Gobierno de Colombia

Agencia Nacional de Tierras

CONCEPTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Subdirección de Sistemas de Información de Tierras

INDICE

Introducción

Actualmente las amenazas y vulnerabilidades a nivel cibernético pueden colocar en peligro a las diferentes organizaciones de cualquier tipo o sector.

En línea con esto, la falta de conocimiento y de apropiación de herramientas para combatir estas amenazas puede repercutir en pérdidas de información importante, así como en el incumplimiento legal asociado a seguridad de la información, lo que podrá llevarnos a interrupciones de la operación y los procesos y por ende a una pérdida de la reputación organizacional.

De esta forma a continuación podrá encontrar una serie de conceptos que permitirán a la Agencia Nacional de Tierras junto con el compromiso de funcionarios, contratistas y proveedores, asegurar el cuidado de la información y los datos ante posibles ataques cibernéticos que puedan afectar la operación de la entidad.

Iniciemos diferenciando algunos conceptos

1. Seguridad de la información, ciberseguridad y protección de datos personales

Cuando nos adentramos en el mundo de la seguridad de la información, se suelen confundir varios conceptos, a continuación, presentamos la diferencia entre seguridad de la información, ciberseguridad y protección de datos personales.

La seguridad de la información es un concepto que encierra todo el conjunto de medidas preventivas y correctivas, para el almacenamiento y la protección de la información. En este sentido este concepto encierra todas las políticas, lineamientos, instructivos, manuales entre otros que permiten la administración y uso adecuado de la información.

La ciberseguridad se encarga de proteger los sistemas informáticos, redes, programas y datos contra ataques, daños o acceso no autorizado.

La protección de datos personales son todos esos procedimientos, normas y regulaciones que buscan resguardar la privacidad de los individuos mediante la regulación del procesamiento de sus datos personales, entendiéndose estos como cualquier información que se pueda utilizar para identificar a una persona, ya sea directa o indirectamente.

De acuerdo con esto en nuestra entidad la seguridad de la información tiene la responsabilidad de asegurar la información para mantener la confianza de sus grupos de interés, la ciberseguridad de la implementación de herramientas para gestionar la defensa digital entre las personas, los procesos y las tecnologías; y la protección de datos personales de proteger la privacidad de los individuos mediante el control y la regulación del procesamiento de información que puede identificarlos

2. Pilares de seguridad de la información

Cuando hablamos de seguridad de la información es muy importante tener en cuenta la triada de la Confidencialidad, la Integridad y la Disponibilidad, estos tres factores son los ejes que establecen la guía para proteger, la información, los datos y garantizar el funcionamiento de los sistemas de información.

Cuando la entidad tiene la capacidad de asegurar esta triada, tiene la capacidad de enfrentar cualquier amenaza:

Entonces hablemos de que se trata cada uno

Confidencialidad: significa que los datos, objetos y recursos están protegidos contra la visualización y otros accesos no autorizados. Esto se logra mediante políticas estrictas de acceso y medidas de seguridad como el cifrado y la autenticación multifactor.

Integridad: significa que los datos están protegidos de cambios no autorizados para garantizar que son fiables y correctos. Para proteger la integridad, se pueden usar técnicas como hash, cifrado, certificados y firmas digitales.

Disponibilidad: significa que los usuarios autorizados tienen acceso a los sistemas y recursos que necesitan. Para establecer acciones eficaces frente a la disponibilidad se debe realizar reparaciones de hardware, conservar los sistemas operativos y el software actualizados, así como crear respaldos.

De forma más practica

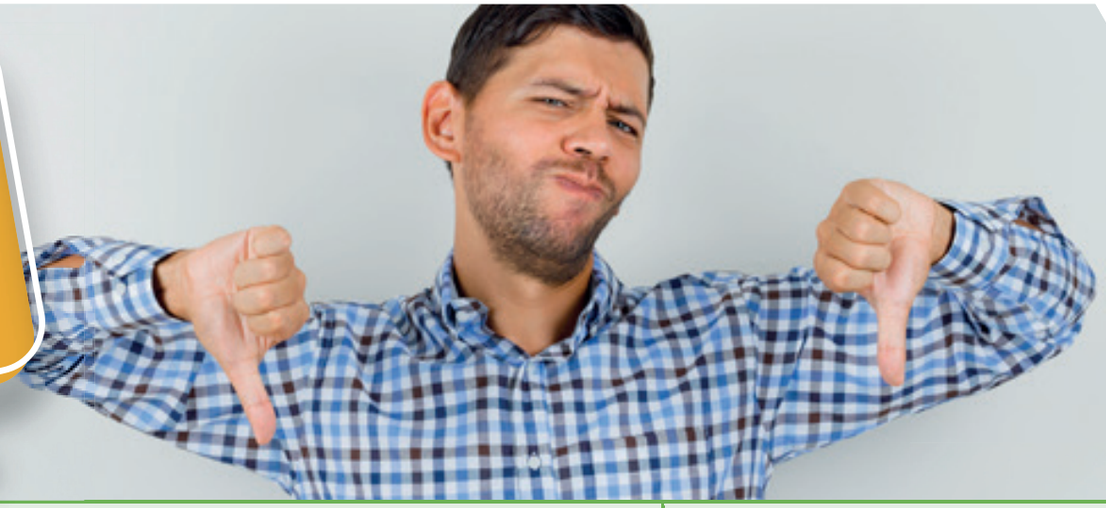
3. Amenazas y vulnerabilidades

Una vez entendidos los conceptos anteriores, es importante reconocer que la seguridad de la información trabaja frente a amenazas y vulnerabilidades. Entendamos entonces de que se tratan estos conceptos.

Vulnerabilidad: se trata de una debilidad o fallo en un sistema de información que abre la puerta para que un atacante o situación no prevista pueda comprometer la integridad, disponibilidad o confidencialidad de los datos.

Amenaza: es una acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Veamos algunos ejemplos muy cotidianos:



Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Daños ocasionados por falta de mantenimiento los equipos.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso

Tipos de amenazas y vulnerabilidades

Dentro de las vulnerabilidades y amenazas que se pueden presentar, estas son las 20 más comunes:

- **Spam:** correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
- **Phishing:** suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
- **Malware o sistema infectado:** sistema comprometido por un software malicioso. *Ejemplo:* *sistema, computadora o celular infectado con un rootkit.*
- **Escaneo de redes (scanning):** envío de peticiones a un sistema para descubrir posibles debilidades. *Ejemplos:* *peticiones DNS, ICMP, SMTP y escaneo de puertos.*
- **Análisis de paquetes (sniffing):** observación y grabación del tráfico de redes.
- **Ataque de fuerza bruta:** múltiples intentos automáticos o semiautomáticos de vulnerar credenciales.
- **Compromiso de cuenta con privilegios:** situación en la que un atacante logra acceder y tomar control de una cuenta de usuario con privilegios elevados en un sistema.
- **Compromiso de aplicaciones:** compromiso de una aplicación mediante la explotación de vulnerabilidades de software. *Ejemplo:* *inyección SQL.*
- **DoS (Denegación de Servicio):** ataque cibernético en el que un atacante intenta hacer que un sistema, servicio o red no esté disponible para sus usuarios legítimos al sobrecargarlo con una gran cantidad de tráfico o solicitudes maliciosas. *Ejemplo:* *envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.*
- **DDoS (Denegación Distribuida de Servicio):** forma avanzada y más potente de ataque DoS en la que múltiples sistemas comprometidos, generalmente coordinados como una botnet, envían grandes cantidades de tráfico o solicitudes maliciosas al objetivo con el fin de saturar sus recursos y hacerlo inaccesible para los usuarios legítimos. *Ejemplos:* *inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.*

- **Ciberterrorismo:** sabotaje y/o uso de redes o sistemas de información con fines de carácter terrorista que afectan la prestación de un servicio esencial. *Ejemplos: cortes de cableados de equipos, incendios, alteración, supresión, inaccesibilidad de datos, etc.*
- **Interrupciones:** interrupciones por causas externas. *Ejemplo: desastre natural.*
- **Acceso no autorizado a información:** acceso a sistemas, bases de datos, archivos o cualquier otro repositorio de información de manera ilícita o sin el debido consentimiento. *Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.*
- **Modificación no autorizada de información:** cualquier alteración de datos en un sistema o red realizada sin el permiso adecuado. *Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación, o encriptado de datos mediante ransomware.*
- **Pérdida de datos:** pérdida de información. *Ejemplos: pérdida por fallo de disco duro o robo físico.*
- **Criptografía débil:** uso de algoritmos y métodos criptográficos que no proporcionan un nivel adecuado de seguridad, haciendo que los datos protegidos sean vulnerables a ataques y accesos no autorizados. *Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.*
- **Servicios con acceso potencial no deseado:** servicios, programas o aplicaciones que, aunque no necesariamente son maliciosos, pueden comportarse de manera indeseada o causar problemas de seguridad y privacidad en un sistema. *Ejemplos: Telnet, RDP o VNC.*
- **Revelación de información:** acceso público a servicios en los que potencialmente pueda revelarse información sensible. *Ejemplos: SNMP o Redis.*
- **Sistema vulnerable:** sistema que tiene fallas de seguridad, deficiencias o debilidades que pone en riesgo la confidencialidad, integridad y disponibilidad de la información que maneja. *Ejemplos: mala configuración de proxy en cliente (WPAD) o versiones desfasadas de sistema.*
- **APT (Amenaza Avanzada Persistente):** ataques muy sofisticados y de alto nivel que se le hacen a países enteros o grandes corporaciones. Utiliza técnicas de hackeo continuas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado.

4. Herramientas y técnicas de seguridad

Cuando se habla de herramientas y técnicas de seguridad, se hace referencia a los diversos recursos y métodos utilizados para proteger los sistemas de información y los datos contra amenazas y vulnerabilidades. Concretamente las herramientas de seguridad son programas, dispositivos o aplicaciones diseñadas para proteger sistemas informáticos, redes y datos contra accesos no autorizados, ataques cibernéticos, y otros tipos de amenazas.

Algunas de las **herramientas de seguridad** son:

- **Antivirus:** programas que detectan y eliminan software malicioso.
- **Firewall:** dispositivos o software que controlan el tráfico de red para bloquear accesos no autorizados.
- **Sistemas de Detección y Prevención de Intrusos (IDS/IPS):** monitorizan y protegen las redes contra actividades sospechosas.
- **Cifrado:** herramientas que codifican la información para protegerla durante su transmisión o almacenamiento.
- **Gestores de contraseñas:** aplicaciones que almacenan contraseñas de forma segura.
- **Análisis de vulnerabilidades:** software que escanea sistemas en busca de posibles fallos de seguridad.
- **Software de copias de seguridad:** programas que crean copias de datos importantes para prevenir su pérdida.

En cambio, **las técnicas de seguridad** son métodos y procedimientos implementados para proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas de información.

Algunas de estas técnicas de seguridad son:

- **Autenticación Multifactor (MFA):** utiliza múltiples métodos de verificación para confirmar la identidad de los usuarios.
- **Principio de Menor Privilegio:** otorga a los usuarios solo los permisos necesarios para realizar sus tareas.
- **Segmentación de red:** divide la red en segmentos más pequeños para limitar el alcance de un ataque.
- **Actualización y parcheo regular:** mantiene los sistemas actualizados para corregir vulnerabilidades conocidas.
- **Seguridad en la nube:** implementa medidas específicas para proteger datos y aplicaciones en la nube.
- **Educación y concientización del usuario:** capacita a los empleados sobre prácticas de seguridad y cómo identificar amenazas.
- **Pruebas de penetración:** simula ataques para identificar y corregir vulnerabilidades.

Ambas son esenciales para una estrategia de seguridad integral en cualquier organización.

5. Gestión de incidentes de seguridad de la información

Actualmente la Agencia Nacional de Tierras cuenta con el **GINFO-P-011 PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**, este no solo facilita una respuesta rápida y efectiva a los incidentes de seguridad, sino que también protege a la organización de daños financieros, legales y reputacionales, así como ayuda a mantener un control sobre los mismos y a establecer acciones de mejora que disminuyan la probabilidad de ocurrencia.

Se entiende como un incidente de seguridad de la información el resultado de un evento o una serie de eventos de seguridad de la información no deseada o inesperada, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Por otro lado, según la norma ISO/IEC 27000, un evento de seguridad de la información es la ocurrencia identificada en un sistema, servicio o red de comunicaciones que sugiere una posible violación de la política de seguridad de la información, una falla en los controles, o una situación desconocida que podría ser importante para la seguridad.

Dentro de este procedimiento y de manera general se establecen unas etapas que se amplían en el documento.

Estos incidentes serán detectados mediante las Herramientas de monitoreo con las que cuenta la entidad y mediante el reporte de las diferentes dependencias de incidentes *relacionados con acceso no autorizado, cambio o pérdida de la información, publicación no autorizada de datos personales, o descarga de información sin autorización.*

Una vez confirmado el incidente, el equipo de **Seguridad de la Información de la SSIT**, debe definir su tratamiento y ejecutar el procedimiento establecido-

Ya implementado el procedimiento para Gestión de incidentes, se le debe comunicar a las partes interesadas, funcionarios, contratistas o clientes, en el caso de que se hayan visto afectados.

Superado el incidente y comunicado a todas las partes que correspondan, se establecen los planes de acción necesarios para evitar que se presente de nuevo dicho incidente o cualquier otro evento relacionado con este.

6. Roles y responsabilidades en seguridad de la información

Para el correcto funcionamiento de la Seguridad de la Información y el alcance de los objetivos establecidos por la entidad, debe existir una responsabilidad compartida que involucra a todos los grupos de interés de la ANT, de acuerdo con esto, se definen una serie de roles y responsabilidades de los diferentes equipos de trabajo, que fomentan la colaboración activa entre estos para lograr la protección eficaz de los datos, la información y los sistemas de información.

ROL	RESPONSABILIDADES	AUTORIDAD
Alta Dirección	•Aprobación de los alcances, políticas, lineamientos, normas, directrices y procedimientos, así como herramientas, manuales, modelos de operación, metodologías y estructuras organizacionales empleadas para la gestión del MSPI y seguimiento a su cumplimiento y actualización permanente. •Asegurar que el Sistema de Gestión de Seguridad de la Información se establezca, implemente y mantenga. •Gestión para la asignación de los recursos para establecer, implementar, operar hacer seguimiento, revisar, mantener y mejorar el MSPI institucional, para que las iniciativas relacionadas con la gestión de seguridad de la información se lleven a cabo y para que los lineamientos definidos se implementen. •Fomentar el cumplimiento de las políticas y lineamientos definidos en materia de seguridad de la información en los colaboradores de la Entidad. •Apoyar la difusión y sensibilización de la seguridad de la información en la Entidad. •Determinar como resultado de la revisión del SGSI, las decisiones y acciones relacionadas con la mejora en la eficacia del SGSI, la mejora del producto o servicio en relación con los requisitos del cliente y las necesidades de recursos	•Tomar las decisiones necesarias para el mantenimiento y mejora del SGSI •Aprobar los actos administrativos y documentos necesarios como compromiso de la Alta Dirección •Aprobar la asignación de recursos para el mantenimiento y mejora del SGSI •Designar responsabilidades relacionadas con el SGSI •Aprobar el informe de revisión por la alta dirección del SGSI y las acciones de mejora propuestas •Solicitar la implementación de modificaciones, mejoras y cualquier necesidad de cambio en el sistema integrado de gestión cuando lo considere pertinente •Solicitar al Oficial de Seguridad de la Información y demás áreas responsables la aplicación de los controles del SGSI •Requerir informes de gestión y evaluación del SGSI, cuando lo considere pertinente
Comité institucional de gestión y desempeño	•Revisar periódicamente las diferentes políticas o propuestas realizadas para el SGSI, aprobándolas o comunicando los ajustes a los que haya lugar •Realiza seguimiento al cumplimiento y actualización permanente de los alcances, planes, políticas, lineamientos, directrices y procedimientos, así como herramientas, manuales, modelos de operaciones, metodologías y estructuras organizacionales empleadas para la gestión del SGSI •Hacer seguimiento a las actividades de actualización a los perfiles de riesgo en Seguridad de la Información y protección de datos personales, así como a los planes de tratamiento de riesgo que surjan como resultado de dicha actualización. •Promover que todos los funcionarios vinculados a la entidad conozcan, entiendan y ejerzan sus responsabilidades frente al cumplimiento del SGSI •Revisión del proyecto de presupuesto relacionado con Seguridad de la Información y continuidad del negocio.	•Tomar decisiones para la mejora continua del SGSI •Requerir informes de gestión y evaluación del SGSI, cuando lo considere pertinente

ROL	RESPONSABILIDADES	AUTORIDAD
Oficial de Protección de Datos	• Velar por el respeto de los derechos de los titulares de los daos personales respecto del tratamiento de datos que realice el prestador de servicios ciudadanos digitales. • Informar y asesorar el prestador de servicios ciudadanos digitales en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales. • Supervisar el cumplimiento de lo dispuesto en la regulación y en las políticas de tratamiento de información del prestador de servicios ciudadanos digitales, así como del principio de responsabilidad demostrada. • Prestar el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos. • Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la Supervisión de Industria y Comercio o quien haga sus veces.	• Tomar decisiones necesarias sobre la gestión y tratamiento de Datos Personales • Reportar las bases de Datos con información personal ante la SuperIntendencia de Industria y Comercio • Reportar los incidentes de Seguridad de la Información que comprometan datos personales ante la SuperIntendencia de Industria y Comercio
Oficial de Seguridad de la Información	• Formular las políticas, lineamientos, controles y procedimientos encaminados a fortalecer la seguridad de la información. • Identificar las necesidades de la Agencia Nacional de Tierras frente al Modelo de Seguridad y Privacidad de la Información de MinTic. • Identificar la brecha entre el SGSI de la información y la situación de la Agencia Nacional de Tierras. • Realizar el autodiagnóstico de Seguridad de la Información de la Entidad. • Coordinar y gestionar los incidentes de seguridad de la información que se presenten en la Entidad. • Realizar seguimiento y monitoreo a la gestión y tratamiento de Riesgos de Seguridad de la Información • Generar el Plan de Trabajo para la implementación y mantenimiento del SGSI, así como el plan de trabajo, entregables y seguimiento de cumplimiento de este.	- Reportar avances en cuanto al desempeño del SGSI al Comité d Gestión y Desempeño. - Reportar ante las entidades competentes los incidentes de seguridad de la información acontecidos en la Entidad
Grupo de Seguridad de la Información	•Análisis y gestión de riesgos en seguridad y privacidad Seguridad de la Información, y liderar coordinación de la gestión de la implementación de controles para su mitigación. •Velar por el cumplimiento normativo asociado a la seguridad y privacidad de la información. •Monitorear y medir del cumplimiento de políticas, lineamientos, normas, estándares y procedimientos en Seguridad y Privacidad de la Información y tratamientos para subsanar las vulnerabilidades identificadas. •Capacitar y sensibilizar en seguridad y privacidad de la información. •Regular la gestión de activos de información, teniendo en cuenta su clasificación y las medidas de seguridad pertinentes. •Monitorear la gestión de vulnerabilidades técnicas de seguridad informática. •Gestión de Incidentes de Seguridad y privacidad de la Información con el apoyo de los grupos involucrados. •Informar sobre los avances en el cumplimiento de las directrices de Seguridad y Privacidad de la Información y por los procedimientos y prácticas que de ellas surjan. •Seguimiento a los incidentes en Seguridad y Privacidad de la Información presentados. •Revisar periódicamente el estado del SGSI a partir de indicadores definidos. •Atender las auditorías internas y externas que se hagan al MSPI •Seguimiento a los resultados del monitoreo realizado a la gestión de Seguridad de la Información, a las medidas de mejoramiento adoptadas por resultados de auditorías internas y externas al SGSI	•Solicitar informes de cumplimiento de controles de seguridad. •Reportar incumplimientos de políticas de seguridad a la Alta Dirección •Autorizar actividades relacionadas con seguridad de la información

ROL	RESPONSABILIDADES	AUTORIDAD
Oficina Asesora de control interno	•Ejecución de la auditoría al SGSI y a la conformidad y cumplimiento de los requisitos legales aplicables a la Entidad en relación con la Seguridad y Privacidad de la Información. •Informar sobre el cumplimiento de las directrices de Seguridad de la Información en el marco de la norma vigente auditada. •Hacer seguimiento a los planes de mejoramiento resultado de las auditorías internas. •Informar los resultados de la auditoría interna al SGSI al Comité Institucional del Gestión y Desempeño.	Requerir información sobre los soportes de implementación de los controles de SGSI
Talento Humano	•Implementar las políticas de seguridad y privacidad de la información asociadas al talento humano. •Gestionar las autorizaciones de tratamiento de datos personales de los funcionarios. •Incluir dentro de los procesos de inducción temas de seguridad y privacidad de la información. •Incluir dentro del plan anual de capacitación todos los temas referentes a seguridad y privacidad de la información. •Realizar convocatorias a las charlas, conversatorios y demás eventos programados que promuevan la concienciación en Seguridad y Privacidad de la Información, así como proveer los recursos para la respectiva ejecución del evento y su control de asistencia.	Escalar a control interno disciplinario las investigaciones por incumplimiento de políticas de seguridad de la información.
Oficina Jurídico	Determinación de la procedencia de abrir procesos disciplinarios por el incumplimiento de políticas y lineamientos de seguridad y privacidad de la información y/u ocurrencia de actos malintencionados que afecten la seguridad de la información que involucren a empleados públicos, trabajadores oficiales y/o contratistas, acorde con lo estipulado en el Código Único Disciplinario (Ley 734 de 2002), o las normas que lo modifiquen o complementen.	Abrir procesos disciplinarios a los funcionarios por incumplimiento de las políticas de seguridad de la información.
Todas las áreas de la Entidad, líderes y Colaboradores	•Conocimiento y cumplimiento de las disposiciones y lineamientos para la Seguridad de la Información establecidos en la entidad. •Asistencia a las capacitaciones y sensibilizaciones que programe la Entidad en temas de Seguridad de la Información •Reporte de eventos e incidentes de Seguridad de la Información y apoyo en la atención e investigación del mismos. •Apoyo en la respuesta a requerimientos internos y externos en materia de Seguridad de la Información. •Apoyo en la identificación y clasificación de activos de información y la realización de los análisis de riesgos y planes de tratamiento respectivos. •Definición y aplicación de mecanismos y controles para la protección de los activos de información.	Toma de decisiones sobre las actividades del proceso Gestionar los recursos necesarios para llevar a cabo las actividades El líder del proceso tiene la autoridad de aprobar la creación, modificación o eliminación de documentos del proceso, riesgos y cualquier cambio que se presente en el proceso.

Una vez identificados los roles y responsabilidades debe haber claridad en que la seguridad de la información hace parte integral de todos los procesos, esto incluye:

- **Planificación y estrategia:** asegurar que las decisiones estratégicas consideren los riesgos de seguridad de la información y que las políticas de seguridad de la información estén alineadas con los objetivos de la entidad.

- **Desarrollo de productos:** integrar la seguridad de la información en cada fase del proceso de desarrollo de productos y nuevos proyectos.

- **Operaciones diarias:** incorporar controles de seguridad en las operaciones diarias y en la implementación de los procedimientos e instructivos de la entidad.

- **Capacitación y concienciación:** educar a todos los funcionarios y contratistas sobre la importancia de la seguridad de la información y cómo pueden contribuir a proteger los activos de la organización, así como sobre las políticas, lineamientos, manuales e instructivos existentes.

7. El Sistema de Gestión de Seguridad de la Información de la ANT

Un Sistema de Gestión de Seguridad de la Información (SGSI) consiste en el conjunto de políticas, procedimientos y directrices que buscan proteger los activos de información, esenciales de una empresa. Es un enfoque sistemático para implementar, monitorear, y mejorar la seguridad de la información de una organización. Implementar un SGSI desde cero puede ser un desafío, pero con una planificación adecuada y el enfoque correcto, es posible establecer una base sólida para la seguridad de la información en la empresa.

¿Por qué tenemos un SGSI?

- Mejora de la reputación.
- Asegura la disponibilidad, confidencialidad e integridad de la Información
- Reducción de riesgos financieros.
- Protección de datos sensibles.
- Preparación para fusiones y adquisiciones.

¿Qué hacemos en la ANT para implementar un SGSI?

1. Existe un compromiso por parte de la alta dirección, compromiso que debe integrarse a todos los equipos de trabajo, para generar una cultura de seguridad de la Información.

2. Está definido el alcance de SGSI, dando claridad sobre los procesos y activos a los cuales se aplicará la política de seguridad y privacidad de la información.

3. Mantenemos actualizado el inventario de activos de información de la entidad.

4. Mantenemos actualizado el mapa de riesgos asociados a los activos de información inventariados, para establecer controles y acciones que los mitiguen.

5. Se establecen y actualizan políticas y procedimientos que direccionen las acciones para alcanzar los objetivos del SGSI.

6. Diseñamos e implementamos un Plan de Capacitación y sensibilización para funcionarios y contratistas sobre conceptos y procedimientos de seguridad de la información.

7. Realizamos seguimiento a la implementación de procedimientos, controles y acciones establecidas para la seguridad de la información.

8. Se gestiona de forma oportuna y eficaz los incidentes de seguridad de la información.

9. Establecemos planes de acción que permitan la mejora continua del SGSI.

8. Plan de Continuidad del negocio y Plan de recuperación ante desastres

Una vez conocidas estas herramientas es importante saber que la ANT cuenta con un Plan de Recuperación ante desastres y un Plan de continuidad del negocio, estrategias que permiten dar respuesta oportuna ante cualquier eventualidad en la que se pueda ver afectada la información de la entidad.

¿Qué es esto?

La continuidad del negocio se centra en mantener el negocio operativo durante un desastre, mientras que **la recuperación ante desastres** se centra en restaurar el acceso a los datos y la infraestructura de TI después de un desastre.

Siendo un poco más detallados

- **Plan de continuidad del negocio (BCP):** Un BCP es un plan detallado que describe los pasos que seguirá una organización para volver a la normalidad en caso de catástrofe. Mientras que otros tipos de planes pueden centrarse en un aspecto específico de la recuperación y la prevención de interrupciones (como una catástrofe natural o un ciberataque), los BCP adoptan un enfoque amplio y pretenden garantizar que una organización pueda hacer frente a una gama de amenazas lo más amplia posible.
- **Plan de recuperación ante desastres (DRP):** de naturaleza más detallada que los DRP, los planes de recuperación ante desastres ↗ consisten en planes de contingencia para que las empresas protejan específicamente sus sistemas de TI y sus datos críticos durante una interrupción. Junto con los BCP, los planes de recuperación ante desastres ayudan a las empresas a proteger sus datos y sistemas informáticos frente a diversas situaciones de catástrofe, como cortes masivos, desastres naturales, ataques de ransomware ↗ y malware ↗, y muchos otros.

- Los planes de continuidad del negocio (BCP) y los planes de recuperación ante desastres (DRP) ayudan a las organizaciones a prepararse para una amplia gama de incidentes no planificados.
- Cuando se implementa de manera efectiva, un buen plan de recuperación ante desastres puede ayudar a las partes interesadas a comprender mejor los riesgos para las funciones comerciales regulares que puede representar una amenaza en particular.
- Las organizaciones que no invierten en la recuperación ante desastres para la continuidad del negocio, tienen más probabilidades de experimentar pérdida de datos, tiempo de inactividad, sanciones financieras y daños a la reputación debido a incidentes no planificados.

Estos son algunos de los beneficios que pueden esperar las empresas que invierten en planes de continuidad del negocio y recuperación ante desastres:

- **Reducción del tiempo de inactividad:** cuando un desastre interrumpe las operaciones normales, puede costar mucho dinero a las entidades, volver a funcionar. Los ciberataques ↗ de alto perfil son particularmente dañinos, con frecuencia atraen atención no deseada y generan una alta pérdida de la reputación. La implementación de un plan sólido puede acortar el tiempo de recuperación, independientemente del tipo de desastre al que se enfrente.
- **Menor riesgo financiero:** según el reciente informe "Cost of a Data Breach" de IBM ↗, el coste medio de una filtración de datos fue de 4,45 millones de dólares en un aumento del 15 % desde 2020. Las organizaciones con planes sólidos de continuidad del negocio han demostrado que pueden reducir esos costos significativamente al acortar los tiempos de inactividad y aumentar la confianza de los clientes e inversores.
- **Reducción de las sanciones:** las vulneraciones de datos pueden conllevar grandes sanciones si se filtra información privada de clientes o cualquier otro grupo de interés. Contar con una sólida estrategia de continuidad del negocio es imperativo para la entidad ya que ayuda a mantener el riesgo de fuertes sanciones legales relativamente bajo.

Ahora te invitamos a conocer en más detalle los documentos del SIG relacionados con seguridad de la información los cuales te permitirán conocer las rutas y las estrategias para que seas parte de aquellos que protegen los datos, los sistemas y la información de la ANT.

¡No bajes la guardia!

Cuida nuestra información y protege tus datos personales

Equipo de Seguridad de la Información

Subdirección de Sistemas de Información de Tierras

Fuentes de Información

- https://crombie.dev/es/
- https://www.ibm.com/es