir que personas no autorizadas inicien en el ordenador.

PRINCIPIOS DE MÍNIMO PRIVILEGIO: El principio de mínimo privilegio significa que cualquier usuario / aplicación / cuenta debe poder acceder solo a la información y los recursos que son necesarios para su propósito legítimo, teniendo el menor número posible de privilegios para realizar un trabajo autorizado.

RECURSOS INFORMÁTICOS: Es cualquier aplicación, herramienta, componente o dispositivo que se puede agregar a una computadora o sistema; por lo tanto, puede ser tanto un recurso de hardware (dispositivos) como de software (programas).

ROOTEAR: El rooting o rooteo de dispositivos Android es el proceso que permite a los usuarios de teléfonos inteligentes, tablets y otros aparatos con el sistema operativo móvil Android obtener control privilegiado.

6.4.5 POLÍTICAS. Las políticas de seguridad en los sistemas de información son un conjunto de reglas, directrices y procedimientos establecidos por una organización con el objetivo de proteger la integridad, confidencialidad y disponibilidad de los recursos y datos de información. Estas políticas definen las medidas de seguridad que deben ser implementadas, así como los roles y responsabilidades de los usuarios y administradores de los sistemas.

6.4.5.1 *Políticas de Seguridad para los Recursos Informáticos*

- Prohibir la divulgación o promoción de información en cualquier medio, propiedad de FESNEPONAL, fuera de la organización, este acto será considerado como fuga de información, lo cual puede acarrear sanciones administrativas de acuerdo a disposiciones legales establecidas en el presente documento y a las que hubiere lugar.
- Prohibir revisiones y configuración de estaciones de trabajo, por personal que no sea de la Unidad de Soporte Tecnológico, por lo tanto, aquellos colaboradores que por negligencia y desconocimiento técnico especializado cause daños a los equipos por su manipulación, serán objeto de sanciones.
- Mantener las áreas donde se lleven a cabo, mesas o sesiones de trabajo, reuniones, presentaciones corporativas, ejecutivas, entre otras, limpias y ordenadas, por lo cual se requiere que se borre la información de pizarra acrílicas, se recoja todo tipo de material que contenga información sobre los temas planteados, a objeto de mantener la confidencialidad del tema discutido, entre los asistentes.
- Bloquear las sesiones al momento de inactividad por un periodo de tiempo de su estación de trabajo, así como bloquear físicamente los portátiles con la guaya de seguridad o resguardarlos en una gaveta con llave al momento de culminar sus labores diarias y retirarse de las instalaciones de FESNEPONAL.

6.4.5.2 *Políticas de Seguridad para el Uso de Computadoras y Estaciones de Trabajo*

- Realizar revisiones y evaluaciones de seguridad de la información en los equipos y estaciones de trabajo con una periodicidad de al menos un año o cuando el CISO lo considere necesario, ya que, todos los equipos de cómputo de FESNEPONAL, así como la información contenida en ellos son activos de la organización, suministrados a los colaboradores para el cumplimiento de sus funciones diarias.

- Prohibir la instalación o desinstalaciones de programas (Software) o dispositivos (Hardware), por personal ajeno a la unidad de Soporte Tecnológico, su desacato ocasionará sanciones administrativas.
- Establecer que los recursos informáticos (computadora, portátil, impresora, fotocopiadora, entre otros), que sean asignados a los colaborares, para el cumplimiento de sus funciones, pertenecen a la unidad de adscripción en la cual están asignados, y deben permanecer en la estación de trabajo donde hayan sido instaladas.
- Prohibir que el colaborador abra, desarme, mueva y reubique, los recursos informáticos (computadora, portátil, impresora, fotocopiadora, entre otros), así como teléfonos (fijos y celulares) asignados por FESNEPONAL, para el cumplimiento de sus funciones diarias, en el caso de requerir este servicio, el supervisor inmediato, debe realizar la solicitud, a través de Mesa de ayuda al buzón: soporteti@fesneponal.com
- Prohibir el uso del computador asignado por FESNEPONAL para fines personales, así como para el almacenaje de fotografías personales, música, juegos y archivos que no correspondan con las funciones para la cual haya sido contratado el colaborador.
- Apagar los equipos (computadora, portátil, impresora, fotocopiadora, entre otros), al momento de culminar con su jornada laboral.

6.4.5.3 *Políticas de Seguridad para el Uso de los Activos de Información*

- Mantener la propiedad intelectual de todo activo desarrollado y administrado por proveedores de servicios de desarrollo de software, así como la información almacenada y gestionada a través de las soluciones tecnológicas y bajo ningún motivo, razón o circunstancia el colaborador ni el proveedor, debe divulgar ningún aspecto de estos desarrollos distintivos para FESNEPONAL o hacer uso de la concepción de las ideas para beneficio personal, de negocios o de terceras partes, su desacato ocasionará sanciones administrativas o legales a las que diera lugar.
- Evitar dejar impresiones de información según su clasificación y nivel de confidencialidad, en áreas de impresión comunes.
- Verificar que el material utilizado para reciclaje no contenga firmas autorizadas, sellos húmedos de la unidad o de la organización o información sensible, a objeto de resguardar la información a manos de terceros, y evitar operaciones fraudulentas que perjudiquen los intereses de FESNEPONAL.
- Realizar un respaldo trimestral de la información administrada por los colaboradores y almacenada en los equipos de FESNEPONAL en el servidor de archivos y/o NAS.

- Evitar utilizar tecnología de terceros o servicios en la nube no autorizados para almacenar, transferir o procesar información de FESNEPONAL.
- Reportar cualquier falla de los recursos tecnológicos ante mesa de ayuda, utilizando el buzón: soporteit@fesneponal.com.
- Evitar compartir información interna, confidencial y secreta de los procesos y Core de negocios de FESNEPONAL con personas externas a la organización y no autorizadas a su disponibilidad.
- Solo el dueño del proceso puede compartir información, únicamente con personas autorizas a su disponibilidad siempre y cuando se traten de creación de alianzas comerciales, contratación de servicios especializados, entre otros, de igual manera solo podrán compartir información interna, la información confidencial y secreta debe contar con el VºBº del CISO y el gerente de área donde se gestiona el proceso y estar justificada la necesidad de ser compartida.

6.4.5.4 *Políticas de Seguridad para el Uso de Medios Removibles (Dispositivos de Almacenaje)*

- Prohibir el uso de dispositivos de almacenaje externo y removible como disco duro portátil, pendrive, CD, DVD, a fin de resguardar la información de los procesos que se gestionan, en caso de ser requerido por la naturaleza de los procesos que gestione, tal excepción debe ser documentada y avalada por el CISO, así como cifrar el medio extraíble en donde se transportarán y almacenarán los datos.
- Documentar toda solicitud de habilitación de puertos USB para utilizar medios extraíbles de almacenamiento con una razonable justificación y llevar un inventario de los puertos habilitados, además del VºBº del CISO.
- Solicitar la habilitación de los puertos USB, a través de mesa de ayuda utilizando el buzón soporteit@fesneponal.com, y el buzón de Seguridad de la Información sistemas@fesneponal.com, a objeto de que el CISO efectúe la evaluación de seguridad correspondiente de la solicitud, a objeto de mantener un control y seguimiento sobre dichas solicitudes, así como la necesidad planteada de la habilitación de puertos.

6.4.5.5 *Políticas de Seguridad para el Uso del Correo Electrónico*

- Todos los colaboradores que ejerzan funciones y ejecuten actividades para FESNEPONAL, se les debe proporcionar una cuenta de correo corporativo, como parte de las herramientas de trabajo, siempre y cuando las funciones inherentes a su cargo así lo determinen.

- Los mensajes emitidos por correo electrónico son considerados comunicaciones formales, siendo parte de seguimientos y comunicación de información, y por ende están sujetos a monitoreo y auditoría, así como representan un soporte sustentable para cualquier punto que requiera ser comprobado.
- Las cuentas de correo electrónico son de carácter personal e intransferible, por lo tanto, ningún colaborador debe utilizar esta herramienta de trabajo haciéndose pasar por otra persona, y emitir comunicados falsos en su nombre, en caso de su incumplimiento podrá ser sancionado por la Gerencia de Gestión Humana de acuerdo a la gravedad del evento suscitado.
- El contenido de los mensajes enviados por medio de los sistemas de correo electrónico de FESNEPONAL, tienen que estar relacionados con las funciones que desempeña el usuario de la cuenta.
- Queda totalmente prohibido el envío de mensajes de correo electrónico, con las siguientes características:

    - Como medio de chat, o con propósitos comerciales y financieros de beneficio propio.
    - Con contenido ofensivo para otros usuarios que dañe o perturbe la moral de las personas, entendiendo por contenido ofensivo aquel relacionado con pornografía, racismo, discriminación, violencia, terrorismo o cualquiera otra forma de agresión contra la moral y buenas costumbres sociales aceptadas.
    - Con cadenas de información que no sean del interés de FESNEPONAL.
    - Con información sobre actividades no relacionadas con el negocio de FESNEPONAL.
    - En los casos de requerir emitir información con fines humanitarios, este requerimiento debe ser canalizado con la Gerencia de Gestión Humana.
    - Con direcciones de correo electrónico y listas de distribución personal.
    - Para registrarse en sitios web no relacionados con la empresa y listas de correo foráneas a FESNEPONAL.
    - Con detalles de tarjetas de crédito, cuentas bancarias o contraseñas, en el caso que se requiera enviar esta información, se sugiere utilizar mecanismos de encriptación y aún con mayor resguardo si se tratan de cuentas relacionadas con FESNEPONAL. De acuerdo a lo establecido en las “Políticas de Seguridad para los Controles Criptográficos”.

- Todos los Sistemas de correo electrónico, son auditables por formar parte de los recursos informáticos de FESNEPONAL, con la finalidad de que al presentarse incidentes de seguridad que estén relacionados con el abuso o su mal uso, puedan ser asociados rápida y directamente con los usuarios titulares de las cuentas, a objeto de aplicar las sanciones administrativas, a las que hubiere lugar.
- El colaborador que se encuentre de vacaciones, incapacidad o permiso por más de tres (3) días hábiles, debe activar la regla de administración del correo electrónico corporativo “Ausente de la Oficina”, dicha opción se encuentra definida en la herramienta del correo electrónico predeterminado, indicando en el mensaje el nombre, apellido, cargo y extensión del responsable de ejecutar sus actividades mientras esté ausente.

6.4.5.6 *Políticas de Seguridad de las Contraseñas*

- El código de usuario (ID) asignado al colaborador y la contraseña de acceso a los sistemas de información de FESNEPONAL, son personales e intransferibles, por lo tanto, tendrán que resguardarlos, sin entregárselos a ningún supervisor o autoridad de mando, manteniendo custodiada la contraseña, a fin de que no sea conocida por terceras personas.
- Toda operación, acción o transacción que se haya ejecutado bajo presunto fraude, será responsabilidad del colaborador, al cual se le fue asignado el usuario y contraseña, utilizado para el hecho, ocasionando sanciones administrativas o imputaciones legales, de acuerdo al grado de perjuicio e impacto organizacional
- Cuando se tenga la sospecha de que su clave de acceso es conocida por un tercero, tendrá que cambiar inmediatamente su contraseña, realizando la solicitud del cambio vía correo electrónico a mesa de ayuda por medio del buzón soporteit@fesneponal.com, y a la seguridad de la información al buzón sistemas@fesneponal.com presentando una exposición de motivos por la cual requiere el cambio de contraseña.
- Los colaboradores deben cumplir los siguientes requisitos para crear contraseñas seguras:

    - Evitar colocar contraseñas de fácil deducción;
    - Evitar utilizar fechas y datos personales;
    - Utilizar mnemotecnia, para recordar su contraseña;
    - Utilizar combinación alfanumérica;
    - Utilizar caracteres alfa en mayúsculas (por ejemplo, de A hasta Z.);

- Utilizar caracteres alfa en minúsculas (por ejemplo, de a hasta z.);
- Utilizar caracteres numéricos con base a 10 dígitos (por ejemplo, 0 hasta 9);
- Utilizar al menos un carácter especial: !@#$%&*_-:;,.
- Evitar reutilizar la contraseña;
- Utilizar como mínimo catorce (14) caracteres.

6.4.5.7 *Política para el Uso del Internet*

- El acceso a Internet será determinado de acuerdo con las funciones y actividades que desempeñe el colaborador, y su uso debe ser solo para los propósitos relacionados con las funciones y responsabilidades inherentes a su cargo. Quedando sujetos a monitoreo y auditoria, como un control previsivo en el uso adecuado de los recursos de información, de comprobar su uso indebido, FESNEPONAL a través de Gestión Humana aplicará sanciones disciplinarias a las que haya lugar.
- Los servicios de Internet serán proporcionados solo al personal cuyas funciones desempeñadas lo justifique según el perfil de usuario establecido y bajo el principio de mínimo privilegio.
- El colaborador, tiene prohibido hacer uso del Internet para:

  - Realizar negocios personales y hostigamiento;
  - Descargar software, música, películas, juegos, programas (Software) de contenido inadecuado.
  - Escuchar música en línea, ver videos musicales y pornográficos.
  - Accesar a redes sociales (Facebook, LinkedIn, Instagram, Twitter, line, entre otros), así como la instalación o activación de sistemas de mensajería instantánea (gtalk, meebo, koolim, ebuddy, entre otros).

- Incorporar información de FESNEPONAL, en sitios Web o páginas públicas, tales como: códigos identificadores de usuarios, direcciones de correos electrónicos, palabras claves de acceso (password) designadas por la institución y utilizadas por el colaborador para su autenticación en los sistemas de información, así como información de los clientes, de los procesos internos y su infraestructura tecnológica, motivado a que puede ser capturada y posteriormente utilizada para intentos de suplantación

de identidad y ataques de denegación de servicios entre otros componentes tecnológicos.

7 CONCLUSIONES

En esta opción de grado se Diseñó la etapa de planificación de un sistema de gestión de seguridad de la información para el área de TI de la empresa FESNEPONAL - Fondo de Empleados Suboficiales y Nivel Ejecutivo de la Policía Nacional basado en la norma ISO/IEC 27001:2013, con el fin de iniciar un proceso de organización y mejora continua que permita la protección de la disponibilidad, integridad y confidencialidad de la información en la ciudad de Bogotá, porque se evidencia la necesidad de implementar un Sistema de Gestión de Seguridad de la información debido a la complejidad en que se encuentra la seguridad de la información y sus procesos, y la normatividad legal vigente.

En este trabajo se evaluó a través de un diagnóstico inicial de la organización mediante la metodología GAP alineado a la ISO/IEC 27001:2013 con el fin de analizar las brechas y conocer la situación actual, se evidencia la falta de seguridad de la información y control sobre los activos de información e incumplimiento de los objetivos corporativos.

Se estableció las vulnerabilidades, amenazas y riesgo de los activos de información del área TI mediante el uso de la metodología Magerit para poder gestionar el impacto de los riesgos asociados, en donde se identificaron los activos de información con mayor exposición que puedan afectarlos con el fin de darle el adecuado tratamiento.

Este documento propone la aplicabilidad basada en la norma ISO/IEC 27002:2013 con el fin de establecer buenas prácticas de seguridad y mitigar el riesgo, con el fin de definir los controles y las políticas a implementar en FESNEPONAL.

Este proyecto elaboro una política de seguridad de la información basado en los riesgos identificados con el fin de promover un manejo seguro a la información, este documento estratégico brinda una guía para especialistas técnicos de los mecanismos de seguridad que deben ser implementados en la plataforma tecnológica que soporta los procesos operativos de la organización.

8 RECOMENDACION

Dada la falta de conocimiento sobre normas de seguridad entre los empleados, se debe implementar un programa de capacitación exhaustivo que aborde las normas, herramientas y controles de seguridad de la información relevantes. Esto garantizará una comprensión completa y una aplicación efectiva de las políticas de seguridad. Se debe crear un equipo dedicado y multidisciplinario para dirigir la implementación del SGSI, con un enfoque específico en la definición clara de la normativa, políticas y procedimientos de seguridad de la información para la organización. La dirección debe demostrar un fuerte compromiso y apoyo continuo a la implementación del SGSI, lo cual se ha demostrado como un factor crítico para el éxito. Esto implica proporcionar recursos adecuados y establecer expectativas claras para la adopción y cumplimiento de las normas de seguridad de la información.

BIBLIOGRAFÍA

ANDRES FELIPE. [Sitio web]. Colombia: Tips Para Implementar La Declaración De Aplicabilidad (incluye Modelo En Excel). [Consulta: 25 de febrero de 2022]. Disponible en: https://blog.kawak.net/mejorando_sistemas_de_gestion_iso/tips-para-implementar-la-declaracion-de-aplicabilidad-descarga-excel

AMBIT. [Sitio web]. Tipos De Vulnerabilidades Y Amenazas Informáticas. [Consulta: 25 de febrero de 2022]. Disponible en: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid: España octubre de 2012.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogos de Elementos. Madrid: España octubre de 2012.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de técnicas. Madrid: España octubre de 2012.

IBERO TIJUANA. [Sitio web]. ¿Qué es La investigación aplicada y cuáles son sus principales
características?. [Consulta: 25 de febrero de 2022]. Disponible en: https://blogposgrados.tijuana.ibero.mx/investigacion-aplicada/

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. [Sitio web]. Bogotá: ICONTEC, Certificación ISO 27001 Sistemas De Gestión De Seguridad De La Información. [Consulta: 25 de febrero de 2022]. Disponible en: https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/.

PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence, ¿Cuáles Son Las Metodologías Para La Gestión De Riesgo?. [Consulta: 25 de febrero de 2022]. Disponible en:
https://www.isotools.com.mx/cuales-las-metodologias-la-gestion-riesgo/.

PMG SSI - ISO 27001 [Sitio web]. ISOTools Excellence, Software ISO Riesgos Y Seguridad. [Consulta: 25 de febrero de 2022]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/.

MINISTERIO DE TECNOLOGIA INFORMACION Y COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Ciberseguridad. [Consulta: 25 de febrero de 2022]. Disponible en: https://www.mintic.gov.co/portal/604/w3- article-6120.html.

MINISTERIO DE TECNOLOGIA INFORMACION Y COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Instructivo Para El Diligenciamiento De La Herramienta De Diagnostico De Seguridad Y Privacidad De La Información. [Consulta: 25 de febrero de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_Instructivo_instrumento_Evaluacion_MSPI.pdf.