Plan Estratégico de Seguridad de la Información (PESI) para la Compañía Propanogas S.A E. S. P

Yeferson Agustín Daza Acevedo

Asesor

Manuel Antonio Sierra

Universidad Nacional Abierta y a Distancia – UNAD.

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2026

Agradecimientos

Agradezco a la Universidad Nacional Abierta y a Distancia por permitirme ser parte de su comunidad, mis logros profesionales los he hecho realidad junto con esta magnífica Universidad, agradezco a cada uno de los tutores que me dieron de su tiempo para guiarme y así obtener buenos resultados, para ellos mi más profundo respeto y honor, gente como ustedes necesita el país cada vez más.

Resumen

La Organización Propanogas S.A.S E.S.P afirma que los datos y los recursos de Información son elementos clave para alcanzar sus metas estratégicas, por lo que considera vital la implementación y mantenimiento de un Plan Estratégico de Seguridad de la Información (PESI) que garantice la protección de su información y, de esta manera, logre su misión y visión.

Para el desarrollo de lo anterior se ejecutará inicialmente un análisis de la situación actual (**GAP**), identificación del nivel de madurez en temas de Seguridad Informática, identificando riesgos mediante el levantamiento de Información y posterior presentación de informes. Se ejecutará una fase de Planeación del proyecto derivando en la Implementación del **PESI**, de igual manera, se discutirán los recursos y varios factores como las iniciativas y tareas necesarias para elevar la organización a un estándar adecuado que garantice la protección de la confidencialidad, integridad y disponibilidad de sus datos, principios esenciales que forman la base de la salvaguarda de los activos informáticos.

Palabras clave: Ciberseguridad, Seguridad de la Información, Análisis de Riesgos, Control, Vulnerabilidad, Gobernanza Corporativa.

Abstract

Propanogas S.A.S E.S.P, establishes that the information and information assets are an essential part for the achievement of its strategic objectives, for which it recognizes as fundamental the need to implement and maintain a Strategic Information Security Plan (PESI) that allows to ensure the protection of your information and with this the achievement of its mission and vision.

For the development of the above, an analysis of the current situation (GAP) will be carried out initially, identification of the level of maturity in matters of Computer Security, identifying risks through the collection of Information and subsequent presentation of reports. A planning phase of the project will be carried out, leading to the Implementation of the PESI, as well as the tools and different aspects such as projects and activities that are required to bring the entity to an adequate level for the protection of confidentiality, integrity and availability of information. your information, fundamental principles that constitute the pillar of the protection of information assets.

Keywords: Cybersecurity, Information Security, Risk Analysis, Control, Vulnerability, Corporate Governance.

Tabla de Contenido

Lista de Figuras

Lista de Apéndices

Introducción

Este proyecto se enfoca en la propuesta de Implementación de Plan Estratégico de la Seguridad de la Información (PESI) para la compañía Propanogas S.A.S E.S.P, aclarando que este nombre de razón social es ficticio teniendo en cuenta el acuerdo de confidencialidad celebrado entre las partes, inicialmente se evaluó el nivel de seguridad de la Información, infraestructura de software y hardware y la apropiación de cada unidad organizacional en temas de seguridad de la información y activos de la información.

El proyecto PESI se enfoca en primera instancia en ejecutar un estudio de la situación actual de la organización mediante un análisis GAP – ISO: 27001: 2013 y los controles a auditar con el fin de descubrir el nivel de madurez en cuanto a la seguridad de la información, y así aplicar campañas de Phishing y Ethical Hacking con el fin de evaluar los riesgos y vulnerabilidades presentes en la Infraestructura TI actual.

Como resultado de lo anterior se presentan los análisis de las brechas de seguridad de la información que se encuentran visibles en la organización derivada en la presentación de la propuesta de la implementación del Plan Estratégico de la Seguridad de la Información - PESI.

Con este trabajo de grado se busca aumentar el conocimiento y experticia en temas de la Seguridad de la Información aprovechando las necesidades que actualmente se presentan en la Organización Propanogas S.A.S E.S.P que a su vez se beneficiará grandemente al encaminarse en los ámbitos de la Seguridad de la Información y las mejores prácticas.

Problemática

Planteamiento del Problema

La Organización Internacional de Normalización (ISO, en inglés) definió la norma ISO 27001, esta se utiliza para certificar los sistemas de gestión de seguridad de la información en las empresas. Ofrece un estándar internacional para sistemas de gestión de la seguridad de la información (Esan, 2018).

La compañía tiene la posibilidad de evidenciar ante sus consumidores actuales y potenciales, además de sus proveedores y accionistas, la integridad en el manejo de la seguridad de los datos con la certificación en la utilización de la norma ISO 27001:2013. Además, le permite aumentar la seguridad de la información y reducir los peligros de fraude, pérdida o filtración de datos. Esta norma fue reestructurada para estar en línea con otras normas internacionales, basándose en el estándar BS 7799, que fue reemplazado por esta misma. Se implementaron nuevos controles, con un enfoque en las métricas relacionadas con la gestión de incidentes y la seguridad de la información. (Esan, 2018).

La norma ISO 27001:2013 se fundamenta además en otros estándares, en la serie ISO 13335, en ISO/IEC TR 18044:2004, en las Directrices de la OCDE para sistemas y redes de seguridad de la información y en ISO/IEC 17799:2005. Estos son útiles para poner en práctica sistemas de seguridad de la información. Los resultados de la implementación de la norma ISO 27001, como consecuencia de este alineamiento con otros sistemas de gestión y su funcionamiento en conjunto con regulaciones relacionadas, son los siguientes resultados: (Esan, 2018)

- La armonización con estándares de sistemas de gestión, como son ISO 9001 e ISO 14001

- La atención en la constante optimización de los procesos del sistema de gestión de seguridad de la información.
- La transparencia en los requisitos de documentación y registros.
- Procedimientos de administración y evaluación de los riesgos implicados a través del modelo del proceso Planificar, Hacer, Verificar, Actuar (PDCA por sus siglas en inglés).
- La protección de los activos de la compañía, que incluye desde documentos e información digital hasta elementos físicos (como redes y computadoras) y saberes del personal.
- Un organismo de certificación independiente autorizado expide el certificado, esta certificación demostrará que la institución ha tomado las medidas necesarias para proteger la información de varios peligros.

ISO 27001 (Requisitos para Sistema de Gestión de Seguridad Informática) un total 36,362 empresas certificadas, esto representa un incremento del 56%, 20,514 empresas más a comparación al año 2018, lo que es un Highlight muy importante, esta norma está tomando mucho auge, debido a que las empresas están tomando más conciencia de sus beneficios y es muy importante tener herramientas de protección de la información y sobre todo de los datos, por las regulaciones internacionales como en el caso de Europa con RGPD que es de debido cumplimiento desde mayo 2018. También cabe resaltar que en Panamá ya contamos con la ley 81 de 26 de marzo de 2019 de Protección de Datos Personales (De León, 2020).

Justificación

La Compañía Propanogas S.A.S E.S.P trabaja permanentemente en pro de la protección de la Información y de sus activos de información pero no tiene implementado o definido un Plan Estratégico de la Seguridad de Información, que como herramienta permita de una manera táctica y operativa organizar y planear las actividades , procesos, proyectos e inversiones de la seguridad de la información en apoyo al cumplimiento los objetivos estratégicos de la Organización desde la perspectiva y alcance del Departamento de TI. La Compañía Propanogas S.A.S E.S.P, aunque cuenta con controles de seguridad básicos no se aplica de forma óptima, evidenciando vacíos y brechas de seguridad frente a la estandarización de los procesos y procedimientos en seguridad de la información, en consecuencia, no están asegurando la integración, mantenimiento y mejora continua que requiere en un futuro alcanzar la implementación de un SGSI y posterior certificación ISO2700.

La empresa Propanogas S.A.S E.S.P, mediante la elaboración, diseño e implementación de un plan estratégico para la administración de la seguridad de la información (PESI), apoyado en modelos de mejores prácticas y directrices de seguridad, como la norma internacional ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, además de la alineación del plan estratégico institucional con los objetivos en materia de seguridad de la información, tendrá una clara dirección hacia el negocio. Esto se convertirá en una herramienta muy valiosa que facilitará la identificación, optimización y enfoque de los variados procesos, procedimientos, proyectos y actividades, todo bajo el marco del Modelo de Seguridad y Privacidad de la información (De León, 2020).

La puesta en marcha de un Plan Estratégico de Seguridad de la Información (PESI) como parte de la Gobernanza Corporativa y la Gestión TI de la Organización garantizará la protección,

privacidad, disponibilidad y confidencialidad de la información, mediante una correcta administración del riesgo, el cumplimiento de la normativa vigente y la adopción de prácticas óptimas en seguridad de la información. Se ha decidido, por tanto, comenzar el proceso de implementación del PESI a través de una auditoría inicial basada en el Análisis de Brechas ISO 27001 y un estudio del contexto organizacional, así como la definición del alcance, para que en el futuro se pueda llevar a cabo la implementación del SGSI y obtener la Certificación ISO 27001. Propanogas S.A.S E.S.P, sus colaboradores y clientes finales se verán grandemente beneficiados con la implementación del PESI por cuanto todos los procesos y procedimientos en temas de Seguridad de la Información estarán alineados a las Estrategias Organizacionales, Misionales y de Visión al ser una compañía líder que provee soluciones de energía a clientes de manera sostenible y que se encuentra enfilada a los estándares y normativa vigente en temas del Sistema de Gestión de la Seguridad de la Información (De León, 2020).

Delimitación del Problema

¿Cómo puede ser desarrollado un Plan Estratégico de la Seguridad de la Información (PESI) basado en la norma ISO 27001, que facilite el aseguramiento de la Información de la compañía Propanogas S.A.S E.S.P?

Objetivos

Objetivo General

Desarrollar un plan estratégico de la seguridad de la información (PESI), con base en la norma ISO 27001, para la compañía Propanogas S.A.S E.S.P, en Cota Cundinamarca.

Objetivos Específicos

Realizar el marco conceptual y teórico del Plan Estratégico de Seguridad de la Información (PESI), metodología, procesos, políticas, normatividad.

Diagnosticar el estado de seguridad de la información de la organización Propanogas S.A.S E.S.P

Diseñar un plan estratégico de seguridad de la información que responda las necesidades de gobierno corporativo y gobernanza de TI.

Implementar un plan estratégico de seguridad de la información (PESI) mediante la norma ISO 27001 en la organización Propanogas S.A.S E.S.P

Marco Teórico

Seguridad de la Información

La protección de la información se refiere a todas las acciones preventivas y de respuesta que toman las personas, las instituciones y las herramientas tecnológicas para salvaguardar los datos, con el objetivo de preservar su confidencialidad, autenticidad e integridad (Universidad Libre, 2015).

Es importante entender que los conceptos de Seguridad de la información y Seguridad Informática no son equivalentes. La segunda se enfoca únicamente en la protección dentro del entorno digital, mientras que la primera abarca cualquier forma de información, ya sea en formato digital o en papel (Universidad Libre, 2015).

La protección de la información incluye varios aspectos, pero todos se centran en la información misma. Por ejemplo, la accesibilidad, la transmisión de datos, la detección de inconvenientes, la evaluación de riesgos, la solidez, la privacidad y la recuperación ante situaciones adversas (Universidad Libre, 2015).

Principios Básicos

Los gobiernos, las fuerzas armadas, las instituciones bancarias, los centros de salud y las compañías privadas poseen un volumen considerable de datos sensibles acerca de su personal, consumidores, mercancías, proyectos de investigación y su estado económico. La mayor parte de estos datos son reunidos, procesados, guardados y accesibles para quienes los utilizan, en computadoras y comunicados a través de redes entre computadoras (Universidad Libre, 2015).

En el caso de que datos sensibles de una empresa, sus consumidores, sus elecciones, su situación financiera o su nueva gama de productos sean obtenidos por un competidor o se hagan públicos sin autorización, esto podría resultar en la pérdida de confianza de los clientes,

disminución en las ventas, litigios legales o incluso la insolvencia de la empresa. Por lo tanto, salvaguardar la información confidencial es fundamental para el negocio y, en muchas ocasiones, también es una necesidad ética y una responsabilidad legal. Para la persona promedio, la Seguridad de la Información tiene un impacto notable en su privacidad, la cual puede variar dependiendo de la cultura del individuo (Universidad Libre, 2015).

Diseño e Implementación de una Estrategia de Seguridad de la Información

El propósito de una Estrategia de Seguridad de la Información es establecer un rumbo que permita a una entidad alcanzar el nivel de desarrollo o competencia anhelado en seguridad de la información. Esta Estrategia tiene que ser creada por la organización y determinada por las características del negocio y de la seguridad de la información. Tal como se explicará en el proceso a seguir para formular e implementar la Estrategia de Seguridad de la Información, la alta dirección y el responsable del proceso deben, de manera consensuada, decidir hasta qué grado de madurez o capacidad quieren llevar el proceso. La Estrategia establece la base para un plan de acción que incluya uno o más programas de seguridad que, en la medida que se vayan ejecutando, logren los objetivos de seguridad de la información y permitan llevar el proceso de seguridad de la información, del nivel en que se encuentra, al nivel de madurez o capacidad esperado. Cada plan de acción debe formularse según los recursos disponibles y las limitaciones existentes, incluyendo la consideración de requerimientos legales y regulatorios. Tanto la Estrategia, como los planes de acción, deben contener mecanismos de monitoreo y métricas definidas para determinar el nivel de éxito (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], s. f.).

Gobierno Corporativo

El gobierno corporativo, que se refiere al conjunto de normas que regulan la interacción entre los directivos y los inversores de la empresa, es crucial para que las organizaciones cuenten con una estructura bien definida, responsabilidades claras y métodos eficientes para identificar, gestionar, controlar y comunicar los riesgos (CAF, 2017).

De la misma forma, un esquema de gobierno corporativo ayuda a la organización a dirigir sus lineamientos estratégicos, aumentar la confianza de inversionistas, prestamistas y usuarios y, por consiguiente, potenciar la eficiencia económica y la sostenibilidad, garantizando la generación de valor a largo plazo (CAF, 2017).

Una manera alternativa de entender el concepto de gobierno corporativo es verlo como una caja de herramientas, que proporciona a cualquier tipo de entidad (ya sea privada, estatal con capital cerrado, que cotiza en bolsa o familiar) recursos específicos que contribuyan a optimizar la administración y la claridad mediante una definida división de funciones entre la Alta Gerencia, la Junta Directiva y la Asamblea General de Accionistas (CAF, 2017).

A medida que las compañías avanzan desde su inicio, deben diversificar las herramientas de gobernanza corporativa, así como mejorar las que ya tienen en su arsenal. Un claro ejemplo es la Junta Directiva, que es un componente esencial de la gobernanza, con amplias responsabilidades en términos de dirección estratégica, supervisión y control de la gestión que se asigna a la alta dirección. En una empresa unipersonal, debido a su tamaño, las responsabilidades operativas recaen en una sola persona, que también es el dueño, lo que dificulta la idea de contar con esta herramienta. Sin embargo, a medida que la empresa se desarrolla y se expande, es posible que, aunque el control sobre la gestión y la propiedad siga en manos de una sola persona,

su tamaño exija la delegación de tareas administrativas a personas ajenas que no necesariamente poseen acciones en la compañía (CAF, 2017).

En esa etapa, considerando la dificultad, la compañía debería tener una Junta Directiva, que actúe como un grupo colegiado, para permitir que el dueño distinga sus responsabilidades como gerente general de las que le corresponden como propietario. Esto facilitaría la revisión de la estrategia a largo plazo y la administración de los riesgos de la empresa.

En este contexto, la Junta Directiva debe tener bien establecidas sus responsabilidades, su tamaño y las características de quienes la integran, adaptándose a las demandas de gestión de la organización. Con el avance y expansión de la empresa, se precisará no solo de un mayor número de integrantes con un perfil profesional diversificado, incluyendo a personas externas e independientes que cuenten con conocimientos en áreas innovadoras, sino que también se requerirán comités de asistencia (los más relevantes son los relacionados con Auditoría/Riesgos, Gobierno Corporativo y Nombramientos/Retribuciones) (CAF, 2017).

Igual que sucede con la Junta Directiva, mecanismos como el Derecho a un Trato Justo para los Accionistas, la Asamblea General de Accionistas, la Estructura de Control y la Transparencia de Información Financiera y No Financiera tienen que adaptarse a la antigüedad de la organización (CAF, 2017).

A medida que se implementen correctamente esos mecanismos de gestión, la entidad estará más preparada para enfrentar nuevos desafíos y continuar su expansión. Es aquí donde se destaca la relevancia de la gobernanza corporativa, una noción que no debe interpretarse como un objetivo final, sino como un instrumento, no el único, que ayuda a la consolidación y permanencia de la empresa (CAF, 2017).

Es por ello que, al ser conscientes de la importancia de fomentar una competitividad responsable, tanto en términos generales como en el ámbito de las empresas, la CAF ha estado apoyando durante más de diez años las buenas prácticas de gobernanza corporativa en la región. Esto incluye la generación de aportes teóricos, la provisión de herramientas y el respaldo en las implementaciones reales para promover y crear conciencia sobre la relevancia del tema, junto con experiencias concretas en su uso práctico (CAF, 2017).

Por esta razón, se han incentivado y reforzado acciones para perfeccionar los marcos normativos, que se han convertido en un modelo para América Latina, colaborando con organismos reguladores, bolsas de valores, asociaciones empresariales, instituciones de gobernanza corporativa, universidades y diversos tipos de empresas (pequeñas y medianas empresas, empresas familiares, compañías cerradas, listadas en bolsa, empresas estatales) (CAF, 2017).

En este aspecto, el Programa de Gobierno Corporativo de CAF ha adquirido una considerable trayectoria, fundamentada en tres bases: (CAF, 2017).

- Creación de Conocimiento: Propuestas conceptuales y recursos, tales como la elaboración y difusión de investigaciones, normativas, directrices, manuales y guías sobre Gobernanza Corporativa para las organizaciones, todas disponibles de manera gratuita en nuestro archivo de publicaciones.
- Compartición de experiencias y capacitación: mediante conferencias y talleres de formación, así como redes regionales que fomenten el intercambio de vivencias.
- Implementaciones exitosas: Realización de proyectos piloto que aplican buenas prácticas en diversas clases de empresas, algunas de las cuales, tras mejorar su estructura de gobernanza, han comenzado a buscar y acceder a nuevas fuentes de financiamiento, alternativas

al sistema bancario, como la entrada a la bolsa de valores, la emisión de obligaciones de deuda o la participación en fondos de inversión.

Gobernanza TI

A través de sus aplicaciones, procesos y sistemas, la tecnología se muestra indispensable en la gestión empresarial. El rol que toma la TI en las empresas se le conoce como la gobernanza de TI, un conjunto de metodologías compuesto de procesos que garantizan una utilización efectiva de la tecnología de la información para asegurar el cumplimiento de objetivos de la organización (Danilo, 2018).

Por medio de la gobernanza de TI, se asegura la identificación y evaluación exitosa de componentes importantes de TI y se supervisa la implementación y extracción de los beneficios de negocio. Como conjunto de procesos, la gobernanza de TI es una inversión, vigilancia y proceso de toma de decisiones empresarial que se desempeña como una responsabilidad de gestión organizacional (Danilo, 2018).

Como parte importante, es un proceso en el que se basan las decisiones sobre inversiones de tecnología. Esto cubre cómo se toman las decisiones, quién toma las decisiones, quién es responsable y cómo se miden y monitorean los resultados (Danilo, 2018).

La mayoría de las empresas tienen algún tipo de gobernanza de TI, aunque usualmente el proceso es informal, lo que vuelve inconsistente a toda la empresa. Si hay un análisis final usualmente no es robusto y no existen mecanismos formales para medir y monitorear los resultados de las decisiones (Danilo, 2018).

Dejar la gobernanza de TI en el azar o en procesos heredados deja a una empresa vulnerable a los riesgos. Las empresas deben priorizar la optimización de las inversiones en TI, especialmente después de una tendencia creciente reciente de grandes organizaciones que llevan

el rendimiento de TI al nivel de la junta directiva. Además del comité de auditoría convencional y el comité de compensación, los consejos ahora forman comités de supervisión de TI para involucrarse más con el rol de TI en la facilitación y ejecución de la estrategia de la empresa (Danilo, 2018).

Este compromiso de la administración demuestra que la gobernanza de TI no puede existir por sí mismo, sino que debe ser un subconjunto del gobierno corporativo. Es responsabilidad de la junta directiva y la gerencia ejecutiva, no solo de la administración de TI (Danilo, 2018).

El IT Governance Institute describe la gobernanza de TI como una parte fundamental del gobierno corporativo e incluye el liderazgo y las estructuras y procesos organizacionales que aseguran que la tecnología informática de la organización sostenga y cubra las estrategias y objetivos de la organización (Danilo, 2018).

El gobierno de TI es en muchos casos una vía rápida para mejorar los controles y procedimientos de información financiera. Esto se debe a que crea informes financieros más transparentes y repetibles, hace que la transición de las capacidades de generación de informes por lotes a en tiempo real sea más rápida, salvaguarda los datos financieros con protección de datos y mayor seguridad y aborda los aspectos de cumplimiento de desastres relacionados con la recuperación (Danilo, 2018).

La gobernanza de TI se enfoca en cuatro áreas: Alineación estratégica, entrega de valor, gestión de recursos, gestión de riesgos y medidas de rendimiento (Danilo, 2018).

Modelo de Seguridad y Privacidad de la Información

El modelo de seguridad y privacidad de la información incluye un ciclo operativo que tiene cinco (5) etapas, las cuales hacen posible que las organizaciones administren correctamente la seguridad y privacidad de sus activos informativos. Este Modelo de Privacidad y Seguridad de la Información incluye seis niveles de madurez, los cuales están relacionados con el progreso en la puesta en práctica del modelo operativo. Al contribuir con el uso estratégico de las tecnologías de la información en la elaboración e implementación del modelo de seguridad orientado a mantener la confidencialidad, integridad y disponibilidad de los datos, la protección y privacidad de la información, que es un elemento transversal a la Estrategia de Gobierno en línea, hace posible alinearse con el componente TIC para gestionar.

La privacidad y la seguridad de la información se ajustan al componente TIC para servicios, respaldando el manejo de los datos empleados en los trámites y servicios brindados por la entidad. Se rige siempre bajo las regulaciones sobre resguardo de datos personales, además de otros derechos que la ley establece, excluyendo el acceso público a ciertos datos. (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], s. f.).

Activos de Información

La administración de activos informativos es una labor de las gerencias dedicadas a la gestión o a la seguridad de la información, y consiste en crear, instaurar y ejecutar un procedimiento que posibilite identificar, clasificar, valorar y tratar los activos informativos más relevantes dentro de una compañía. (Eduba, n.d).

Según Eduba (n.d.), en el marco de la norma ISO/IEC 27001, un activo de información es "algo que una organización aprecia y, por ende, tiene que proteger". A continuación, se presenta un activo informático:

- Los datos generados o empleados por un procedimiento de la organización en medios digitales, impresos u otros.
- El hardware y el software que se emplean para almacenar, transportar o procesar información.
- Los servicios que se emplean para controlar, transmitir y recibir información.
- Los recursos o instrumentos que se utilizan para el desarrollo y la asistencia de los sistemas de información.
- Personas que gestionen información, o un conocimiento particular de gran relevancia para la empresa (como, por ejemplo: secretos industriales, gestión de datos críticos).

Gap Analysis

Este análisis recibe su nombre de la palabra inglesa gap (es decir, hueco o brecha), que ya indica en qué consiste: el análisis gap es una herramienta de marketing estratégico tradicional que se utiliza para mostrar las discrepancias entre los objetivos de planificación deseados y los posibles resultados reales, basándose en el día a día de la empresa. De esta manera, se identifican desde el principio las deficiencias de la planificación estratégica, lo que ayuda a la empresa a poner remedio a los problemas inminentes, revisando la estrategia o cambiando los procedimientos (IONOS, 2023).

Hay que tener en cuenta que el gap analysis no tiene ningún efecto a menos que se evalúen sus resultados y se tomen las medidas correspondientes. Este análisis, simplemente, describe la situación actual y muestra si los objetivos empresariales que se pretenden alcanzar son realistas. Por lo tanto, solo promoverá cambios positivos si se aplican otras herramientas de marketing estratégico sobre la base de los datos obtenidos (IONOS, 2023).

Estrategias Organizacionales de Seguridad Informática

La revolución digital ha transformado las operaciones y modelos empresariales en muchas maneras positivas, y está ofreciendo beneficios que van desde un servicio de atención al cliente mejorado para una mayor productividad hasta nuevas fuentes de ingresos. Pero la transformación del negocio digital también ha presentado nuevas oportunidades para hackers, cibercriminales, y otras malas personas. Nunca las aplicaciones y datos han sido más críticos para las operaciones del negocio, o han estado más en riesgo ante el hurto, la exposición, y la corrupción. A pesar de que las organizaciones gastan colectivamente miles de millones de dólares para contrarrestar las amenazas cibernéticas, la diversidad, volumen y sofisticación de esas amenazas continúa expandiéndose. Los modelos cambiantes de la informática y las redes lo complican aún más. En el pasado, las corporaciones rutinariamente mantenían sus sistemas y datos más confidenciales asegurados en sus centros de datos centrales y los portátiles administrados por la empresa. Sin embargo, hoy en día, los datos y aplicaciones suelen residir en dispositivos móviles dentro de soluciones establecidas en el departamento, o en servidores basados en la nube.

Todas estas plataformas y ubicaciones, además de las redes que las interconectan, requieren fuertes controles de seguridad que deben proporcionar un perímetro de seguridad definido por software que lo abarque todo. Las herramientas y métodos tradicionales para asegurar las aplicaciones y los datos han demostrado ser insuficientes para abordar adecuadamente las complejidades inherentes a los diversos negocios actuales y el panorama de amenazas. Las organizaciones, en particular las de sectores altamente regulados, necesitan administrar y mitigar los riesgos cibernéticos de forma que protejan los datos en reposo, en uso y

en tránsito. Además, deben cumplir estos objetivos incluso su comunidad de *usuarios (*Citrix, n.d).

Al hablar de usuarios de incluye a los empleados móviles, remotos; consultores de terceros; externalización; y otros socios comerciales. “Las empresas necesitan tomar medidas más inteligentes para proteger su información confidencial, especialmente mientras que las amenazas vayan en aumento y más empleados estén pasando por alto las prácticas y políticas de seguridad porque son demasiado complejas”, dice Stan Black, jefe de seguridad de Citrix. “La demanda de dispositivos y acceso en cualquier momento y lugar a menudo sobrepasan las precauciones por la seguridad estos días. Nadie puede darse el lujo de asumir que un dispositivo o red es inherentemente seguro” (Citrix, n.d).

Sistema de Gestión de la Seguridad Informática

La información es un capital muy importante, además de ser una parte esencial del rendimiento y la rentabilidad de las empresas. Por lo tanto, se hace indispensable desarrollar sistemas capaces de administrar y protegerla. Un Sistema de Gestión de Seguridad Informática (SGSI) asegura que estos datos sean confidenciales, integrados y accesibles. (Esan, 2018).

El establecimiento y desarrollo de un SGSI se fundamenta en reconocer los datos relevantes, sus dueños y el sitio donde están, además de conocer las amenazas a las que podrían estar expuestos. Es inviable en la actualidad desarrollar un sistema perfecto a causa de los continuos avances de la tecnología, así que tener conocimiento de los riesgos, aceptarlos y saber manejarlos contribuye a su minimización y a que su aparición sea menor. (Esan, 2018).

Conocer las normas que comprenden los SGSI, es decir, las ISO 27001, es una manera de asegurar la información. Desde el director hasta los operarios que utilizarán el sistema, las compañías deben estar informadas sobre estas normativas y capacitar a su personal en ellas. Para

detectar cualquier grieta en el sistema, también es fundamental tener asesores que estén siempre al día. (Esan, 2018).

Según el experto, la mayoría de las organizaciones emplean una LAN (red de área local) para almacenar información. Estas emplean un firewall para salvaguardar la información contra la intrusión de individuos ajenos en Internet. Sin embargo, el cortafuegos no es capaz de salvaguardar la información de todas las amenazas posibles, especialmente de los hackers expertos o de los comportamientos descuidados de los usuarios. (Esan, 2018).

Instalar programas antivirus en cada uno de los dispositivos utilizados es otra herramienta crucial para proteger la información. Así mismo, hay otros programas informáticos especializados que deben operar en armonía con las herramientas previamente citadas y que bloquean o notifican la intrusión de componentes externos (Esan, 2018).

Mediante la manipulación engañosa, los hackers pueden obtener datos valiosos que resulten perjudiciales para una compañía (Esan, 2018).

Los Sistemas de Gestión de la Seguridad de la Información tienen que incluir un apartado para instruir a los usuarios y prevenir que sean víctimas de ingeniería social, dada esta circunstancia. Además, deben disponer de todas las herramientas a su alcance para identificar y eliminar las amenazas externas, además de un manual de acciones frente a los riesgos. (Esan, 2018).

Para cualquier profesional de la administración y la gestión, es esencial tener una perspectiva completa de la aplicación de sistemas de gestión de seguridad informática y su relevancia. La implementación de un SGSI le permitirá a tu entidad gestionar la seguridad de activos como información financiera, propiedad intelectual, datos de los trabajadores o información que se le haya confiado por parte de terceros. (Esan, 2018).

Políticas de Seguridad Informática

Las políticas de seguridad informática son un conjunto de pautas y normativas que hacen posible asegurar la confidencialidad, integridad y disponibilidad de los datos, al tiempo que reducen los riesgos que estos sufren. ¿Te gustaría conocer más acerca de las políticas de seguridad informática? En UNIR estudiamos sus atributos y su relevancia en el área de la ciberseguridad. (Unir, 2020a).

Se define una política de seguridad a gran escala, es decir, qué se tiene que proteger y cómo, o, en otras palabras, el grupo de controles que se deben poner en práctica. Esta se lleva a cabo a través de una serie de procedimientos e instrucciones técnicas que implementan las pautas técnicas y organizativas determinadas para hacer cumplir la política mencionada (Unir, 2020a).

Para establecer una política de seguridad, se debe hacer primero una identificación y evaluación de los peligros a los que la información está sujeta. La política debe abarcar todos los procedimientos, sistemas y empleados de la organización. Asimismo, debe contar con la aprobación de la dirección de la organización y debe comunicarse a todos los empleados (Unir, 2020a).

Information Technology Infrastructure Library - ITIL

ITIL, del inglés Information Technology Infrastructure Library, se refiere a una biblioteca de infraestructura de tecnologías de la información. Este concepto es utilizado para definir una metodología de gestión a través de la cual se plantean ciertas prácticas estandarizadas cuyo objetivo es optimizar la prestación de un servicio. Es decir, la idea de este programa es reorganizar los procesos de la empresa para mejorar los resultados (emagister, 2021).

Los estándares que se presentan en este programa permiten que la empresa pueda tomar el control absoluto de la gestión de sus recursos a través de la reestructuración de sus procesos. Todo ello facilitará la identificación de fallas y carencias en los procesos, de manera que se puedan aplicar acciones para contrarrestar estas deficiencias (emagister, 2021).

Funcionamiento de Itil

Antes que nada, es importante tener en cuenta que este programa abarca una serie de conceptos y herramientas que facilitan la gestión de la prestación de servicios, especialmente aquellos relacionados con las tecnologías de la información y la comunicación – TICs (emagister, 2021).

El ITIL no es un plan totalmente estricto; es un programa que se adapta a las necesidades de la compañía, por lo tanto, puede implementarse de acuerdo con los lineamientos y objetivos de ella (emagister, 2021).

Fases de ITIL

- Estrategia: Se enfoca en el mejoramiento de la gestión a través de la implementación de estrategias empresariales alineadas con el propósito de la organización.
- Diseño: Se trata de la creación de métodos para transformar los procesos referentes a la prestación del servicio.
- Transición: Es el tiempo en que se aplican los cambios para transformar los procesos.
- Operación: Se refiere a la aplicación de ciertas prácticas que permiten el mejoramiento de los procedimientos rutinarios. Mejora continua. Aquí, la idea es aplicar estrategias para ofrecer valor agregado a los servicios e innovar en cada proceso (emagister, 2021).

Seguridad en Redes Informáticas

Conceptos Básicos de Seguridad en Red

Las definiciones son buenas como declaraciones de intenciones de alto nivel. ¿Cómo planeas implementar esa visión? Stephen Northcutt escribió una introducción a los conceptos básicos de la seguridad de la red durante más de una década atrás CSO online, nosotros nos fijamos en tres fases de la seguridad de la red que deberían ser el marco de referencia base para su estrategia (Computerword, n.d).

- Protección: debe configurar sus redes y redes lo más correctamente posible.
- Detección: debe ser capaz de identificar cuándo ha cambiado la configuración o si algún tráfico de red indica un problema.
- Reacción: después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro.

Esto, en resumen, es una estrategia de defensa en profundidad. Si hay un tema común entre los expertos en seguridad, es cualquier herramienta defensiva individual puede ser derrotada por un adversario determinado. Su red no es una línea o un punto: es un territorio, e incluso si ha organizado su defensa correctamente (Computerword, n.d).

Método de Seguridad de Red

Para implementar este tipo de defensa en profundidad, hay una variedad de técnicas especializadas y tipos de seguridad de red (Computerword, n.d).

- Control de acceso: debe poder bloquear a usuarios y dispositivos no autorizados de su red. Los usuarios que tienen acceso autorizado a Internet solo han sido autorizados para utilizar el sitio web.

- Antimalware: virus, gusanos y troyanos por definición de una red, y puede permanecer inactivo en las máquinas infectadas durante días o semanas. Su esfuerzo de seguridad debe hacerse para prevenir infecciones y también para el malware raíz que se dirige a su red.
- Seguridad de la aplicación: su red suele acceder a las aplicaciones no seguras, debe usar hardware, software y procesos de seguridad para bloquear esas aplicaciones.
- Análisis de comportamiento: debe saber cómo es el comportamiento normal de la red para poder detectar anomalías o infracciones a medida que ocurren.
- Prevención de pérdida de datos: los seres humanos son inevitablemente el enlace de seguridad más débil. Debe implementar tecnologías y procesos para garantizar que los empleados no envíen deliberada o inadvertidamente datos confidenciales fuera de la red.
- Seguridad del correo electrónico: el phishing es una de las formas más comunes de obtener acceso a una red. Las herramientas de seguridad de correo electrónico pueden bloquear tanto los mensajes entrantes como los salientes con datos confidenciales.
- Firewalls: quizás el abuelo del mundo de la seguridad de la red, siguen las reglas de su red o de Internet, estableciendo una barrera entre su zona de confianza y el salvaje oeste. No excluyen la necesidad de una estrategia de defensa en profundidad, pero siguen siendo imprescindibles.
- Detección y prevención de intrusos: estos sistemas escanean el tráfico de red para identificar y bloquear ataques.

Phishing

El phishing es una forma popular de ciberdelincuencia debido a su eficacia. Los ciberdelincuentes han tenido éxito al usar correos electrónicos, mensajes de texto o mensajes

directos en las redes sociales o en videojuegos para que las personas respondan con su información personal. La mejor defensa es el conocimiento y saber qué buscar (Microsoft, n.d).

Algunas formas de reconocer un correo electrónico de phishing: (Microsoft, n.d).

- Llamada urgente a la acción o amenazas: Desconfíe de los correos electrónicos que dicen que debe abrir un archivo adjunto, hacer clic o llamar de inmediato. Con frecuencia, dicen que tienes que actuar ahora para evitar una sanción o recibir una recompensa. Un método frecuente de las estafas y los ataques de phishing consiste en generar una sensación artificial de urgencia. Lo hacen para que no lo medite demasiado o consulte con un asesor de confianza que podría advertirle.
- Remitentes de primera vez o poco frecuentes: Recibir un correo electrónico de alguien por primera vez no es raro, en particular si la persona está fuera de su organización; sin embargo, esto puede ser una señal de suplantación de identidad (phishing). Si recibe un correo electrónico de alguien a quien no reconoce o que Outlook señala como un remitente nuevo, revise el mensaje con atención antes de proceder.
- Ortografía y mala gramática: Las empresas y organizaciones profesionales suelen contar con un equipo editorial para asegurar que los clientes reciban contenido de alta calidad. Es probable que un correo electrónico sea una estafa si contiene fallos gramaticales o de ortografía evidentes. En ocasiones, estos errores son fruto de una traducción errónea procedente de otro idioma. En ocasiones, se hace de manera deliberada para eludir filtros que buscan impedir estos ataques.
- Saludos genéricos: Una entidad que colabora con usted tiene que saber su nombre y, en la actualidad, es sencillo personalizar un correo electrónico. Si el correo electrónico

comienza con un mensaje genérico, tal como "Estimado señor o señora", eso podría indicar que no es su banco o lugar de compras auténtico.

- Dominios de correo electrónico no coincidentes: Si el correo electrónico afirma ser de una compañía confiable, como Microsoft o su banco, pero se envía desde un dominio de correo electrónico distinto, por ejemplo Gmail.com o microsoftsupport.ru, es muy probable que se trate de un fraude. Además, mantenga la atención en los errores ortográficos muy sutiles del nombre de dominio legítimo. Son trucos habituales de los defraudadores, como en micros0ft.com, donde la segunda letra "o" se ha sustituido por un cero; o rnicrosoft.com, donde una "m" ha sido sustituida por una "r" y una "n".

Ethical Hacking

Ethical Hacking es una práctica autorizada para eludir la seguridad del sistema e identificar posibles violaciones de datos y amenazas en una red (Ingenio learning, 2021).

La empresa propietaria del sistema o la red permite que los ingenieros de seguridad cibernética realicen tales actividades para probar las defensas del sistema. Por lo tanto, a diferencia de la piratería maliciosa, este proceso está planificado, aprobado y, lo que es más importante, legalizado (Ingenio learning, 2021).

Los ingenieros o especialistas informáticos éticos son contratados por organizaciones para investigar las vulnerabilidades de sus sistemas y redes, y desarrollar soluciones para prevenir violaciones de datos (Ingenio learning, 2021).

Lo más importante para los hackers éticos es verificar vulnerabilidades clave que incluyen las siguientes: (Ingenio learning, 2021)

- Ataques de inyección
- Cambios en la configuración de seguridad

- Exposición de datos sensibles
- Violación de los protocolos de autenticación
- Componentes usados en el sistema o red que pueden usarse como puntos de acceso, entre otros.

Análisis de Riesgos Informáticos

Según Tipton Harold y Krause Micki (2006), la seguridad informática se puede definir, en esencia, como la salvaguarda de la integridad, la confidencialidad y la disponibilidad de los sistemas de información. Existen diversas amenazas que pueden poner en peligro los objetivos previamente mencionados, dependiendo del ambiente de la organización. Cuando se presenta un riesgo específico, la organización dispone de tres opciones: asumir el riesgo, tomar acciones para reducir la probabilidad de que ocurra o transferirlo, como podría ser a través de un contrato de seguro. Las medidas o salvaguardas que se implementan para reducir un riesgo son conocidas como controles de seguridad. (Tipton Harold & Krause Micki, 2006).

Normalmente, los controles de seguridad informática se dividen en tres tipos: controles técnicos o lógicos, controles físicos y controles administrativos. (Tipton Harold & Krause Micki, 2006).

Para que los controles sean eficaces, necesitan estar incorporados en lo que se conoce como arquitectura de seguridad informática. Esta debe ser coherente con las metas de la organización y las prioridades de las potenciales amenazas según el efecto que estas tengan en la misma. En consecuencia, la etapa de análisis de riesgos es esencial en el diseño de la arquitectura de seguridad informática. (Peltier Thomas, 2005).

El análisis de riesgos incluye las siguientes etapas, sin importar el procedimiento que se realice:

- Determinar los activos informáticos que se van a examinar.
- Reconocer las amenazas que tienen el potencial de poner en riesgo la seguridad de los activos.
- Establecer la probabilidad de que las amenazas se materialicen.
- Evaluar el impacto de la amenaza con el fin de determinar su orden de prioridad.
- Proponer controles que reduzcan la probabilidad de los riesgos.
- Registrar el procedimiento.

Ciberseguridad

La ciberseguridad consiste en proteger los servidores, las computadoras, las redes, los sistemas electrónicos, los dispositivos móviles y la información de los ataques malintencionados. También se le denomina seguridad de la información electrónica o seguridad de la tecnología de la información. El término se utiliza en una variedad de contextos, desde la informática móvil hasta los negocios, y puede ser segmentado en varias categorías comunes. (Kaspersky, n.d.-b).

- La seguridad de red consiste en proteger una red informática contra los intrusos, que pueden ser atacantes específicos o malware oportunista.
- La seguridad de las aplicaciones tiene como objetivo preservar el software y los dispositivos alejados de cualquier riesgo. Una aplicación que se ve afectada podría permitir el acceso a los datos que debería proteger. La seguridad efectiva empieza en la fase de diseño, mucho antes de que un programa o dispositivo sea puesto en funcionamiento.
- La seguridad de la información salvaguarda la privacidad y la integridad de los datos, tanto durante su almacenamiento como cuando están en tránsito.
- La seguridad operacional abarca los procedimientos y las decisiones que se toman para gestionar y salvaguardar los recursos de datos. Esta categoría incluye tanto los permisos que

poseen los usuarios para ingresar a una red como las prácticas que establecen la manera y el lugar donde es posible almacenar o compartir información.

- La manera en la que una entidad responde a un suceso de ciberseguridad o cualquier otro acontecimiento que provoque la interrupción de sus operaciones o la pérdida de datos está determinada por la continuidad del negocio y la recuperación ante desastres. Las políticas de recuperación ante desastres establecen cómo la organización restablece su información y sus operaciones para volver a estar en la misma capacidad operativa que antes del acontecimiento. El plan al que la organización acude es el de continuidad del negocio.
- La capacitación del usuario final trata el elemento de ciberseguridad más incierto: los seres humanos. Cualquier persona puede introducir un virus en un sistema que normalmente sería seguro si se violan las buenas prácticas de seguridad. Para la seguridad de cualquier organización, es esencial instruir a los usuarios para que eliminen archivos adjuntos de emails sospechosos, no conecten unidades USB no identificadas y otras enseñanzas relevantes (Kaspersky, s.f.-b).

Gestión del Riesgo Informático

Un Sistema de Gestión de Seguridad de la Información, que se basa en la norma ISO 27001, se basa principalmente en identificar y analizar las amenazas más significativas para la seguridad de la información. Desde allí, es posible planear y evaluar esos riesgos (IsoTools, 2019).

Puede definirse una amenaza como cualquier acontecimiento que tiene el potencial de impactar los activos de información, y está vinculada, sobre todo, con recursos humanos, sucesos naturales o errores técnicos. Algunos ejemplos pueden incluir: una inundación, un incendio, ataques de malware o ciberataques externos, y cortes del suministro eléctrico (IsoTools, 2019).

Sin embargo, a veces una simple pulsera imantada o un descuido de los empleados de la empresa pueden causar daños graves en la información, incluso irreparables. En resumen, se trata de desarrollar una gestión de riesgos apropiada que posibilite a las entidades identificar cuáles son las vulnerabilidades más importantes de sus activos de información (IsoTools, 2019).

Un proceso de identificación de riesgos adecuado incluye: (IsoTools, 2019).

- Reconocer todos los activos de información que poseen algún valor para la institución.
- Vincular las amenazas significativas con los activos que se han identificado.
- Identificar las vulnerabilidades que podrían ser explotadas por estas peligros.
- Reconocer las consecuencias que podría acarrear una pérdida de la confidencialidad, integridad y disponibilidad para todos los activos.

Firewall

Los firewalls de hardware vienen incluidos en algunos enrutadores y requieren poca o ninguna configuración, ya que están incorporados en su hardware. Estos firewalls monitorean el tráfico de todas las computadoras y dispositivos que están conectados a la red de dicho enrutador, lo que significa que usted puede filtrar el acceso a todos ellos solo con una pieza de equipo (McAfee, n.d).

Los firewalls de hardware brindan seguridad esencial para el Internet de las cosas (IoT), como termostatos y bombillas inteligentes. A menudo, estos nuevos dispositivos vienen con funciones de seguridad débiles, que pueden dejar su red vulnerable, pero un firewall de hardware ayuda a prevenir esta deficiencia de seguridad (McAfee, n.d).

Para configurar su firewall de hardware, use el firewall de hardware integrado en el enrutador o en el portal de su hogar. Consulte el manual que vino con su enrutador o realice una búsqueda rápida en línea para encontrar los pasos que lo guiarán a través de la configuración (McAfee, n.d).

Sin embargo, los firewalls de hardware solo lo protegen en casa, por lo que, si lleva su computadora a un café o usa su dispositivo mientras viaja, deberá buscar un firewall de software para mantener su dispositivo protegido (McAfee, n.d).

Criptografía

Conocida como la base matemática que soporta la seguridad informática, la criptografía es una ciencia que estudia la información, cómo preservarla y protegerla. El profesor Daniel Cabarcas, de la Escuela de Matemáticas de la Universidad Nacional de Colombia (UNAL) Sede Medellín, explica cuál es su aplicación y su importancia (Universidad Nacional de Colombia, 2020).

“Su objetivo es definir algoritmos y protocolos que permitan proteger la información. La seguridad de la información va más allá de la transmisión privada de datos; incluye que esta tenga integridad, que nadie pueda cambiar su contenido, su autenticidad y su disponibilidad cuando se necesite”, destaca el doctor en Ciencias Matemáticas (Universidad Nacional de Colombia, 2020).

A partir de la criptografía es posible identificar amenazas en la seguridad de la información tanto en protocolos y programación de esta como en errores humanos, como olvidar los cambios de contraseñas o compartir información indebida (Universidad Nacional de Colombia, 2020).

“La seguridad de la información se busca mediante un proceso continuo que incluye

perfeccionar bases, mejorar los protocolos y tener buenas prácticas todo el tiempo" (Universidad Nacional de Colombia, 2020).

Denegación de Servicio

Este tipo de ataques tienen como objetivo degradar la calidad de un servicio, por ejemplo, una página web, y dejarlo en un estado no funcional. Para lograrlo, se saturan los recursos del sistema que aloja el servicio que se quiere interrumpir, enviándoles una avalancha de peticiones que no son capaces de atender (INCIBE, 2019).

Una evolución de este tipo de ataque es la denegación de servicio distribuido o DDoS por sus siglas en inglés Distributed Denial of Service. Consiste en utilizar un elevado número de dispositivos atacantes contra el objetivo. Los ataques DDoS muchas veces son llevados a cabo por bots, sistemas infectados cuyo propietario muchas veces desconoce que sus dispositivos forman parte de esta red maliciosa (INCIBE, 2019).

Los ataques de denegación de servicio, ya sea distribuido o no, causan graves consecuencias en los sistemas atacados. Implementar medidas preventivas será imprescindible ya que, en caso contrario, solamente sabremos que hemos sido víctimas de este ataque cuando el servicio deje de funcionar. Para minimizar las consecuencias de estos ataques sobre nuestros sistemas se deberán incorporar distintas medidas de seguridad (INCIBE, 2019).

Medidas de Protección en la Red Interna

Si la página web está en la red interna de una empresa, es necesario implementar medidas de protección perimetral para salvaguardarla, entre otras acciones:

- Situar el servidor web en una zona desmilitarizada (entre cortafuegos), también conocida como DMZ, para prevenir que un intruso logre entrar a la red interna si compromete el servidor web.

- Establecer un sistema de detección y prevención de intrusiones (IDS/IPS) que supervisa las conexiones y nos avisa si identifica intentos de acceso no autorizados o un uso inapropiado de protocolos.
- Emplear un software o dispositivo con funciones mixtas (cortafuegos, antivirus y otros), tal como un UTM que posibilita la administración de la mayor parte de las ciber amenazas que pueden dañar a una empresa de manera integrada.
- El uso combinado de estos elementos, que pueden ser tanto software como hardware, y su correcta configuración, reducirá las posibilidades de sufrir un ataque de denegación de servicio (INCIBE, 2019).

Fuga de Datos

En seguridad informática, la fuga de datos, también conocida como filtración de la información o escape de datos sensibles o confidenciales, se lleva produciendo a lo largo de los últimos años cada vez de manera más frecuente. Pero fue a raíz de las filtraciones de Wikileaks, a partir del año 2010, que adquirieron importancia mediática (Banco Santander, n.d.-a).

Una fuga de datos o Data Leakage es la pérdida de confidencialidad de la información de una organización, empresa o individuo, mediante la obtención de esta o el conocimiento del contenido de esta por parte de personas no autorizadas para ello (Banco Santander, n.d.-a).

A menos que se apliquen diligentemente los controles adecuados, cabe esperar que la información acabe en las manos de gente no deseada. Incluso implementando controles, el riesgo de una fuga de información no desaparece (Banco Santander, n.d.-a).

Las fugas de datos pueden ser ocasionadas por causas internas o externas a las organizaciones:

- Internas: causadas, por ejemplo, intencionada o accidentalmente por personal interno de la organización.
- Externas: por ejemplo, la filtración de los datos personales de los empleados de una empresa por un incidente de seguridad de un proveedor. Además, pueden ser deliberadas o involuntarias: (Banco Santander, n.d.-a)
- Deliberadas: se filtran o revelan datos confidenciales con el propósito de obtener una ventaja económica o causar un daño o perjuicio a las organizaciones: sanciones económicas, la pérdida de una ventaja competitiva, la pérdida de imagen o reputación, etc.
- Involuntarias: se filtran o revelan datos confidenciales de manera accidental o no intencionada, por ejemplo, por no seguir las buenas prácticas de seguridad de la información.

Incidente de Seguridad Informática

Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella (Banco Santander, n.d.-a).

En todas las organizaciones existen debilidades y/o vulnerabilidades que pueden ser explotadas de manera intencionada o no intencionada y causar la pérdida de confidencialidad, de integridad y/o de disponibilidad de la información. Algunos ejemplos de incidentes de seguridad son: (Banco Santander, n.d.-a)

- Filtración o revelación de información confidencial.
- Infección por malware.
- Acceso no autorizado a la información o los sistemas.
- Destrucción o corrupción de la información.

- Ataques de denegación de servicio (DoS o DDoS).

Hay muchas maneras de poder identificar un incidente de seguridad, entre ellas, las principales son: (Banco Santander, n.d.-a)

- Monitorizar adecuadamente los sistemas, al menos los críticos para el negocio o que contienen información sensible o confidencial.
- Implantar herramientas de correlación y revisión de logs de los principales sistemas para detectar posibles incidentes de seguridad o patrones de comportamiento anómalos.
- Implementar un servicio de ciberinteligencia que pueda detectar fugas de datos, contraseñas comprometidas, etc.
- Concienciar a los usuarios en la importancia de comunicar cualquier incidente de seguridad que hayan sufrido o que crean haber sufrido, o cualquier comportamiento extraño que detecten.
- El eslabón más débil en cuanto nos referimos a incidentes de seguridad siempre es el propio personal de las organizaciones, que bien accidentalmente o de manera intencionada pueden ocasionar o ser colaboradores necesarios para que se produzca un incidente de estas características.

Ingeniería Social

La ingeniería social es un grupo de métodos que los delincuentes cibernéticos utilizan para engañar a las personas desprevenidas y conseguir que envíen información confidencial, contaminen sus computadoras con malware o accedan a enlaces a páginas contaminadas. Además, los hackers pueden intentar sacar partido de la ignorancia de un usuario; debido a lo rápido que va la tecnología, muchos clientes y empleados no tienen conciencia del verdadero

valor de sus datos personales ni saben con certeza cómo proteger esta información. (Kaspersky, n.d.-a).

Funcionamiento de la Ingeniería Social

Prácticamente todos los tipos de ataques incluyen algún tipo de ingeniería social. Por ejemplo, existen los tradicionales correos electrónicos de phishing y fraudes de virus, que cuentan con un alto contenido social. Los correos electrónicos de phishing buscan persuadir a los usuarios de que su procedencia es auténtica, con la expectativa de conseguir datos personales o información sobre la compañía, sin importar cuán insignificantes puedan parecer. Por otro lado, los correos electrónicos que tienen archivos adjuntos infectados con virus suelen parecer que proceden de contactos seguros o que brindan contenido multimedia que parece inocuo, como videos graciosos o entrañables (Kaspersky, n.d.-a).

En ciertas circunstancias, los atacantes emplean técnicas más sencillas de ingeniería social para ingresar a una computadora o red. Un hacker, por ejemplo, puede visitar de manera habitual el comedor público de un gran complejo de oficinas, observar a los usuarios que estén trabajando en sus computadoras portátiles o tabletas y ver los dispositivos por encima del hombro. Con esta estrategia es posible obtener una enorme cantidad de contraseñas y nombres de usuario, sin tener que enviar un único correo electrónico o redactar una línea de código malicioso. Otros ataques necesitan de una comunicación verdadera entre la víctima y el atacante; en estas situaciones, este último presiona al usuario para que le conceda acceso a la red bajo el pretexto de un problema serio que necesita ser solucionado. (Kaspersky, n.d.-a).

Los asaltantes emplean de manera equitativa la tristeza, la culpa y la rabia para persuadir a los usuarios de que requieren su asistencia y no tienen el poder de negársela. En conclusión, es fundamental tomar en cuenta la ingeniería social como una forma de generar confusión. Muchos

empleados y clientes ignoran que los hackers pueden entrar a varias redes suplantando la identidad de usuarios legítimos o miembros del personal de TI con solo una pequeña cantidad de información, como el nombre, la dirección o la fecha de nacimiento. Una vez lo consiguen, les resulta sencillo restablecer contraseñas y tener acceso casi sin límites. (Kaspersky, n.d.-a).

La educación es el primer paso en la protección contra la ingeniería social. Los usuarios deben ser instruidos para no hacer clic en enlaces que despierten sospechas y para proteger sus credenciales de inicio de sesión, tanto en casa como en la oficina. No obstante, si las estrategias sociales tienen éxito, es probable que se produzca una infección de malware. Es crucial implementar una solución de seguridad de Internet de alta calidad para erradicar infecciones y rastrear su origen, con el fin de luchar contra los bots, rootkits y troyanos. (Kaspersky, n.d.-a).

Parche de Seguridad

Los sistemas operativos, navegadores web, programas y aplicaciones son susceptibles de tener fallos de seguridad. Por este motivo, pueden necesitar ser actualizados, independientemente del dispositivo en el que se encuentren instalados. Esto incluye los programas y sistemas operativos de ordenadores, tablets, smartphones, consolas de videojuegos e incluso televisiones inteligentes (INCIBE, 2019).

Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad (INCIBE, 2019).

Por tanto, si se quiere mantener la seguridad de los dispositivos, debemos: (INCIBE, 2019)

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de actualizaciones automáticas siempre que esté disponible.

- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar usar aplicaciones y sistemas antiguos que ya no dispongan de actualizaciones de seguridad.
- Es importante no confundir tener una aplicación actualizada con tener la última versión. Podemos tener instalado y actualizado Windows 10, a pesar de no tratarse de la última versión de este sistema operativo. Los fabricantes no solo comercializan nuevas versiones que incorporan mejoras, sino que mantienen un largo periodo de tiempo las antiguas versiones a través de actualizaciones (INCIBE, 2019).

Pentesting

Toda organización maneja información para su funcionamiento diario. Es habitual que se utilicen herramientas para su tratamiento en ordenadores, teléfonos móviles, tabletas, líneas de comunicaciones, etc. En cualquier caso, trabajar con información, conlleva una serie de riesgos (INCIBE, 2019).

¿Qué pasaría si nuestra empresa fuera víctima de una fuga de información o sufriera un ataque de denegación de servicio? Ante estas amenazas, tenemos que analizar los sistemas que soportan la gestión de la información en la empresa, para evaluar los riesgos asociados a su utilización (INCIBE, 2019).

Para facilitar esta labor, existen una serie de métodos y herramientas que permiten realizar un análisis conocido como test de penetración, test de intrusión, pen test o pentesting.

El Pentesting y sus Características

Un pentesting es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas. Estas auditorías comienzan con la recogida, en fuentes de acceso abierto, de información sobre la empresa, los empleados, usuarios, sistemas y equipamientos (INCIBE, 2019).

Continúa con un análisis de vulnerabilidades que se intentarán explotar, incluso con técnicas de ingeniería social, atacando a los sistemas hasta conseguir sus objetivos. Finalmente, se realiza un informe que indica si los ataques tuviesen éxito, y en caso afirmativo porqué y qué información o acceso obtendrían, es decir, se simulan ataques tal y como los llevaría a cabo un ciberdelincuente que quisiera hacerse con el control del sistema o con la información en él contenida. De esta forma, se puede determinar: (INCIBE, 2019)

- Si el sistema informático es vulnerable o no.
- Evaluar si las defensas con las que cuenta son suficientes y eficaces, y
- Valorar la repercusión de los fallos de seguridad que se detecten.

En la preparación del pentesting se realiza un plan con un conjunto de ataques dirigidos, según la tecnología que se utilice en la empresa y sus necesidades de seguridad. Para ello, los auditores cuentan con metodologías, —algunas específicas según la tecnología o estándares de seguridad que queramos implantar, y otras más generales—, que les ayudan a realizarlas de forma sistemática.

Tendremos que elegir qué pruebas queremos que realicen y sobre qué aplicaciones o servicios. También existen diferentes tipos de pruebas de penetración según la información inicial con la que cuenta el auditor, así, pueden ser:

- Caja blanca: si disponen de toda la información sobre los sistemas, aplicaciones e infraestructura, pudiendo simular que el ataque se realiza por alguien que conoce la empresa y sus sistemas.
- Caja gris: si dispone de algo de información, pero no de toda.
- Caja negra: si no dispone de información sobre nuestros sistemas; en este caso, se simula lo que haría un ciberdelincuente ajeno.

No obstante, cuando contratamos un servicio de pentesting además de acordar la finalidad del servicio, el objeto del análisis y qué tipo de prueba queremos que realicen, como se trata de un ataque *permitido* debemos tener en cuenta algunas cuestiones legales (INCIBE, 2019).

Suplantación de Identidad Informática

La suplantación de identidad digital consiste en el uso ilícito de la identidad ajena para actuar en nombre de esta; las motivaciones del que suplanta pueden ser variadas, desde hacer una broma pesada hasta dañar la reputación o, en el caso más grave, perpetrar ciberataques desde la cuenta aprovechando la confianza que se establece con otros. (Escobar Carolina, 2021).

En la actualidad es muy frecuente que las personas sean víctimas de la suplantación de identidad sin saberlo, puede ocurrir tras la pérdida de documentos de identidad, tarjetas de crédito o documentos que contengan información personal; también se da por medio de la captación de datos con virus y por páginas fraudulentas en internet (Escobar Carolina, 2021).

Durante la pandemia por Covid-19 la ciberdelincuencia se ha disparado de forma alarmante, la suplantación de identidad se da a mayor medida a través de correos electrónicos con los cuales se busca la falsificación de documentos para acceder a cuentas bancarias, obtener créditos financieros y hasta para realizar compras por internet (Escobar Carolina, 2021).

Algunos de los modus operandi más comunes para suplantar la identidad en Internet:

- Conseguir acceso a la cuenta real del usuario: Este es el peor escenario para la víctima, dado que el perfil es real, esto facilita al atacante el acceso a la información personal existente (datos privados, mensajes, contraseñas, etc.). El atacante puede crear y modificar la información, las imágenes, enviar mensajes privados o incluso dar opiniones y publicar. Dado que el perfil goza de credibilidad, el atacante puede aprovechar dicha confianza para enviar ciberataques a los contactos mediante el envío de mensajes con enlaces o archivos infectados (Escobar Carolina, 2021).
- Crear un perfil falso con información real de la víctima suplantada: Este escenario no tiene tanto impacto en la información personal de la víctima, pero sí en su reputación. A mayor exposición tenga la víctima de su imagen y datos personales, más fácil podrá el atacante crear un perfil creíble "a su imagen y semejanza" (Escobar Carolina, 2021).

Auditoría Informática

Es la revisión que tiene como objetivo evaluar los métodos y procedimientos utilizados en una entidad para establecer si su diseño y ejecución son adecuados. También se encarga de comprobar el sistema de procesamiento de información como parte de la evaluación del control interno, así como detectar aspectos que puedan ser mejorados o eliminados. (Ecured, n.d).

La Auditoría de Sistemas es la verificación de controles en el procesamiento de la Información, desarrollo de sistemas e instalaciones. Es una actividad dirigida a verificar y juzgar la información, se realiza un examen y evaluación de los Procesos del área de Procesamiento automático de datos y de la utilización de los recursos que en ello intervienen. Es la verificación en la eficiencia del uso de los Recursos informáticos (Ecured, n.d).

Posición Actual de la Auditoria de Sistemas

Es importante en el uso de pruebas en la auditoría de sistemas informáticos (A.S.I.) en la parte de la evaluación de sistemas en operación. Se piensa que para realizar una auditoría de sistemas informáticos es necesario utilizar el computador, siendo esta tarea muy sencilla y más que todo es parte sustancial de la Auditoria Financiera (Ecured, n.d).

Objetivos de la Auditoría

- Busca una mejor relación, costo – beneficio de los sistemas automáticos diseñados e implementados por el área de Procesamiento de datos.
- Mejora la satisfacción de los usuarios de sistemas informáticos.
- Mediante la recomendación de seguridad y control, garantiza que la información sea más confiable, confidencial e íntegra.
- Entender la situación presente del sector de informática y las acciones, esfuerzos requeridos para alcanzar las metas planteadas.
- Proporcionar protección a los empleados, la información, el hardware, el software y las instalaciones.
- Minimizar existencia de riesgo usando la tecnología de información.
- Decisiones de inversión, evitar gastos innecesarios.
- Capacitación y educación sobre controles en los sistemas informáticos.

Informática Forense

La informática forense juega un papel fundamental en la investigación y persecución de los cibercriminales, pues su objetivo principal es la obtención de evidencias relativas a un crimen digital (Unir, 2021).

La informática forense se refiere a un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias del equipamiento de computación de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo en un juzgado (Unir, 2021).

La informática es una parte vital en la investigación forense en el ámbito digital, pues está específicamente focalizada en los delitos cometidos mediante dispositivos de computación**,** como redes, ordenadores y medios de almacenamiento digital, especialmente en aquellos casos que involucran a la tecnología como fuente o víctima de un delito (Unir, 2021).

La informática forense es esencial para: (Unir, 2021)

- Asegurar la integridad y disponibilidad de la infraestructura de red cuando sucede un incidente de ciberseguridad o ataque informático.
- Identificar y obtener evidencias de los cibercrímenes de manera apropiada.
- Asegurar la protección adecuada de los datos y el cumplimiento regulatorio.
- Proteger a las organizaciones para que no vuelvan a suceder en el futuro los incidentes ocurridos.
- Ayudar en la protección de crímenes online, como abusos, bullying, entre otros
- Minimizar las pérdidas tangibles o intangibles de las organizaciones o individuos relativas a incidentes de seguridad.
- Soportar el proceso judicial de enjuiciamiento de los criminales.

Integridad de la Información

La confidencialidad, la integridad y la disponibilidad de la información son los tres fundamentos de la seguridad de la información (y el propósito de poner en marcha medidas organizativas y técnicas de seguridad). Para llevar a cabo sus actividades comerciales diarias y

tomar decisiones más acertadas, las organizaciones globales requieren información confiable, que es de lo que se ocupa la integridad de la información. (Banco Santander, n.d.-a).

En el contexto de la seguridad informática, este concepto se puede definir como la certeza de que la información es precisa y confiable. Prevenir cualquier alteración no autorizada de la información y los datos es posible garantizando su integridad. (Banco Santander, n.d.-b).

Para que los datos sean mantenidos y procesados adecuadamente, así como para que sean enviados a sus destinatarios sin sufrir alteraciones, el software y el hardware que soportan los datos, junto con los sistemas de comunicación, tienen que funcionar de forma coordinada (Banco Santander, n.d.-b).

Lograr la Integridad de los Datos

Con el fin de garantizar la integridad de los datos, se deberían restringir a lo mínimo necesario los permisos que poseen los usuarios sobre la información y reducirlos solamente a los sistemas que la respaldan. Asimismo, se aconseja limitar el acceso a los archivos críticos de los sistemas y ocultarlos. Asimismo, la validación de los datos de entrada y la escritura en bases de datos deberían estar limitadas a los usuarios con autorización. (Banco Santander, n.d.-b). Ejemplos de controles o medidas técnicas que aseguran la integridad informática son:

- Hashing de los datos para garantizar que no han sufrido alteraciones.
- Administración de la configuración de los sistemas para garantizar que no ha sufrido modificaciones sin permiso.
- Administración de cambios para garantizar la integridad de los procedimientos.
- Control de acceso lógico a la información, los sistemas y las aplicaciones, así como a la red; y control de acceso físico a las instalaciones.
- Firmar digitalmente la información.

- Verificaciones de redundancia en las informaciones transmitidas.

Ejemplos de Aseguramiento de Integridad de la Información

La mayoría de las veces, cuando nos descargamos de una web fiable (por ejemplo, un fabricante…) cualquier tipo de software, en el lugar de descarga del fichero suele aparecer un archivo con su código hash. ¿Pero por qué hacen esto? Para tener la completa seguridad de que el archivo no ha sido modificado hasta llegar a nuestro equipo (Banco Santander, n.d.-b).

La integridad de la información o de los datos asegura que la precisión de aquellos que se transportan o almacenan es exacta, garantizando que no ha habido alteraciones, pérdidas o destrucción, sean estas intencionadas o accidentales. (Banco Santander, n.d.-b).

Disponibilidad, confidencialidad e integridad de la información

La seguridad informática, la ciberseguridad o la seguridad de la información pueden definirse como el conjunto de políticas, procedimientos y medidas técnicas y organizativas que se implementan para salvaguardar los datos. En UNIR, examinamos tanto los procedimientos requeridos para asegurar la seguridad informática como los principios que la rigen. (Unir, 2020a).

La protección de los datos implica asegurar que se cumplan las tres bases esenciales de la seguridad informática: la disponibilidad, la confidencialidad y la integridad de los datos. Para lograr esto, es necesario establecer controles de seguridad y estrategias de respuesta que reduzcan los diversos peligros que impactan la información mientras está en tránsito y almacenada. (Unir, 2020a).

Los Tres Principios de la Ciberseguridad

Confidencialidad de la Información

También llamada privacidad, se refiere a que la información solo debe ser conocida por las personas autorizadas para ello y que necesitan tener acceso a ella. Este principio garantiza que la información no se divulgará accidentalmente ni deliberadamente. (Unir, 2020b).

Integridad de la Información

Se refiere a que los datos almacenados en los dispositivos o transmitidos por cualquier medio de comunicación no han sido manipulados con malas intenciones por terceros. Esto asegura que la información no será alterada por individuos sin autorización. (Unir, 2020b).

Disponibilidad de la Información

Se refiere a que los datos almacenados en los dispositivos o transmitidos por cualquier medio de comunicación no han sido manipulados con malas intenciones por terceros. Esto asegura que la información no será alterada por individuos sin autorización. (Unir, 2020b).

Software Antivirus

Inicialmente, un programa antivirus era un software que identificaba y en ocasiones suprimía virus informáticos de los equipos infectados; por ende, colaboraba también con la interrupción de la difusión del contenido malicioso. Principalmente eso ocurría en la década de 1990 y a inicios del año 2000. (Eset, n.d).

Sin embargo, debido al enorme crecimiento del número de malware en otras categorías, los programas antivirus han evolucionado hacia soluciones de seguridad complejas (Eset, n.d).

La mayor parte de los productos de protección modernos utilizan diversas tecnologías para asegurar la seguridad de sus usuarios. Estas posibilitan el enfrentamiento de una extensa gama de acciones maliciosas, tales como la grabación de las pulsaciones del teclado, el espionaje, el robo de credenciales, la minería no autorizada de criptomonedas, el cifrado no

deseado de archivos (por ransomware), la extracción de información (por troyanos bancarios), los correos electrónicos no deseados (spam) y estafas que constituyen otras modalidades de ciberataques. (Eset, n.d).

Los productos de seguridad también alertan, y si el usuario lo permite, protegen frente a aplicaciones sospechosas o potencialmente no seguras o no deseadas. Estos programas no son directamente maliciosos, pero pueden influir negativamente en el rendimiento del dispositivo o molestar al usuario (Eset, n.d).

Aunque el término *antivirus* ha perdido la mayoría de su significado original, el término todavía se usa comúnmente para referirnos a soluciones de seguridad modernas y mucho más avanzadas (Eset, n.d).

Software de Seguridad Informática

La información almacenada en el sistema informático de una empresa es de vital importancia para cualquier negocio, por eso es crucial protegerla con la máxima eficiencia (Soler Lluís, n.d.).

De lo contrario, corres el riesgo de que se produzcan filtraciones hacia la competencia, salgan a la luz datos de tus clientes o no puedas cumplir con tus servicios habituales al bloquearse el sistema, entre otras posibles amenazas (Soler Lluís, n.d).

Un software de seguridad informática es un programa que sirve para proteger la privacidad de la información contenida en un sistema informático. Esta solución de ciberseguridad permite a las empresas garantizar la seguridad de sus datos y protegerse ante posibles ataques informáticos (Soler Lluís, n.d.).

Objetivos de un Software de Ciberseguridad

- Garantizar la integridad y la confidencialidad de los datos.

- Asegurar la disponibilidad de la información en todo momento.
- Evitar el rechazo de las operaciones realizadas y autenticar los datos.

Programa de Seguridad Informática

Los peligros de un ciberataque son reales en la actualidad. Afectan a grandes compañías y hasta a algunas organizaciones que parecen más seguras. Por lo tanto, no deberías dudar en tener un plan de seguridad informática. (Universidad VIU, 2016).

Un plan de seguridad informática te ayuda a identificar los puntos vulnerables en tus sistemas, para que, una vez localizados, puedas implementar las acciones necesarias para evitar esos problemas. No es necesario que tu plan de seguridad informática sea un documento excesivamente largo que abarque toda clase de seguridad posible. (Universidad VIU, 2016).

Debe ser capaz de ayudar a proteger los datos y los sistemas críticos de tu negocio, asegurándote además que se ajuste a la legislación vigente y a la Ley de Protección de Datos. Tu plan de seguridad debe de tener varios pasos que debes dejar por escrito (Universidad VIU, 2016).

Pasos para Elaborar un Plan de Seguridad Informática

- Identificación: Para resguardar a tu organización, lo primero que necesitas hacer es conocer qué es aquello que quieres proteger de ella. Esta etapa inicial consiste en determinar la totalidad de los activos de la entidad, incluyendo el personal, el hardware, el software, los sistemas y la información que integran tu sistema informático. Algunos ejemplos son programas de computadora, servidores y servicios externos como el alojamiento web. (Universidad VIU, 2016).

- Evaluación de riesgos: Ahora tienes que determinar qué podría amenazar los activos previos. Por ejemplo, los virus de computadora, los piratas informáticos, los daños físicos

o las equivocaciones cometidas por los trabajadores. Ten en cuenta la naturaleza y el alcance del daño que podría ocasionarse en cada situación. Si, por ejemplo, el servidor se desconecta, ¿sería capaz tu empresa de seguir operando? Incluye toda esta información en tu plan de seguridad informática. (Universidad VIU, 2016).

- Priorizar la protección IT: Cuando hayas determinado el daño que podría causar cada amenaza y la probabilidad de su ocurrencia, podrás decidir cuáles son las amenazas más relevantes e interesantes para iniciar su protección. Por ejemplo, podrías decidir que proteger tu servidor es más importante que proteger los equipos individuales. (Universidad VIU, 2016).
- Tomar las precauciones indicadas: Determina los pasos que debes seguir para protegerte de los peligros que has detectado en la totalidad de la parte anterior de este plan de seguridad informática, y garantiza que tu empresa podrá continuar funcionando si algo sale mal. Deberías, por ejemplo, limitar el acceso a tu servidor o poner un firewall de hardware. Tu estrategia de recuperación ante desastres tiene que detallar las acciones a seguir en caso de una crisis. (Universidad VIU, 2016).

Mecanismos Básicos de Seguridad

Autenticación

Confirmación de la identidad del usuario, normalmente cuando se incorpora al sistema o a la red, o cuando tiene acceso a una base de datos. Para acceder al sistema informático se emplea generalmente un nombre de usuario y una contraseña. Se emplean cada vez más otras técnicas seguras (Calderón Laura, 2015).

Hay tres formas posibles de autenticarse:

- Por lo que uno conoce (una contraseña).
- Por lo que uno posee (una tarjeta magnética).

- Por lo que uno es (las huellas dactilares).

Emplear simultáneamente más de un método incrementa la posibilidad de que la autenticación sea adecuada. No obstante, la elección de adoptar más de un método de autenticación por parte de las compañías debe estar relacionada con el valor de la información que se quiere proteger. (Calderón Laura, 2015).

La autenticación por medio de contraseñas es el método más común. La eficacia de este método dependerá de las particularidades de la contraseña. Mientras más compleja y extensa sea la contraseña, será más complicado eludir esta técnica. (Calderón Laura, 2015).

La contraseña también debe ser secreta. No puede ser conocida por nadie más que la persona que la usa. Los usuarios a menudo comparten sus contraseñas o las escriben en un papel que está pegado en el escritorio y es accesible para otros usuarios, poniendo así en riesgo tanto la empresa como el propietario mismo, puesto que cualquier acción realizada con dicha contraseña es responsabilidad del propietario. (Calderón Laura, 2015).

Para que la contraseña sea difícil de adivinar, es necesario que contenga un conjunto extenso y diverso de caracteres (números, símbolos, letras mayúsculas y minúsculas). El inconveniente es que los usuarios tienen dificultades para recordar contraseñas tan complejas y emplean palabras predecibles (el nombre, el apellido, el nombre de usuario, el grupo musical preferido...), lo cual hace más fácil la tarea a quien intenta acceder al sistema sin autorización. (Calderón Laura, 2015).

Verificación

Proceso mediante el cual se define qué, cuándo y cómo puede emplear los recursos de la entidad un usuario autenticado. El sistema o nivel de autorización puede cambiar en función de qué es lo que se protege. No toda la información organizacional tiene el mismo grado de

criticidad. Los datos y los recursos, en general, están estructurados por niveles, y cada uno requiere su propia autorización. (Calderón Laura, 2015).

La autorización puede llevarse a cabo a través de la firma en un formulario o una contraseña, dependiendo del recurso; sin embargo, es indispensable que esta autorización esté siempre registrada para su posterior control. En lo que respecta a los datos, la autorización debe garantizar la integridad y confidencialidad de estos, permitiendo o negando el acceso a su modificación, eliminación, creación o lectura. De otro lado, solo se debe permitir el acceso a un recurso a los usuarios que lo requieran para realizar su trabajo; de lo contrario, se les negará. A pesar de que también se pueden otorgar permisos temporales o alterarlos cuando cambien las necesidades del usuario. (Calderón Laura, 2015).

Administración

Define, sostiene y suprime las autorizaciones de los usuarios del sistema, así como la relación entre estos y los recursos del sistema. Los administradores tienen el deber de convertir las políticas y los permisos concedidos por la organización a un formato que pueda ser utilizado por el sistema. (Calderón Laura, 2015).

La gestión de la seguridad informática dentro de la empresa es una labor que está en constante cambio y evolución, debido a que las tecnologías empleadas cambian rápidamente y con ellas los peligros. (Calderón Laura, 2015).

Auditoría y Registro

La auditoría es una supervisión constante de los servicios en producción, para lo cual se recopila y analiza información. Este procedimiento posibilita que los administradores comprueben que las técnicas de autorización y autenticación empleadas se hacen conforme a lo estipulado y que se logran las metas establecidas por la organización. (Calderón Laura, 2015).

El registro es el procedimiento que permite almacenar en una base de eventos cualquier intento de violar las reglas de seguridad establecidas para su posterior análisis. Sin embargo, solo auditar y registrar carece de sentido si no se realiza un análisis posterior de la información recopilada. La auditoría o el monitoreo de la información registrada se pueden llevar a cabo a través de medios automáticos o manuales, y con una frecuencia que variará dependiendo del nivel de riesgo y de cuán crítica sea la información protegida.
(Calderón Laura, 2015).

Mantenimiento de la Integridad

Conjunto de procesos establecidos para prevenir o gestionar que los archivos sean objeto de modificaciones no permitidas y que la información enviada desde un punto llegue al destino sin alteraciones. Algunas de las técnicas más empleadas para preservar (o gestionar) la integridad de los datos son el uso de antivirus, cifrado y funciones hash. (Calderón Laura, 2015).

Análisis del Marco Teórico para la Implementación de un Plan Estratégico de Seguridad de la Información

En las Organizaciones la seguridad de la información tiene que ser tratada desde una perspectiva estratégica integral, que esté en línea con los objetivos empresariales y respaldada por la gobernanza TI y el gobierno corporativo. No se trata solo de aplicar controles tecnológicos, sino de establecer un Sistema de Gestión de Seguridad de la Información (SGSI), que se fundamenta en la administración de riesgos, el reconocimiento y salvaguarda de activos esenciales y la formulación de políticas organizacionales precisas. En esta línea, aspectos como el análisis de riesgos, la clasificación de activos y el gap analysis son esenciales para determinar prioridades y guiar las decisiones estratégicas en términos de seguridad.

Además, la puesta en marcha del plan estratégico demanda un enfoque de mejora continua que incorpore controles técnicos, humanos y administrativos bajo un modelo de defensa en profundidad. Esto comprende la capacitación de los usuarios, la supervisión continua, la auditoría y validación a través de pruebas como el pentesting y el manejo de incidentes. En última instancia, la efectividad del plan está determinada por el liderazgo de la alta dirección, la cultura organizacional y el empleo de métricas que faciliten la valoración del rendimiento y el grado de madurez en seguridad. Esto garantiza que la información esté protegida y que el negocio sea sostenible ante las amenazas presentes.

Es también esencial que la estrategia incluya un plan claro con etapas de diagnóstico, diseño, implementación y mejora constante para posibilitar que la organización progrese gradualmente en su nivel de madurez. La incorporación de marcos de referencia como ITIL e ISO 27001, además de adoptar buenas prácticas de gobernanza, ayuda a optimizar los recursos, estandarizar procesos y cumplir con las regulaciones. Así, la seguridad de la información se

convierte en un facilitador estratégico que no solo disminuye los riesgos, sino que además potencia la confianza, la capacidad de competir y la resiliencia a nivel empresarial.

Diseño Metodológico

Ciclo PHVA: Planear, Ejecutar o Hacer, Verificar o Controlar y Actuar

Planear, ejecutar o hacer, verificar o controlar y actuar son los cuatro conceptos que integran el ciclo. Cada organización tiene que instaurarlos en todos sus procesos, empezando por el más importante y siguiendo con los demás. Este ciclo es una herramienta centrada en la resolución de problemas y en la mejora constante. A través de un diagnóstico inicial, se detectan los errores para optimizar mediante la comparación entre los planes y los resultados. Posteriormente, se examina el resultado no deseado y se rediseñan las medidas para eliminar el problema y evitar que vuelva a suceder, con el fin de lograr un resultado satisfactorio. Lo que posibilita el crecimiento sistemático fundamentándose en la innovación y la mejora constante. (Pineda, n.d.).

El proceso se define así:

Planear: Se materializan los proyectos y la visión de la meta de la compañía, donde aspira a estar en un periodo específico. Cuando el objetivo ya ha sido definido, se lleva a cabo un diagnóstico para conocer la situación presente y las áreas que deben ser mejoradas. Esto incluye identificar los problemas y el impacto que puedan tener sobre su vida. Luego, se elabora una teoría de posible solución para optimizar un aspecto. Se elabora un plan de trabajo para poner a prueba la teoría de solución. (Pineda, n.d.)

Hacer: Se ejecuta el plan de trabajo definido en la etapa "Planear", además de algún control para asegurar que se está llevando a cabo como se ha indicado. La gráfica de Gantt, que permite calcular las tareas y el tiempo invertido, es uno de los métodos de control más sobresalientes.

Verificar: Esta verificación enfrenta los resultados planeados con los obtenidos efectivamente, basándose en los indicadores de medición previamente definidos, porque lo que no puede medirse no puede mejorarse de manera sistemática. Un caso ilustrativo de esto podría ser un deportista que se prepara para calificar a los Juegos Olímpicos. A este atleta se le organiza una competencia semanal con oponentes de su nivel, lo cual le permite comprobar si realmente está mejorando su desempeño. (Pineda, n.d.).

Actuar: Esta fase termina el ciclo de calidad. Si los resultados se corresponden con lo planeado, se sistematizan y documentan las modificaciones realizadas. Sin embargo, si la verificación muestra que no se ha alcanzado lo esperado, es necesario actuar rápidamente: corregir lo propuesto y crear un nuevo plan de trabajo, repitiendo así el ciclo. (Pineda, n.d.).

Figura 1

Ciclo PHVA

Nota. Ciclo PHVA (Planificar, Hacer, Verificar, Actuar), también conocido como ciclo de Deming.

Se puede observar en la figura No. 1 el ciclo PHVA descrito anteriormente donde se evidencia el paso de una fase a otra de manera cíclica.

El desarrollo del proyecto para la implementación de PESI se propone la metodología basada en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), que garantiza que este modelo sea sometido a revisiones constantes cuando se producen cambios significativos en la infraestructura o si se necesita mejorar su eficacia, en función de las evaluaciones de los parámetros operacionales clave.

En la fase inicial del proyecto se presentan el análisis y recomendaciones relacionadas con la evaluación de controles de tecnología de información de los procesos involucrados en la gestión de la Seguridad de la Información bajo la norma ISO 27001:2013.

Se realizarán entrevistas a los líderes de los procesos, a fin de evaluar el grado de apropiación que tiene cada líder entrevistado respecto a la Seguridad de la información. (véase Gap Análisis Checklist 27001-27002).

Posteriormente se desplegarán campañas de ataques tipo *Phishing y Ethical Hacking* con el fin de evaluar los riesgos y vulnerabilidades presentes en la Infraestructura TI actual.

Phishing

Objetivos de la Campaña

- Validar y evaluar internamente las acciones de reacción y respuesta de los usuarios frente a la recepción de correos de phishing, identificar si reportaban los eventos a la mesa de ayuda y tener estadísticas que permitan tomar acción utilizando otro tipo de control de seguridad o mayor entrenamiento de funcionarios.

- Identificar puntos de mejora de controles que deben ser abordados en la protección de amenazas de correo electrónico, que son recibidas por empleados en diferentes

tipos de dispositivos y navegadores, con el fin de reducir la posibilidad de que este tipo de correos ingresen a la organización y afecten el sistema.

Alcance

Realización de Campañas de phishing:

- Se enviaron 2 campañas de simulación Phishing (Office 365 y team).
- La prueba se realizó sobre 394 cuentas de la Organización.

Resultados de la Campaña de Phishing

Figura 2

Resultado de la Campaña de Phishing

Numeración	Nombre	Phished	% Entregado	Cant. Entregado	Link Clicked	Attachment Opened	Data Entered
Campaña 1	Validación Cuenta O365	12,13% 48 users	98,98%	396	48	No tenia	36
Campaña 2	Teams Grupos de Colaboración	33,8% 134 users	98,98%	396	92	76	47

Nota. Figura tomada del Resultado de la campaña de Phishing.

Conclusión

Frecuencia de Campañas

- La realización de campañas phishing se deben generar con mayor frecuencia para mejorar la detección y entendimiento de los usuarios.
- Las personas son un control de detección y reacción importante dentro de la organización.

Foco en la Siguiente Campaña

- Se recomienda agregar la realización de entrenamientos en línea para los usuarios y de esta forma las personas que no detecten el phishing inicien un entrenamiento de varios módulos en temas de importancia y seguridad de la información.
- Revisar la posibilidad que los usuarios que se vean víctimas del phishing dentro de las pruebas puedan recibir un mensaje en pantalla indicando que fueron víctimas y adicional se agregue información corporativa para mejorar su entendimiento del phishing.

Ethical Hacking

La realización de actividades de Hacking sobre las infraestructuras demuestra que son una manera eficiente y real de identificar el riesgo al cual están expuestas nuestras infraestructuras y aplicaciones donde de cierta forma la idea es ponerse en la posición de un atacante para intentar vulnerar un grupo de sistemas, este tipo de pruebas puede tener diferentes contextos dependiendo de la posición del ethical hacker y de la información que tenga para hacerlo

Para la presentación de los resultados de las pruebas el ethical hacking se utiliza la base de caja negra (Black Box) donde el security tester solo tiene la información del sitio a generar la intrusión desde el Front del portal, pero también con base de Caja Gris (Grey Box) donde el security tester realizara las pruebas desde el Backend con dos tipos de credenciales de alto y bajo privilegios para identificar hasta donde podría llegar un atacante si lograra tener acceso.

Los resultados de la aplicación de Ethical Hacking no son publicados en este documento por cuanto hace parte del acuerdo de confidencialidad celebrado entre la Organización y la parte receptora (Estudiante – Yeferson daza).

Marco Normativo

El Proyecto Aplicado se apoya en la norma NTC-ISO-IEC-27001:2013 y el ciclo Deming que se representan en un base que facilita el aseguramiento de la información implementando las mejores prácticas en los procesos, procedimientos que desarrolla la compañía, a continuación, se enuncian algunos detalles:

Ntc-Iso-Iec-27001:2013

Sistema de Gestión de la Seguridad de la Información

La norma ISO 27001 es de carácter internacional y posibilita la garantía, la integridad y la confidencialidad de los datos e información, además de los sistemas que los procesan. (ISOTools, S, F).

El estándar ISO 27001:2013 de los Sistemas de Gestión de Seguridad de la Información posibilita que las organizaciones evalúen el riesgo y apliquen los controles pertinentes para disminuirlos o incluso erradicarlos. (ISOTools, S, F).

La implementación de ISO-27001 marca una distinción en comparación con los demás, lo que potencia la competitividad y la reputación de una entidad. La gestión de la seguridad informativa se complementa con los controles o buenas prácticas que establece la norma ISO 27002. (ISOTools, S, F).

Ciclo Deming

El ciclo de Deming se compone de cuatro conceptos: planificar, hacer o ejecutar, verificar o controlar y actuar. La organización debe implementar estos conceptos en cada uno de sus procesos, comenzando por el más importante y siguiendo con los demás. Este ciclo es una herramienta centrada en la resolución de problemas y en la mejora constante. A través de un diagnóstico inicial, se detectan los errores para optimizar mediante la comparación entre los planes y los resultados. Posteriormente, se examina el resultado no deseado y se rediseñan las

medidas para eliminar el problema y evitar que vuelva a suceder, con el fin de lograr un resultado satisfactorio. Esto posibilita un crecimiento sistemático fundamentado en la innovación y la mejora constante.

Las leyes y marcos legales que rigen a Colombia en ámbitos de Seguridad de la Información:

Ley estatutaria 1266 de 2008: La presente ley tiene como finalidad desarrollar el derecho constitucional de todas las personas a saber, actualizar y corregir los datos acerca de ellas que se hayan almacenado en bancos de datos, así como otros derechos, garantías y libertades constitucionales vinculadas con la recolección, tratamiento y difusión de información personal mencionados en el artículo 15 de la Constitución Política. También busca fortalecer el derecho a la información establecido en el artículo 20 de la misma Constitución, especialmente respecto a la información financiera y crediticia, comercial y sobre servicios, incluyendo aquella proveniente del extranjero.

Ley 1273 de 2009: Se establece un nuevo bien jurídico, llamado "de la protección de datos e información", y se protege completamente los sistemas que empleen tecnologías de la información y de las comunicaciones, entre otras normas.

Ley estatutaria 1581 de 2012: El propósito de la ley actual es fomentar el derecho constitucional que cada individuo posee a informarse, actualizar y corregir los datos que se han almacenado sobre ellos en bases de datos o archivos, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, además de las demás libertades, derechos y garantías constitucionales mencionados en el artículo 20.

Diagnóstico del Estado de Seguridad de la Información de la Organización Propanogas S.A.S E.S.P

Se diagnostica el estado de seguridad de la información de la Organización Propanogas S.A.S E.S.P evaluando los controles de tecnología de la información de los procesos involucrados en la gestión de la Seguridad de la Información bajo la norma ISO 27001:2013.

El diagnóstico fue realizado, utilizando y aplicando las plantillas y documentos provistos por Propanogas S.A.S E.S.P - GAP ANÁLISIS CHECKLIST 27001-27002", diligenciando tanto los numerales de la Norma ISO 27001 como el Anexo A ISO 27002, el cual presenta los controles de cada uno de los dominios y subdominios definidos en la norma mencionada.

Se realizaron una serie de entrevistas virtuales y presenciales dirigidas con los lideres de los procesos, con preguntas previamente diseñadas con el propósito de evaluar el grado de apropiación que tiene cada líder entrevistado, con respecto a la Seguridad de la información.

El propósito del diagnóstico es mostrar el nivel de cumplimiento de Seguridad de información con base en el estándar ISO 27001:2013.

Alcance

El criterio de evaluación para obtener el nivel de madurez es el cumplimiento de los numerales de la norma (del 4 al 10) y los 114 controles de los 14 dominios del Anexo A de la norma NTC-ISO-IEC 27001:2013, los cuales se detallan a continuación:

Numerales de la Norma Ntc-Iso-Iec 27001:2013

- Numeral 4 -Contexto de la organización
- Numeral 5 –Liderazgo
- Numeral 6 –Planificación
- Numeral 7 –Soporte

- Numeral 8 –Operación
- Numeral 9 -Evaluación de desempeño
- Numeral 10 –Mejora

Dominios del Anexo A de la Norma Ntc-Iso-Iec 27001:2013

- A.5. Políticas de Seguridad de la Información.
- A.6. Organización de la Seguridad de la Información.
- A.7. Seguridad de los Recursos Humanos.
- A.8. Gestión de Activos.
- A.9. Control de Acceso.
- A.10. Criptografía.
- A.11. Seguridad Física y del Entorno.
- A.12. Seguridad de las Operaciones.
- A.13. Seguridad de las Comunicaciones.
- A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas.
- A.15. Relaciones con los Proveedores
- A.16. Gestión de Incidentes de Seguridad de la Información
- A.17. Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio.
- A.18. Cumplimiento.

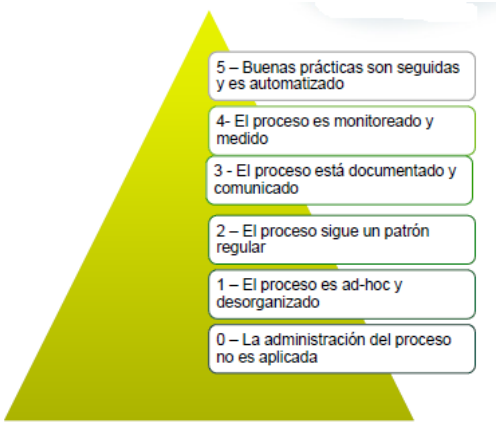
Metodología Utilizada para el Diagnóstico

Se utiliza el modelo estándar Capability Matury Model (CMM) COBIT 4, que permite priorizar y mejorar las acciones de gobierno, prevención, detección, respuesta y recuperación.

El objetivo de lograr un nivel específico de madurez para la seguridad de la información se define como el estado deseado del control de seguridad. Esto implica calificar cada área definida en una escala que va del 0 al 5, dependiendo de la madurez de los procedimientos.

Figura 3

Modelo de Madurez Software Engineering ISO 27001:27001:2013



Nota. Modelo de madurez para la planificación, implementación, supervisión y mejora de un SGSI.

Resultados

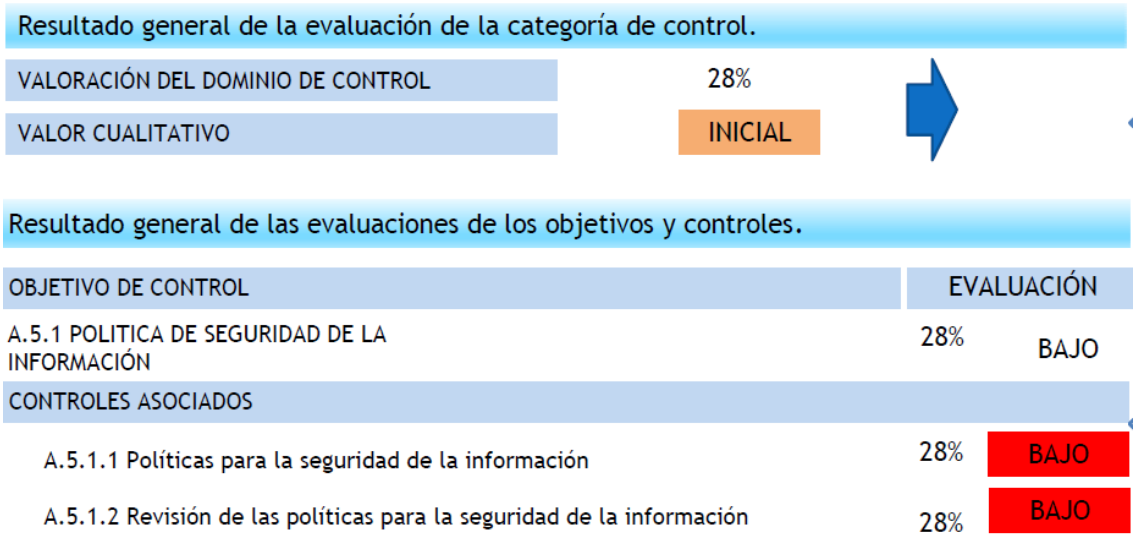
Indicaciones para el Entendimiento del Informe

Descripción de los resultados cualitativos y cuantitativos de los dominios o categorías de control, objetivos de control y controles correspondientes.

Indicaciones para el entendimiento del informe.

Figura 4

Indicaciones para el Entendimiento del Informe



Nota. Figura recuperada del PESI propuesto.

Como se puede observar en la figura No. 4 se presentan Información cuantitativa y cualitativa del control Evaluado, y la descripción del nivel de madurez de la categoría de control, además la Información cuantitativa y cualitativa de cada objetivo de control y sus correspondientes controles asociados.

Figura 5

Nivel de Madurez de los Controles Evaluados

Nota. Figura recuperada del PESI propuesto.

En la figura No. 5 se observa el grado en que los controles de una organización están formalizados, estandarizados, operando eficazmente y mostrando eficiencia y mejora continua, se describe cada nivel, y se relacionará con los niveles que arroje el GAP Analisys.

Nivel de Madurez General

Teniendo en cuenta la información proporcionada en las entrevistas realizadas, se obtuvo como resultado la siguiente valoración de los numerales del 4 al 10:

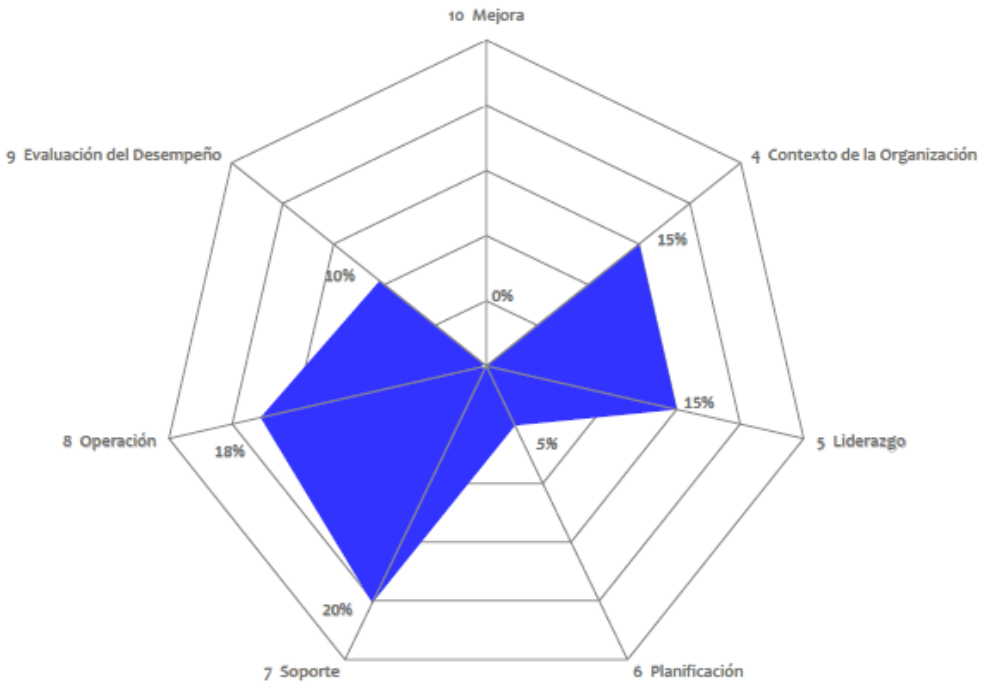
Numerales de la Norma Ntc-Iso-Iec 27001:2013

- Numeral 4 -Contexto de la organización.
- Numeral 5 –Liderazgo.
- Numeral 6 –Planificación.
- Numeral 7 –Soporte.

- Numeral 8 –Operación.
- Numeral 9 -Evaluación de desempeño.
- Numeral 10 –Mejora.

Figura 6

Nivel de Madurez General



Nota. Figura tomada del GAP Análisis Checklist 27001 – 27002.

Se puede evidenciar en la figura No. 6 el nivel de madurez general valorando los numerales del 4 al 10 en la Organización producto de las entrevistas ejecutadas.

A continuación, los porcentajes resultantes:

- Contexto de la Organización – 15%
- Liderazgo – 15%

- Planificación – 5%
- Soporte – 20%
- Operación – 18%
- Evaluación del desempeño – 10%
- Mejora – 0%

De acuerdo con la actividad realizada y teniendo en cuenta el resultado de las entrevistas, consignadas en el **"**GAP Análisis Checklist 27001 - 27002**"**, se obtiene el siguiente nivel de madurez relacionado al Sistema de Gestión de Seguridad de la Información – SGSI.

Figura 7

Nivel de Madurez - SGSI

Nota. Resultado del análisis de madurez – Gap Análisis Checklist 27001 – 27002.

La figura No. 7 muestra el porcentaje y nivel en que se ubica la Organización según el análisis realizado, el resultado promedio del nivel de madurez respecto a los requisitos específicos de los numerales 4 al 10 de la norma Ntc-Iso-Iec 27001:2013 es de 13,05%; lo anterior indica que aún no ha establecido, implementado, mantenido y mejorado continuamente el Sistema de Gestión de Seguridad de la información, así mismo no cuenta con información documentada que la norma Ntc-Iso-Iec 27001:2013 establece como requisito.

Hallazgos Generales

- No se cuenta con un marco de gestión estratégica, así como, sistemas de gestión ya implementados y certificados bajo estándar ISO, tal y como son (9001;45001 y 14001), a la fecha no se tiene definido un marco para la gestión de seguridad de la información.

- Se tiene establecido una política de seguridad de la información, sin embargo, está no se encuentra actualizada, comunicada y aprobada por la Alta Dirección.
- La Alta Dirección de la Empresas no tiene establecidos los roles y responsabilidades de Seguridad de la Información.
- Actualmente cuenta con Sistema de Gestión de Riesgos operativos por procesos, donde se identifican transversalmente riesgos tecnológicos, sin embargo, actualmente está no incluye aspectos de seguridad de información e impactos relativos a Confidencialidad, Integridad y Disponibilidad de la Información y que se asocien a los activos de información de cada proceso.
- No se evidencia un proceso formal de cultura y toma de conciencia de los colaboradores en relación con la Seguridad de la Información y Ciberseguridad.
- Se cuenta con indicadores generales de gestión para el proceso de gestión de tecnología, sin embargo, dichas mediciones no contemplan aspectos de Seguridad de la Información.

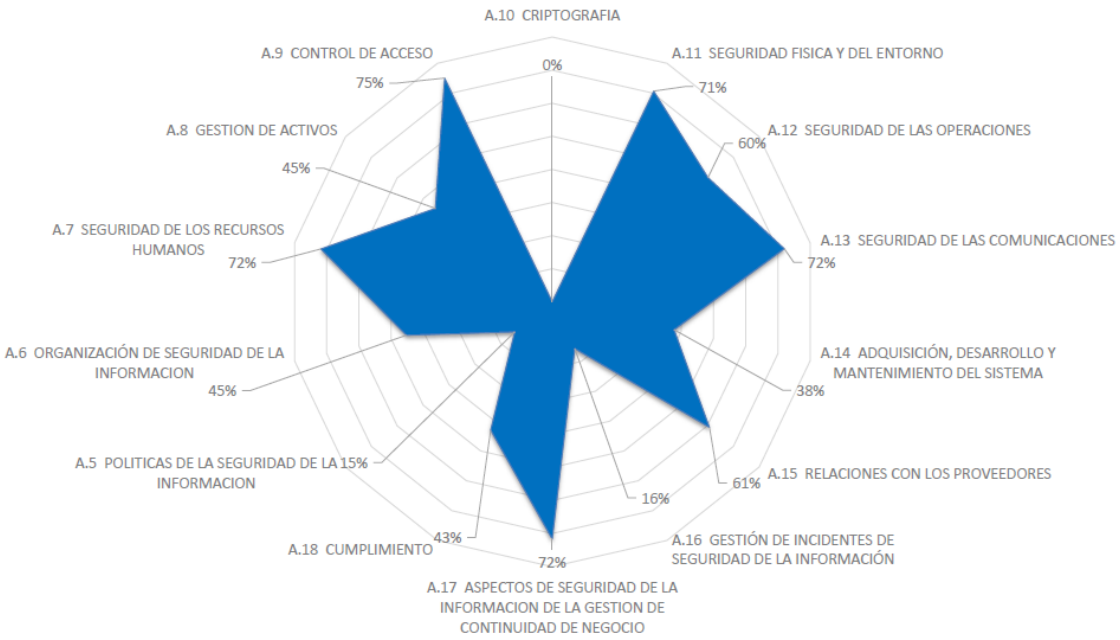
Valoración General

Dominios Anexo 5 - 18

Teniendo en cuenta la información proporcionada en las entrevistas realizadas, se obtuvo como resultado la siguiente valoración de los controles por cada uno de los dominios, así:

Figura 8

Nivel de Madurez - Dominios Anexo A / 5 -18



Nota. Figura tomada del GAP Análisis Checklist 27001 – 27002.

En la figura No. 8 se pueden observar las valoraciones obtenidas con respecto a los dominios 5 al 18 del Anexo A.

- A.5. Políticas de Seguridad de la Información – 15 %
- A.6. Organización de la Seguridad de la Información – 45 %
- A.7. Seguridad de los Recursos Humanos – 72 %
- A.8. Gestión de Activos – 45 %
- A.9. Control de Acceso – 75%
- A.10. Criptografía – 0 %

- A.11. Seguridad Física y del Entorno – 71 %
- A.12. Seguridad de las Operaciones – 60 %
- A.13. Seguridad de las Comunicaciones – 72 %
- A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas – 38 %
- A.15. Relaciones con los Proveedores – 61 %
- A.16. Gestión de Incidentes de Seguridad de la Información – 16 %
- A.17. Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio – 72 %
- A.18 Cumplimiento – 43 %

Teniendo en cuenta la información proporcionada de manera en las entrevistas realizadas, se obtuvo como resultado el siguiente nivel de madurez:

Figura 9

Nivel de Madurez

OBJETIVO DE CONTROL	CUANTITATIVO	ESCALA	Nivel de Madurez
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	15,0 %	0	Inexistente
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	45,33%	2	Repetible
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	71,81%	3	Definido
A.8 GESTION DE ACTIVOS	45,28%	2	Repetible
A.9 CONTROL DE ACCESO	75,03%	3	Definido
A.10 CRIPTOGRAFIA	0,00%	0	Inexistente
A.11 SEGURIDAD FISICA Y DEL ENTORNO	70,69%	3	Definido
A.12 SEGURIDAD DE LAS OPERACIONES	60,24%	3	Definido
A.13 SEGURIDAD DE LAS COMUNICACIONES	72,00%	3	Definido
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA	37,78%	1	Inicial
A.15 RELACIONES CON LOS PROVEEDORES	60,83%	3	Definido
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	15,71%	0	Inexistente
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO	71,67%	3	Definido
A.18 CUMPLIMIENTO	43,00%	2	Repetible

Nota. Figura tomada del GAP Análisis Checklist 27001 – 27002.

Figura 10

Nivel de Madurez Dominios – Propanogas S.A.S E.S.P

Nota. Resultado del análisis de madurez – Gap Análisis Checklist 27001 – 27002.

Según lo mostrado en la figura No. 9 y de acuerdo con la actividad realizada y teniendo en cuenta el resultado de las entrevistas, consignadas en el "GAP ANÁLISIS CHECKLIST 27001-27002", se obtiene el siguiente nivel de madurez para Propanogas S.A.S E.S.P

La figura No. 10 muestra el resultado en términos de % de la actividad realizada y teniendo en cuenta el resultado de las entrevistas, consignadas en el "GAP ANÁLISIS CHECK LIST 27001-27002", se obtiene el siguiente nivel de madurez para Propanogas S.A.S E.S.P.

Los controles y los procesos se rigen por un patrón normal. Los procesos han evolucionado hasta llegar a una etapa en la que diversas personas de un área determinada siguen diferentes procedimientos. No existe capacitación ni comunicación formal acerca de los estándares y procedimientos. Se confía mucho en lo que cada individuo sabe, por lo que existe la posibilidad de errores.

Hallazgos Generales

- Todos los procesos evaluados tienen una orientación muy clara al negocio y están liderados por personal de altísimas calidades profesionales, que tienen muy claras las funciones y compromiso con la Organización y es indispensable que se vayan acercando al compromiso con la seguridad de la información.

- Al momento de realizar este diagnóstico - GAP Analysis, no cuenta con un Sistema de Gestión de Seguridad de la Información definido e implementado; sin embargo, desde el punto de vista técnico y procedimental cuentan con controles de seguridad básicos y evidencias buenas prácticas de seguridad informática. Se identifica que en su mayoría los controles y buenas prácticas relativas a aspectos de seguridad y privacidad de la información se han realizado de manera centralizada por el área de tecnología.
- Se puede evidenciar que se reconoce oportunidades de mejora las cuales se deben implementar, sin embargo, no se encuentran procesos estandarizados de seguridad de la información que aseguren la integración, mantenimiento y mejora de requisitos de un Sistema de Gestión de Seguridad de la Información SGSI.
- Los riesgos que actualmente gestionan y que han sido identificados, valorados y tratados corresponden a los riesgos operativos, no obstante, se deben identificar riesgos que puedan afectar la Seguridad de la Información, teniendo en cuenta la integridad, disponibilidad y confidencialidad de esta.
- Actualmente la Organización se encuentra en el desarrollo de varias iniciativas y proyectos de alto nivel definidas “Plan Estratégico de Tecnología de la Información y Comunicación – PETIC”; lo que constituye una oportunidad para la interacción de los lineamientos de Seguridad de la Información.
- La Organización no cuenta con un proceso de toma de conciencia relacionado a la seguridad de la información, por lo tanto, es indispensable diseñar e implementar mecanismos de concientización sobre el Sistema de Gestión de Seguridad de la Información.

- Para los Dominios evaluados: Políticas de Seguridad de la Información, Gestión de Activos, Criptografía, Gestión de Incidentes de Seguridad de la Información, la Organización no cuenta con políticas, procesos y procedimientos formales diseñados e implementados, con el fin de dar cumplimiento a lo exigido en la norma NTC-ISO-IEC 27001:2013.
- Se resalta la documentación de los planes de continuidad operativos y el Plan de Recuperación de Desastres lo que garantiza la disponibilidad tanto de las operaciones del negocio como de los sistemas de información críticos de la organización ante escenarios de eventos disruptivos, se sugiere la ejecución de pruebas a dichos planes y la validación de controles de seguridad de la información. Así como establecer contingencias para escenarios de amenazas tecnológicas o cibernéticas.

Análisis de Resultados por Dominios

En el encabezado del Anexo A donde se evidencia el desarrollo del control A.5.1.1 concerniente a: Políticas para la seguridad de la información.

El desarrollo de los demás controles de la norma se puede explorar en el Anexo A - Gap Análisis Checklist 27001-27002 junto con los demás apartados derivados del diagnóstico.

Figura 12

Control A.5.1.1 Políticas para la Seguridad de la Información

Num	Control y Controles		Respuesta	Porcentaje	Cumplimiento	Escala	Nivel de Madurez
A.5	POLITICAS DE LA SEGURIDAD DE LA INFORMACION				14,58%	0	Inexistente
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información				14,58%	0	Inexistente
A.5.1.1	Políticas para la seguridad de la información	La Organización cuenta con un documento de política(s) de Seguridad de la Información	Parcial	70%	21,67%	1	Inicial
		Existe normativa relativa a la Seguridad de la Información	Parcial	30%			
		Existen procedimientos relativos a la Seguridad de la Información	Parcial	30%			
		Existen mecanismos para la comunicación a los usuarios de la política	No	0%			
		La política ha sido publicada y comunicada a todos los empleados y partes externas pertinentes	No	0%			
		La política de Seguridad de la Información esta aprobada por la dirección	No	0%			

Nota. Se observa el resultado de la valoración por dominio específicamente del A.5

Derivándose este en INEXISTENTE con un 15 %, evidenciándose que no hay procesos de control reconocidos, no se reconoce el problema y por ende la necesidad de su tratamiento.

Diseño del Plan Estratégico de Seguridad de la Información

Conscientes de la protección y aseguramiento de los datos, es necesario examinar y dar el visto bueno a los asuntos de alto nivel relacionados con la seguridad de la información. Para esto, se debe establecer un Plan Estratégico de Seguridad de la Información (PESI), que es el producto del diagnóstico GAP y contempla una proyección estratégica a corto, mediano y largo plazo. Además, este plan necesita ser renovado cada año debido a las variaciones en las estrategias del sector, de la organización, así como por el avance en amenazas, vulnerabilidades y tendencias tecnológicas.

El plan de seguridad informática incluye un conjunto de tácticas y acciones destinadas a garantizar la operatividad, el perfeccionamiento constante y la sostenibilidad del Sistema de Gestión de Seguridad Informativa.

Modelo de Implementación de Seguridad de la Información

El modelo de seguridad de la información para Propanogas S.A.S E.S.P, se establece basados en el ciclo de mejora continua definido para implementar mantener, evaluar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Figura 14

Ciclo de Mejora Continua

Nota. Fases fundamentales que se repiten en espiral para elevar los estándares de calidad.

La figura No. 12 muestra el ciclo de mejora contina definido para implementar, mantener, evaluar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

El modelo de seguridad de la información para Propanogas S.A.S E.S.P, se estructura según la definición estratégica del Sistema de Gestión de Seguridad de la Información ISO 27001:2013

Fases

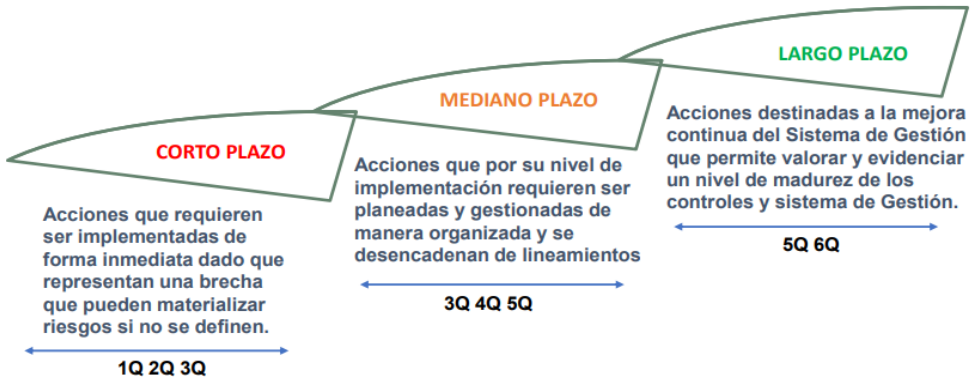
- Fase de diagnóstico: Identificar el estado Actual de Propanogas S.A.S E.S.P con respecto a la seguridad de la información.
- Fase de planeación: numerales 4,5,6 y 7: Durante esta etapa, se definen los objetivos que se quieren lograr y las actividades del proceso que pueden mejorarse. También se determinan los indicadores de medición para controlar y cuantificar dichos objetivos.
- Fase de implementación - numerales 8- requisitos anexo A: La organización tiene que planear, poner en marcha y supervisar los procedimientos requeridos para satisfacer las metas y demandas de seguridad, así como para realizar la evaluación y el tratamiento de los riesgos relacionados con la seguridad de la información.
- Fase evaluación del desempeño: numeral 9: Condiciones necesarias para el análisis periódico de la eficiencia del sistema de gestión de seguridad de la información y del rendimiento en términos de seguridad de la información.
- Fase de mejora continua: numeral 10: Proceso de optimización del modelo de seguridad de la información, que consiste en determinar las medidas más eficaces para resolver las no conformidades que surjan y analizar lo que se necesita hacer para erradicar sus causas con el fin de evitar su repetición.

Despliegue de Iniciativas Seguridad de la Información

El Plan Estratégico en Seguridad de la Información pretende identificar los objetivos y actividades que de manera estratégica dan cumplimiento a las 16 iniciativas establecidas, según las prioridades y objetivos del negocio, para que sean evaluadas y desarrolladas, para así mismo asegurar la reducción de los impactos adversos en la organización. Cada objetivo tiene un nivel de cumplimiento en corto, mediano y largo plazo.

Figura 17

Plazos de Ejecución de la Implementación - PESI



Nota. Estructura en fases clave basadas en el ciclo de mejora continua.

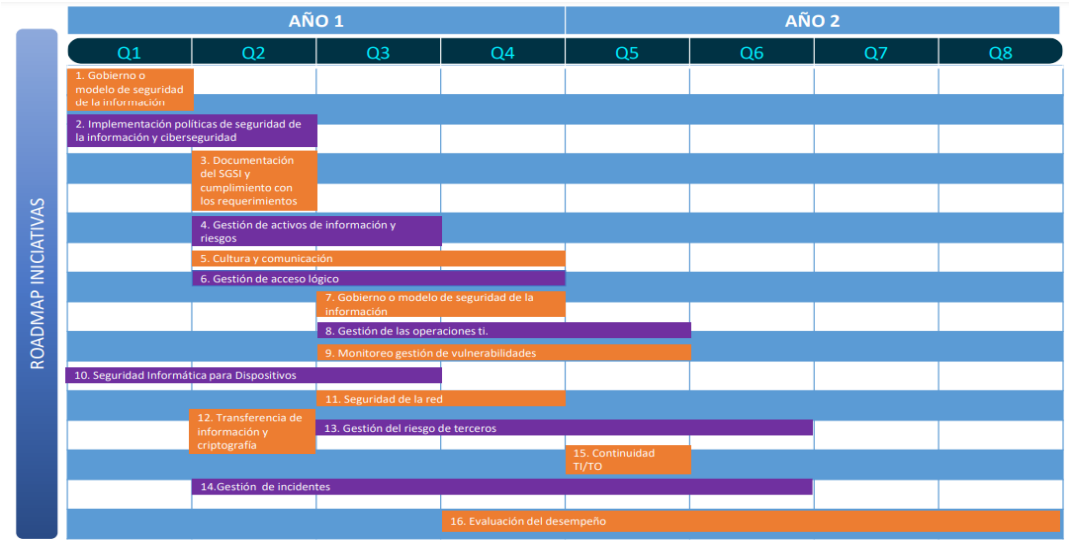
La figura No. 13 muestra la descripción de las acciones que se requieren a corto, mediano y largo plazo según prioridad y objetivos de la Organización.

Iniciativas Seguridad de la Información

Tomando en consideración, el estado de la seguridad de la información en Propanogas S.A.S E.S.P, haciendo una extracción de dicho modelo hacia seguridad de la información, se puede considerar que, para la organización, obtener un estado de madurez aceptable, tanto a nivel de Seguridad de la Información como el cumplimiento de controles, se plantean 16 iniciativas enfocadas a dar cumplimiento en el corto y mediano plazo.

Figura 19

Control ROADMAP Iniciativas



Nota. Control PESI – Propuesto.

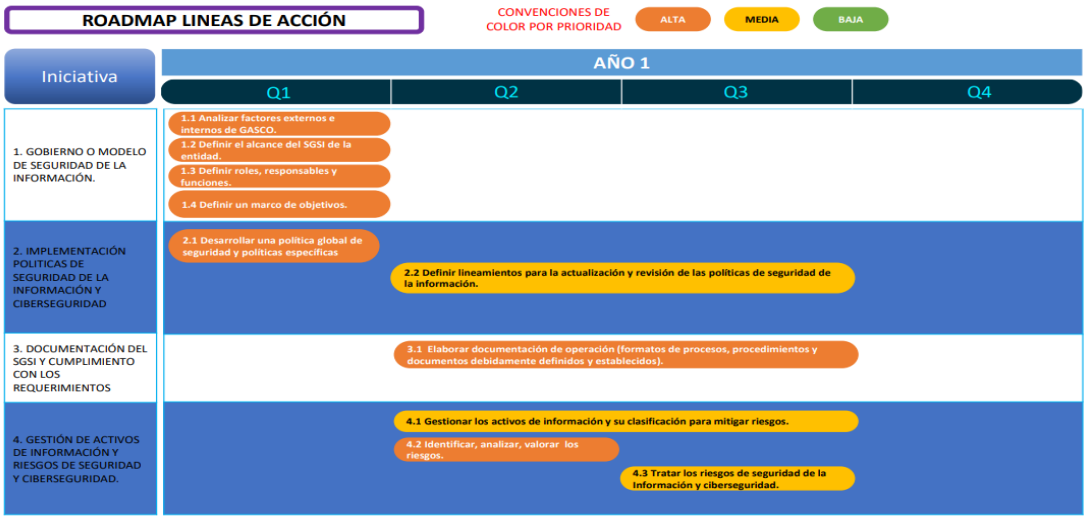
En la figura No. 14 se pueden observar el ROADMAP de 16 iniciativas que se desarrollarán en periodos de Q en un total de 2 años. Se desarrollarán según prioridad y objetivos planteados por la Organización:

- Gobierno o modelo de seguridad de la información.
- Implementaciones políticas de seguridad de la información y ciberseguridad
- Documentación del SGSI y cumplimiento con los requerimientos
- Gestión de activos de información y riesgos
- Cultura y comunicación
- Gestión de acceso lógico
- Gobierno o modelo de seguridad de la información
- Gestión de las operaciones TI.
- Monitoreo gestión de vulnerabilidades

- Seguridad Informática para Dispositivos
- Seguridad de la red
- Transferencia de información y criptografía
- Gestión del riesgo de terceros
- Gestión de incidentes
- Continuidad TI/TO
- Evaluación del desempeño

Figura 21

Control - Líneas de Acción ROADMAP

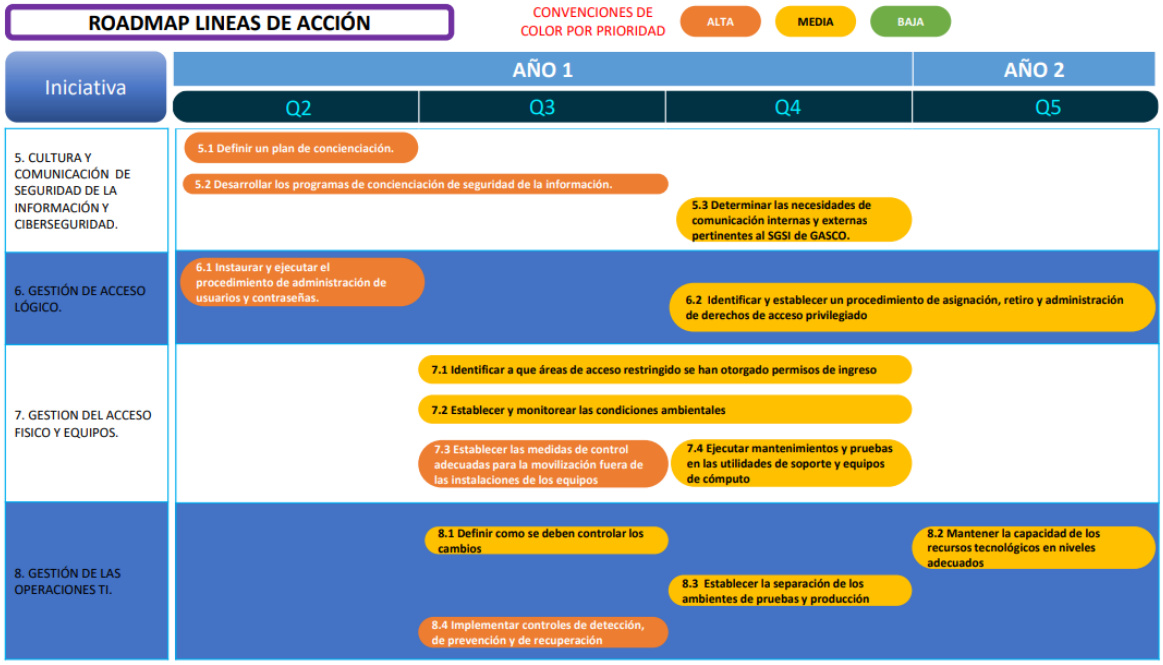


Nota. Control PESI – Propuesto.

En la figura No. 15 se pueden observar las líneas de acción para las primeras 4 iniciativas del ROADMAP General, se desarrollarán según prioridad y objetivos planteados por la Organización.

Figura 25

Control - Líneas de Acción ROADMAP

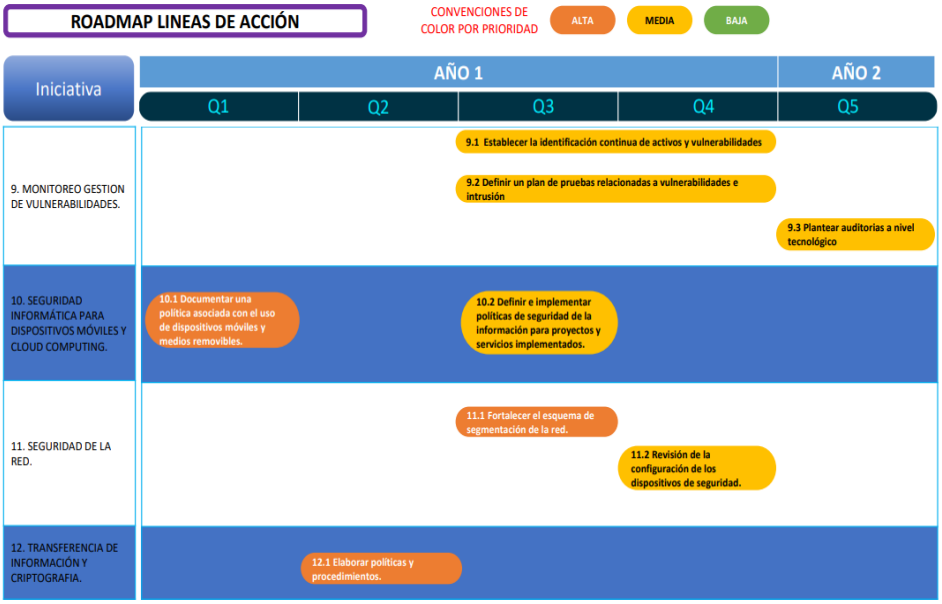


Nota. Control PESI – Propuesto.

En la figura No. 16 se pueden observar las líneas de acción para las iniciativas 5 a la 8 del ROADMAP General, se desarrollarán según prioridad y objetivos planteados por la Organización.

Figura 28

Control - Líneas de Acción ROADMAP

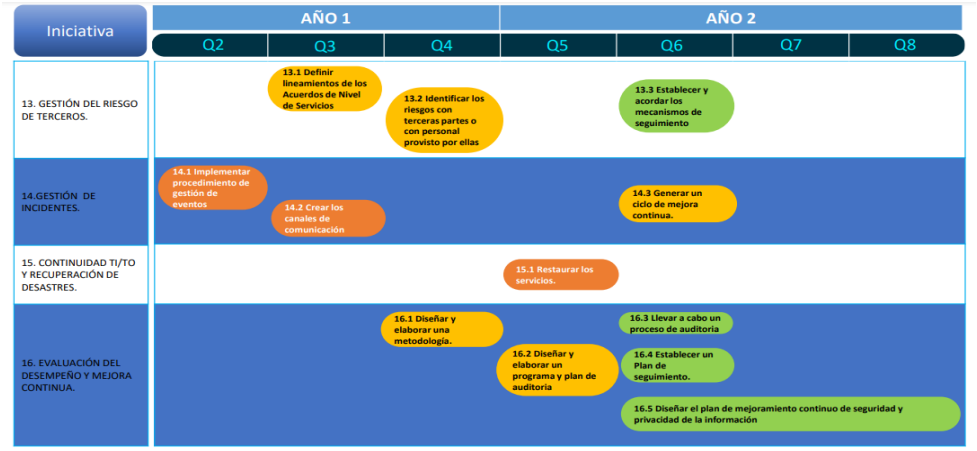


Nota. Control PESI – Propuesto.

En la figura No. 17 se pueden observar las líneas de acción para las iniciativas 9 a la 12 del ROADMAP General, se desarrollarán según prioridad y objetivos planteados por la Organización.

Figura 31

Control - Líneas de Acción ROADMAP



Nota. Control PESI – Propuesto.

En la figura No. 18 se pueden observar las líneas de acción para las iniciativas 13 a la 16 del ROADMAP General, se desarrollarán según prioridad y objetivos planteados por la Organización.

La organización tiene que planear, poner en marcha y supervisar los procedimientos requeridos para satisfacer las metas y demandas de seguridad, así como para realizar la evaluación y el tratamiento de los riesgos relacionados con la seguridad de la información.

Para esta fase se desarrollarán las iniciativas propuestas en el ROADMAP DE INICIATIVAS y sus LÍNEAS DE ACCIÓN para cada AÑO, TRIMESTRE y su nivel de PRIORIDAD de ejecución.

A continuación, se presentan los avances de la puesta en marcha de la implementación basados en el ROADMAP DE INICIATIVAS:

Desarrollo del Roadmap

Iniciativa Número 1

Gobierno y modelo de seguridad de la información – Prioridad alta.

Línea de acción # 1: Analizar factores externos e internos de Propanogas S.A.S E.S.P.

Resultado: Los factores externos e internos fueron analizados basados en el GAP Análisis encontrando que:

- Todos los procesos evaluados tienen una orientación muy clara al negocio y están liderados por personal de altísimas calidades profesionales, que tienen muy claras las funciones y compromiso con la Organización y es indispensable que se vayan acercando al compromiso con la seguridad de la información.
- Se puede evidenciar que se reconoce oportunidades de mejora las cuales se deben implementar, sin embargo, no se encuentran procesos estandarizados de seguridad de la información que aseguren la integración, mantenimiento y mejora de requisitos de un Sistema de Gestión de Seguridad de la Información SGSI.
- Los riesgos que actualmente gestionan y que han sido identificados, valorados y tratados corresponden a los riesgos operativos, no obstante, se deben identificar riesgos que puedan afectar la Seguridad de la Información, teniendo en cuenta la integridad, disponibilidad y confidencialidad de esta.
- Actualmente la Organización se encuentra en el desarrollo de varias iniciativas y proyectos de alto nivel definidas “Plan Estratégico de Tecnología de la Información y Comunicación – PETIC”; lo que constituye una oportunidad para la interacción de los lineamientos de Seguridad de la Información.

Línea de acción # 2: Definir el alcance del SGSI de la entidad.

Para esta iniciativa se tienen los siguientes avances:

Se define el ALCANCE del Sistema de gestión de Seguridad de la información, este se encuentra en el Modelo de SGSI de Propanogas S.A.S E.S.P, documento que se encuentra en construcción.

Este documento tiene como finalidad establecer, implementar, mantener y mejorar, la Seguridad y Privacidad de la Información digital en Propanogas S.A.S E.S.P, para todos sus procesos identificando sus activos críticos, implementando controles y gestionando los riesgos de seguridad.

Los lineamientos y directrices aquí establecidas son de obligatorio cumplimiento en todos los niveles; su omisión podrá conllevar a sanciones disciplinarias y/o acciones legales según sea el caso.

Las actividades y controles implementados son accionados de manera diligente siendo su naturaleza de medios y no de resultados.

Línea de acción # 3: Definir Roles, Responsables y Funciones

Para esta línea de acción se crea el comité del SGSI, grupo interdisciplinario que está encargado de Implementar, monitorear, gestionar y mejorar el sistema de la Organización garantizando la confidencialidad, disponibilidad e integridad de la información; y la protección de datos personales de las contrapartes.

El equipo está conformado por:

- Gerente Administrativa y Financiera.
- Gerente de Auditoría y Compliance.
- Director de Tecnología.
- Jefe de Compliance

- Profesional de Compliance
- Jefe de Riesgos
- Líder de Proyectos de IT
- Coordinador de Informática.

Se definen los responsables y sus funciones así:

- Gerencia General
- Aprobar el SGSI y política general.
- Promover y promulgar la política general.
- Destinar los recursos necesarios para su efectiva implementación.
- Exigir el cumplimiento del SGSI y su regulación interna.

Gerencias y Líderes de Procesos

- Manejar la distribución de los recursos y el personal requeridos para poner en marcha el Sistema de Gestión de Seguridad de la Información (SGSI) en sus Planes administrativos y operativos.
- Cumplir y hacer cumplir en sus áreas el SGSI.
- Reportar cualquier omisión al SGSI sin importar nivel del cargo.

Comité SGSI

- Fomentar y administrar la aplicación de estándares y buenas prácticas en materia de seguridad digital en la organización.
- Elaborar informes que midan el progreso de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información.

- Administrar, conservar y documentar el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización.
- Fomentar la administración de seguridad de la información en los procedimientos y en la cultura organizacional.
- De acuerdo con los requisitos del SGSI, propagar la relevancia de una gestión eficaz de la seguridad de la información a las partes interesadas.
- Asegurar que se logre los resultados previstos del SGSI, con un enfoque de mejora continua del referido sistema.
- Dirigir y apoyar a las personas y a los otros roles relevantes para que contribuyan con la efectividad del SGSI.

Todos los Colaboradores

- Implementar en todas sus funciones lo establecido en el SGSI, políticas, procedimientos y cualquier otro.
- Reportar cualquier omisión al SGSI sin importar nivel del cargo a las
- Políticas y procedimientos relacionados con el SGSI.
- Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- La Compañía establecerá a criterio las políticas, procedimientos, instructivos o cualquier otro necesario para hacer efectivo el SGSI.

Iniciativa Número 2

Implementaciones Políticas de Seguridad de la Información y Ciberseguridad.

Línea de acción # 1: Desarrollar una Política Global de Seguridad y Políticas Específicas

Resultado: Se analiza, redacta y publica la Política de Gestión de Seguridad de la Información de la Organización, a continuación, el texto:

Para Propanogas S.A.S E.S.P, como organización responsable de soluciones energéticas, líder en el ámbito energético con un modelo de negocio que integra actividades de aprovisionamiento, gestión logística y comercializadora de gas, Es consciente de que la información es un activo clave para brindar servicios y tomar decisiones eficaces. Por lo tanto, ha asumido el compromiso de salvaguardar la confidencialidad, integridad y disponibilidad, además de gestionar los riesgos relacionados con la seguridad digital, la continuidad del negocio y el establecimiento de una cultura de seguridad dentro de la organización.

Por lo que todos los colaboradores internos de la organización, tanto personas naturales como jurídicas, tendrán la responsabilidad de cumplir las políticas, controles, normas, procedimientos y estándares vigentes en relación con la seguridad de la información. Esto posibilitará determinar y reducir al mínimo los riesgos a los que está expuesta dicha información e instaurar una cultura de seguridad que asegure el cumplimiento de los requerimientos legales, contractuales y técnicos mediante la implementación de las mejores prácticas.

Con la finalidad de proteger la información de los procesos de negocio, en cumplimiento con la normativa vigente y en línea con los objetivos estratégicos de la Organización, la Alta Dirección de Propanogas S.A.S E.S.P, en nombre de todos los colaboradores de la Empresa, se compromete a:

1. Establecer, implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información - SGSI alineado a estándares internacionales.

2. Garantizar la confidencialidad, disponibilidad e integridad de la información significativa de la organización y grupos de interés, según corresponda.

3. Acatar los requisitos legales y otros suscritos aplicables concernientes a la seguridad de la información.

4. Desarrollar acciones de tipo formativo necesarias relativas a la seguridad de la información para nuestros colaboradores.

5. Garantizar que nuestros procesos y sistemas de gestión estén orientados a la mejora continua.

Se han analizado, redactado y publicado las siguientes políticas específicas:

- Política de uso adecuado de correo electrónico corporativo.
- Política de uso de contraseñas.
- Política de uso de equipos móviles corporativos.

Para las demás iniciativas y líneas de acción la Organización continúa trabajando en su desarrollo, basándose en su prioridad e interés se avanzará con apoyo del Comité de Seguridad de la Información y demás responsables.

Conclusiones

Es de considerar la Seguridad de la Información bajo el modelo de mejoramiento continuo tomando como base los Sistemas ya implementados y certificados por la organización, lo que no necesariamente desprende al corto plazo un incremento en su nivel de madurez y el cumplimiento de los requisitos de la norma NTC-ISO-IEC 27001: 2013 y su Anexo A, ya que el cierre de las brechas identificadas en este análisis se desprende de una decisión que compete a Propanogas S.A.S E.S.P, teniendo en cuenta recursos financieros, humanos y operativos.

Propanogas S.A.S E.S.P al momento de realizar este diagnóstico, no cuenta con un Sistema de Gestión de Seguridad de la Información definido e implementado; sin embargo, desde el punto de vista técnico y procedimental cuentan con controles de seguridad básicos.

Se identifica que en su mayoría los controles y esfuerzos relativos a aspectos de seguridad y privacidad de la información se centran en el proceso Core del negocio, sin embargo, no se tienen estandarizados y gestionados dichos aspectos para las áreas o procesos de apoyo.

Es importante realizar la formalización de políticas y procedimientos que se realizan en la actualidad, con el fin de socializarlos y que el Know How (Saber cómo hacer) que tienen los colaboradores dentro de su conocimiento quede formalizado, y estén alineados con Seguridad de la Información.

El área de Tecnología Informática ha ido adquiriendo una importancia representativa en Propanogas S.A.S E.S.P, lo cual es esencial en el esquema de gobierno corporativo y particularmente en los aspectos relacionados con los servicios brindados dentro del negocio. La dirección del modelo de gestión y el compromiso de la alta dirección, dan una muestra de respaldo y liderazgo en la compañía frente a los aspectos relacionados con Tecnología Informática, es indispensable que todos los lineamientos y directrices que se definan para un

Sistema de Gestión de Seguridad de la Información, se desarrollen transversalmente a todos los procesos definidos en la Cadena de Valor de la organización, involucrar a todos los colaboradores en el cumplimiento de las políticas y procedimientos que se van a definir para Seguridad de la Información.

Con el Sistema de Gestión de Seguridad de la Información ya implementada y en funcionamiento, se puede establecer un principio de apropiación del sistema de gestión de ciberseguridad, conforme a lo establecido por el estándar ISO 27032:2012 y la NIST Cibersecurity Framework.

Recomendaciones

Es necesario identificar y documentar de manera explícita todos los requisitos contractuales, reglamentarios y estatutarios relevantes, así como la perspectiva de la organización para cumplirlos. Además, se deben mantener actualizados para cada sistema informático y para la entidad.

Para garantizar el cumplimiento de las exigencias contractuales, legislativas y reglamentarias que tienen que ver con los derechos de propiedad intelectual y la utilización de productos de software patentados, es necesario poner en marcha procesos adecuados.

Conforme a las exigencias legislativas, reglamentarias, contractuales y comerciales, es necesario salvaguardar los registros de la pérdida, el borrado, la falsificación, el acceso no autorizado y la divulgación no autorizada.

Se considera relevante diseñar, documentar, implementar, formalizar y evaluar el Sistema de Gestión de Seguridad de la Información en el menor tiempo posible, definiendo mecanismos de seguimiento y control que permitan un sostenimiento y mejora continua. Considerando, además, las iniciativas y proyectos que se encuentran en curso en Propanogas S.A.S E.S.P, con el fin de integrar y trabajar transversalmente en el contexto actual de la organización.

Referencias Bibliográficas

Banco Santander, (n.d.-a). *¿Qué es la integridad de los datos?*

Banco Santander, (n.d.-b). *¿Qué es la integridad de los datos?* Retrieved October 11, 2024, from: https://www.bancosantander.es/glosario/integridad-seguridad-online

CAF. (2017).) *El gobierno corporativo debe entenderse como un medio, no el único, para contribuir al fortalecimiento y sostenibilidad de la empresa. Banco De Desarrollo de América Latina y El Caribe.*

Calderón Laura, (2015). *Seguridad informática y seguridad de la información*. http://polux.unipiloto.edu.co:8080/00002658.pdf

Citrix. (n.d.). *Estrategias de seguridad para el Éxito.* Retrieved October 11, 2024, from https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/security-leadership-series-security-strategies-for-success-es.pdf

Computerword. (n.d.). *¿Qué es la seguridad de la red?* Retrieved October 11, 2024, from https://www.computerworld.es/seguridad/que-es-la-seguridad-de-la-red

Danilo, (2018). *Gobernanza de las tecnologías de la información.* https://es.linkedin.com/pulse/gobernanza-de-las-tecnolog%C3%ADas-la-informaci%C3%B3n-danilo-antunez

De León, (2020). *Estadística de las Normas ISO más Implementadas a Nivel Mundial. R&D Consulting.* https://www.rd.com.pa/2020/09/22/estadistica-de-las-normas-iso-mas-implementadas-a-nivel-mundial/

Ecured. (n.d.). *Auditoría de sistemas*. Retrieved October 11, 2024, from https://www.ecured.cu/Auditor%C3%ADa_de_sistemas

Eduba. (n.d.). *Activos de Información.* Retrieved October 11, 2024, from https://eduba.gov.co/index.php/eduba/gestion-documental/activos-de-informacion

Emagister. (2021). *ITIL: Qué es y cómo funciona*. https://www.emagister.com/blog/que-es-itil/

Esan, (2018). *Sistema de Gestión de Seguridad Informática: ¿por qué es útil y cómo se aplica?* https://www.esan.edu.pe/conexion-esan/sistema-de-gestion-de-seguridad-informatica-por-que-es-util-y-como-se-aplica

Escobar Carolina, (2021). *¿Qué es una suplantación de identidad digital y cómo puede afectarte?* https://colnodo.apc.org/es/experiencias/que-es-una-suplantacion-de-identidad-digital-y-como-puede-afectarte#:~:text=La%20suplantaci%C3%B3n%20de%20identidad%20digital,la%20confianza%20que%20se%20genera

Eset. (n.d.). *¿Qué es el antivirus?* Retrieved October 11, 2024, from https://www.eset.com/es/caracteristicas/antivirus-software-que-es/

INCIBE. (2019). *Medidas de prevención contra ataques de denegación de servicio*.

Ingenio learning. (2021). *¿Qué es Ethical Hacking?* https://ingenio.edu.pe/blog/que-es-ethical-hacking-y-por-que-estudiarlo-en-2021/

IONOS. (2023). *GAP Analysis. ¿Qué es el GAP Analysis?* https://www.ionos.es/startupguide/gestion/gap-analysis/

IsoTools. (2019). *Software ISO Riesgos y Seguridad. ¿Qué es la ISO 27001?* https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Kaspersky. (n.d.-a). *Ingeniería Social.* Retrieved October 11, 2024, from https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kaspersky. (n.d.-b). *¿Qué es la ciberseguridad?* Retrieved October 11, 2024, from https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

McAfee. (n.d.). *¿Qué son los firewalls de hardware?* Retrieved October 11, 2024, from https://www.mcafee.com/es-co/antivirus/firewall.html#:~:text=Los%20firewall%20son%20programas%20de,de%20su%20conexi%C3%B3n%20a%20Internet.

Microsoft. (n.d.). *Protéjase del Phishing*. Retrieved October 11, 2024, from https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-

Ministerio de las TIC. (n.d.). *Diseño e implementación de una estrategia de seguridad de la información.* Retrieved October 11, 2024, from https://www.mintic.gov.co/arquitecturati/630/articles-9483_recurso_pdf.pdf

Peltier Thomas, (2005). *Information Security Risk Analysis*. https://www.academia.edu/40140524/Information_security_risk_analysis_thomas_r_peltier

Soler Lluís, (n.d.). *Que es un software de Seguridad Informática.* Retrieved October 11, 2024, from https://www.softwaredoit.es/software-seguridad/index.html

Tipton Harold, & Krause Micki. (2006). *Information Security Management Handbook.* https://engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf

Unir. (2020a). *¿Cómo incrementar la seguridad Informática?* https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

Unir. (2020b). *¿Cómo incrementar la seguridad Informática?* https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

Unir. (2021). *Informática forense: en qué consiste, ámbitos de aplicación y perfiles profesionales*. https://www.unir.net/ingenieria/revista/informatica-forense/

Universidad Libre. (2015). *Seguridad de la información*. https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-

Universidad Nacional de Colombia. (2020). *¿Qué es la criptografía y cómo incide en la seguridad informática?* https://unperiodico.unal.edu.co/pages/detail/que-es-la-criptografia-y-como-incide-en-la-seguridad-informatica/

Universidad VIU. (2016). *Cómo crear un plan de seguridad informática fácilmente*.

Pineda, L. C. (n.d.). *El modelo Deming (PHVA) como estrategia competitiva para realzar el potencial administrativo*.

Apéndices

Apéndice A

Gap Análisis Check List 27001-27002

Link: *https://docs.google.com/spreadsheets/d/1AQDQty6Jo3x22IxOvFng81tN2HtqaH-H/edit?usp=sharing&ouid=114301552232655257099&rtpof=true&sd=true*