DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA EL ASEGURAMIENTO DE LA INFORMACIÓN EN LA EMPRESA TECNO FUEGO S.A.S. DE LA CIUDAD DE BARRANQUILLA

ALBERTO ENRIQUE TORRES PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2020

TABLA DE CONTENIDO

RESUMEN

Esta disertación comprende la preparación para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en las pautas de la familia de estándares ISO / IEC 27000 y fue desarrollado en un entorno organizacional. En el desarrollo de este plan de implementación, formó parte de un conjunto de procesos específicos para cumplir con los requisitos de NP ISO / IEC 27001: 2013 y, dada la amplitud de su alcance y la caracterización de la organización donde se realizó este trabajo, adicional y particularmente marcos adoptados para uso interno de la organización. Presenta un enfoque teórico sobre la caracterización de un Sistema de Gestión de Seguridad de la Información (SGSI) y su relevancia en el contexto de la dinámica de la organización, su impacto en la estructura de los sistemas y tecnologías de la información, que continuamente requieren generar nuevos desafíos a la seguridad de la información. Se enfatiza el marco documental de los estándares requeridos en la gestión de la seguridad de la información y la estructura de recursos y responsabilidades para asegurar la implementación y continuidad de un SGSI.

A través de análisis documental, con entrevistas semiestructuradas y observación directa, se realizó una evaluación de la situación actual en respuesta a los requisitos de control recomendados por ISO / IEC 27001. Además, el proceso de gestión de riesgos de seguridad de la información como herramienta facilitadora en el análisis, evaluación y control de los factores de riesgo organizacionales y que dieron como resultado la realización de la matriz de riesgo que evoca el tratamiento que se aplicará al riesgo en cuestión. El resultado final de este trabajo, representa la "primera piedra" para la construcción del sistema de gestión de seguridad de la información. La "Declaración de Aplicabilidad" presenta un conjunto de propuestas divididas en cinco ejes de acción: organizacional, personal, tecnológico, físico y ambiental, legal y regulatorio. Para cada eje de acción, se definen medidas específicas a implementar. Las medidas presentadas, acciones a tomar, son el resultado del vasto trabajo realizado aguas arriba, en el que fue posible analizar y evaluar el estado actual de madurez y la capacidad procesal, tecnológica y de recursos y, por lo tanto, documentar, definir y estructurar las líneas lineamientos para implementar un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de ISO / IEC 27001 y 27002, en línea con los objetivos estratégicos de TECNO FUEGO S.A.S. y con el alcance previamente definidos, en su primera etapa.

Palabras Claves: *ISO 27001, Información, seguridad, sistema, riesgo, amenaza, confidencialidad, controles, activo informático, MAGERIT, impacto, SGSI, análisis.*

ABSTRAC

This dissertation comprises the preparation for the implementation of the Information Security Management System (ISMS) based on the guidelines of the family of ISO / IEC 27000 standards and was developed in an organizational environment. In the development of this implementation plan, it was part of a set of specific processes to comply with the requirements of NP ISO / IEC 27001: 2013 and, given the breadth of its scope and the characterization of the organization where this work was carried out, additionally and particularly frameworks adopted for internal use by the organization. It presents a theoretical focus on the characterization of an Information Security Management System (ISMS) and its relevance in the context of the dynamics of the organization, its impact on the structure of information systems and technologies, which continuously require create new challenges to information security. The documentary framework of the standards required in the management of information security and the structure of resources and responsibilities to ensure the implementation and continuity of an ISMS are emphasized.

Through documentary analysis, with semi-structured interviews and direct observation, an evaluation of the current situation was carried out in response to the control requirements recommended by ISO / IEC 27001. In addition, the information security risk management process as a tool facilitator in the analysis, evaluation and control of organizational risk factors and that resulted in the creation of the risk matrix that evokes the treatment that will be applied to the risk in question. The final result of this work represents the "first stone" for the construction of the information security management system. The "Statement of Applicability" presents a set of proposals divided into five lines of action: organizational, personal, technological, physical and environmental, legal and regulatory. For each axis of action, specific measures to be implemented are defined. The measures presented, actions to be taken, are the result of the vast work carried out upstream, in which it was possible to analyze and evaluate the current state of maturity and the procedural, technological and resource capacity and, therefore, document, define and structure the guidelines to implement an information security management system, in accordance with the requirements of ISO / IEC 27001 and 27002, in line with the strategic objectives of TECNO FUEGO SAS and with the previously defined scope, in its first stage.

Key Words: *ISO 27001, Information, security, system, risk, threat, confidentiality, controls, computer asset, MAGERIT, impact, ISMS, analysis.*

INTRODUCCIÓN

TECNO FUEGO SAS es una compañía colombiana, dedicada a la evaluación, estudio y protección especializada de todo tipo de riesgos de incendio; protección respiratoria con aire suministrado y aire purificado y señalización de emergencia. Fundada el 8 de agosto de 1.984, con sede principal en Barranquilla. Su actividad económica está registrada como Ingeniería especializada en sistemas contra incendio y sus productos son:

- Diseño, instalación y puesta en marcha de sistemas automáticos de detección, alarma y extinción de incendio cumpliendo normas NFPA.
- Diseño, cálculos de flujo y presión, instalación de sistemas de extinción con agente limpio como: FM 200, FE-13 y CO2
- Diseño, cálculos de flujo y presión, instalación y puesta en marcha de sistemas contra incendio basados en agua, en todas sus aplicaciones tales como redes de sprinklers, rociadores de water spray, hidrantes y gabinetes, casetas de bombas, sistemas de espuma, etc.
- Diseño, construcción e instalación de puertas y muros corta fuego con materiales sellantes y retardantes de fuego.
- Diseño, suministro, ensamble y pruebas de Máquinas de Bomberos.

TECNO FUEGO actualmente maneja más de 150 proyectos en ejecución, más de 500 clientes y su fuerza de trabajo consta de más de 200 empleados. Teniendo en cuenta estas cifras, es fundamental la protección de la información la cual se ha convertido en el activo más preciado para ella. TECNO FUEGO actualmente cuenta con una infraestructura tecnológica adecuada e implementa mecanismos de seguridad para mantener la confidencialidad, disponibilidad e integridad de la información, estos mecanismos y procesos son físicos y algunos lógicos, por lo cual

se ha visto la necesidad de crear lineamientos para poder conocer el estado real de los riesgos y seguridad de la red.

Con el presente proyecto se busca diseñar un Sistema de Gestión de Seguridad de la Información para TECNO FUEGO S.A.S. teniendo en cuenta los lineamientos de la norma ISO 27001:2013 la cual proporciona un marco metodológico basado en las buenas prácticas para llevar a cabo el diseño del Sistema de Gestión de Seguridad y permite garantizar el aseguramiento y permanencia del SGSI.

1. **PROBLEMA**

1.1. PLANTEAMIENTO DEL PROBLEMA

Teniendo en cuenta los múltiples riesgos y amenazas a las que cada día se exponen las grandes y medianas empresas, el cambio constante y la evolución de las tecnologías de la información, es necesario que las organizaciones implementen estrategias de seguridad evaluando y determinando las necesidades del negocio, es importante contar con un modelo de Seguridad de la Información que respalde los objetivos estratégicos de la empresa.

Los Sistemas de Gestión y Seguridad de la Información, son herramientas de gran utilidad para la gestión de la seguridad en la empresa, permiten establecer políticas, procedimientos y controles en relación a los objetivos la organización. Brindan una visión general del estado de los sistemas de información y permiten conocer la efectividad de las medidas de seguridad que se implementen, lo cual, es fundamental para apoyar la toma de decisiones por parte de la alta directiva con relaciones a las estrategias a seguir.

En la actualidad la empresa TECNO FUEGO S.A.S, no cuenta con un sistema de gestión de seguridad y el manejo de la información no tiene lineamientos ni mecanismos para su aseguramiento, en algunas ocasiones, se ha tenido indicios de filtración o fugas de información e incluso perdida de la misma, por lo que sus directivos están dispuestos a buscar métodos que permitan tener asegurada dicha información de forma más eficaz.

Con la existencia de un Sistema de Gestión de Seguridad de la Información en la empresa TECNO FUEGO S.A.S., se pretende generar sentido de pertenencia en los temas de seguridad en los usuarios que cada día manejan la información, logrando su participación en la planeación, definición e implementación de políticas y procedimientos para el aseguramiento de la misma.

El diseño de un Sistema de Gestión de Seguridad de la Información en la empresa TECNO FUEGO S.A.S., requiere que inicialmente se realicé una clasificación los activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización, con el propósito de identificar los riesgos de seguridad asociados con la información y de esta forma realizar un análisis para definir y establecer los mecanismos más convenientes para protegerla.

Con base al problema que hoy día está latente, en la empresa TECNO FUEGO S.A.S. se requiere el diseño de un Sistema de Gestión De Seguridad de la información con el objetivo de fortalecer la integridad, disponibilidad y confidencialidad de la información para garantizar la protección y seguridad de la misma, implementando en ella procesos para la gestión eficaz de acceso a la información, gestión de activos de información los cuales permitan su clasificación, priorización y determinación de su valor en caso de pérdida de información y mecanismos para evaluación de posibles riesgos y amenazas que puedan causar daños significativos en la operación de la organización.

1.1.1. Formulación del Problema

¿El diseño del sistema de gestión de seguridad de la información le proveerá a TECNO FUEGO S.A.S los elementos, técnicas y parámetros adecuados para mejorar la seguridad de la información de la empresa, la gestión y tratamiento de los riesgos asociados al uso de su información?

1.2. OBJETIVOS

1.2.1. Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información para la empresa TECNO FUEGO S.A.S. el cual mantenga la integridad, disponibilidad y confidencialidad de la información y sus activos tecnológicos, tomando como referencia la norma ISO 27001.

1.2.2. Objetivos Específicos

- Realizar el levantamiento de la información actual de seguridad, metodologías, procesos, procedimientos y controles de seguridad existente en la organización, así como procesos normativos aplicados en la seguridad de la información.
- Identificar los riesgos y amenazas que pueden afectar el normal funcionamiento de los procesos informático de la empresa con el fin de hacer una valoración de los mismos, alineados al estándar ISO 27001.
- Diseñar un Sistema de Gestión de Seguridad de la información que permita establecer políticas, lineamientos y estrategias para desarrollar soluciones tecnológicas para la protección de sus activos e infraestructura.
- Implementar el Sistema de Gestión de Seguridad de la información con el fin de proteger los activos informáticos, monitoreando y controlando los riesgos y amenazas con el fin de mantener la confidencialidad, integridad y disponibilidad de la información.

1.3. JUSTIFICACIÓN

El diseño de un Sistema de Gestión de Seguridad de la información, es vital en toda organización, ya que actualmente la información y sus activos informáticos se han convertido en un tesoro preciado para las empresas, por lo tanto, es de vital importancia protegerla y evitar que personas mal intencionadas accedan y hagan uso indebido de ella. En la empresa TECNO FUEGO S.A.S. se maneja un alto volumen de información la cual está compuesta por diseños y planos específicos creados por la compañía para la elaboración de sistemas contra incendio, certificados en las normas NFPA y con apoyo de los más importantes fabricantes de equipos como los son ANSUL, KIDDE, FEMWALL y HONEYWELL los cuales son apetecidos por la competencia por su alto costo y facilidad al momento de ejecutar uno de estos proyectos, por lo tanto es importante mantener controlada esta información, además el servidor cuenta con información comercial altamente confidencial que se debe resguardar para evitar la filtración de la misma y perdidas de licitaciones en contratos de alto volumen.

En algunas ocasiones se ha tenido indicios de fugas de información por parte de usuarios que se han retirado de la compañía, lo cual es preocupante para los directivos quienes exigen implementar controles para evitar este tipo de sucesos. Debido a esta clase de sucesos, se propone realizar un análisis profundo para hallar las vulnerabilidades existentes, riesgos y posibles amenazas en la red de datos compartidos, además se propone la implementación de un Sistema de Gestión de Seguridad de la información, para el resguardo de esta, con el fin de controlar lo que cada usuario tiene derecho a ejecutar y hasta donde puede manejar dicha

información para su protección, adicionalmente se implementaran acuerdos de confidencialidad los cuales abarcaran un tiempo después del despido o retiro voluntario.

1.4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

La empresa TECNO FUEGO S.A.S. es una empresa prestadora de servicios de ingeniería contra incendios, consta de tres sedes Cali, Bogotá y la principal en Barranquilla. El proyecto se llevará a cabo en Barranquilla ya que es la sede principal y en esta se centraliza toda la información, es accedida en las sedes alternas por medio de conexión VPN, se pretende iniciar con un estudio a fondo de las posibles vulnerabilidades que existen actualmente en la empresa. Luego se procederá a estudiar la norma ISO 27001 y evaluar la operación de la empresa para pactar los puntos que realmente se necesitan manejar dependiendo a la actividad y de acuerdo al resultado se crearan las políticas y procedimientos necesarios para mantener segura la información.

Se hará socialización a los directivos de los resultados adquiridos de las pruebas de penetración y a los usuarios y directivos sobre las nuevas políticas y procedimientos creados en el Sistema de Gestión de Seguridad de la información, la empresa será la encargada de ejecutar auditorias para comprobar su correcto funcionamiento y penalizar la violación de dichos controles.

2. MARCO DE REFERENCIA

2.1. ANTECEDENTES

2.2. MARCO TEORICO

2.2.1. Concepto de sistema de gestión de seguridad de la información

El concepto de Sistema de Gestión de Seguridad - SGSI, también se vuelve relevante en el alcance del desarrollo de esta disertación, para que los destinatarios de este documento puedan tener un registro y una comprensión uniforme basada principalmente en la definición de algunos autores.

El estándar ISO / IEC 27001: 2013 define que un SGSI es parte de los procesos de la organización y la estructura global y está integrado con ellos, y que la seguridad de la información se considera en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se dimensione de acuerdo con las necesidades de la organización.

La definición recomendada por la norma se ajusta al SGSI como parte integral del sistema de gestión global de una organización y, como tal, tiene un impacto en los objetivos y requisitos de la organización; y las políticas y procedimientos deben adaptarse al tamaño y estructura de la organización. En el componente de procedimiento y en el desarrollo de sistemas de información nuevos y actuales, debe considerarse la seguridad de la información, así como el cumplimiento de los objetivos de los controles de referencia especificados en la norma. Cabe señalar que, dado que el SGSI es una parte integral de la organización y, como la

organización es un organismo dinámico, implica que los factores circunscritos en el conjunto de prácticas y controles implementados deberán revisarse de manera continua.

2.2.2. Caracterización de un sistema de gestión de seguridad de la información

Las organizaciones "*trabajan principalmente en base a procesos formales o ad-hoc, respaldados por flujos de información, manejados por personas y respaldados por una infraestructura tecnológica*"[1] de información y comunicación. Dado que la información es uno de los activos más importantes de una organización y dada su importancia y sensibilidad, su seguridad se vuelve necesaria e indispensable.

En esta perspectiva, la seguridad de la información es un área de conocimiento que tiene como objetivo proteger la información y los sistemas de información de las amenazas a su integridad (la información no cambia de manera inesperada), la disponibilidad (información disponible cuando sea necesario) y la confidencialidad (acceso restringido usuarios legítimos). Además de estas propiedades fundamentales (atributos), la utilidad (identificación inequívoca de la persona responsable de información), utilidad (la información sirve para el propósito para el que fue creada) y peso (control exclusivo por parte del titular de la información) para garantizar el correcto funcionamiento y la continuidad operativa y comercial de la organización, minimizando los riesgos.

NP ISO / IEC 27001: 2013, en su sección introductoria, establece que "*un Sistema de Gestión de Seguridad de la Información (SGSI) debe ser parte de los procesos de la organización y la estructura de gestión global y esa seguridad, e integrarse con ellos. La información se considera en el diseño de procesos, sistemas de*

[1] Martins, A. y Santos, C. (2005). Una metodología para implementar un sistema de gestión de seguridad de la información. Journal of Information Systems and Technology Management

información y controles. De esta manera, un SGSI debe dimensionarse de acuerdo con las necesidades de la organización"[2].

Dada la relevancia, importancia y sensibilidad de la información generada, los sistemas de información y comunicación de la empresa TECNO FUEGO S.A.S, Garantiza un conjunto de características de seguridad:

Confidencialidad: es necesario garantizar que los datos de los usuarios / ciudadanos rescatados y los colaboradores estén protegidos, y que personas no autorizadas no puedan acceder a ellos, ya sea accidental o deliberadamente. La confidencialidad de la información garantizará que solo las personas autorizadas tengan acceso a la información de acuerdo con su clasificación (pública, interna o confidencial), es decir, de acuerdo con el grado de secreto de su contenido.

2.2.3. La norma ISO / IEC 27000 y su conexión con otras normas

La ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrotécnica Internacional) desarrollaron la familia de normas **ISO / IEC 27000**[3] con el objetivo principal de ayudar a las organizaciones a mantener sus activos de información de manera segura, como, información financiera, propiedad intelectual, datos personales de empleados, clientes, usuarios o información que se ha confiado a terceros.

Estas normas proporcionan pautas para la introducción, implementación y mantenimiento del SGSI que se aplicará en una organización. Estas recomendaciones también pretenden proporcionar una base común para el

[2] ibídem

[3] ISO / IEC 27000:2014 Information Technology – Security Techniques – Information security management systems – Overview and vocabulary. *Esta tercera edición, anula y reemplaza la anterior, publicada en 2012. La primera edición (ISO / IEC 27000: 2009) reemplazó el estándar emitido por el estándar británico BS7799-2, publicado en 2002.*

desarrollo de prácticas y técnicas destinadas a la seguridad organizacional y para establecer la confianza en las relaciones intra e interorganizacionales.

Esta familia es parte de un conjunto de estándares que especifican cuáles son los requisitos necesarios para un sistema de gestión de seguridad de la información, gestión de riesgos, métricas y pautas para la implementación de un sistema de gestión de seguridad de la información.

En resumen, la familia de estándares ISO / IEC 27000 incluye estándares para[4]:

a) Definir los requisitos para un SGSI;
b) Proporcionar apoyo directo, orientación y / o interpretación detallada para el proceso global de establecer, implementar, mantener y mejorar un SGSI;
c) Sector proveedor y directrices específicas para el SGSI; y
d) Abordar las pautas para realizar una auditoría y evaluación de conformidad para el SGSI.

La lista de estándares de la familia ISO / IEC 27000 es la siguiente [5]

- I SO / IEC 27000, Sistemas de gestión de seguridad de la información - Descripción general y vocabulario

[4] ISO / IEC 27000 (2008). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información.
[5] ISO / IEC 27000 (2008). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información.

- I SO / IEC 27001, Sistemas de gestión de seguridad de la información - Requisitos
- I SO / IEC 27002, Código de prácticas para controles de seguridad de la información
- I SO / IEC 27003, Guía de implementación del sistema de gestión de seguridad de la información
- I SO / IEC 27004, Gestión de seguridad de la información - Medición
- I SO / IEC 27005, Gestión de riesgos de seguridad de la información
- I SO / IEC 27006, Requisitos para organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información
- I SO / IEC 27007, Directrices para la auditoría de sistemas de gestión de seguridad de la información
- I SO / IEC TR 27008, Directrices para auditores sobre controles de seguridad de la información
- ISO / IEC 27010, Gestión de seguridad de la información para comunicaciones intersectoriales e interorganizacionales.
- ISO / IEC 27011, Directrices de gestión de seguridad de la información para organizaciones de telecomunicaciones basadas en I SO / IEC 27002
- ISO / IEC 27013, Orientación sobre la implementación integrada de I SO / IEC 27001 y
- I SO / IEC 20000-1
- ISO / IEC 27014, Gobierno de la seguridad de la información
- ISO / IEC TR 27015, Directrices de gestión de seguridad de la información para servicios financieros
- ISO / IEC TR 27016, Gestión de seguridad de la información - Economía de la organización

- ISO 27799: 2008, Informática sanitaria - Gestión de la seguridad de la información en salud utilizando I SO / IEC 27002
- ISO / IEC 27034: 2011, Tecnología de la información - Técnicas de seguridad - Seguridad de la aplicación

Cabe señalar que de este conjunto / serie de estándares, el único sujeto a certificación es el estándar ISO / IEC 27001, con los otros complementos para ayudar a la certificación en áreas específicas de actividad.

ISO / IEC 27001: 2013 Tecnología de la información - Técnicas de seguridad - Requisitos es el estándar más conocido en la familia ISO / IEC 27000, que proporciona los requisitos para un sistema de gestión de seguridad de la información. Este estándar fue desarrollado con el propósito de proporcionar los "*requisitos para establecer, implementar, operar, monitorear, analizar críticamente, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), dentro del contexto de la organización."* [6]

Basado en buenas prácticas de gestión de la información, ISO / IEC 27002: 2013[7] Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información, establece pautas y principios generales para analizar los requisitos de cada uno de los controles definidos en ISO / IEC

[6] ibídem

[7] La segunda edición de esta norma tiene fecha del 10-10-2013. Esta última edición ISO / IEC 27002: 2013 reemplaza a la primera edición ISO / IEC 27002: 2005, publicada en octubre de 2005. Esta primera edición reemplazó al estándar emitido por el estándar británico BS7799-1, publicado en 2002.

27001: 2013, teniendo en cuenta el entorno de los riesgos de seguridad de la información de la organización.

Este estándar está diseñado estructuralmente para ser utilizado por organizaciones que desean:

1. Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001;
2. Implementar controles de seguridad de la información generalmente aceptados;
3. Desarrolle sus propias pautas de gestión de seguridad de la información.

Sin embargo, debe tenerse en cuenta que, al contrario de lo que sucede con el estándar ISO / IEC 27001, que es obligatorio en el contexto de un eventual proceso de certificación, el estándar ISO / IEC 27002 es una mera guía (código de práctica) con una amplia gama de sugerencias de control de seguridad, integradas en una visión muy amplia de la organización y su gestión de seguridad de la información.

ISO / IEC 27003: 2010 Tecnología de la información - Técnicas de seguridad - La implementación del sistema de gestión de seguridad de la información se centra en los aspectos críticos necesarios para el diseño y la implementación exitosos de un SGSI, de acuerdo con el estándar ISO / IEC 27001: 2013.

ISO / IEC 27003: 2010 describe el proceso de especificación y el diseño de un SGSI, desde su concepción hasta la producción de los planes de implementación, es decir, proporciona orientación sobre cómo planificar un proyecto de SGSI, lo que resulta en el plan de implementación final del SGSI.

ISO / CEI 27004: 2009 Tecnología de la información - Técnicas de seguridad - La medición proporciona una guía con orientación sobre el desarrollo y uso de métricas y mediciones, con el fin de evaluar la efectividad de un sistema de gestión de seguridad de la información ya implementado con Los controles o grupos de controles especificados en ISO / IEC 27001: 2013.

ISO / CEI 27005: 2011: la gestión de riesgos de seguridad de la información contiene directrices para gestionar los riesgos de seguridad de la información. Esta norma admite los conceptos generales especificados en ISO / IEC 27001: 2013 y está diseñada para ayudar en la implementación de un sistema de gestión de seguridad de la información basado en el enfoque de gestión de riesgos.

ISO / IEC 27005: 2011 es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

2.3. MARCO CONCEPTUAL

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Causa: Razón por la cual el riesgo sucede.

Ciclo de Deming: Modelo de mejora continua, para la implementación de un sistema de mejora continua.

Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Administrador de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Administrador del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información. Este permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada

2.4. MARCO CONTEXTUAL

TECNO FUEGO SAS es una compañía colombiana, dedicada a la evaluación, estudio y protección especializada de todo tipo de riesgos de incendio; protección respiratoria con aire suministrado y aire purificado y señalización de emergencia. Fundada el 8 de agosto de 1.984, con sede principal en Barranquilla.

Actividad económica:

Ingeniería especializada en sistemas contra incendio

- Diseño, instalación y puesta en marcha de sistemas automáticos de detección, alarma y extinción de incendio cumpliendo normas NFPA.
- Diseño, cálculos de flujo y presión, instalación de sistemas de extinción con agente limpio como: FM 200, FE-13 y CO2
- Diseño, cálculos de flujo y presión, instalación y puesta en marcha de sistemas contra incendio basados en agua, en todas sus aplicaciones tales como redes de sprinklers, rociadores de water spray, hidrantes y gabinetes, casetas de bombas, sistemas de espuma, etc.

- Diseño, construcción e instalación de puertas y muros corta fuego con materiales sellantes y retardantes de fuego.
- Diseño, suministro, ensamble y pruebas de Máquinas de Bomberos.

ORGANIGRAMA:

Figura 1. Organigrama de la organización.

2.4.1. Cargos en área de sistemas

Ingeniero analista de TI

- Objetivo del cargo

  Administrar eficientemente las tecnologías de información y comunicación poniendo los recursos informáticos a disposición de los usuarios, velando por su adecuado uso y liderando proyectos tecnológicos; así como elaborar y supervisar las políticas

de uso de la tecnología de información, mediante el desarrollo de sistemas y el soporte técnico a los usuarios para contribuir al logro de los objetivos organizacionales.

- Funciones del cargo

- Responder por el mantenimiento, control, actualización y disposición final del hardware y software de la empresa, buscando el óptimo funcionamiento de la empresa.
- Apoyar a las otras áreas de la empresa en la logística informática para la realización de reuniones, conferencias y otras.
- Administrar el software de la empresa, asignando los usuarios, perfiles y copias necesarias para que se conserve la información.

- Implementar y supervisar políticas y normas para el aseguramiento de los activos tecnológicos
- Solucionar los impases tecnológicos y de equipos que se presenten en la organización para evitar pérdidas de tiempo y de productividad.
- Liderar proyectos de mejora o modernización de los procesos de la empresa buscando las mejores opciones para la empresa, cumpliendo los requerimientos de la Gerencia y/o departamento solicitante.
- Verificar y controlar los trabajos o servicios prestados por contratistas o proveedores del área de informática, garantizando que se cumplan los requerimientos y se satisfagan las necesidades de la empresa.
- Investigar y evaluar permanentemente los productos y servicios de tecnología de la información, así como los riesgos de seguridad en la infraestructura informática.
- Administrar y controlar los accesos a internet, asegurando una navegación óptima a los usuarios y aplicando medidas para asegurar los activos tecnológicos.

Técnico de soporte

- Objetivo del cargo

  Mantener en condiciones óptimas la infraestructura tecnológica de la empresa y dar soporte a usuarios e ingeniero residente.

- Funciones del cargo

- Mantenimiento de hardware y software a servidor, estaciones de trabajo y red interna.
- Alistar y asignar los equipos de computación requeridos por los empleados, garantizando que se cumplan los procedimientos y los requisitos legales.
- Mantener los equipos informáticos, de sistemas y audiovisuales de la empresa para prestar el mejor servicio a las labores de la compañía.
- Realizar los backup a servidores, equipos locales y gerencia.
- Dar soporte eventual físico y online a ingeniero de planta.

3. METODOLOGÍA

Para el análisis de riesgo y gestión del mismo en la empresa TECNO FUEGO S.A.S. se ha elegido la metodología MAGERIT, ya cuenta con lineamientos y está directamente relacionada con la generalización del uso de las tecnologías de la información, también cuenta con las medidas apropiadas para dar tratamiento adecuado y cuantificar de forma adecuada los activos de la compañía.

Se hace necesario la elaboración de un diagrama de procedimiento, en función de las necesidades específicas para producir un plan de implementación que, en ISO / IEC 27001: 2013, se conoce como la "Declaración de Aplicabilidad" (NP ISO / IEC 27001 Cláusula 6.1.3d, p. 9)

Dado que este trabajo, en particular, se centra en el Diseño de un SGSI, el Diagrama presenta en detalle los procesos necesarios para esta fase y la identificación, que forman parte de los procesos identificados del uno al diez y la producción de sus respectivos entregables.

Se buscó con este modelo, de manera genérica, definir un conjunto de actividades que permitieran comprender la interconexión de los procesos funcionales actuales, la estrategia de la organización y su alineación con los sistemas y tecnologías de información circundantes, así como identificar el nivel de capacidad y madurez que la organización tiene para responder y lograr la implementación de un Sistema de Gestión de Seguridad de la Información, guiándolo con un conjunto de objetivos a alcanzar (actividades a realizar) aplicables al proceso de implementación de la norma ISO / IEC 27001: 2013

3.2. TÉCNICAS DE RECOPILACIÓN Y ANÁLISIS DE DATOS

El tema de la seguridad de la información y el papel de los sistemas y tecnologías de la información en la organización es hoy en día un tema ampliamente discutido. Para minimizar el riesgo de dispersión, se tomó como punto de partida realizar una revisión de la literatura sobre un sistema de gestión de seguridad de la información, la importancia de la seguridad de la información en el contexto de una organización, las ventajas de un sistema de gestión de seguridad de la información puede aportar al proceso de implementación, especialmente en alineación con las buenas prácticas y al aumentar las capacidades operativas, de gestión y de gobierno de los sistemas y tecnologías de la información. La revisión literaria sobre el tema permitió un enfoque más efectivo y explorar opiniones contrastantes.

Además de esta exploración bibliográfica, se exploraron técnicas para recopilar y analizar información. Estas técnicas tienen como objetivo guiar la selección del problema a abordar en diferentes áreas, así como la forma de análisis sobre ellas.

La recopilación de información para el análisis y la posterior formulación de las actividades a realizar se basaron en una recopilación de información basada en tres técnicas básicas:

Análisis de documentos: Análisis de documentos como procedimientos, instrucciones y presentaciones institucionales. La documentación técnica sobre los sistemas de información también se analizó en términos de su implementación, gestión operativa y mantenimiento actual. En el contexto de la gestión estratégica de la institución, se consultaron documentos sobre la definición del plan estratégico y el conocimiento de las diferentes herramientas de gestión existente, así como los estatutos emitidos a la institución, lo que permite la identificación previa y relevante

de las principales responsabilidades y actividades desarrolladas por cada uno. Una de las áreas orgánicas y su interconexión. La combinación de toda esta información recopilada permitió identificar de manera ordenada y efectiva los temas que se abordarán en las entrevistas realizadas más adelante.

Entrevista semiestructurada: la aplicabilidad de esta técnica tenía el objetivo principal de obtener información detallada dentro del alcance de los objetivos de control recomendados por la norma ISO / IEC 27001: 2013, identificando el estado de los controles implementados o parcialmente implementados e identificando qué controles no existen o mejorar en el contexto de la gestión de riesgos de seguridad de la información. Las entrevistas permitieron absorber la información necesaria sobre los procesos organizacionales, sus relaciones interfuncionales, los recursos circundantes, identificando vulnerabilidades y puntos de mejora.

Este enfoque metodológico cuantitativo y cualitativo se complementó con la creación de grupos de trabajo, donde se realizaron entrevistas basadas en las preguntas formuladas, investigando temas delicados o información privilegiada y obteniendo una percepción personal, explorando emociones, experiencias o sentimientos.

Observación directa: esta técnica permitió completar la información recopilada en las entrevistas y debates de los grupos de trabajo, ya que permitió recopilar información y "ver" aspectos que los entrevistados y los participantes desconocen o de los que no desean hablar o aclarar puntos que puedan han sido menos explorados Esta técnica se ha vuelto de suma importancia debido al refuerzo naturalista de la recopilación de datos, convirtiéndose en un proceso interactivo e incremental.

4. LEVANTAMIENTO DE LA INFORMACIÓN ACTUAL

4.1. ANÁLISIS DE LA APLICACIÓN DE LA NORMA ISO 27001

Para llevar a cabo el plan de implementación, el diagrama del proceso se tomó como una guía, permitiendo la producción de varios entregables que justifican el material necesario para la implementación del SGSI. Si no se sabe "*qué es importante proteger y cuál es el modelo base en el que debe basarse esta protección, no es posible concebir e implementar una seguridad adecuada*"[8]. De esta manera, los principales procesos y activos fueron encuestados e integrados con el alcance de la seguridad de la información. En vista de los objetivos estratégicos y operativos de la organización, se definieron el alcance y la estructura del SGSI a implementar.

En el diseño para la implementación del SGSI, también se realizó una evaluación de riesgos. Esta etapa extremadamente relevante involucró las actividades de identificación de riesgos, análisis y evaluación de cada riesgo. La matriz de riesgos producida tuvo como entrada el resultado de actividades previas y el plan de tratamiento de riesgos a aplicar.

[8]Zúquete, A. (2015). Seguridad de la red informática

3.1. CRONOGRAMA DE ACTIVIDADES

Tabla 1. Cronograma de actividades.

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
Planificación y Definición del diseño SGSI				25 abril								
Identificación de Metodología para evaluar el riesgo (Magerit, PHVA)					15 de mayo							
Investigación y Levantamiento de Información					30 mayo							
Desarrollo de Manual de Seguridad						30 junio						
Creación de Políticas de Seguridad							30 Julio					

4.2. SITUACIÓN ACTUAL

Los objetivos del diseño del SGSI deben considerarse teniendo en cuenta los requisitos de información y las prioridades de la organización. Para la producción de este producto, se aplicó un enfoque de arriba hacia abajo que busca identificar las funciones críticas y vitales en la organización TECNO FUEGO S.A.S, desde la perspectiva de la disponibilidad y seguridad de la información, teniendo como aspecto crítico la garantía de la continuidad funcional y operativa de TECNO FUEGO S.A.S en el cumplimiento de la misión-

La información se obtuvo mediante la consulta de diversos documentos de TECNO FUEGO S.A.S y un cuestionario estructurado que sirvió de guía para determinar los objetivos para el diseño del SGSI, pero también, con el propósito de definir prioridades y transformar lo implícito en explícito.

Los puntos cubiertos fueron los siguientes:

i. Áreas orgánicas críticas de la organización que sirven a la empresa en su misión.
ii. Estudio de la infraestructura TIC y clasificación de activos.
iii. Vínculos contractuales / formales con entidades externas y áreas orgánicas.
iv. Servicios subcontratados dentro del alcance de los sistemas y la infraestructura de telecomunicaciones.
v. Información crítica y / o sensible.
vi. Probables consecuencias por la divulgación de cierta información por partes no autorizadas.

vii. Acuerdos contractuales, organizacionales o legales relacionados con la seguridad de la información, en términos de requisitos de almacenamiento de datos, privacidad o calidad de datos y requisitos específicos.

viii. Las leyes relacionadas con el tratamiento del riesgo o la seguridad de la información se aplican a TECNO FUEGO S.A.S.

Al realizar este trabajo, se consultaron los siguientes documentos internos de TECNO FUEGO S.A.S:

- Plan Estratégico de Sistemas de Información
- Política interna de sistemas de información y tecnologías Política de gestión de riesgos
- SGIQAS (ISO 9001: 2015 e ISO 14000) Sistema Integrado de Gestión de Calidad, Medio Ambiente y Seguridad y Política Integrada de Calidad, Medio Ambiente y Seguridad
- Proceso de gestión P.10-5.GSTI - Proceso de gestión de gestión de telecomunicaciones e informática PG.13-1.GSTI-Backoffice de la estación de trabajo de instalación
- Lista de servidores y aplicaciones (servicios de aplicaciones) y lista de equipos de red activos

4.3. ANÁLISIS FODA

El análisis FODA presentado se basa en la información obtenida en la encuesta de la situación actual. Está circunscrito dentro del alcance de la seguridad de la información en la infraestructura de los sistemas y tecnologías de la información en línea con la misión y los objetivos estratégicos 2016-2018 de TECNO FUEGO S.A.S., teniendo en cuenta la línea de proyectos diseñados.

El análisis realizado permite relacionar las fortalezas y debilidades de la organización con las principales tendencias en su entorno, con el objetivo de generar medidas para hacer frente a las oportunidades y amenazas identificadas.

Tabla 2. Análisis FODA

Fortalezas	**Debilidades**
• Organización crítica con cobertura nacional, en el servicio de urgencias de incendio. • Infraestructura de centros de procesamiento de datos (Centros de datos) ubicados geográficamente por la oficina local. • Disponibilidad asegurada con arquitectura redundante en servicios de voz y SIADEM. • Configuración estandarizada de software base en puntos finales. • Alta confianza y conocimiento experiencial del equipo técnico de GSTI. • Reconocimiento de la aplicabilidad e implementación de buenas prácticas.	• Arquitectura LAN en estrella; Equipo central con tecnología obsoleta (activos y pasivos) sin posibilidad de expansión y sin redundancia en la capa de distribución. • Infraestructura de almacenamiento obsoleta y sin cobertura técnica por parte del fabricante. Centralización de sistemas críticos en un único centro de datos. • Gobierno de las TIC con configuración reactiva y poco preventiva. Administración y mantenimiento de los principales sistemas de información controlados por proveedores externos. • Control descentralizado de los activos de información e identificación inadecuada. Ninguna política sobre control de acceso a aplicaciones. • Proceso de contratación pública que consume mucho tiempo.

Tabla 3. Análisis FODA

Oportunidades	Amenazas
• Conceptualizar la arquitectura de red LAN integrada con la red SIRESP, la aplicación y la infraestructura del servidor de voz asegurando disponibilidad, redundancia de servicio y monitoreo. • Implementar un controlador LAN inalámbrico con gestión centralizada. • Nueva tecnología de almacenamiento integrada con la infraestructura de computación en la nube. • Implementar una arquitectura redundante (AlwaysON) en SIADEM con distribución geográfica. • Implementar planes de recuperación ante desastres con recursos físicos para centros de datos y firewall con IDS / IPS: monitoreo e informes. • Permitir a los empleados con una cultura de seguridad de la información. En el equipo GSTI, adapte el know-how en los componentes de seguridad de la información.	• Falta de disponibilidad en la recuperación de datos y / o pérdida de datos. • Interrupción de LAN y pérdida total o parcial del servicio. Incapacidad para implementar un plan efectivo de recuperación ante desastres. Red wifi sin control / monitorización. • Vulnerabilidades de seguridad perimetral, con posibilidad de ataque. • Incumplimiento de la confidencialidad en el acceso a los datos. Transacción de documentos con pérdida de integridad y confidencialidad. • Dificultad en la implementación oportuna de controles, por razones contractuales (productos y servicios).

4.4. DEFINICIÓN DEL ALCANCE Y ALCANCE DE LOS SGSI

Teniendo en cuenta el diseño del SGSI, se debe definir su estructura. El diseño del alcance del SGSI tuvo como insumo la fase anterior: los requisitos y prioridades de la información de TECNO FUEGO S.A.S. El resultado de esta fase fue preparar un documento con la definición del alcance y que servirá como guía para las decisiones de implementación que surgirán durante el proceso.

El resultado incluyó las siguientes definiciones:

i. Implemente una política de seguridad ajustada a los objetivos estratégicos de la organización y su misión.
ii. Cumplimiento de la confidencialidad de los datos clínicos del ciudadano rescatado, de conformidad con la Ley 67/98, de 26 de octubre - Ley de Protección de Datos Personales y Ley 46/2007, de 24 de agosto - Ley de acceso a los documentos administrativos.
i. Mantener una relación integrada entre los requisitos incluidos en la norma ISO / IEC 27001 y las otras normas existentes en la organización, como SGIQAS (ISO 9001: 2015 e ISO 14000) y la Política de gestión de riesgos (ISO / IEC 31000).
ii. Implemente los requisitos de ISO / IEC 27001 como una herramienta para ayudar a la gestión de las TIC, mejorando sus procesos asociados con un enfoque en el componente de seguridad de la información.

4.5. RESPONSABILIDADES Y CARGOS

Las estructuras organizativas se consideran las entidades clave para la toma de decisiones dentro de la organización. Este facilitador presenta un conjunto de funciones directamente relacionadas con la seguridad de la información y tiene la intención de ejecutar un conjunto de prácticas asociadas con cada una de ellas, que ofrecen buenas decisiones como resultado para la organización. La estructura organizacional y los recursos para garantizar la seguridad de la información varían de una compañía a otra, dependiendo, entre otros aspectos, de su tamaño. Por ejemplo, en una empresa pequeña, la misma persona ocupa varios puestos.

Dentro del alcance del SGSI, el requisito 5.3 Roles, responsabilidades y autoridades en la organización de la norma ISO / IEC 27001: 2013, establece que "*la alta dirección debe garantizar que las responsabilidades y autoridades sean asignadas y comunicadas para funciones que son relevantes para la seguridad información*"[9].

ISO / IEC27003 precisa detalles que ayudan a puntualizar las responsabilidades y posiciones de la gestión de seguridad de la información. Además, el reciente Reglamento de la UE 2016/679[10] del Parlamento Europeo y del Consejo de la Unión Europea, de 27 de abril de 2016, designa el nombramiento del Oficial de Protección de Datos. Con base en estos documentos, se describen los roles / cargos y

[9] ISO/IEC 27002 (2013) - Information Technology - Security Techniques

[10] El Reglamento 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, de 27 de abril de 2016, designado como Reglamento General de Protección de Datos, se publicó el 4 de mayo de 2016 y entró en vigor el 24 de mayo de 2016. 2016 y será aplicable a partir del 25 de mayo de 2018. El presente Reglamento define el nuevo régimen legal para la protección de las personas físicas con respecto al tratamiento de datos personales y la libre circulación de dichos datos, derogando la Directiva 95/46 / CE (Reglamento General de Protección de Datos).

responsabilidades que son necesarios, en la empresa TECNO FUEGO SAS., para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

- La responsabilidad final de la seguridad de la información debe estar en el nivel jerárquico de la administración: el Consejo Directivo (CD), y también es el organismo responsable de promover la mejora continua y evaluar el desempeño del Sistema de Gestión Integrado - Calidad, Medio Ambiente y Seguridad.
- La organización debe designar un promotor y coordinador de los procesos de seguridad de la información, normalmente designado como Director de Seguridad de la Información (CISO) o Gerente de Seguridad.
- El nombramiento del Oficial de Protección de Datos a cargo de la Administración de Salud Pública y el marco legal vigente.
- Cada trabajador / colaborador es responsable de su rol / posición y de mantener la seguridad de la información en el lugar de trabajo y en la organización.
- Creación de un comité de seguridad de la información para establecer un vínculo estrecho entre los roles / puestos de gestión de seguridad de la información.
- Equipo técnico multidisciplinario ISIRT: Equipo de respuesta a incidentes de seguridad de la información que puede estar disponible, es decir, dedicado al análisis, evaluación y resolución de eventos e incidentes relacionados con la seguridad de la información.
- Coordinador de Recursos Humanos: miembro del Departamento de Recursos Humanos (RR. HH.) con la responsabilidad de establecer la conexión entre la seguridad de la información y los empleados y

colaboradores de la empresa TECNO FUEGO S.A.S. Planifique y gestione acciones de formación y sensibilización sobre seguridad de la información, gestione y controle el proceso a tener con los empleados / trabajadores y proveedores de servicios externos antes, durante y después de la contratación.

- Responsable del Área Orgánica o Jefe de Departamento / Oficina Persona responsable de la seguridad de la información en un área orgánica o departamental responsable de implementar los requisitos de seguridad de la información, definidos en la (s) Política (es) de Seguridad.
- Propietarios / Propietarios responsables (seguridad de la información): persona directamente responsable de la gestión de un activo y de todos los eventos o incidentes de seguridad que ocurran relacionados con ese activo.

- Responsable de los procesos en áreas estratégicas: tener la responsabilidad de un proceso considerado crítico para la empresa, por ejemplo, un gerente de proyecto en la implementación de una nueva tecnología o cambio funcional y / u operativo.

En la organización, se debe designar a una persona responsable como jefe de seguridad de la información, llamado Gerente de Seguridad (también llamado Director de Seguridad de la Información (CISO) o Gerente de Seguridad de la Información) y el resto debe ser designado teniendo en cuenta las habilidades demostradas para ocupación, puesto / función. Paralelamente y en línea con el CISO, el Oficial de Protección de Datos también debe ser designado como la entidad responsable y centralizada para el cumplimiento del Reglamento de la UE 2016/679.

Los responsables de las áreas orgánicas, departamentos y / o oficinas integradoras dentro del alcance del SGSI, son miembros potenciales del equipo de implementación del SGSI y potenciales promotores de la conciencia e importancia de la seguridad de la información.

Tabla 4. Responsabilidad de la gestión de documentos en el ámbito del riesgo y la seguridad de la información

NÍVEL		TIPOS DE DOCUMENTOS	EJEMPLOS DE DOCUMENTOS	RESPONSABLE	APROBADOR
1	CONTEXTO	DOCUMENTOS DE CONTEXTO	Descripción de Contexto interno y externo Requisitos legales y contractuales Requisitos de las partes interesadas	Coordinador de Gabinete de Sistemas y Tecnologías de Información (GSTI)	Coordinador de GSTI
		GESTION DOCUMENTAL	*Frameworks* de Documentacion Procedimientos de Gestión Documental	Coordinador de Gabinete de calidad (GQ)	Coordinador do GQ
2	ESTRATÉGICO	DOCUMENTOS DE ORIENTACION	Ambito de SGSI, Princípios SI, Estratégia SI, Objetivos SI, Estructuras Organizacionales SI	Gestor de Seguridad	Consejo Diretivo
		POLÍTICA SI	Política de Seguridad de la Informacion	Gestor de Seguridad	Consejo Diretivo
		POLÍTICAS ESPECÍFICAS	Políticas específicas de alto nível dentro de las respectivas áreas de SI mapeadas de cláusulas de la norma ISO/IEC	Gestor de Seguridad	Comité de Segurança da Informação

3	TÁCTICO		27001:2013		
		NORMAS Y REGLAS	Normas y Reglas técnicas dentro de las respectivas áreas de SI mapeadas de las cláusulas de la norma ISO/IEC 27001:2013	Gestor de Seguridad	Comité de Segurança da Informação
4	OPERACIONAL	PROCESOS Y PROCEDIMIENTOS	Processos e procedimentos detalhados	Gestores de procesos y estruturas TIC	Gestor de Seguridad
		MODELOS	Modelos de registros, relatórios, planos y programas, cláusulas contractuales, etc	Gestores de procesos Gestores de las estruturas TIC	Gestor de Seguridad
		EVIDENCIAS	Registros, Relatórios, Planos etc.	Responsable GSTI Gestores de procesos Gestores de las estruturas TIC	Gestor de Seguridad

El Reglamento de Seguridad de la Información se clasificará de la siguiente manera:

- La "*Política de seguridad de la información de la empresa TECNO FUEGO S.A.S."* es el documento del nivel estratégico que es efectivo y define la seguridad de la información de TECNO FUEGO S.A.S para guiar el desarrollo de todos los documentos de los niveles tácticos y operativos del marco, así como todas las actividades operativas relacionadas con la seguridad de la información. Todos los reglamentos de seguridad de la información tácticos y operativos (políticas específicas, normas internas, procedimientos, etc.) deben basarse o reflejar las inquietudes y consideraciones establecidas en este documento.

- Las políticas específicas de seguridad de la información son los documentos que establecen reglas, pautas y responsabilidades de alto nivel dentro de las áreas respectivas de seguridad de la información asignadas a las cláusulas de la norma ISO / IEC 27001: 2013. Las políticas específicas también deben basarse o reflejar las preocupaciones y consideraciones establecidas por la "*Política de seguridad de la información de la empresa TECNO FUEGO S.A.S*." y respetar los "*Principios de seguridad de la información de TECNO FUEGO S.A.S.*";

- Las normas y reglas de seguridad de la información son los documentos más detallados que hacen mención especial de las tecnologías, métodos, procedimientos de implementación y otros detalles, siendo el tiempo de su aplicabilidad menor que el de las políticas, teniendo en cuenta su naturaleza más técnica. Las normas y reglas deben basarse o reflejar las inquietudes y consideraciones establecidas por las políticas específicas dentro del dominio de seguridad de la información respectivo.

5. ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

En el contexto específico de la seguridad de la información, el riesgo es la posibilidad de que una amenaza explote las vulnerabilidades de un activo o conjunto de activos, lo que puede ocasionar daños a un sistema. Se mide en términos de una combinación de la probabilidad de que ocurra un evento negativo (por ejemplo, una amenaza logra explotar una vulnerabilidad) y las pérdidas o pérdidas causadas por un activo o conjunto de activos. Un sistema de gestión de seguridad de la información "*Preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos*" [11]

Por lo tanto, la organización debe definir y aplicar un proceso de gestión de riesgos de seguridad de la información que, además de identificar y analizar los riesgos, también debe evaluar los riesgos de seguridad de la información. Identificar los riesgos de seguridad de la información en una organización es el primer paso para diseñar un sistema de gestión de seguridad de la información. Existen tres fuentes principales para identificar riesgos de información:

- Se obtiene una fuente del análisis de riesgos [12] para una organización, teniendo en cuenta sus objetivos y estrategias globales. A través del análisis

[11] ISO 2701: 2013 p.5

[12] Proceso diseñado para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la evaluación de riesgos y las decisiones de tratamiento de riesgos. (NP ISO 31000: 2013)

de riesgos, será posible identificar amenazas y vulnerabilidades a los activos de información y estimar la probabilidad[13] de que ocurran las amenazas y el impacto potencial que pueden tener en los procesos funcionales y operativos.

- Otra fuente es la legislación actual, los estatutos, reglamentos y cláusulas contractuales que la organización tiene con sus socios, empleados y proveedores de servicios, además de su entorno sociocultural.

- El tercero es un conjunto particular de principios, objetivos y requisitos comerciales para el procesamiento de información que una organización debe desarrollar para respaldar sus operaciones.

En esta fase del proyecto, que se enfoca en identificar, analizar y evaluar los riesgos de seguridad de la información, las escalas que se definen y aplican en la empresa TECNO FUEGO S.A.S., incluidas en la "Política de gestión", se tomaron como criterios para la clasificación y evaluación de riesgos. Riesgo" en vigor desde enero de 2016.

Se tomó esta opción, dado que la gestión de riesgos debe integrarse en todos los procesos y prácticas de la organización para que sea efectiva y eficiente. En este sentido, es importante definir su alcance, sus objetivos y la forma en que se implementará. El proceso de gestión de riesgos de TECNO FUEGO S.A.S., se definió en base al proceso de gestión de riesgos sugerido por ISO 31000: 2013

[13] En la terminología de gestión de riesgos, la palabra probabilidad es el término de probabilidad equivalente, usado para indicar la posibilidad de que ocurra algo, ya sea que esa posibilidad se defina, mida o determine objetiva o subjetivamente, cualitativa o cuantitativamente [como probabilidad o frecuencia durante un período de tiempo dado]. (NP ISO 31000: 2013)

- Gestión de riesgos - Principio y directrices.

La norma NP ISO 31000: 2013 recomienda que "*Las organizaciones desarrollen, implementen y mejoren continuamente una estructura cuyo objetivo es integrar un proceso para gestionar el riesgo en la gobernanza, estrategia y planificación, gestión, procesos de informes, políticas, valores y cultura*"[14].

5.1. CATEGORIZACIÓN DE RIESGOS

La norma NP ISO 31000: 2013 define el riesgo de manera integral y generalizada: "*Efecto de la incertidumbre en el logro de los objetivos*". Siendo eso, un efecto es una desviación, positiva o negativa, en relación con lo esperado. La incertidumbre es el estado, aunque parcial, de la deficiencia de información relacionada con la comprensión o el conocimiento de un evento, sus consecuencias y probabilidad.

El riesgo a menudo se caracteriza por la referencia a eventos y consecuencias potenciales o una combinación de ambos. El riesgo también se expresa a menudo como una combinación de las consecuencias de un evento dado y la probabilidad respectiva de ocurrencia.

Es importante comprender que los riesgos se clasifican de formas diferentes y pueden manifestarse igualmente. Se debe tener en cuenta que cada organización es única y, como tal, se deben definir sus riesgos específicos. La "*Política de gestión*

[14] ISO 31000: 2013

de riesgos" de TECNO FUEGO S.A.S., define que las categorías de riesgo se insertan en diferentes niveles y áreas, a saber:

Tabla 5. Categorías de Riesgos

Estratégicos	Riesgos relacionados con la implementación de la estrategia de la compañía – organización.
Regulatorios	Riesgos relacionados con los requisitos y cambios en el marco legal y regulatorio.
Entorno	Riesgos de relación interna y externa, inherentes al contexto económica, sociocultural y política donde se inserta la organización.
Financieros	Riesgos relacionados con la gestión financiera y la contratación pública
Recursos Humanos	Riesgos relacionados con la gestión de recursos humanos, entre otros, procesos de reclutamiento y salario.
Operacionales	Riesgos asociados con las operaciones de la organización, incluidos, entre otros, el desempeño operativo, la seguridad y la salud en el trabajo, seguridad de infraestructuras y equipos y gestión medioambiental.

5.2. MÉTODO DE EVALUACIÓN DE RIESGOS

La norma NP ISO 31000: 2013 define que el análisis de riesgos implica la evaluación de las causas y fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que estas consecuencias puedan ocurrir.

El propósito de la evaluación de riesgos es ayudar en la toma de decisiones basada en los resultados del análisis de riesgos, qué riesgos necesitan tratamiento y la prioridad para implementar el tratamiento (NP ISO 31000: 2013). Compara el nivel de riesgo encontrado durante el proceso de análisis, con los criterios de riesgo establecidos cuando se consideró el contexto.

Insertado en el proceso de análisis y evaluación de riesgos, se utilizará una matriz de riesgos, basada en las variables de probabilidad e impacto, presentada con el siguiente modelo:

Tabla 6. Matriz de valoración de riesgos

Área	Identificacion del Riesgo	Valoración de Riesgos			Medidas a implementar	Responsable
		Probabilidades	Impactos	Nivel de Riesgo		

Para esto, es necesario definir la probabilidad y el impacto / severidad (dependiendo de la situación).

Probabilidad - (P) - El nivel de probabilidad refleja la verificación de una o más condiciones que son razonables de esperar de un incidente que involucra el factor de riesgo evaluado.

Tabla 7. Tabla de probabilidades

Nível	Calificacion	Descripcion
1	Muy remoto	Probabilidad de 1 ocurrencia hasta una vez cada 50 años. (P ≤ 1 aparición / 50 años)
2	Remoto	Probabilidad de 1 ocurrencia cada 5 años. (1 vez / 50 años <P ≤ 1 vez / 5 años)
3	Improbable	Probabilidad de 1 ocurrencia cada 5 años. (1 vez / 50 años <P ≤ 1 vez /año)
4	Probable	Probabilidad de 1 ocurrencia por mes (1 vez / año <P ≤ 1 vez / mes)

5	Frecuente	Probabilidad de ocurrir más de una vez al mes. (P> 1 vez / mes)

Impacto - (I) - Pérdida o ganancia en caso de amenaza. Se puede determinar evaluando y procesando varios resultados de la ocurrencia de un evento o extrapolando estudios experimentales o datos y registros pasados.

Tabla 8. Tabla de impacto

Nível	Calificacion	DESCRIPCION
1	Baja	Degradación de las operaciones, actividades, proyectos, programas o procesos de la organización, que causan impactos mínimos en los objetivos (fecha límite, costo, calidad, imagen, etc.) relacionados con las metas o estándares o capacidad de entregar productos / servicios a las partes interesadas (clientes externos/ internos, beneficiarios).
2	Ligera	Degradación de las operaciones, actividades, proyectos, programas o procesos de la organización, causando pequeños impactos en los objetivos.
3	Moderado	Interrupción Moderada de las operaciones o actividades de la organización, proyectos, programas o procesos, que tienen un impacto significativo en los objetivos, pero son recuperables.
4	Grave	Interrupción grave de las operaciones, actividades, proyectos, programas o procesos de la organización, que causan impactos de reversión muy difíciles en los objetivos.
5	Muy Grave	Cierre muy severo de las operaciones, actividades, proyectos, programas o procesos de la organización, que causan impactos irreversibles en los objetivos.

El riesgo se clasifica según la combinación de Impacto (I) y Probabilidad (P).

(P x I = Riesgo)

Para determinar cualitativamente el nivel de riesgo, la probabilidad (P) debe multiplicarse por el impacto (I). Usando la tabla a continuación, se puede identificar el nivel de riesgo asociado con un riesgo identificado en particular.

Tabla 9. Tabla de evaluación de nivel de riesgo

***NIVELES DE RIESGO* = (P x I = Riesgo)**					
Probabilidades de Impacto	***1***	***2***	***3***	***4***	***5***
	Muy Remota	*Remota*	*Improbable*	*Probable*	*Frecuente*
1 - Bajo	***1***	***2***	***3***	***4***	***5***
2 - Ligero	***2***	***4***	***6***	***8***	***10***
3 - Moderado	***3***	***6***	***9***	***12***	***15***
4 - Grave	***4***	***8***	***12***	***16***	***20***
5 - Muy Grave	***5***	***10***	***15***	***20***	***25***

El código de color de la tabla de matriz forma la base para decidir sobre la aceptabilidad del riesgo y sobre las medidas de prevención y control a tomar.

Como se muestra en la Tabla 8 a continuación, se deben establecer las prioridades y los plazos respectivos para la acción. Entre los niveles de riesgo, se debe dar prioridad, por un lado, a los más fáciles de implementar y, por otro lado, a aquellos con el mayor grado de riesgo.

Tabla 10. Tabla de fijación de prioridades

NIVELES DE RIESGO /PRIORIDAD DE INTERVENCION/ PLAZO		
Nível de Riesgo	Prioridad de Intervencion	Plazo
1 – Bajo [1-4]	Acción no prioritaria	*Tan pronto como sea posible*
2 – Significativo [5-9]	Intervencion a médio plazo	*06 Meses*
3 – Elevado [10-15]	Intervencion a corto plazo	*03 Meses*
4 - Muy Elevado [16-20]	Acción urgente	*01 Mês*
5- Inaceptable (25)	Acción muy urgente	*Inmediato*

Como resultado de este análisis, se definirá una lista de riesgos priorizados, de acuerdo con los criterios de evaluación de riesgos, en relación con los escenarios de incidentes que pueden conducir a estos riesgos.

5.3. TRATAMIENTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Después de un análisis de los riesgos y contrastando con el nivel de riesgo que se considera apropiado en vista de la evaluación realizada, se tomará una decisión sobre el tratamiento que se le dará al riesgo en cuestión. Las opciones de tratamiento de riesgos deben seleccionarse en función del resultado del proceso de evaluación de riesgos, el costo calculado para implementar estas opciones y los beneficios esperados.

ISO / IEC 27005: 2008 define cuatro opciones como pautas para el tratamiento del riesgo:

i) Modificación del riesgo; ii) retención de riesgos; iii) acciones para evitar el riesgo y iv) compartir el riesgo. El tratamiento del riesgo es la implementación de medidas que permiten modificar el riesgo, con un mayor control o reducción del riesgo.

- Acción de modificación de riesgos: esta actividad incluye la aplicación de controles apropiados y debidamente justificados, para satisfacer los requisitos legales, reglamentarios y contractuales. Esta opción debe tener y tener en cuenta los costos y plazos para la implementación de controles, además de los aspectos técnicos, culturales y ambientales.
- Retención / aceptación del riesgo: después de un análisis y una evaluación crítica del posible plan de tratamiento del riesgo, la organización puede decidir aceptar las condiciones del riesgo, sin más acciones. Si el nivel de riesgo cumple con los criterios de aceptación del riesgo, no hay necesidad de implementar controles adicionales y el riesgo puede ser retenido. NP 27001: 2013 en el punto 6.1.3 en el subpárrafo f) recomienda que “obtenga de los gerentes de riesgos la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos de seguridad de la información residual”. Más allá de que “la organización debe mantener información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información”.

- Acción para evitar el riesgo: esta actividad o condición tendrá como origen que se evite el riesgo determinado. Cuando los riesgos identificados se consideran demasiado altos y cuando los costos de implementar otras opciones de tratamiento de riesgos exceden los beneficios, se puede decidir que el riesgo se evita por completo, ya sea mediante la eliminación de una actividad planificada o existente (o conjunto de actividades), o mediante cambios en las condiciones bajo las cuales opera la actividad. Por ejemplo, para los riesgos causados por daños naturales, puede ser una alternativa más rentable mover físicamente las instalaciones de un centro de datos a una ubicación donde el riesgo no existe o está bajo control.

- Compartir riesgos: la acción de compartir un riesgo implica la decisión de compartir ciertos riesgos con entidades externas. La distribución de riesgos puede crear nuevos riesgos o modificar los riesgos existentes e identificados. El intercambio se puede hacer contratando un seguro para cubrir las consecuencias o subcontratando a un socio cuya función es monitorear el sistema de información y tomar medidas inmediatas para prevenir un ataque antes de que pueda causar un cierto nivel de daño o lesión.

  Cabe señalar que es posible compartir la responsabilidad de la gestión de riesgos, sin embargo, normalmente no es posible compartir la responsabilidad legal de un impacto. Es probable que los clientes / usuarios atribuyan un impacto adverso como el fracaso de la organización.

Las cuatro opciones para lidiar con el riesgo no son mutuamente excluyentes. A veces, la organización puede beneficiarse sustancialmente de una combinación de opciones, como reducir la probabilidad de riesgo, compartir o retener los riesgos residuales. Algunas formas de gestión de riesgos pueden hacer frente a más de un riesgo de manera efectiva, por ejemplo, capacitación técnica para un grupo específico en la organización y conciencia de seguridad de la información dirigida a toda la comunidad de una organización.

ISO / IEC 27005: 2008 establece en sus directrices que la definición de un plan de tratamiento de riesgos debe identificar claramente el orden de prioridad y qué formas específicas de tratamiento de riesgos se implementarán, así como sus plazos de ejecución.

La información sobre riesgos debe intercambiarse y / o compartirse entre el tomador de decisiones y todas las demás partes interesadas e involucradas. El desarrollo de

un plan de comunicación de riesgos debe incluir operaciones normales / rutinarias, pero también situaciones de emergencia. Por lo tanto, la actividad de comunicación de riesgos debe llevarse a cabo continuamente.

5.4. MATRIZ DE RIESGO

Siguiendo la "*buena práctica*", después de la definición de la metodología para la evaluación de riesgos, la Matriz de Riesgos se realizó dentro del alcance de las responsabilidades de la Oficina de Sistemas y Tecnologías de la Información (GSTI), registrada en los estatutos de la empresa TECNO FUEGO S.A.S., pero también en los activos infraestructura de soporte para sistemas y tecnologías de información, actualmente en TECNO FUEGO S.A.S. Teniendo en cuenta las categorías de riesgo establecidas en la "*Política de gestión de riesgos*" de TECNO FUEGO S.A.S., la identificación y evaluación de riesgos se llevó a cabo en seis dimensiones:

(i) Riesgos estratégicos relacionados con la organización;

(ii) Marcos regulatorios;

(iii) Participación en sus relaciones internas y externas;

(iv) Finanzas relacionadas con la gestión financiera y la contratación pública;

(v) Con la gestión de recursos humanos en el proceso de reclutamiento y capacitación; y

(vi) Riesgos operativos relacionados con el desempeño y la gestión operativa.

Figura 2. Categorización para la identificación y evaluación de riesgos

La metodología aplicada para la elaboración de la Matriz de Riesgos contó con la participación de un gran número de miembros del GSTI, a través de grupos de trabajo enfocados en la identificación de amenazas y vulnerabilidades existentes y la estimación de la probabilidad de ocurrencia e impacto potencial, de acuerdo con el método definido para la evaluación de riesgos (ítem 5.2.- Método de evaluación de riesgos).

La matriz de riesgos producida después de la identificación y evaluación del nivel de riesgo permitió la elaboración de una de las etapas más importantes de la planificación del SGSI, el plan de tratamiento de riesgos. Para cada riesgo identificado, se definieron las medidas a implementar, correspondientes al plan de acción del tratamiento. El plan de acción presentado ha enumerado y registrado para cada amenaza o riesgo, una medida de tratamiento con la identificación de la persona responsable de su implementación, además de la información detallada de la acción que se llevará a cabo.

Cabe señalar que la mayoría de las evaluaciones de riesgos, así como la mayoría de los procesos de gestión de riesgos implementados, no apuntan a obtener un sistema completamente seguro, sobre todo porque en la mayoría de los casos esto sería imposible. En cambio, el objetivo final es llegar a lo que se puede entender como un nivel aceptable de seguridad a un costo aceptable. Los diversos marcos

existentes en este contexto difieren en la interpretación que hacen de este proceso y en la forma en que lo logran y lo mantienen[15]. Por otro lado, se debe ser consciente de que "*La gestión de riesgos es un proceso continuo y no termina con la implementación de una medida de seguridad. A través del monitoreo constante, es posible identificar qué áreas son exitosas y cuáles necesitan revisiones y ajustes*". [16]

[15] Oliveira, R. (2015). Análisis de riesgo asociado con interrupciones del servicio

[16] Martins, A. y Santos, C. (2005). Una metodología para implementar un sistema de gestión de seguridad de la información

6. DISEÑO SGSI, DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad es un documento de importancia y utilidad relevantes en el proceso de implementación de NP ISO / IEC 27001: 2013 y uno de los principales entregables de la fase de planificación. Este documento es el vínculo principal entre la evaluación, el tratamiento de riesgos y la implementación del sistema de seguridad de la información donde se define, qué se pretende, es decir, qué hacer con la seguridad de la información, proporcionando una visión general pero efectiva qué debe hacerse, por qué debe hacerse y cómo debe hacerse. Es un documento dirigido a los gerentes y auditores superiores / intermedios, por lo que debe presentar un idioma y una interfaz con una lectura adecuada, que no se dirija al funcionamiento diario.

En resumen, la Declaración de Aplicabilidad debe contener:

- Controles seleccionados
- Motivo o razones para seleccionar los controles.
- Objetivos de los controles y controles implementados actualmente
- Exclusiones (incluida la justificación para la exclusión)
- Interfaz fácil de leer.

Se debe "*producir una Declaración de Aplicabilidad que contenga los controles necesarios y la justificación para la inclusión de los controles, ya sea que se*

implementen o no"[17], es decir, la Declaración de Aplicabilidad debe documentar para cada control aplicable si ya está implementado o no y la forma en que se implementa cada control, por ejemplo, haciendo referencia a un documento (política, proceso, instrucción de trabajo, etc.) o describiendo el procedimiento o la tecnología / equipo utilizado en la implementación de la medida de seguridad.

Por otro lado, un control puede justificarse como "no aplicable", si realmente no es posible aplicarlo o si su aplicabilidad está fuera del alcance y alcance de la organización. Los controles "no aplicados" también son controles sin riesgo y justificados como controles "no aplicables", o debido a la superposición de otro control.

6.1. DECLARACIÓN DE APLICABILIDAD: EJES DE ACCIÓN

En la práctica, la Declaración de Aplicabilidad se refiere claramente al "Informe de análisis y evaluación de requisitos de control", donde describe en detalle los objetivos y controles aplicados y que se aplicarán en el Sistema de Gestión de Seguridad de la Información y la forma en que se aplicarán.

Sin embargo, teniendo en cuenta que la Declaración de Aplicabilidad está dirigida a gerentes, auditores y tomadores de decisiones, se tomó como un enfoque para presentar el plan de acción de manera concisa y con un lenguaje sin una conexión literalmente técnica. El plan de acción se basa en cinco ejes de acción: organizacional, físico y ambiental, personal, tecnológico y de cumplimiento y regulación, en el horizonte temporal 2017-2018.

[17] NP ISO / IEC 27001 6.1.3.d

Los ejes de acción indicados: Organizacional, Físico y Ambiental, Personal, Tecnológico y de Cumplimiento y Regulación, son el resultado de la percepción de que la seguridad de la información "*como una cuestión transversal que es, debe involucrar a todos los niveles de la organización y verse como un facilitador de procesos y aumentar los niveles de confianza internos y externos. Este es el gran argumento sobre el cual cualquier organización puede capitalizar su inversión en esta área. Al implementar este programa, transmitirá una imagen de preocupación en este asunto, que es cada vez más importante y con mayor visibilidad, mientras logra administrar el riesgo al que está sujeto*"[18].

En la selección de las medidas presentadas, se trata de considerar los siguientes criterios de validación:

- La existencia de una justificación para su necesidad basada en el análisis y la evaluación de riesgos realizados previamente;
- Es específico, medible, alcanzable dentro de un período de tiempo aceptable y su implementación es realista;
- Conduce a la creación de procedimientos o instrucciones de trabajo para resolver o limitar el problema y la necesidad de asignar responsabilidades de control;
- La implementación reina con las nuevas tecnologías, debido a su naturaleza obsoleta y la no garantía del modelo conceptual del SGSI.

[18] Silva, P. T., Carvalho, H. y Torres, C. B. (2003). Seguridad de los sistemas de información.

Cabe señalar que existe una relación entre las líneas de acción y las medidas propuestas. Sin embargo, la secuencia con la que deben implementarse es relevante. Para ello, se deben aplicar las prioridades y los plazos respectivos establecidos de acuerdo con la tabla que relaciona los niveles de riesgo con el plazo / prioridad de intervención.

6.2. EJE I: ORGANIZACIONAL

El eje de acción I: Organizacional, tiene como objetivo proporcionar directrices y establecer un modelo de Operacionalización para apoyar la implementación y gestión de la seguridad de la información.

Para el eje I: se definen cuatro medidas organizativas, que se desarrollan a continuación, a saber:

- Medida 1: Política de seguridad de la información
- Medida 2: Estructura de seguridad de la información organizacional
- Medida 3: Liderazgo y compromiso
- Medida 4: marco documental del SGSI

Para cumplir con los requisitos del Eje I, se deben realizar las siguientes acciones:

Medida 1: Política de seguridad de la información

- Definir y aprobar la política de seguridad de la información
- Comunicar y poner a disposición la política de seguridad de la información

Tabla 11. Política de Seguridad de la información

Medida 1 - Política de Seguridad de la informacion				
	Acciones	**Descripcion**	**Conclusión**	**Responsáble**
Definir y aprobar la política de seguridad de la información				
1.1.1	Estabelecer política de seguridad de la informacion	Una política de seguridad que es un compromiso con los requisitos aplicables a NP 27001: 2013; diseñado para el propósito de la misión de TECNO FUEGO S.A.S.; Un modelo de referencia en la definición clara de la estrategia y los objetivos relacionados con la seguridad de la información y la mejora continua.	2ºtrimestre 2020	CD e GSTI; GQ
1.1.2	Revisar la política de seguridad de la información	Establecer un plan de revisión de la política de seguridad de la información, al menos, anualmente o cuando lo justifiquen los objetivos de TECNO FUEGO S.A.S.. (continua)	2ºtrimestre 2020	CD e GSTI; GQ

Tabla 12. Política de Seguridad de la información

Medida 1 - Política de Seguridad de la informacion				
	Acciones	**Descripcion**	**Conclusión**	**Responsáble**
Definir y aprobar la política de seguridad de la información				
1.1.3	Establecer acciones de comunicación para la política de seguridad de la información.	Definición de un programa para comunicar la política de seguridad de la información a todos los empleados, socios y proveedores de servicios de TECNO FUEGO S.A.S., con el propósito de una comprensión y compromiso adecuados de todas las partes.	3ºtrimestre 2020	CD e GQ; GMC
1.1.4	Hacer disponible la política de seguridad de la información	Establecer una plataforma con varios canales de comunicación y disponibilidad de la política de seguridad de la información y que sea accesible y actualizada.	3ºtrimestre 2020	GQ; GMC

Medida 2: Estructura de seguridad de la información organizacional

- Responsabilidades y Posiciones
- Contacto con autoridades competentes y grupos de interés.

Tabla 13. Estructura organizativa de seguridad de la información

Medida 2 - Estructura organizativa de seguridad de la información				
	Acciones	**Descripcion**	**Conclusion**	**Responsable**
Responsabilidades y Cargos				
1.2.1	Asignar responsabilidades, cargos y autoridades.	Definir una estructura organizativa enmarcada con seguridad de la información (ver detalles, subcapítulo Responsabilidades y cargos), destacó: la Junta Directiva como el organismo responsable de promover el SGSI; Gerente de Seguridad de la Información (CISO); Comité de seguridad de la información; Equipo técnico pluridisciplinario; Responsable de los activos de proceso y seguridad de la información.	2ºtrimestre 2020	CD
		La alta dirección debe asegurarse de que los recursos necesarios para el SGSI estén disponibles, a fin de garantizar que el SGSI cumple con los requisitos y se comunica internamente dentro de la organización e informa sobre su desempeño.		
Contacto con autoridades competentes y grupos de interés.				

1.2.2	Establecer protocolos con las autoridades estatales.	Establecer un protocolo articulado con la Oficina de Seguridad Nacional; (Departamento Nacional de Ciberseguridad); CNPD (Comisión Nacional de Protección de Datos)	2ºtrimestre 2020	Gerente de seguridad; Oficial de protección de datos; Oficina de crisis
1.2.3	Mantener contactos con grupos especializados en seguridad de la información.	Se deben mantener contactos apropiados con grupos y asociaciones dedicados y especializados en seguridad de la información, por ejemplo, Information Society Security Group (GSSI)	2ºsemestre 2020	Gerente de Seguridad y GSTI

Medida 3: Liderazgo y compromiso

- Asegurar la alineación con la política de seguridad
- Promover la mejora continua.

Tabla 14. Liderazgo y compromiso

Medida 3: Liderazgo y compromiso				
	Acciones	**Descripcion**	**Conclusion**	**Responsable**
Garantizar la alineación con la Política de seguridad de la información				
1.3.1	Garantizar la alineación con la Política de seguridad de la información	La alta dirección debe asegurarse de que la política de seguridad de la información esté alineada e integrada con la estrategia y misión de TECNO FUEGO S.A.S., comunicando su importancia en gestión operativa y que todas las funciones son relevantes para los resultados previstos.	2ºsemestre 2020	CD

Tabla 15. Promoción de la mejora continua

Promover la mejora continua.				
1.3.2	Proporcionar la aplicabilidad de la mejora continua en el SGSI	Establecer un compromiso con la alta dirección para mejorar continuamente el sistema de gestión de seguridad de la información.	2ºtrimestre 2020	Comité de seguridad

Medida 4: marco documental del SGSI

- Estructura documental
- Responsabilidades para la gestión de documentos.

Tabla 16. Marco documental del SGSI

Medida 4: marco documental del SGSI				
	Acciones	**Descripcion**	**Conclusion**	**Responsable**
Estructura documental				
1.4.1	Implementar estructura documental bajo el SGSI	La estructura documental dentro del alcance del Sistema de Gestión de Seguridad de la Información debe incluir un conjunto de políticas y normas (Normativas) que guíen las actividades en la protección de la información, así como que preparen documentación operativa que sirva como evidencia para las auditorías "muestra que usted lo hace, como dices ". (ver detalles en el Marco de documentación del SGSI)	2ºsemestre 2020	Gerente de Seguridad y GSTI
Responsabilidades para la gestión de documentos				
1.4.2	Definir a los responsables de redactar el Reglamento y su aprobación.	La elaboración del documento normativo debe respetar lo que se define en su estructura, con respecto a la elaboración y aprobación.	2ºsemestre 2020	Gerente de Seguridad

6.3. EJE II: PERSONAL

Eje de acción II: El personal, en el ámbito de la seguridad de la información, tiene como componentes principales la (i) admisión y rescisión del contrato; (ii) roles y responsabilidades; (iii) capacitación técnica;

(iv) acciones de sensibilización, educación.

En el componente de contratación de proveedores de servicios y contratación de empleados, "*la idoneidad de los empleados es necesaria, llevando a cabo la verificación de sus datos, acreditándolos para manejar los datos y la información a los que tendrán acceso, presentando la filosofía de seguridad de la compañía. Información de la organización y garantizando su aceptación"*[19]. (Al finalizar y cambiar la relación contractual, se deben garantizar los procedimientos para recopilar todos los recursos de la organización en su poder (por ejemplo, computadora portátil, teléfono móvil), así como garantizar la desactivación de todas las formas de identificación y autenticación en los sistemas de la organización, como, por ejemplo, desactivar la cuenta en el dominio y cambiar las contraseñas para acceder a los recursos de la aplicación.

Las responsabilidades deben asignarse adecuadamente para eliminar las oportunidades de modificaciones no autorizadas. Si no es posible la separación, se deben proporcionar otros tipos de control, como el monitoreo por parte de la administración o el registro de actividades. Debe garantizarse que las áreas y servicios técnicos, cuya responsabilidad es solo de una persona, no estén sujetos a modificaciones / alteraciones que no puedan detectarse.

La evolución constante de los sistemas y tecnologías de la información y el consiguiente refinamiento de las formas de ataque que surgen, exige un plan de capacitación técnica constante y específico para el equipo GSTI, a fin de responder a la dimensión tecnológica de la seguridad de Requisitos de información y control de ISO / IEC 27001.

[19] Martins, A. y Santos, C. (2005). Una metodología para implementar un sistema de gestión de seguridad de la información

Desarrolle un programa de concientización con la aplicabilidad de una política técnica, desde la perspectiva del usuario, donde aborde acciones para crear conciencia de una cultura de secreto y la rendición de cuentas de todos los empleados en el ámbito de la seguridad de la información y los sistemas de información.

Para el **Eje II - Personal**, se identifican las siguientes tres medidas:

- Medida 5: Política de seguridad en el alcance del contrato y los recursos de la función
- Medida 6: Programa de concientización sobre seguridad de la información
- Medida 7: formación técnica.

En cumplimiento de los requisitos del Eje II - Personal, se deben tomar las siguientes acciones:

Medida 5: Política de seguridad en el ámbito contractual y en los recursos de la función.

- Verificación de antecedentes en el proceso de contratación
- Definición del perfil funcional.

Tabla 17. Política de seguridad en el ámbito contractual y en los recursos de la función.

Medida 5: Política de seguridad en el ámbito contractual y en los recursos de la función.				
	Acciones	**Descripción**	**Conclusión**	**Responsable**
Verificación de antecedentes en el proceso de contratación				
2.5.1	Verifique los antecedentes en la contratación de nuevos empleados y proveedores de servicios.	Al contratar nuevos empleados, se debe requerir una verificación de antecedentes al seleccionar candidatos, así como referencias de empleadores anteriores. Para los empleados fuera de la entidad (por ejemplo, consultores), el solicitante respectivo (o la persona responsable del presupuesto del departamento) debe llevar a cabo un proceso de revisión similar. Deben celebrarse acuerdos de secreto y confidencialidad antes de acceder a los datos o sistemas de información.	Julio del 2020	Depto. Recursos Humanos
Definición del perfil funcional.				

2.5.2	Defina el perfil funcional correspondiente al nivel de acceso a la red y los recursos de la aplicación.	En correspondencia con el rol y las responsabilidades, asigne un Perfil funcional específico que defina el acceso a la red y los niveles de acceso a los recursos de la aplicación y sus funcionalidades. Durante la ruta contractual, cualquier cambio en el rol / responsabilidades implica un cambio en el Perfil Funcional.	Julio de 2020	GSTI y Depto. Recursos humanos; Responsable jerárquico

Medida 6: programa de concientización sobre seguridad de la información.

- Política sobre el uso de sistemas y tecnologías de información.
- Acciones de capacitación sobre cuestiones de seguridad de la información.
- Conciencia en el uso de la Política de Seguridad en el lugar de trabajo.
- Proporcionar y difundir información relacionada con la seguridad de la información.

Tabla 18. Programa de concientización sobre seguridad de la información.

Medida 6: programa de concientización sobre seguridad de la información.				
	Acciones	**Descripción**	**Conclusión**	**Responsable**
Política sobre el uso de sistemas y tecnologías de información				
2.6.1	Implementar políticas para el uso de sistemas y tecnologías de información.	Presente formalmente un conjunto de reglas que deben aplicarse al usar los diversos servicios relacionados con los sistemas de información y las tecnologías asociadas. En esta política debe haber referencia a un procedimiento disciplinario formal que sea procesable en caso de una violación de la seguridad de la información.	en marcha	GSTI y Oficina legal

Tabla 19. Acciones de capacitación

Acciones de capacitación sobre cuestiones de seguridad de la información				
2.6.2	Desarrollar acciones de capacitación sobre inquietudes relacionadas con la seguridad de la información.	Todos los empleados de la organización que hacen uso directo o indirecto de los servicios de la red deben ser receptores de acciones de concientización sobre seguridad de la información. El empleado debe acusar recibo de la capacitación por escrito.	Julio 2020	GSTI y Depto. Recursos humanos; Oficina de marketing y comunicación
Conciencia en el uso de la Política de Seguridad en el lugar de trabajo				
2.6.3	Promover o conhecimento da Política de Segurança da Informação	Promover el conocimiento de la política de seguridad de la empresa. Informacion	Julio 2020	CD

		Que todas las áreas orgánicas son responsables de implementar la seguridad de la información tal como se define en las reglas, procedimientos y reglas.		Depto. Recursos Humanos; Responsable sJerárquicos
Proporcionar y difundir información relacionada con la seguridad de la información.				
2.6.4	Definir plataforma (s) para difusión, consulta y capacitación (e-learning)	Establezca una plataforma o adaptación de una existente accesible a todos los empleados, socios y proveedores de servicios con información, para que los usuarios estén al tanto de las amenazas relacionadas con la seguridad de la información y estén preparados para aplicar la Política de seguridad de la información. Implementar una plataforma de aprendizaje electrónico que permita la capacitación sobre temas relacionados con la seguridad de la información, pero que se pueda utilizar con una herramienta de autoaprendizaje en varias áreas. Diseñar un volante con diez reglas básicas que se aplicarán en el lugar de trabajo de conformidad con las medidas de seguridad, como la adopción de la política	Septiembre 2020	GSTI y Depto. Recursos Humanos; Responsable jerárquico

6.4. EJE III: FÍSICO Y AMBIENTAL

Eje de acción III: físico y ambiental, se ajusta a los aspectos relacionados con la protección física de las instalaciones de la organización, donde operan los sistemas informáticos y las áreas operativas que operan o contienen información sensible o crítica y recursos de procesamiento de información en apoyo de sus actividad este eje de acción tiene como objetivo garantizar la prevención en la ocurrencia de eventos graves o catástrofes donde, a nivel físico, ya sea nacional o regional, existan consecuencias que puedan dañar el funcionamiento normal en respuesta a su misión y consecuencias en el acceso a la información. "*Estos eventos fortuitos son normalmente predecibles, aunque el instante en que ocurren no es predecible, ni es a menudo la gravedad con la que ocurren*"[20]. Por lo tanto, se debe establecer un conjunto de procedimientos y medios que puedan responder efectivamente a fallas previsibles o fallas y defenderse contra actividades no autorizadas[21].

En este contexto, debemos considerar los siguientes aspectos:

- Identificación de áreas afectadas por el procesamiento, tratamiento y archivo de información.
- Infraestructura eléctrica con autonomía redundante en caso de falla / roturas.
- Infraestructura adecuada y segregada de rutas de cables eléctricos y el cableado de red de datos. En el caso de los centros de procesamiento de

[20] Zúquete, A. (2015). Seguridad de la red informática

[21] Las actividades no autorizadas pueden originarse: en los sujetos que pertenecen a la organización, el propietario del sistema informático a proteger y los sujetos que no pertenecen al mismo. Los primeros son más difíciles, ya que generalmente tienen mayores privilegios sobre los segundos, que pueden usar para iniciar actividades no autorizadas. (Zúquete, A. 2014)

datos (centros de datos), garantice sistemas adecuados de control de refrigeración, incendio, inundación y alarma.

- Acceso físico controlado a instalaciones clasificadas como de riesgo, integradas con acreditación personal.
- Procedimientos de protección y prevención en los componentes computacionales de hardware, software, medios magnéticos y documentación, en términos de riesgos de robo, pérdida, pérdida o daño físico.

En esta línea de acción, la empresa TECNO FUEGO S.A.S., cubre satisfactoriamente los requisitos recomendados por ISO / IEC 27001; a saber: en la definición de perímetros de seguridad física con controles de entrada física; Las áreas críticas han agregado infraestructura redundante de energía eléctrica, medios de enfriamiento, seguridad contra incendios, control y detección. Tiene planes de mantenimientos preventivos definidos y aplicables con pruebas funcionales regulares, es decir, contra interrupciones de energía eléctrica. El tratamiento de equipos electrónicos sigue procedimientos cubiertos y certificados por ISO 14001 (Sistema de Gestión Ambiental) y las áreas de carga y descarga de equipos informáticos, están cubiertos por procedimientos logísticos. El mantenimiento del equipo se mantiene correctamente; GSTI tiene un programa de reutilización en curso (5R-Reciclar, Rechazar, Reducir, Reutilizar, Repensar) de los equipos informáticos, lo que garantiza su disponibilidad e integridad de forma continua.

Como puntos de cobertura a los requisitos de ISO / IEC 27001, se proponen las siguientes medidas:

- Medida 7: Ejecución de pruebas, en centros de datos, para fallas predecibles
- Medida 8: Realizar planes de contingencia y plan de recuperación ante desastres

En cumplimiento de las medidas a aplicar en el eje III-Físico, se describen las siguientes acciones:

Medida 7: Ejecución de pruebas, en centros de datos, para fallas predecibles

- Realizar simulaciones operacionales en los sistemas informáticos en caso de falla de energía
- Documentar y aplicar la mejora continua en la mitigación de riesgos.

Tabla 20. Ejecución de pruebas, en centros de datos, para fallas predecibles

Medida 7: Ejecución de pruebas, en centros de datos, para fallas predecibles				
	Acciones	**Descripción**	**Conclusión**	**Responsable**
Realizar simulaciones operacionales en los sistemas informáticos en caso de falla de energía				
3.8.1	Planifique y realice simulaciones operativas para fallas de electricidad predecibles.	La redundancia en el componente de energía implica demoras entre el UPS - pasaje del generador. Es obligatorio validar la vida útil del UPS con los procedimientos de apagado / arranque de los sistemas de información. Evaluar el comportamiento (continuo) del generador en funcionamiento.	2º sem. 2020	GSTI y Unidades Orgánicas
Documentar y aplicar la mejora continua en la mitigación de riesgos.				
3.8.2	Documente el modus operandi en la interconexión con los planes de recuperación ante desastres para los sistemas de información.	La "buena práctica" sugiere documentar el método operativo con la identificación de los actores en el proceso (GSTI y Unidades Orgánicas), la definición del procedimiento de escalamiento, los tiempos de respuesta y resolución. La realización de pruebas planificadas permite mitigar los riesgos de manera controlada, mejorar los procedimientos y validar los procedimientos entre las partes involucradas.	2º sem. 2020	GSTI y Unidades Orgánicas

Medida 8: Llevar a cabo planes de contingencia y plan de recuperación ante desastres.

- Llevar a cabo y documentar planes de contingencia en caso de cortes de energía y telecomunicaciones prolongados.
- Validar el plan de recuperación ante desastres.
- Revisar y evaluar los planes de continuidad del negocio.

Tabla 21. Llevar a cabo planes de contingencia y plan de recuperación ante desastres.

Medida 8: Llevar a cabo planes de contingencia y plan de recuperación ante desastres.				
	Acciones	**Descripción**	**Conclusión**	**Responsable**
Llevar a cabo y documentar planes de contingencia en caso de cortes de energía y telecomunicaciones prolongados.				
3.9.1	Planifique la realización de planes de contingencia operativos y funcionales en caso de cortes de energía prolongados.	La falla de energía prolongada puede implicar inaccesibilidad a los sistemas de información, también por un tiempo determinado. Un fallo del servicio o una interrupción de las telecomunicaciones en la red de datos pone en peligro el acceso a los sistemas críticos. La predicción de fallas o cortes de energía parciales y / o telecomunicaciones de datos / voz en términos geográficos, implica el paso de servicios y la reorganización funcional y operativa. El retorno al estado inicial también implica oscilación en el acceso a los sistemas de información y telecomunicaciones.	2º sem. 2020	GSTI y Unidades Orgánicas

Validar el plan de recuperación ante desastres.				
3.9.2	Validar los planes de continuidad del negocio entre las partes afectadas.	Siguiendo el ítem anterior 3.9.1, los planes de contingencia para la continuidad operativa deben ser validados por las unidades orgánicas cubiertas. La participación y la participación en estas acciones aportan un mayor y mejor conocimiento compartido y una mejora continua.	1º sem. 2021	GSTI y Unidades Orgánicas
Revisar y evaluar los planes de continuidad del negocio.				
3.9.3	Revisar y evaluar periódicamente los planes de contingencia.	Los cambios operativos o los cambios tecnológicos o de sistemas de información implican una revisión de los planes de contingencia.	2º sem. 2020	GSTI y Unidades Orgánicas

6.5. DIMENSIÓN DE RED

La dimensión de la red abarca la gestión de la infraestructura de red de datos (LAN, WAN, NAS o SAN)[22] y la red de telecomunicaciones responsable de garantizar la interconexión del servidor y la plataforma del cliente (puntos finales). Además, incluye el componente tecnológico de seguridad de los activos de protección de la información y la comunicación, con la aplicabilidad de los sistemas de control de

[22] LAN-Área local Nework; (red de computadoras en red en un área geográfica pequeña, por ejemplo, en el edificio de la sede); WAN-Wide Área Network (red de comunicaciones de datos en la interconexión entre ubicaciones con larga distancia, por ejemplo, en la interconexión entre delegaciones);
Almacenamiento conectado a la red NAS; Red de área de almacenamiento SAN (redes diseñadas exclusivamente para almacenar datos)

tráfico (firewall), el sistema de inspección del contenido de datos en tránsito en la red (Sistema de detección de intrusiones IDS) y sistemas antivirus para detectar y eliminar códigos maliciosos en el sistema de archivos y encriptación.

En el análisis y la evaluación de riesgos llevados a cabo en esta dimensión y para cumplir con las características básicas de disponibilidad, integridad y confidencialidad de la seguridad de la información, se presentan las siguientes medidas de acción:

Medida 9: planifique e implemente una arquitectura LAN / WAN redundante

- Definir e implementar la arquitectura de red LAN.
- Redundancia en la red VPN y la infraestructura de servicios de Internet.
- Monitoreo y administración centralizada de la red LAN e inalámbrica (WLAN)
- Estandarización / Certificación del tipo de cable (cat.6) red pasiva

Medida 10: sistema de firewall redundante

- Reemplazar e implementar un nuevo sistema de firewall redundante con IPS
- Desarrollar una prueba de concepto de solución

Medida 11: sistema antivirus

- Implemente una política antivirus activa en todos los equipos cliente y servidor.
- Informes de rendimiento y estado actual de las instalaciones antivirus.

7. CONCLUSIONES

En primer lugar, hay que señalar que el desarrollo de este trabajo en un entorno organizacional, proporcionó una experiencia enriquecedora en la participación con varias personas en el tema de la gestión de riesgos y la seguridad de la información, así como el conocimiento adquirido sobre los procesos de seguridad, basado en la infraestructura de los sistemas y tecnologías de información de la empresa TECNO FUEGO S.A.S. Por otro lado, existe un convencimiento de que el intercambio de conocimientos entre los diversos actores que formaron parte de este trabajo resultó en una experiencia enriquecedora para todos.

La realización de este trabajo permitió aprovechar un conjunto de factores beneficiosos para la gobernanza de los sistemas y tecnologías de la información en uso en la organización TECNO FUEGO S.A.S., en los que la capa de riesgo y seguridad de la información, permitió "*una mirada diferente*" al desarrollar nuevas acciones. Los proyectos, aumentaron la sensibilidad y la participación de los empleados involucrados en la gestión de sistemas y redes y, sobre todo, permitieron reconocer que la aplicabilidad de las "*buenas prácticas*" son herramientas facilitadoras en un proceso de mejora continua. La prueba es que, durante el curso de este trabajo, el equipo GSTI / TECNO FUEGO S.A.S., inició ciertas acciones como resultado de su participación en el desarrollo de este proyecto y el reconocimiento de la aplicabilidad de las "*buenas prácticas*" como un factor diferenciador y facilitador en los procesos de gestión y administración de sistemas de información. Estos primeros pasos registran evidencia de que es posible superar barreras, incluso cuando hay dificultades u oposiciones internas.

Se puede decir que, dado el nivel actual de madurez obtenido en el área de gestión de seguridad de los sistemas de información, permite prever que existen condiciones favorables para la implementación de las medidas propuestas y que no existen factores inhibidores para obtenerlas en el mediano plazo, certificación en gestión de seguridad de sistemas de información, es decir, en la obtención de la certificación de ISO / IEC 27001.

Se sabe que no hay sistemas con arquitecturas perfectas, así como tampoco hay seguridad de la información con total efectividad. De hecho, se acostumbra decir que "*no hay seguridad efectiva de la información. Cualquier sistema es vulnerable a los ataques*". Sin embargo, también se sabe que al implementar un SGSI, se transmite una imagen de preocupación con la integridad y la preservación de sus activos de información, que es cada vez más importante y con mayor visibilidad, al mismo tiempo que se gestiona el riesgo al que está sujeto. Al implementar el Sistema de Gestión de Seguridad de la Información (SGSI), siempre es necesario evaluar bien cuáles son los riesgos reales y cuáles son las pérdidas inherentes. Desde una perspectiva financiera, se requerirá una inversión adicional para implementar el SGSI. Esta inversión depende del tamaño y el impacto de las vulnerabilidades identificadas y los factores de riesgo asociados con el desempeño de la institución, pero también del impacto en su reputación.

Por otro lado, la seguridad de la información es sinónimo de acciones limitantes, imposición de barreras, acciones de monitoreo, lo que puede crear fricciones con el funcionamiento, más o menos liberalmente, en el ámbito de la gestión de redes

computacionales y organizacionales. De esta forma y, como cuestión transversal, será necesario un cambio cultural en la compañía en la forma en que tendrá que ver la información y la seguridad de la información. Un cambio que debe ser aceptado y practicado por todas las unidades orgánicas, socios y proveedores de servicios.

En vista del objetivo establecido, desde el principio, este trabajo se hizo factible. Se tiene el convencimiento de que su aplicación necesariamente tendrá un impacto en los objetivos y requisitos de la organización, convirtiéndose en una opción estratégica. El compromiso de la alta gerencia en la implementación del SGSI es vital para asegurar y reforzar los recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información. Será una tarea ardua, pero los beneficios resultantes de la construcción de este sistema de gestión recompensan todo el esfuerzo que la organización, en su conjunto, debe tener para implementar el SGSI.

8. RECOMENDACIONES

Si, por un lado, el desempeño de este trabajo y el análisis de los resultados obtenidos permitieron obtener beneficios relevantes para la definición del curso que se implementará con el Sistema de Gestión de Seguridad de la Información, por otro lado, tenía algunas limitaciones técnicas ya que no era posible realizar pruebas de penetración a algunas de las aplicaciones, utilizando herramientas especializadas y por lo tanto, ser capaz de definir recomendaciones y medidas más rigurosas que puedan analizar y validar la arquitectura de un sistema informático.

Como trabajo futuro, las tareas desafiantes que surgirán al implementar el SGSI, en su contexto en la Operacionalización de las etapas DO (Implementar y Operar) - COMPROBAR (Monitorear y Revisar) - ACT (Mantener y Optimizar), además de la interacción transversal con las unidades orgánicas en la implementación de las diversas medidas propuestas.

La seguridad de la información, además de tener un componente técnico e infraestructura en tecnologías de la información, también tiene un componente humano y procesal “*fuerte*" dentro de la organización. Involucrar, desde el principio, a las personas que forman parte de los procesos organizacionales en el tema de la seguridad de la información y las buenas prácticas a aplicar es, sin duda, un activo en el desarrollo de este trabajo porque la adquisición y el intercambio de conocimiento es inmenso Esta participación e intercambio es extremadamente

importante en la fase de planificación del SGSI porque abrirá el camino para su implementación.

9. BIBLIOGRAFÍA

CARNEIRO, A. Auditoría y Control de Sistemas de Información. FCA- Editora de Informática, Lda. Lisboa (2016).

CASACA, J. y CORREIA, M. ¿Por qué es necesaria la seguridad de la información? De la estrategia a las políticas de seguridad. Lusíada Política internacional y seguridad, (2010). Nº3, pp.89-116.

CASACA, J. Gestión de riesgos en seguridad de la información: conceptos y metodologías. (2014).

CERT.PT Coordinación de respuesta a incidentes. Disponible en: http://www.cncs.gov.pt/cert- pt / / index.html [consultado el 8 de abril de 2020].

CNCS Centro Nacional de Ciberseguridad. Disponible en: http://www.cncs.gov.pt/pagina- inicial / index.html [accedido el 7 de Mayo de 2020].

ISO / IEC 27000. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. BSI-Norma Británica. Reino Unido. (2008).

ISO/IEC 27002 - Information Technology - Security Techniques: Code of practice for information security management. International Standard. www.iso.org. (2013)

ISO/IEC 27003 - Information Technology - Security Techniques: Information security management system implementation. International Standard. www.iso.org. (2010)

ISO/IEC 27005. Information technology - Security techniques - information security management. BSI-British Standard. UK (2008).

ISO27K Forum information Security http://www.iso27001security.com/html/toolkit.html [consultado en Abril, 2 2020].

MARTINS, A. y SANTOS, C. Una metodología para implementar un sistema de gestión de seguridad de la información. Journal of Information Systems and Technology Management, (2005). V. n.2, pp. 121-136.

MELO, M. Ciclo de conferencias - Protección de datos y ciberseguridad. Reglamento general de protección de datos. Nova Facultad de Derecho. Lisboa (2016).

OLIVEIRA, R. Análisis de riesgo asociado con interrupciones del servicio. Tesis de Maestría en Seguridad Informática. Universidad de Lisboa-Facultad de Ciencias-Departamento de Informática. (2015).

REGLAMENTO DE LA UE 2016/679. Reglamento general de protección de datos. Parlamento Europeo y Consejo de la Unión Europea, 27 de abril de 2016. Publicado el 4 de mayo de 2016.

RIGON, E. y WESTPHALL, C. Modelo de evaluación de madurez de seguridad de la información. Revista electrónica de sistemas de información, v.12 (enero-abril 2020), pp. 1-19.

SEIXAS, S. M. Modelo para la gestión de eventos de seguridad de la información. España: Universidad de la Rioja - Escuela de Ingeniería. (2013).

SILVA, D. Beneficios y factores condicionantes de la obtención de la certificación en la gestión de seguridad de sistemas de información. Disertación de Maestría en

INGENIERÍA Y GESTIÓN DE SISTEMAS DE INFORMACIÓN, España: Universidad de la Rioja - Escuela de Ingeniería. (2011).

SILVA, P. T., Carvalho, H. y Torres, C. B. Seguridad de los sistemas de información. España: Universidad de la Rioja - Escuela de Ingeniería. (2003).

VIAN, P. Desarrollo de un marco situacional para la ciberseguridad en Portugal. Nueva Universidad de Lisboa - Facultad de Derecho

ZÚQUETE, A. Seguridad de la red informática (3ª ed. Actualizado y aumentado). FCA-Editora de Informática, Lda. Reino Unido. (2015).

10. ANEXOS

10.1. ANEXO (A) RESUMEN ANALÍTICO RAE

Anexo (A) RESUMEN ANALÍTICO DE EDUCACIÓN – RAE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FECHA			17/05/2020				
TITULO			DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL ASEGURAMIENTO DE LA INFORMACIÓN EN LA EMPRESA TECNO FUEGO S.A.S. DE LA CIUDAD DE BARRANQUILLA				
AUTOR			ALBERTO ENRIQUE TORRES PADILLA				
DIRECTOR (ES)/ASESOR(ES)			MARTIN CAMILO CANCELADO				
AÑO ELABORACIÓN			2020				
DESCRIPCIÓN							
PAGINAS	89	**TABLAS**	21	**FIGURAS**	1	**ANEXOS**	1
CONTENIDO							
PALABRAS CLAVES							
ISO 27001, Información, seguridad, sistema, riesgo, amenaza, confidencialidad, controles, activo informático, magerit, impacto, SGSI, análisis.							
FORMULACIÓN DEL PROBLEMA							
¿El diseño del sistema de gestión de seguridad de la información le proveerá a TECNO FUEGO S.A.S los elementos, técnicas y parámetros adecuados para mejorar la seguridad de la información de la empresa, la gestión y tratamiento de los riesgos asociados al uso de su información?							
DESCRIPCIÓN DEL PROBLEMA							
En la actualidad la empresa Tecno Fuego S.A.S no cuenta con un sistema de gestión de seguridad y los manejos de la información no tienen lineamientos ni mecanismos para su aseguramiento, en algunas ocasiones se ha tenido indicios de filtración o fugas de información incluso perdida de la misma por lo que sus directivos están dispuestos a buscar métodos los cuales permitan tener asegurada dicha información de forma eficaz. Con la existencia de un Sistema de Gestión de Seguridad de la Información en la empresa Tecno Fuego S.A.S., se pretende generar sentido de pertenencia en los temas de seguridad en los usuarios que cada día manejan la información, logrando su participación en la planeación, definición e implementación de políticas y procedimientos para el aseguramiento de la misma. Para lograrlo, se requiere que inicialmente se realicé una clasificación los activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización, con el propósito de identificar los riesgos de seguridad asociados con la							

información y de esta forma realizar un análisis para definir y establecer los mecanismos más convenientes para protegerla.

OBJETIVOS

Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información para la empresa TECNO FUEGO S.A.S. el cual mantenga la integridad, disponibilidad y confidencialidad de la información y sus activos tecnológicos, tomando como referencia la norma ISO 27001.

Objetivos Específicos

- Realizar el levantamiento de la información actual de seguridad, metodologías, procesos, procedimientos y controles de seguridad existente en la organización, así como procesos normativos aplicados en la seguridad de la información.
- Identificar los riesgos y amenazas que pueden afectar el normal funcionamiento de los procesos informático de la empresa con el fin de hacer una valoración de los mismos, alineados al estándar ISO 27001.
- Diseñar un Sistema de Gestión de Seguridad Informática que permita establecer políticas, lineamientos y estrategias para desarrollar soluciones tecnológicas para la protección de sus activos e infraestructura.
- Implementar el Sistema de Gestión de Seguridad Informática con el fin de proteger los activos informáticos, monitoreando y controlando los riesgos y amenazas con el fin de mantener la confidencialidad, integridad y disponibilidad de la información.

CONTENIDO

MATRIZ DE RIESGO
DISEÑO SGSI, DECLARACIÓN DE APLICABILIDAD
DECLARACIÓN DE APLICABILIDAD: EJES DE ACCIÓN
EJE I: ORGANIZACIONAL
EJE II: PERSONAL
EJE III: FÍSICO Y AMBIENTAL
DIMENSIÓN DE RED
CONCLUSIONES
RECOMENDACIONES
BIBLIOGRAFÍA

METODOLOGÍA DE INVESTIGACIÓN

Para el análisis de riesgo y gestión del mismo en la empresa TECNO FUEGO S.A.S. se ha elegido la metodología MAGERIT, ya cuanta con lineamientos y está directamente relacionada con la generalización del uso de las tecnologías de la información, también cuanta con las medidas apropiadas para dar tratamiento adecuado y cuantificar de forma adecuada los activos de la compañía. Se hace necesario la elaboración de un diagrama de procedimiento, en función de las necesidades específicas para producir un plan de implementación que, en ISO / IEC 27001: 2013, se conoce como la "Declaración de Aplicabilidad" (NP ISO / IEC 27001 Cláusula 6.1.3d, p. 9)

Dado que este trabajo, en particular, se centra en la fase Diseño de un SGSI, el Diagrama presenta en detalle los procesos necesarios para esta fase y la identificación, que forman parte de los procesos identificados del 1 (uno) al 10 (diez) y la producción de sus respectivos entregables.

Se buscó con este modelo, de manera genérica, definir un conjunto de actividades que permitieran comprender la interconexión de los procesos funcionales actuales, la estrategia de la organización y su alineación con los sistemas y tecnologías de información circundantes, así como identificar el nivel de capacidad y madurez que la organización tiene para responder y lograr la implementación de un Sistema de Gestión de Seguridad de la Información, guiándolo con un conjunto de objetivos a alcanzar (actividades a realizar) aplicables al proceso de implementación de la norma ISO / IEC 27001: 2013

TÉCNICAS DE RECOPILACIÓN Y ANÁLISIS DE DATOS

Se tomó como punto de partida realizar una revisión de la literatura sobre un sistema de gestión de seguridad de la información, la importancia de la seguridad de la información en el contexto de una organización, las ventajas de un sistema de gestión La seguridad de la información puede aportar al proceso de implementación, especialmente en alineación con las buenas prácticas y al aumentar las capacidades operativas. También se exploraron técnicas para recopilar y analizar información. Estas técnicas tenían como objetivo guiar la selección del problema a abordar en diferentes áreas, así como la forma de análisis sobre ellas.

La recopilación de información para el análisis y la posterior formulación de las actividades a realizar se basaron en una recopilación de información basada en tres técnicas básicas:

Análisis de documentos: Análisis de documentos como procedimientos, instrucciones y presentaciones institucionales.

Entrevista semiestructurada: la aplicabilidad de esta técnica tenía el objetivo principal de obtener información detallada dentro del alcance de los objetivos de control recomendados por la norma ISO / IEC 27001: 2013, identificando el estado de los controles implementados o parcialmente implementados e

identificando qué controles no existen o mejorar en el contexto de la gestión de riesgos de seguridad de la información.
Observación directa: esta técnica permitió completar la información recopilada en las entrevistas y debates de los grupos de trabajo, ya que permitió recopilar información y "ver" aspectos que los entrevistados y los participantes desconocen o de los que no desean hablar o aclarar puntos que puedan han sido menos explorados Esta técnica se ha vuelto de suma importancia debido al refuerzo naturalista de la recopilación de datos, convirtiéndose en un proceso interactivo e incremental.

CONCLUSIONES

Se debe señalar que el desarrollo de este trabajo en un entorno organizacional, proporcionó una experiencia enriquecedora en la participación con varias personas en el tema de la gestión de riesgos y la seguridad de la información, así como el conocimiento adquirido sobre los procesos de seguridad, basado en la infraestructura de los sistemas y tecnologías de información de la empresa TECNO FUEGO S.A.S. Por otro lado, existe un convencimiento de que el intercambio de conocimientos entre los diversos actores que formaron parte de este trabajo resultó en una experiencia enriquecedora para todos.
La realización de este trabajo permitió aprovechar un conjunto de factores beneficiosos para la gobernanza de los sistemas y tecnologías de la información en uso en la organización TECNO FUEGO S.A.S., en los que la capa de riesgo y seguridad de la información, permitió "una mirada diferente" al desarrollar nuevos lineamientos. Los proyectos, aumentaron la sensibilidad y la participación de los empleados involucrados en la gestión de sistemas y redes y, sobre todo, nos permitieron reconocer que la aplicabilidad de las "buenas prácticas" son herramientas facilitadoras en un proceso de mejora continua. La prueba es que, durante el curso de este trabajo, el equipo GSTI / TECNO FUEGO S.A.S., inició ciertas acciones como resultado de su participación en el desarrollo de este proyecto y el reconocimiento de la aplicabilidad de las "buenas prácticas" como un factor diferenciador y facilitador en los procesos de gestión y administración de sistemas de información.

RECOMENDACIONES

El desempeño de este trabajo y el análisis de los resultados obtenidos permitieron obtener beneficios relevantes para la definición del curso que se implementará con el Sistema de Gestión de Seguridad de la Información, pero aun, se tienen algunas limitaciones técnicas ya que no era posible realizar pruebas de penetración a algunas de las aplicaciones, utilizando herramientas especializadas y por lo tanto, ser capaz de definir recomendaciones y medidas más rigurosas que puedan analizar y validar la arquitectura de un sistema informático. Se prevé que las tareas desafiantes que surgirán al implementar el SGSI, en su contexto en la operacionalización de las etapas DO (Implementar y Operar) - COMPROBAR (Monitorear y Revisar) - ACT (Mantener y Optimizar), además de la interacción transversal con las unidades orgánicas en la implementación de las diversas medidas propuestas.

FUENTES BIBLIOGRÁFICAS

Carneiro, A. (2016). Auditoría y Control de Sistemas de Información. FCA- Editora de Informática

Casaca, J. y Correia, M. (2010). ¿Por qué es necesaria la seguridad de la información?

Casaca, J. (2014). Gestión de riesgos en seguridad de la información: conceptos y metodologías.

CERT.PT (2016). Coordinación de respuesta a incidentes. Disponible en: http://www.cncs.gov.pt/cert- pt / / index.html [consultado el 8 de abril de 2020].

CNCS (2015). Centro Nacional de Ciberseguridad. Disponible en: http://www.cncs.gov.pt/pagina- inicial / index.html [accedido el 7 de Mayo de 2020].
ISO / IEC 27000 (2008). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. BSI-Norma Británica. Reino Unido.
ISO/IEC 27002 (2013) - Information Technology - Security Techniques:
ISO/IEC 27003 (2010) - Information Technology - Security Techniques:
ISO/IEC 27005 (2008). Information technology - Security techniques
ISO27K Forum information Security (2015).
Martins, A. y Santos, C. (2005). Una metodología para implementar un sistema de gestión de seguridad de la información.
Melo, M. (2016). Ciclo de conferencias - Protección de datos y ciberseguridad.
Oliveira, R. (2015). Análisis de riesgo asociado con interrupciones del servicio.
Reglamento de la UE 2016/679 (2016). Reglamento general de protección de datos.
Rigon, E. y Westphall, C. (2013). Modelo de evaluación de madurez de seguridad de la información. Revista electrónica de sistemas de información, v.12 (enero-abril 2020), pp. 1-19.
Seixas, S. M. (2013). Modelo para la gestión de eventos de seguridad de la información.
Silva, D. (2011). Beneficios y factores condicionantes de la obtención de la certificación en la gestión de seguridad de sistemas de información.
Silva, P. T., Carvalho, H. y Torres, C. B. (2003). Seguridad de los sistemas de información.
Vian, P. (2016) Desarrollo de un marco situacional para la ciberseguridad en Portugal.
Zúquete, A. (2015). Seguridad de la red informática (3ª ed. Actualizado y aumentado). FCA-Editora de Informática, Lda. Reino Unido.