Unidad 1
Sistema de gestión de seguridad de la información

Normas de seguridad

UNIVERSIDAD MAYOR
para espíritus emprendedores

Introducción

La seguridad de la información es fundamental en las organizaciones actuales debido a varios factores. En primer lugar, la evolución de la tecnología ha generado un entorno cada vez más virtual y digitalizado, lo que ha provocado el aumento en la cantidad de datos sensibles y la complejidad y necesidad de protegerlos.

Además, la seguridad de la información es crucial para proteger los activos, la reputación y la imagen de una organización, así como para cumplir con las expectativas y regulaciones tanto internas como externas.

Para proteger la información al interior de las organizaciones, es importante tener en cuenta varios aspectos:

1. **Implementar un sistema de gestión de seguridad de la información.**
2. **Conocer la normativa aplicable.**
3. **Identificar los activos y riesgos.**
4. **Promover una cultura de seguridad.**
5. **Utilizar herramientas y tecnologías adecuadas.**
6. **Capacitar al personal.**
7. **Mantener la seguridad de manera continua.**

Para resguardar la seguridad de la información, es necesario implementar un sistema de gestión de seguridad, cumplir con la normativa, identificar riesgos, promover una cultura de seguridad, utilizar herramientas adecuadas, capacitar al personal y mantener la seguridad de manera continua. De esta manera se protegen los activos y la reputación de una organización en un entorno cada vez más digitalizado.

1. Seguridad de la información en la actualidad

Para proteger la información al interior de las organizaciones, es importante tener en cuenta varios aspectos:

- **Implementar un sistema de gestión de seguridad de la información:** establecer un sistema estructurado y documentado para gestionar y proteger la información de la organización.

- **Conocer la normativa aplicable:** entender y cumplir con las regulaciones y normativas relacionadas con la seguridad de la información, tanto a nivel nacional como internacional.

- **Identificar los activos y riesgos:** identificar y clasificar los activos de información, así como analizar los riesgos a los que están expuestos, para poder implementar controles adecuados.

- **Promover una cultura de seguridad:** fomentar la conciencia y la responsabilidad en todos los niveles de la organización sobre la importancia de proteger la información y los activos de la empresa.

- **Utilizar herramientas y tecnologías adecuadas:** seleccionar y utilizar herramientas y tecnologías que ayuden a proteger la información de manera eficaz y eficiente, como firewalls, sistemas de detección de intrusiones, cifrado, entre otros.

- **Capacitar al personal:** proporcionar formación y capacitación regular sobre seguridad de la información para que todos los empleados estén familiarizados con las políticas, procedimientos y mejores prácticas de seguridad.

- **Mantener la seguridad de manera continua:** la seguridad de la información no es un evento único, sino un proceso continuo que requiere monitoreo constante, evaluaciones periódicas y actualizaciones según sea necesario.

Los tres pilares fundamentales que indica la norma ISO 27001 que se deben considerar para proteger los activos de una organización son: **confidencialidad, integridad y disponibilidad**. Revisemos a continuación cada uno de ellos:

Confidencialidad

Este pilar se refiere a garantizar que la información sensible esté protegida contra el acceso no autorizado. Es crucial restringir el acceso solo a aquellos usuarios que tienen el permiso adecuado para ver o manejar determinados datos. La confidencialidad se logra mediante la implementación de controles de acceso, cifrado y gestión de identidades, entre otros.

Integridad

La integridad se refiere a la precisión y la fiabilidad de la información. Es esencial asegurarse de que los datos no se vean comprometidos, alterados o corrompidos durante su almacenamiento, procesamiento o transmisión. Para garantizar la integridad de la información, se pueden implementar medidas como firmas digitales, control de versiones y técnicas de detección de manipulación de datos.

Disponibilidad

La disponibilidad implica asegurar que la información esté accesible y utilizable cuando sea necesario. Esto implica evitar interrupciones no planificadas en los sistemas y servicios que manejan la información crítica de la organización. Para garantizar la disponibilidad, se pueden implementar medidas como la redundancia de datos, la gestión de la capacidad y la planificación de la continuidad del negocio.

Es importante destacar que estos tres pilares no deben considerarse de forma independiente, sino como componentes interconectados de un enfoque integral de seguridad de la información. Además, en el contexto de la virtualidad y las comunicaciones en línea, es crucial adaptar las estrategias de seguridad para abordar los riesgos específicos asociados con los entornos digitales, como el ciberdelito, la

piratería informática y la fuga de datos. La seguridad de la información debe ser una prioridad constante y una parte integral de la cultura organizacional en la era digital.

2. Introducción al sistema de gestión de la información (SGSI)

Cuando hablamos de seguridad de la información, estamos refiriéndonos a aspectos puntuales, de un conjunto de actividades donde implementamos controles o procedimientos para proteger la información. Este sistema de Gestión de Seguridad de la Información debe estar alineado con otros sistemas de gestión de la organización y debe ser conocido por todos los funcionarios de la misma.

Un sistema de gestión debe tener un ciclo PHVA (Planificar-Hacer-Verificar-Actuar) como estrategia interactiva de resolución de problemas para mejorar procesos e implementar cambios. Además, debe implementar unos procesos de mejoramiento continuo, un liderazgo, condiciones y variables que permitan hablar de que es un sistema de gestión.

La seguridad de la información debe ser vista como un sistema de gestión global, y no como algo que está ahí aparte o que está definido solo para un grupo o para un sector en especial de la organización. Debe cubrir absolutamente a toda la organización dentro del sistema de gestión de seguridad.

Debemos tener en cuenta este alcance, ya que puede variar de acuerdo con el sector al que estamos haciendo referencia. Por ejemplo, en temas de seguridad, la información del sector financiero está muy digitalizado y virtualizado hoy en día, entonces necesita procesos robustos, digitales, y de ciberseguridad para proteger la información, mientras que en el sector de la construcción aún podemos ver que se maneja mucha información física.

Por lo tanto, hay que tener en cuenta esas diferencias para ver de qué manera debemos implementarlo en cada uno de los sectores, viendo que cada día los sectores están más interesados y las organizaciones están más conscientes de implementar seguridad de la información y de robustecer la ciberseguridad.

Se destacan varios puntos importantes sobre la relevancia y la importancia de la seguridad de la información en las organizaciones. A continuación, revisemos un resumen de los aspectos clave:

- **Contexto variado:** se debe reconocer que la seguridad de la información no tiene un enfoque único y que su implementación puede variar según el sector, el tamaño y los procesos de cada organización. Es necesario adaptar las estrategias de seguridad a las necesidades específicas de cada organización.
- **Evolución y conciencia:** se debe observar que, a lo largo del tiempo, las organizaciones han incrementado su conciencia sobre la importancia de la seguridad de la información. Sin embargo, aún queda mucho por hacer en términos de implementar sistemas robustos y efectivos.
- **Relevancia actual:** se debe destacar la creciente relevancia de la información en la era digital, donde la protección de datos personales, la privacidad y la seguridad en línea son preocupaciones cada vez más importantes. Por esta razón nace la ciberseguridad, la cual se convierte en un aspecto esencial en este contexto.
- **Sistema de gestión integral:** se debe subrayar la importancia de ver la seguridad de la información como un sistema de gestión integral, que abarca políticas, procedimientos y controles, que está alineado con otros sistemas de gestión de la organización.
- **Diversos sectores:** se debe reconocer que la seguridad de la información es relevante en todos los sectores, desde el financiero hasta el de la construcción, y que las estrategias deben adaptarse a las particularidades de cada uno.
- **Gestión de activos:** las organizaciones deben contar con un inventario de activos, y dentro de esa gestión de activos se definen unos controles, unos procedimientos y unos protocolos que ayuden a proteger la información. De esta manera se asumen los mejores mecanismos y lineamientos para que la gestión en la protección de los activos se haga de manera adecuada, se puedan mantener en el tiempo los controles, y se tengan roles y responsabilidades de quiénes son los que deben administrar y gestionar esos controles asociados a cada uno de los activos de la organización.
- **Gestión de la información:** se debe enfatizar en los riesgos, en las políticas, en los roles que debe tener la información.
- **Importancia central de la información:** se debe enfatizar que la información es el activo y pilar principal de las organizaciones, porque una organización que no tiene información no es una organización. Por eso es necesario implementar un sistema

de gestión de seguridad de la información robusto de manera estratégica y que sea conocido por todos los funcionarios.

3. Normativas aplicables a un SGSI

Es esencial tener en cuenta los estándares y las normas establecidas, como la ISO 27001, para garantizar una implementación organizada y efectiva de gestión de seguridad de la información.

También es interesante ver cómo diferentes normas y estándares abordan aspectos específicos de la seguridad de la información, como la gestión de riesgos, la ciberseguridad y la protección de datos personales. Estos marcos proporcionan una guía sólida para las organizaciones, independientemente de si eligen seguir una norma internacional como ISO 27001 o si optan por normas específicas de su región o sector.

En lo comentado anteriormente, podemos encontrar los siguientes estándares:

3.1 ISO/IEC 27001 y 27002

La norma **ISO/IEC 27001** es un estándar internacional que proporciona un marco para establecer, implementar, mantener y mejorar contínuamente un sistema de gestión de la seguridad de la información (SGSI). Nombra una lista de controles de seguridad agrupados en diferentes dominios, que pueden ser implementados para abordar diversos aspectos de la seguridad de la información. Estos controles están diseñados para ser personalizables y adaptables a las necesidades específicas de cada organización.

La norma ISO/IEC 27002 proporciona las orientaciones y directrices para la implementación de los controles de la norma 27001.

3.2 ISO/IEC 27005

ISO/IEC 27005 es una norma internacional que establece pautas y principios para la gestión de riesgos de seguridad de la información. Proporciona un marco sistemático para identificar, evaluar y gestionar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los activos de información de una organización.

Algunos puntos clave sobre ISO/IEC 27005 son:

- **Marco de Gestión de Riesgos:** la norma ofrece un marco para que las organizaciones puedan identificar, evaluar y gestionar los riesgos de seguridad de la información de manera efectiva.
- **Proceso de Evaluación de Riesgos:** define un proceso de evaluación de riesgos que implica identificar activos, amenazas y vulnerabilidades, y evaluar la probabilidad e impacto de los riesgos.
- **Toma de Decisiones Informadas:** ayuda a las organizaciones a comprender su entorno de riesgo y tomar decisiones informadas para mitigar o aceptar los riesgos.
- **Enfoque Sistemático:** proporciona un enfoque sistemático y estructurado para la gestión de riesgos de seguridad de la información, lo que permite a las organizaciones mejorar su postura de seguridad y proteger sus activos críticos de información.

3.3 ISO/IEC 27005

ISO/IEC 27035 es una norma internacional que se centra en la gestión de incidentes de seguridad de la información. Proporciona pautas y principios para ayudar a las organizaciones a detectar, gestionar y responder a los incidentes de seguridad de manera efectiva.

Algunos puntos clave sobre ISO/IEC 27035 son:

- **Gestión de Incidentes de Seguridad**: la norma establece un marco para la gestión de incidentes de seguridad de la información, incluida la detección, evaluación, notificación, respuesta y recuperación de los mismos.
- **Proceso de Gestión de Incidentes**: define un proceso detallado para la gestión de incidentes, que abarca desde la preparación y la identificación inicial hasta la resolución y el análisis post-incidente.
- **Mejora Continua:** fomenta la mejora continua mediante la revisión y el análisis de los incidentes pasados, para aprender de ellos y fortalecer las medidas de seguridad.
- **Coordinación y Comunicación**: destaca la importancia de la coordinación y la comunicación efectivas tanto internamente dentro de la organización como externamente con partes interesadas relevantes, como clientes, proveedores y autoridades reguladoras.

ISO/IEC 27035 es una herramienta importantísima para ayudar a las organizaciones a prepararse, detectar y responder de manera efectiva a los incidentes de seguridad de la información, contribuyendo así a proteger la confidencialidad, integridad y disponibilidad de los activos de información críticos.

3.4 ISO/IEC 22301

ISO/IEC 22301 es una norma internacional que establece requisitos para un sistema de gestión de la continuidad del negocio (SGCN). Su objetivo principal es ayudar a las organizaciones a prepararse, responder y recuperarse de manera efectiva ante interrupciones que puedan afectar su capacidad para operar normalmente.

Algunos puntos clave sobre ISO/IEC 22301 son:

- **Gestión de la Continuidad del Negocio:** la norma proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio.
- **Identificación de Amenazas y Vulnerabilidades:** ayuda a las organizaciones a identificar y evaluar las amenazas y vulnerabilidades que podrían afectar su capacidad para operar, así como los impactos potenciales de dichas interrupciones.
- **Planificación y Respuesta a Incidentes:** define requisitos para la planificación y la respuesta a incidentes, incluida la elaboración de planes de continuidad del negocio, la asignación de roles y responsabilidades, y la realización de ejercicios y pruebas periódicas.
- **Mejora Continua:** promueve la mejora continua mediante la revisión y la actualización periódica del sistema de gestión de la continuidad del negocio, así como la realización de análisis de lecciones aprendidas después de incidentes reales o simulados.

ISO/IEC 22301 es una herramienta que ayuda a las organizaciones a prepararse para enfrentar interrupciones en sus operaciones y garantizar la continuidad de sus actividades comerciales, lo que contribuye a proteger la reputación, la confianza del cliente y la viabilidad a largo plazo de la organización.

3.5 NIST

El National Institute of Standards and Technology (NIST) es una agencia del Departamento de Comercio de los Estados Unidos que desarrolla y promueve estándares, guías y mejores prácticas para mejorar la seguridad y la eficiencia de los sistemas de información y tecnología en diversos sectores.

Algunos aspectos clave sobre el NIST son:

- **Desarrollo de Estándares y Guías:** el NIST desarrolla y mantiene una amplia gama de estándares y guías, incluidos los relacionados con la ciberseguridad, la criptografía, la gestión de riesgos, la privacidad y la tecnología de la información.
- **Marco de Ciberseguridad:** el NIST es conocido por su Marco de Ciberseguridad (NIST Cybersecurity Framework), que proporciona un conjunto de estándares, directrices y prácticas recomendadas para ayudar a las organizaciones a gestionar y mejorar su postura de ciberseguridad.
- **Publicaciones Técnicas:** el NIST publica regularmente documentos técnicos, informes y recomendaciones que abordan diversos aspectos de la seguridad de la información y la tecnología, dirigidos a profesionales de la seguridad, desarrolladores de software y otros interesados en el campo.
- **Colaboración y Cooperación:** el NIST colabora estrechamente con la industria, el gobierno y la comunidad académica para desarrollar estándares y guías que sean relevantes, prácticos y efectivos para abordar los desafíos actuales y emergentes en el campo de la tecnología y la seguridad de la información.

El NIST desempeña un papel fundamental en la promoción de la seguridad y la eficiencia de los sistemas de información y tecnología a través del desarrollo de estándares, guías y mejores prácticas reconocidas a nivel internacional.

En conclusión, hay que destacar que la aplicación de normas, especialmente la ISO 27001 y otras normas relacionadas, sirve como una herramienta invaluable para implementar y gestionar eficazmente la seguridad de la información en las organizaciones.

4. Cómo implementar SGSI

En este punto veremos cómo implementar un sistema de gestión de seguridad de la información. Para implementar este sistema debemos tener mucha claridad, ya que de esto depende el éxito de esta implementación y vamos a poder gestionarlo de manera adecuada para llegar a la mejora continua.

Hay que tener en cuenta que al interior de la organización tenemos una serie de procedimientos y una serie de controles. Una implementación de SGSI, se realiza basandose en el el estandar ISO/IEC 27001.

Entonces, bajo ese estándar, vamos a encontrar una serie de dominios, los que están enfocados en la gestión de riesgos y la gestión de activos.

Evolución de la Norma ISO/IEC 27001

Fuente: Elaboración propia

ISO/IEC 27002: 2022

La norma ISO 27001:2022 se centra en la gestión de la seguridad de la información mediante la implementación de controles organizacionales y técnicos. Los dominios de control se agrupan en varias categorías. A continuación, se presentan los dominios de control de la ISO 27001:2022:

1. **Contexto de la Organización**: Establece el contexto interno y externo de la organización, así como las necesidades y expectativas de las partes interesadas en relación con la seguridad de la información.
2. **Liderazgo**: Enfocado en la alta dirección y su compromiso con la seguridad de la información, incluyendo la definición de políticas y la asignación de responsabilidades.
3. **Planificación**: Trata sobre la evaluación de riesgos y oportunidades, así como la definición de objetivos de seguridad de la información y la planificación para lograrlos.
4. **Apoyo**: Incluye recursos, competencia, concienciación, comunicación y control de la documentación relacionada con la seguridad de la información.

5. **Operación**: Enfocado en la implementación y control de los procesos necesarios para cumplir con los requisitos de seguridad de la información.
6. **Evaluación del Desempeño**: Trata sobre el seguimiento, medición, análisis y evaluación del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), así como auditorías internas y revisiones por la dirección.
7. **Mejora**: Enfocado en la mejora continua del SGSI, incluyendo la gestión de no conformidades y la implementación de acciones correctivas.
8. **Controles de Seguridad de la Información**:
    - **A.5 Políticas de Seguridad de la Información**: Establecimiento y gestión de políticas para orientar la seguridad de la información.
    - **A.6 Organización de la Seguridad de la Información**: Estructura organizacional y roles para gestionar la seguridad de la información.
    - **A.7 Seguridad de los Recursos Humanos**: Controles relacionados con el personal antes, durante y después de su empleo.
    - **A.8 Gestión de Activos**: Identificación y protección de activos de información.
    - **A.9 Control de Acceso**: Gestión del acceso a la información.
    - **A.10 Criptografía**: Uso de criptografía para proteger la información.
    - **A.11 Seguridad Física y Ambiental**: Protección de instalaciones y equipos.
    - **A.12 Seguridad en las Operaciones**: Gestión de las operaciones y procedimientos de seguridad.
    - **A.13 Seguridad en las Comunicaciones**: Protección de la información en las redes.
    - **A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**: Seguridad en el ciclo de vida del desarrollo del software y sistemas.
    - **A.15 Relaciones con Proveedores**: Gestión de la seguridad en las relaciones con proveedores.

MPORTANTE

¡A considerar!

Es importante considerar la alta dependencia que tienen las organizaciones de los proveedores. Por eso es fundamental que estos también manejen los protocolos y las políticas que define la organización para proteger la información, sobre todo con aquella que es confidencial.

- **A.16 Gestión de Incidentes de Seguridad de la Información**: Respuesta y gestión de incidentes de seguridad de la información.
- **A.17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio**: Continuidad del negocio y recuperación ante desastres.
- **A.18 Cumplimiento**: Cumplimiento de requisitos legales y normativos.

Estos dominios y controles ayudan a las organizaciones a gestionar la seguridad de la información de manera integral y sistemática, alineando las prácticas de seguridad con los objetivos y requisitos específicos de la organización.

PREGUNTA

¿Qué tipos de riesgos se deben identificar?

Los riesgos de la organización con base a la información que maneja, entonces hay que hacer un levantamiento de riesgos para poder identificar qué riesgos puede tener esa información que está en los diferentes activos de la organización.

5. Modelo PDCA

En el ámbito empresarial actual, la capacidad de adaptación y **mejora continua** es esencial para mantenerse competitivo y satisfacer las demandas del mercado en constante

cambio. En este contexto, el modelo **PDCA** (Planificar, Hacer, Verificar, Actuar) emerge como una herramienta que necesita la organización para poder mantener un SGSI.

En una mejora continua para un SGSI, existen entradas que son la partes interesadas y requisitos para el sistema de información para llegar a un ciclo que comienza con la etapa de **establecer (planificar)**, avanza con **implementar y operar (hacer)**, sigue con el **monitoreo (verificar)** y finaliza con la **mantencion (actuar)**.

Revisemos estas etapas.

Planificar

La fase de planificación constituye el punto de partida del modelo PDCA. En esta etapa, se establecen claramente los objetivos y metas que se desean alcanzar. Además, se identifican los procesos que necesitan mejoras y se elabora **un plan** detallado que incluye las estrategias, recursos y plazos necesarios para alcanzar dichos objetivos. La planificación proporciona una dirección clara y un marco de referencia para guiar las acciones futuras.

Hacer

La fase de hacer implica la implementación del plan elaborado durante la fase de planificación. Aquí es donde se ponen en práctica las estrategias y se llevan a cabo las acciones planificadas. Es esencial garantizar una ejecución eficiente y eficaz de las tareas, así como una comunicación clara. Durante esta fase, se recopilan datos y se realizan observaciones que servirán de base para la fase de verificación.

Verificar

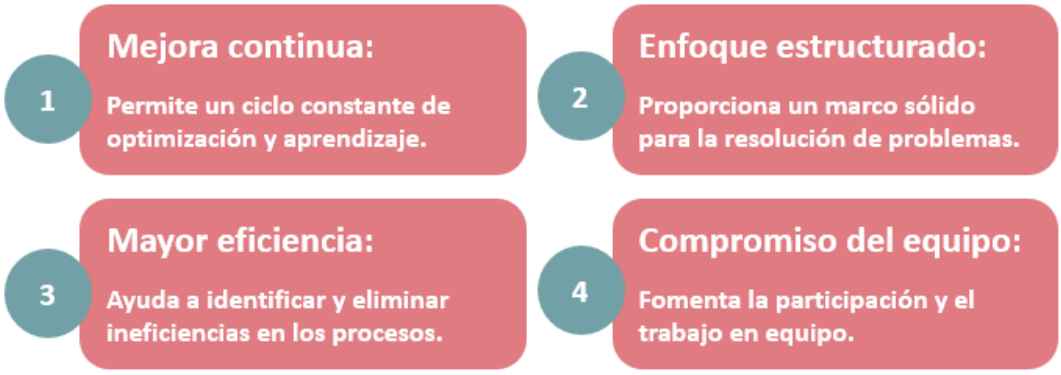
En la fase de verificación, se evalúan los resultados obtenidos durante la fase de hacer en comparación con los objetivos establecidos en la fase de planificación. Se lleva a cabo un análisis exhaustivo de los datos recopilados para determinar si se han alcanzado los resultados deseados y si se han cumplido los estándares de calidad establecidos. En caso de desviaciones o áreas de mejora identificadas, se procede a la fase de actuar.

Actuar

La fase de actuar se centra en la implementación de acciones correctivas y preventivas basadas en los hallazgos y conclusiones obtenidos durante la fase de verificación. Aquí es donde se realizan ajustes en los procesos, se introducen cambios necesarios y se refuerzan las mejores prácticas identificadas. La fase de actuar cierra el ciclo PDCA y sienta las bases para un nuevo ciclo de mejora continua.

El modelo PDCA se presenta como una herramienta poderosa y efectiva para impulsar la mejora continua en las organizaciones. Al seguir este enfoque sistemático y cíclico, las empresas pueden identificar áreas de oportunidad, implementar mejoras efectivas y alcanzar niveles más altos de desempeño operativo. En un entorno empresarial cada vez más competitivo y dinámico, el modelo PDCA se convierte en un aliado indispensable para la innovación, la eficiencia y el éxito a largo plazo.

Beneficios del Modelo PDCA



Fuente: Elaboración propia

Ejemplos de aplicación

Fuente: Elaboración propia

6. Liderazgo en el SGSI

Es necesario hablar de liderazgo, porque siempre que se realiza una implementación de un sistema de gestión, debe existir un líder que planifique para que este se pueda implementar. Por lo tanto, este liderazgo es fundamental y se debe dar a nivel de la alta gerencia, ya que es quien autoriza los recursos, monitorea y lidera la implementación. Además, debe apoyar con las políticas y objetivos del Sistema de Información.

Dependerá del líder del proyecto que se aplique la política de seguridad al interior de la organización y que sea entendida por todos sus miembros. En este sentido, la alta gerencia tiene la responsabilidad de establecer un marco claro de roles y responsabilidades dentro del SGSI. Esto implica definir quiénes son los responsables de la gestión, supervisión y ejecución de las políticas y procedimientos de seguridad de la información.

Al asignar roles específicos, se crea un sentido de responsabilidad y *accountability* en toda la organización, lo que facilita la toma de decisiones y la implementación efectiva de medidas de seguridad.

6.1 Funciones de estructura de gobierno en el SGSI

Las funciones de estructura de gobierno en el SGSI incluyen:

- **Definición de roles y responsabilidades:** la alta gerencia debe establecer claramente quiénes son los responsables de la seguridad de la información en diferentes niveles de la organización, desde el equipo directivo hasta los empleados de base.
- **Autoridad para tomar decisiones:** es fundamental que las personas designadas tengan la autoridad necesaria para tomar decisiones en materia de seguridad de la información. Esto incluye la capacidad de asignar recursos, implementar controles y responder a incidentes de seguridad.
- **Supervisión y Control:** además de definir roles y responsabilidades, la alta gerencia debe asegurarse de que exista un sistema de supervisión y control para garantizar el cumplimiento de las políticas y procedimientos de seguridad de la información.

6.2 Beneficios de una definición clara de roles y responsabilidades

- **Claridad y coherencia:** al definir roles y responsabilidades, se establece una estructura clara y coherente que facilita la comunicación y la coordinación entre los diferentes departamentos y equipos.
- **Eficiencia operativa**: la asignación adecuada de responsabilidades permite una gestión más eficiente de los recursos y una respuesta más rápida a las amenazas y vulnerabilidades de seguridad.
- **Responsabilidad y rendición de cuentas:** al identificar claramente quiénes son los responsables de la seguridad de la información, se promueve una cultura de responsabilidad y rendición de cuentas en toda la organización.

7. Política de Seguridad de la Información

Una Política de Seguridad de la Información (PSI) es un documento formal que establece los principios, objetivos y responsabilidades relacionadas con la protección de la información dentro de una organización. Proporciona un marco para la gestión de la seguridad de la información y define las reglas y procedimientos que deben seguirse para garantizar la confidencialidad, integridad y disponibilidad de los datos. Su importancia radica en varios aspectos clave. Estos son:

Protección de activos de información:

La PSI ayuda a proteger los activos de información crítica de la organización, como datos de clientes, información financiera y propiedad intelectual, contra amenazas internas y externas.

Cumplimiento legal y regulatorio:

La PSI ayuda a garantizar el cumplimiento de las leyes, regulaciones y estándares de seguridad aplicables, lo que reduce el riesgo de sanciones legales y financieras.

Gestión de riesgos:

La PSI establece un marco para identificar, evaluar y mitigar los riesgos de seguridad de la información, lo que contribuye a la protección contra pérdidas financieras y daños a la reputación.

Promoción de una cultura de seguridad:

Al definir roles, responsabilidades y procedimientos relacionados con la seguridad de la información, la PSI fomenta una cultura de seguridad en toda la organización, donde todos los empleados son conscientes de los riesgos y responsables de proteger la información.

7.1 Elementos de una Política de Seguridad de la Información

Una PSI efectiva debe abordar varios elementos clave. Estos son:

Alcance y objetivos: definición clara del alcance de la política y los objetivos que se pretenden alcanzar.

Responsabilidades y roles: asignación de responsabilidades específicas para la gestión y protección de la información en todos los niveles de la organización.

Gestión de riesgos: identificación, evaluación y tratamiento de los riesgos de seguridad de la información.

Controles de seguridad: implementación de controles técnicos y procedimentales para proteger la información contra amenazas.

Concientización y capacitación: programas de concientización y formación para sensibilizar a los empleados sobre los riesgos de seguridad y las mejores prácticas.

8. Roles y responsabilidades en un SGSI

La implementación y operación de un Sistema de Gestión de Seguridad de la Información (SGSI) requieren la definición clara de roles y responsabilidades para asegurar que todos los aspectos de la seguridad de la información sean gestionados de manera efectiva. A continuación, se describen los roles y responsabilidades clave en un SGSI:

Alta Dirección

Responsabilidades:

- Establecer la Política de Seguridad de la Información: Definir y aprobar las políticas de seguridad de la información.
- Compromiso y Liderazgo: Proveer liderazgo y apoyo para la implementación y mejora continua del SGSI.
- Asignación de Recursos: Garantizar que se asignen los recursos necesarios para implementar y mantener el SGSI.
- Revisión y Mejora: Revisar periódicamente el SGSI para asegurarse de que sigue siendo adecuado, efectivo y alineado con los objetivos estratégicos de la organización.

Director de Seguridad de la Información (CISO)

Responsabilidades:

- Desarrollo de la Estrategia de Seguridad: Desarrollar y mantener la estrategia de seguridad de la información.
- Supervisión del SGSI: Supervisar la implementación y operación del SGSI.
- Gestión de Riesgos: Identificar, evaluar y gestionar los riesgos de seguridad de la información.
- Cumplimiento Normativo: Asegurarse de que la organización cumple con las leyes, regulaciones y estándares relevantes de seguridad de la información.

Comité de Seguridad de la Información

Responsabilidades:

- Coordinación de Actividades de Seguridad: Coordinar las actividades de seguridad de la información en toda la organización.
- Revisión de Incidentes: Revisar y analizar incidentes de seguridad de la información y proponer medidas correctivas.

- Aprobación de Políticas y Procedimientos: Revisar y aprobar políticas, procedimientos y controles de seguridad de la información.

Responsable de Seguridad de la Información (ISO)
Responsabilidades:

- Implementación de Controles: Implementar y gestionar los controles de seguridad de la información.
- Evaluación de Riesgos: Realizar evaluaciones de riesgos y recomendar medidas de mitigación.
- Capacitación y Concienciación: Proveer capacitación y programas de concienciación sobre seguridad de la información para el personal.
- Gestión de Incidentes: Coordinar la respuesta a incidentes de seguridad de la información.

Administradores de Sistemas y Redes
Responsabilidades:

- Mantenimiento de Infraestructura: Asegurar el mantenimiento y la seguridad de la infraestructura de TI.
- Gestión de Accesos: Implementar y gestionar controles de acceso a los sistemas y datos.
- Monitoreo de Seguridad: Monitorear los sistemas y redes para detectar y responder a amenazas de seguridad.

Propietarios de Activos de Información
Responsabilidades:

- Identificación de Activos: Identificar y documentar los activos de información bajo su responsabilidad.
- Clasificación de Información: Clasificar la información de acuerdo con su criticidad y sensibilidad.
- Protección de Activos: Asegurar que los activos de información están protegidos de acuerdo con las políticas y procedimientos de seguridad de la información.

Usuarios Finales
Responsabilidades:

- Cumplimiento de Políticas: Cumplir con las políticas y procedimientos de seguridad de la información.

- Protección de Información: Proteger la información a la que tienen acceso y reportar cualquier incidente de seguridad.
- Capacitación Continua: Participar en programas de capacitación y concienciación sobre seguridad de la información.

Auditores Internos de Seguridad
Responsabilidades:

- Evaluación del SGSI: Realizar auditorías internas para evaluar la efectividad del SGSI.
- Identificación de No Conformidades: Identificar no conformidades y áreas de mejora.
- Reporte de Resultados: Informar los resultados de las auditorías a la alta dirección y al comité de seguridad de la información.

Estos roles y responsabilidades aseguran que todas las partes relevantes dentro de la organización participen en la protección de la información, contribuyendo a un SGSI efectivo y alineado con los objetivos estratégicos de la organización.

8.1 Beneficios de una definición clara de roles y responsabilidades

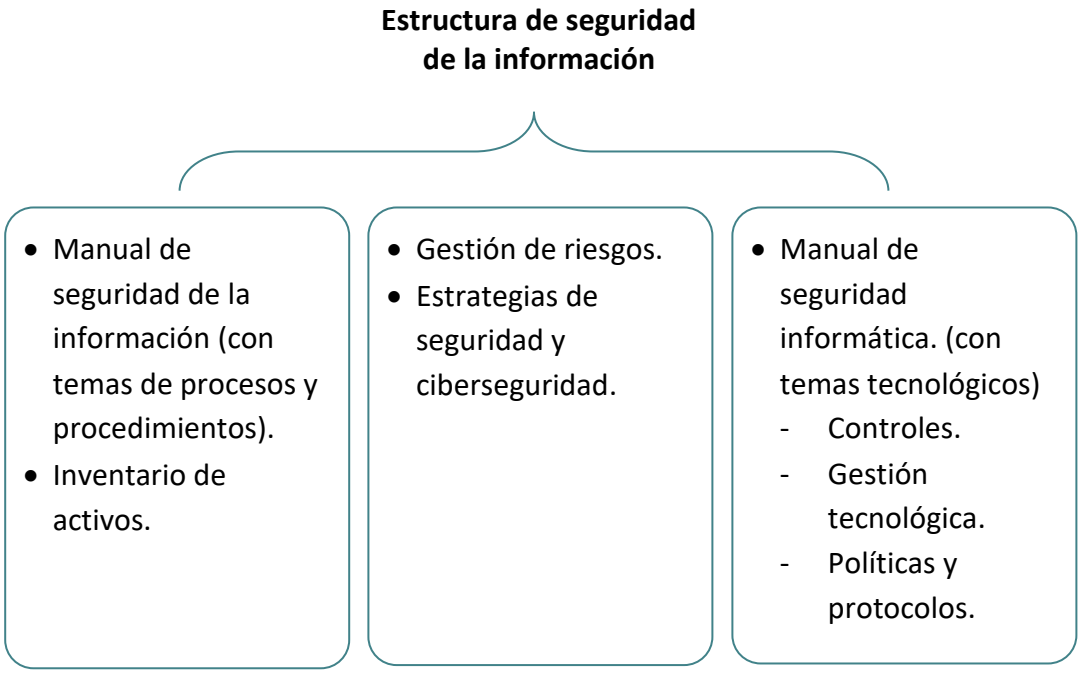
- **Claridad y coherencia:** al definir roles y responsabilidades, se establece una estructura clara y coherente que facilita la comunicación y la coordinación entre los diferentes departamentos y equipos.
- **Eficiencia operativa**: la asignación adecuada de responsabilidades permite una gestión más eficiente de los recursos y una respuesta más rápida a las amenazas y vulnerabilidades de seguridad.
- **Responsabilidad y rendición de cuentas:** al identificar claramente quiénes son los responsables de la seguridad de la información, se promueve una cultura de responsabilidad y rendición de cuentas en toda la organización.

9. Estructura del SGSI

Para implementar un SGSI se debe realizar un análisis de la estructura con dos miradas a nivel estratégico; una organizacional y otra estructura documental de seguridad de la información.

Estructura de seguridad de la información

La estructura desde el punto de vista **organizacional** y **documental** de un Sistema de Gestión de Seguridad de la Información debe esta definido de acuerdo al tamaño de la empresa, productos, servicios, camacidad económica, sucursales, recursos, herramientas tecnológicas etc.



DEFINICIÓN

Plan estratégico de seguridad de la información:

Define cuáles son las necesidades y mecanismos de control hacia seguridad de la información que debe implementar la organización y que están dentro de este plan con un presupuesto calculado para ser ejecutado en un tiempo determinado.

Estructura de documental

Es la estructura dentro del SGSI para gestionar la documentación asociada, de tal forma que se garantice la calidad y oportunidad de la información contenida. Esta estructura debe garantizar su disponibilidad para su uso. Esta estructura se organiza de forma jerarquizada dentro del SGSI , con el fin de garantizar la comprensión de su rol y funcionalidad dentro del mismo.

10. Realizar una implementación a partir de la norma ISO/IEC 27001

Este estándar se ha apoyado en muchos estándares nacionales e internacionales para poder definir conceptos y poder alinear a un sistema de gestión. Estamos hablando de un sistema cuya estructura básica está alineada con otras normas asociadas al sistema de gestión, como continuidad, gestión ambiental, gestión de calidad, entre otras.

La implementación de la norma ISO 27001 , nos presenta dentro de su estructura los dominios de control: conceptos, contexto en la organización, referencias, aspectos operacionales de riesgos y diferentes lineamientos.

Esta norma tiene 14 dominios de control.

Dominios de control:

- **Políticas.**
- **Organización.**
- **Recurso humano.**
- **Recursos.**
- **Accesos.**
- **Criptografía.**
- **Seguridad física.**
- **Operación.**
- **Comunicaciones.**
- **Sistemas.**
- **Proveedores.**
- **Incidentes.**
- **Continuidad de negocio.**
- **Cumplimiento.**

Por lo tanto, una organización que quiere implementar un sistema de gestión de seguridad de la información, deberá tener en cuenta estos 14 dominios y con base a esto, deberá definir unos controles, unas políticas, unos lineamientos para dichos dominios.

IMPORTANTE

¡A considerar!

Puede ocurrir que, de acuerdo con la organización, su tamaño o el sector en el que se encuentre, no se aplique uno o dos dominios, pero por lo general se aplican todos.

Por eso es importante que llevemos a cabo pasos que consideremos relevantes, y valorarlos y entenderlos para poder implementar de manera adecuada y organizada un sistema de gestión de seguridad de la información.

Vamos a presentar cada uno de ellos para entender e identificar qué debemos considerar en cada concepto.

Pasos para implementar un SGSI

Fuente: Elaboración propia

10.1 Definición de la estructura

Siempre que vamos a implementar un sistema de gestión de seguridad de la información, debemos empezar por definir de qué manera va a quedar estructurado.

PREGUNTA

¿De qué manera va a estar definido el liderazgo?

Hay que recordar que el liderazgo tiene que partir de la alta gerencia, de las directivas, de la organización, entonces hay que definir quién va a ser el responsable y en quién recae ese liderazgo de seguridad de la información.

10. 2 Definición recursos de implementación

Después de que definimos una estructura de liderazgo, tenemos que tener los recursos, el dinero para implementar SGSI (esos recursos hay que definirlos desde el principio)

En este segundo paso establecemos las siguientes interrogantes: cuáles son los recursos con los que contamos, en qué debemos invertir, qué costo debemos asumir, qué tenemos que tener en cuenta para poder hacer una planeación, etcétera. Con esta información podemos obtener un presupuesto de cómo vamos a implementar ese sistema de gestión de seguridad de la información. Esto es fundamental.

10. 3 Identificar riesgos de seguridad de la información

Un tercer paso son los riesgos de seguridad de la información. Se debe hacer una identificación de los riesgos relacionados con la seguridad de la información como punto inicial para poder saber a qué nos vamos a enfrentar, qué vamos a encontrar en esa implementación, qué debemos considerar, cuáles pueden ser esos riesgos que se pueden materializar, cuáles son las consecuencias, cuáles son los impactos, cuál es la probabilidad. Por ejemplo, un riesgo que se puede identificar es , si la aplicación se encuentra expuesta a clientes de una organización y transacciona datos sensibles, sus inicios de seción no posean segundo factor de autenticación.

Para todo lo que tiene que ver con la gestión de riesgos, debemos definir una matriz de riesgos de seguridad de la información para empezar a hacer la implementación.

10.4 Definición de activos de información

Después de que tenemos definidos los riesgos, definiremos los activos de información que deben estar alineados con los riesgos y hacer un inventario de activos de información. Un ejemplo de activos de información puede ser los tipos de datos que utiliza la organización (datos de clientes, datos de colaboradores, etc.).

10.5 Definición de procedimientos de seguridad de la información

Vamos a definir unos procedimientos de seguridad de la información, identificando con qué se encuentran asociados, ya sea con manuales, políticas, roles, etc.

Se debe definir qué debe hacer el responsable y los funcionarios asociados con el tema de seguridad de la información.

y 10.6 Definición dominios de control

Para implementar esos controles, debemos tener los recursos, debemos tener las personas, debemos tener unas definiciones muy claras para poder hacerlo y para apoyarnos en los dominios de control, que señalan de qué manera se debe realizar, teniendo en cuenta cada uno de los dominios para los diferentes aspecto de la organización.

10.7 Definición de las pruebas

Después de que se haya implementado y considerado controles, procedimientos, directrices, lineamientos, recursos, se deben hacer pruebas para el sistema de gestión de seguridad, la información.

Estas son pruebas asociadas a poder evidenciar qué pasaría si se presenta un incidente a nivel tecnológico o tecnológico y que pueda afectar mi información.

Por eso es importante en todo sistema de gestión las pruebas. Como análisis de vulnerabilidades, como hacking ético, como pruebas asociadas a los sistemas de información, pruebas que revisen las diferentes maneras de accesos, que pasa si alguien saca información de la organización, qué pasa si alguien cambia la información, etc.

10.8 Sensibilización y actualización

Este es el último paso, ya que después de que se haya implementado, se han realizado pruebas, se debe sensibilizar a todas las personas a través de actividades de capacitación, concientización, tender a una cultura de seguridad que se debe dar a nivel transversal en toda la organización o.

La actualización es muy importante para la mejora continua. Por eso debe darse un buen proceso, un buen lineamiento de sensibilizar a toda la organización frente al sistema de gestión de seguridad de la información, promoviendo los beneficios, y los aspectos positivos.

Conclusión

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es una estrategia fundamental para cualquier organización que busca proteger su información y asegurar la continuidad de sus operaciones. En un entorno digital donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, contar con un SGSI robusto y bien estructurado se convierte en una necesidad imperativa. Este ensayo explora las principales razones y beneficios de implementar un SGSI, así como su impacto en la organización.

En primer lugar, un SGSI permite a la organización establecer un marco estructurado y sistemático para la gestión de la seguridad de la información.

Además, un SGSI facilita el cumplimiento de las leyes, regulaciones y estándares internacionales de seguridad de la información, como ISO 27001.

Otro beneficio significativo de implementar un SGSI es la mejora de la confianza y la reputación de la organización.

La implementación de un SGSI también promueve una cultura de seguridad dentro de la organización. Al involucrar a todos los empleados en la protección de la información y proporcionarles la capacitación adecuada, se fomenta una mentalidad de seguridad que permea toda la organización.

Por último, un SGSI proporciona a la organización un enfoque proactivo para la gestión de riesgos.

Referencias bibliográficas

Gómez Fernández, L. y Fernández Rivero, P. P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad: (ed.). Madrid, Spain: AENOR - Asociación Española de Normalización y Certificación. Recuperado de https://elibro-net.bibliotecadigital.umayor.cl:2443/es/ereader/umayor/53624?page=14.

Este material fue desarrollado por el docente Joaquín Morales para la Universidad Mayor y ha sido diseñado para su lectura en formato digital.

Última actualización agosto, 2024.