Curso Fundamentos de Ciberseguridad

Módulo 2

Relator: José Morales Antúnez
Normas y Políticas de Seguridad

¿Qué son las normas de Ciberseguridad?

Las podemos definir como un conjunto de reglas y estándares los cuales se establecen para proteger los sistemas informáticos y sus datos de amenazas cibernéticas. Asociadas a la ciberseguridad se intenta perseguir o garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos.
Algunos ejemplos de normas que podemos mencionar son:

- **Estándar ISO/IEC 27001:** Este estándar establece los requisitos para implementar y mantener un sistema de gestión de la seguridad de la información (ISMS, por sus siglas en inglés).
- **Estándar NIST Cybersecurity Framework:** Este marco de referencia proporciona una guía para la implementación de medidas de ciberseguridad en organizaciones gubernamentales y empresariales

Adicionalmente existen los CIS Controls que no son una norma de ciberseguridad en sí mismos, sino más bien un conjunto de recomendaciones y directrices para la implementación de medidas de ciberseguridad. Sin embargo, pueden utilizarse como un marco de referencia para establecer normas de ciberseguridad en una empresa u organización. Muchas empresas y organizaciones utilizan los CIS Controls como guía para establecer sus propias políticas y procedimientos de ciberseguridad y garantizar que están protegiendo adecuadamente sus sistemas y datos contra posibles amenazas de ciberseguridad.

¿Qué son las políticas de Ciberseguridad?

Corresponden a documentos que establecen los principios y directrices para proteger los sistemas informáticos y los datos de una empresa o organización de posibles amenazas de ciberseguridad. Estas políticas también suelen ser internas para una empresa, pero también puede existir políticas nacionales, como lo es la Política Nacional de Ciberseguridad para el caso de Chile que contiene lineamientos políticos del Estado de Chile en materia de Ciberseguridad que tiene como objetivo poder contar un ciberespacio libre, abierto, seguro y resiliente.
Es muy importante que las políticas a nivel empresarial se comuniquen a todos los empleados y implementen para garantizar la seguridad de los sistemas informáticos y de la información de la empresa.
Una política de ciberseguridad debe contener información detallada sobre cómo proteger los sistemas informáticos y los datos de una empresa o organización de posibles amenazas de ciberseguridad. Algunos elementos que pueden incluirse en una política de ciberseguridad son:

- Una declaración de propósito que explique el objetivo de la política y cómo se aplica a todos los empleados y sistemas de la empresa u organización.

- Requisitos de contraseña y autenticación, incluyendo la frecuencia con la que se deben cambiar las contraseñas y el uso de métodos de autenticación adicionales como tokens de seguridad o autenticación de dos factores.
- Normas para el uso apropiado de los sistemas informáticos y de la red, incluyendo restricciones para el acceso a ciertos sitios web y la descarga de software no autorizado.
- Procedimientos para la detección y la respuesta a posibles amenazas de ciberseguridad, incluyendo la notificación de personal de seguridad y la implementación de medidas de contención y recuperación.
- Normas para el manejo de datos sensibles y confidenciales, incluyendo requisitos para la encriptación y la protección de la información almacenada y transmitida.
- Requisitos de seguridad física para proteger los sistemas informáticos y los datos de posibles accesos no autorizados.
- Procedimientos de seguimiento y revisión para asegurar que se cumplan las políticas de ciberseguridad y se realicen actualizaciones periódicas.

También para complementar podemos mencionar que también existen regulaciones de ciberseguridad.
Una regulación es un conjunto de disposiciones obligatorias y de carácter legal que, en este caso, aplican sobre la seguridad de la información o ciberseguridad que rige para algunos sectores o empresas en un país.
Puede parecerse a una normativa, pero hay una diferencia importante y que una regulación está enmarcada en una ley o decreto, por lo tanto, su nivel de obligatoriedad es mayor. Además, los entes o empresas reguladoras son más exigentes al auditar el cumplimiento. Por ejemplo, para el caso de Chile existe un organismo regulador es la CMF (Comisión para el Mercado Financiero) que dispuso un requerimiento de Gestión de la Seguridad de la Información y Ciberseguridad

Dentro de las normas más conocidas podríamos indicar las siguientes:
ISO 27001: es una norma internacional que permite el aseguramiento, la confidencialidad, integridad y disponibilidad de los datos y la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistema de Gestión de Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.
En la actualidad para las empresas significa una diferenciación respecto al resto mejorando la competitividad y la imagen de la empresa.
Gestión de la calidad PDCA
La ISO 27001 se basa en la teoría de gestión de la calidad PDCA (también conocida como ciclo de Deming), como se podrá observar en la estructura de esta.

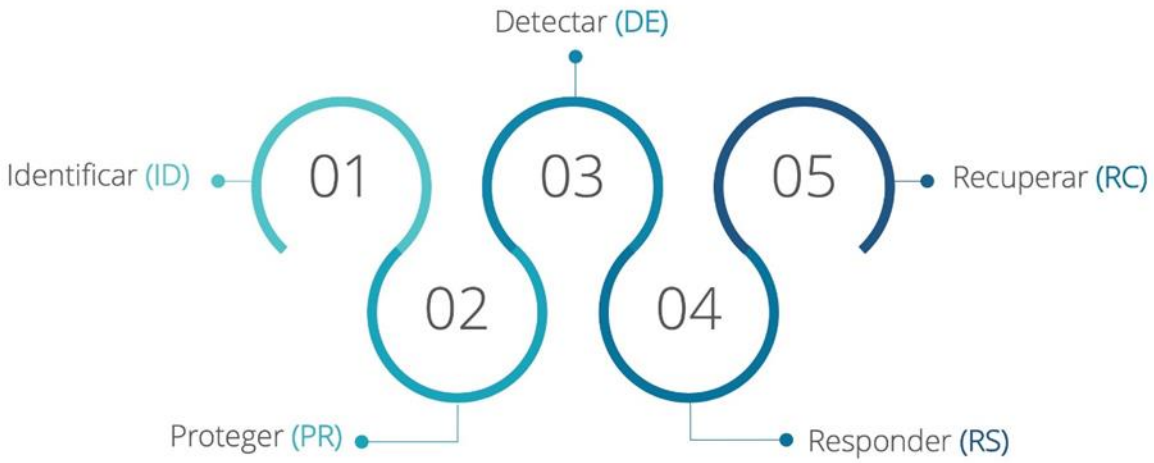
- Planificar (“Plan”): etapa inicial de diseño del SGSI en la que se realiza la identificación inicial de los riesgos asociados con la Seguridad de la información. Esta cuestión se complementa con un análisis cualitativo y cuantitativo (si es necesario) de los riesgos identificados y la planificación de la respuesta y los controles necesarios para la mitigación de estos.
- Hacer (“Do”): implantación y operación del Sistema de Gestión de Seguridad de la Información definido y desarrollado.

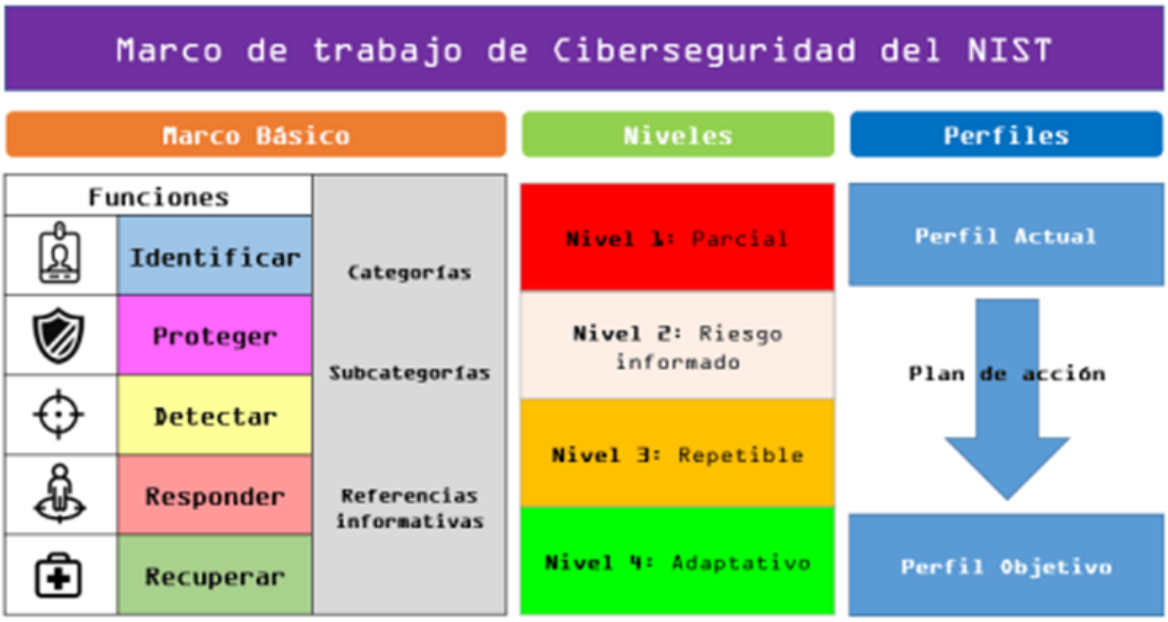
- Verificar (“Check”): revisar y evaluar su eficacia y eficiencia. Si el desempeño no es el esperado analizar las causas y determinar las mejoras.
- Actuar (“Act”): mejora continua del SGSI.

Se puede complementar también con la norma ISO 27002. La Organización Internacional de Estandarización (ISO, por sus siglas en inglés) también tiene otras normas ISO como son ISO 9001, ISO 14001 e ISO 45001.
Los 114 controles de la norma ISO 27001 están divididos en 14 secciones:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Controles de acceso.
- Criptografía – Cifrado y gestión de claves.
- Seguridad física y ambiental.
- Seguridad operacional.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento del sistema.
- Gestión de incidentes de seguridad de la información.
- Cumplimiento.

NIST Cybersecurity Framework: Marco desarrollado por el Instituto Nacional de Normas y Tecnologías (NIST), perteneciente al Departamento de Comercio de los Estados Unidos es utilizado por empresas de todos los tamaños para guiarlas a gestionar y reducir sus riesgos de ciberseguridad y protección de su información.
Funciona de la siguiente manera:





¿Cómo se implementa el CSF?

La implementación de un programa de ciberseguridad basado en CSF consta de los siguientes pasos iterativos:

- Paso 1 – Priorización y definición de alcance: Mediante la identificación de los objetivos y misión del negocio y las prioridades de alto nivel en términos organizacionales, se decide de forma estratégica el entorno de aplicabilidad de los controles. Este entorno puede ser toda la organización, una línea de negocio en particular o un proceso, teniendo presente que cada uno de estos elementos puede tener diferentes niveles de tolerancia al riesgo.
- Paso 2 – Orientación: Se identifican los sistemas, activos, requerimientos regulatorios, amenazas y vulnerabilidades vinculadas al entorno de aplicabilidad definido.
- Paso 3 – Crear un perfil actual: A través de las funciones del marco básico y empleando las categorías y subcategorías, se obtienen los resultados de implementación de controles en el entorno.
- Paso 4 – Ejecutar un análisis de riesgos: Se ejecuta un análisis de riesgos que permita determinar la probabilidad y el impacto de eventos de ciberseguridad en el entorno analizado.
- Paso 5 – Crear un perfil objetivo: Se establecen los objetivos que en términos de ciberseguridad la organización pretende cubrir.
- Paso 6 – Determinar, analizar y priorizar las brechas detectadas: Mediante el análisis diferencial entre el perfil actual y el perfil objetivo, se define un plan de acción priorizado en términos de coste/beneficio, que permita la determinación de recursos y acciones de mejora.
- Paso 7 – Implementar el plan de acción: Se procede con la alineación de controles y despliegue de mejoras de forma paulatina y monitorizada.

Todas estas acciones deben ser implementadas dentro de un entorno de mejora continua, permitiendo que de forma continua la organización optimice sus controles de seguridad y escale a niveles superiores dentro del marco de trabajo.

El Core consta de tres partes: Funciones, Categorías y Subcategorías. Incluye cinco funciones de alto nivel:
Identificar, Proteger, Detectar, Responder y Recuperar.
El siguiente nivel hacia abajo son las 23 categorías, que se dividen en las cinco funciones. Fueron diseñadas para cubrir la amplitud de los objetivos de ciberseguridad para una organización, sin ser demasiado detalladas, cubriendo temas relacionados a los aspectos técnicos, las personas y los procesos, con un enfoque en los resultados.
Las subcategorías son el nivel más profundo de abstracción en el Core. Hay 108 Subcategorías, que son declaraciones basadas en resultados que proporcionan consideraciones para crear o mejorar un programa de ciberseguridad. Debido a que el Marco está orientado a los resultados y no establece cómo una organización debe lograr esos resultados, permite implementaciones basadas en el riesgo que se adaptan a las necesidades de las distintas organizaciones.

PCI DSS: corresponde a un estándar global de protección de datos en industrias que manejan tarjetas de pago de crédito o débito. Su objetivo es asegurarse de que todas las empresas posean un nivel básico mínimo de seguridad que proteja los datos de los titulares de tarjetas de los datos considerados como críticos que son: PAN, nombre del titular de tarjeta, fecha de expiración, código de servicio, datos de banda magnética o su equivalente en chip, CAV2, CVC2, CVV2, CID, número de identificación personal y bloques de PIN.
En total, el estándar PCI DSS cuenta con 12 requisitos que se esquematizan en 6 grupos o "metas" de cumplimiento. Para que te hagas una idea, estos requisitos, a su vez, contemplan en total más de 300 controles de seguridad.

¿Quiénes deben cumplir con PCI DSS?
Si tu modelo de negocio almacena, procesa o transmite datos de titulares de tarjetas de pago, entonces debes cumplir con PCI DSS. No importa el tamaño de tu empresa.
Si acaso tu empresa no procesa ni almacena datos de tarjeta, pero usa pasarelas de pagos de terceros, también es muy probable que debas adherirte al cumplimiento de este estándar. Porque tal vez sea menos rígida la exigencia, pero debes estar certificado de igual manera.
Por otro lado, PCI DSS establece diferentes requisitos dependiendo de la cantidad de transacciones anuales de la compañía. Es decir, las agrupa según los siguientes niveles:

- Nivel 1: más de seis millones de transacciones anuales
- Nivel 2: entre uno y seis millones de transacciones anuales
- Nivel 3: entre 20.000 y un millón de transacciones anuales
- Nivel 4: menos de 20.000 transacciones anuales

Usualmente para los niveles 2, 3 y 4 solicitan que llenes un cuestionario de autoevaluación llamado SAQ o Self-Assessment Questionnaire, una herramienta de validación cuya intención es asistir a las empresas en el proceso de evaluar su cumplimiento con la norma PCI DSS.
Para el nivel 1, además de completar este SAQ, piden evidencia mucho más exhaustiva de cada requisito, ya que suelen ser empresas grandes como procesadoras de pago, bancos, Fintech dueñas de los botones de pagos, etc. En estos casos, la cantidad de controles y tiempos de auditoría suelen ser mayores.
PCI Data Security Standard (PCI DSS), es un estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el

tratamiento, procesado o almacenamiento de información de tarjetas de crédito. Su finalidad, la reducción del fraude relacionado con las tarjetas de pago e incrementar la seguridad de estos datos. Actualmente se encuentra en la versión 4.0

HIPAA: HIPAA (Health Insurance Portability and Accountability Act) es una ley de Estados Unidos que establece normas de privacidad y seguridad para la protección de la información médica confidencial de las personas. Esta ley establece reglas sobre cómo se deben utilizar y proteger los registros médicos y otra información personal sobre la salud de una persona. También establece normas para el envío de información médica a través de medios electrónicos y establece sanciones en caso de incumplimiento de estas normas. HIPAA es importante porque protege la privacidad de la información médica de las personas y garantiza que esta información solo sea utilizada para fines médicos legítimos.
La normativa HIPAA incluye dos reglamentos principales: el Reglamento de Privacidad de HIPAA y el Reglamento de Seguridad de HIPAA.
El Reglamento de Privacidad de HIPAA establece normas para proteger la privacidad de la información médica de las personas. Estas normas incluyen lo siguiente:
Las organizaciones que procesan o utilizan información médica deben tomar medidas para proteger la privacidad de esta información.
Las organizaciones deben informar a las personas sobre cómo utilizan su información médica y deben proporcionarles una copia de sus derechos de privacidad.
Las organizaciones solo pueden compartir información médica con terceros si el paciente ha dado su consentimiento o si es necesario para fines médicos legítimos.
El Reglamento de Seguridad de HIPAA establece normas para proteger la información médica de las personas de la pérdida, el uso indebido o la revelación no autorizada. Estas normas incluyen lo siguiente:
Las organizaciones deben tomar medidas para proteger la información médica de las personas de la pérdida, el uso indebido o la revelación no autorizada.
Las organizaciones deben utilizar medidas de seguridad apropiadas para proteger la información médica de las personas cuando se transmite a través de medios electrónicos.
Las organizaciones deben reportar cualquier pérdida o revelación no autorizada de información médica a las autoridades y a los pacientes afectados.
Es importante tener en cuenta que la normativa HIPAA solo se aplica a ciertas organizaciones y profesionales médicos, como los proveedores de atención médica, las aseguradoras médicas y otros procesadores de información médica.

Beneficios de cumplimiento de normas y estándares

- Permite optimizar los procesos y actividades de negocio desde el punto de vista operativo (aplicación de políticas, respuesta a incidentes…).
- Permite garantizar mayores niveles de seguridad y servicio a nuestros proveedores, clientes, partners y socios.
- Permite mejorar la reputación de la empresa, al ofrecer mayores garantías de seguridad y privacidad de los clientes.
- Permite que las empresas puedan destacar sobre la competencia y, por tanto, le aporta un valor diferencial.
- Permite conocer, identificar, analizar y prevenir los riesgos y vulnerabilidades, algunos de los cuales pueden derivar en sanciones legales, pudiendo reducir así sus impactos negativos.

- Permite ofrecer mecanismos para concienciar a los empleados de las buenas prácticas de seguridad.

Tipos de Políticas

Según el Instituto Nacional de Ciberseguridad (INCIBE):
"las políticas de ciberseguridad son las decisiones o medidas que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información".
Aunque bien es cierto que cada empresa, en función de su sector, tamaño, actividad o número de empleados, debe realizar su propia política de ciberseguridad, existen algunos puntos comunes que toda compañía debe tener en cuenta sobre esta cuestión, sobre todo en lo referente a contraseñas, RGPD, actualizaciones o softwares de protección (antivirus).

1 – Política de protección de datos
Un punto fundamental en cualquier política de ciberseguridad que incide, principalmente, en el área de sistemas es el cumplimiento de la seguridad legal.
Con este aspecto nos referimos a las normativas legales, aplicables a todas las empresas, relacionadas con la gestión y la protección de la información de los usuarios y los clientes, así como los sistemas informáticos que la procesan.

Estas normativas son:

- Reglamento General de Protección de Datos (RGPD)
- Ley Orgánica de Protección de Datos (LOPD)
- Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

2 – Política de contraseñas
Usar contraseñas personales y específicas para cada acceso es una de las principales medidas de ciberseguridad.
Se deben modificar de forma periódica, incluyendo en su formato letras, números, símbolos o caracteres especiales, mayúsculas y minúsculas.
También es conveniente utilizar doble factor de autentificación, como medida de seguridad extra para proteger las cuentas de los usuarios, a través de un mensaje SMS automático o una aplicación que genera códigos de acceso.

3 – Política de actualizaciones
Un aspecto al que algunas pymes no conceden la importancia que se merece es el de la política de actualizaciones de sus softwares.
Estas son necesarias para mantener la seguridad de nuestros sistemas de información, ya que cualquier programa o aplicación está expuesta a determinados riesgos, es decir, son vulnerables.
Para mantener una adecuada política de actualizaciones, es recomendable estar al tanto de las correcciones y parches que lanzan los fabricantes de los programas e implementarlos lo antes posible. De esta manera, evitaremos una falla en nuestros sistemas de seguridad y reduciremos el riesgo de exposición ante ciberamenazas.
Los atacantes suelen escanear las redes en busca de equipos desactualizados para intentar atacarlos. También se aprovechan de defectos de la configuración.

Te recomendamos activar las actualizaciones automáticas del sistema operativo y del software que uses en tus equipos y dispositivos de empresa.

4 – Política de almacenamiento y copias de seguridad

Entre las políticas de ciberseguridad básicas para la pyme se encuentran las políticas de almacenamiento y las copias de seguridad.

Toda empresa debe realizar un inventario y clasificación de activos de información, así como determinar la periodicidad de los backups y su contenido.

Se deben identificar los responsables de estas copias de seguridad y el procedimiento de estas para garantizar la continuidad del negocio. El control de acceso debe estar restringido a este personal autorizado.

5 – Política de seguridad en el puesto de trabajo

Las empresas también deben implementar una política de protección y seguridad del puesto de trabajo para garantizar un correcto uso de los dispositivos y medios que los empleados puedan utilizar. De esta manera, se minimizan riesgos y se trabaja en un entorno más seguro.

Para llevarla a cabo, los empleados deben conocer sus responsabilidades y obligaciones en materia de seguridad. La organización debe ser la responsable de facilitar esta información.

El objetivo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo a través de diferentes dispositivos (ordenadores de sobremesa, portátiles, móviles, impresoras, redes Wi-Fi…).

6 – Política de uso del correo electrónico

El email es una de las herramientas más utilizadas por los empleados en la mayoría de las empresas. Su uso se extiende tanto para la comunicación interna como externa.

Por eso, es imprescindible contar con una política de seguridad del correo electrónico que garantice su correcto uso y sirva para impedir errores, incidentes y usos ilícitos, así como para evitar ataques por esta vía.

Algunos de los puntos clave de esta política son:

- Normativa de uso
- Instalación de aplicaciones antimalware y antispam
- Cifrado y firma digital
- Desactivar el formato HTML y la descarga de imágenes
- Uso apropiado del correo corporativo
- Utilizar una contraseña segura
- Aprender a identificar correos sospechosos
- No responder al spam
- Inspección de enlaces

7 – Política de uso de Wifi y redes externas

Otra política de ciberseguridad para empresas que, en este caso afecta directamente a los empleados, es la del uso de wifi y redes externas inalámbricas. En muchas ocasiones, cuando

estamos fuera de la oficina, es necesario acceder a datos de la compañía y, en esos casos, la información puede quedar comprometida.
La empresa debe establecer las condiciones y circunstancias en las que se permite el acceso remoto a los servicios corporativos. Es decir, determinar quién puede acceder a qué, cómo y cuándo.
El objetivo de esta política de uso de redes externas es, por tanto, garantizar la protección de los datos e informaciones corporativas cuando el acceso a los mismos tenga lugar fuera de la oficina. Una de las herramientas que, por ejemplo, se pueden implantar para ello es la utilización de una Red Privada Virtual o VPN.

8 – Política de clasificación de la información
Por último, pero no menos importante, algunas organizaciones consideran clave definir una política de clasificación de la información para protegerla de forma adecuada. Los activos de información de una empresa pueden estar en formato digital o en otros soportes, como papel. Para aplicar las medidas de seguridad ajustadas a estos activos debemos realizar un inventario y clasificación, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración.
Para ello se aplicarán criterios de confidencialidad, integridad y disponibilidad, que conforman las principales áreas de la ciberseguridad en empresas. De esta manera podremos determinar qué información cifrar, quién puede utilizarla o quién es responsable de su seguridad.

Conclusiones

Las políticas de ciberseguridad en las empresas han tomado una mayor relevancia en la última década a raíz del acelerado proceso de digitalización y del consiguiente aumento de ciberataques por parte de los hackers de todo el mundo.
Las claves para implementar una estrategia efectiva es elaborar políticas y procedimientos adecuados, establecer una cultura empresarial de ciberseguridad y disponer de un plan de continuidad.
Por todo ello, la ciberseguridad debe ser un aspecto prioritario para todas las empresas, independientemente de su tamaño y el sector en el que operen.

ISO 27001:

BENEFICIOS DE LA NORMA ISO 27001
Los riesgos de seguridad de la información representan una amenaza considerable para las empresas debido a la posibilidad de pérdida financiera o daño, la pérdida de los servicios esenciales de red, o de la reputación y confianza de los clientes.
La gestión de riesgos es uno de los elementos clave en la prevención del fraude online, robo de identidad, daños a los sitios Web, la pérdida de los datos personales y muchos otros incidentes de seguridad de la información. Sin un marco de gestión de riesgos sólida, las organizaciones se exponen a muchos tipos de amenazas informáticas.
La nueva norma internacional ISO / IEC 27001 - seguridad de la información, ayudará a las organizaciones de todo tipo para mejorar la gestión de sus riesgos de seguridad de la información.

Hoy en día, seguridad de la información está constantemente en las noticias con el robo de identidad, las infracciones en las empresas los registros financieros y las amenazas de terrorismo cibernético. Un sistema de gestión de seguridad de la información (SGSI) es un enfoque sistemático para la gestión de la información confidencial de la empresa para que siga siendo seguro. Abarca las personas, procesos y sistemas de TI.

El diseño y la implementación de un SGSI (ISO / IEC 27001:2005) dará confianza a clientes y proveedores que la seguridad de la información se toma en serio dentro de la organización, estando a la vanguardia en la aplicación de la técnica de procesos para hacer frente a las amenazas de la información y a y los problemas de la seguridad.

¿QUÉ ENTENDEMOS POR INFORMACIÓN EN ISO 27001?

Sin duda, gran parte de la Información de una empresa se encuentra en los sistemas informáticos, sin embargo, la Norma ISO 27001 define la información como:

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

Metodología sugerida por la norma

1.- Identificar los Activos de Información y sus responsables, entendiendo por activo todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos ...) así como la marca, la reputación etc.
2.- Identificar las Vulnerabilidades de cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.
3.- Identificar las amenazas: Aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc.
4.- Identificar los requisitos legales y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores.
5.- Identificar los riesgos: Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación con su disponibilidad, confidencialidad e integridad del mismo.
6.- Cálculo del riesgo: Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.
7.- Plan de tratamiento del riesgo: En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección. En este punto, es donde seleccionaremos los controles adecuados para cada riesgo, los cuales irán orientados a :

- Asumir el riesgo
- Reducir el riesgo
- Eliminar el riesgo
- Transferir el riesgo

NIST CSF

El marco de ciberseguridad de NIST
El Instituto Nacional de Normas y Tecnología (NIST), una agencia perteneciente al Departamento de Comercio de los Estados Unidos desarrolló este marco voluntario de manera coherente con su misión de promover la innovación y la competitividad en el país. El Cybersecurity Framework de NIST utiliza un lenguaje común para guiar a las compañías de todos los tamaños a gestionar y reducir los riesgos de ciberseguridad y proteger su información.
Este marco no provee nuevas funciones o categorías de ciberseguridad, sino recopila las mejores prácticas (ISO, ITU, CIS, NIST, entre otros) y las agrupa según afinidad. Se centra en el uso de impulsores de negocio para guiar las actividades de ciberseguridad y considerar los riesgos cibernéticos como parte de los procesos de gestión de riesgos de la organización. El framework consta de tres partes: el marco básico, el perfil del marco y los niveles de implementación.

Marco básico (Framework Core)	Niveles de implementación del marco (Framework Implementation Tiers)	Perfiles del marco (Framework Profiles)
Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el de implementación/operación. El Framework Core consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar.	Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa.	Los perfiles se emplean para describir el estado actual (Current Profile) y el estado objetivo (Target Profile) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

El Framework Core comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía. Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Por su parte, los niveles de implementación del marco (tiers) proporcionan un mecanismo para que las empresas puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad.

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Niveles de implementación

Los tiers proporcionan un contexto sobre cómo una organización ve el riesgo de la ciberseguridad y los procesos implementados para manejarlo. Las escalas describen el grado en que las prácticas de gestión de riesgos cibernéticos de una empresa exhiben las características definidas en el marco. Por ejemplo: riesgo y amenaza, repetible y adaptable.

Los niveles de implementación caracterizan las prácticas de una compañía en un rango, desde parcial hasta adaptativo. Estos niveles reflejan una progresión desde respuestas informales y reactivas hasta enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de un tier, la empresa debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio/misión y restricciones de organización.

NIVEL	TIPO	PROCESO DE GESTIÓN DE RIESGOS	PROGRAMA DE GESTIÓN INTEGRADA DE RIESGOS	PARTICIPACIÓN EXTERNA
1	PARCIAL	No se formalizan las prácticas organizativas de gestión de riesgos de ciberseguridad y se gestiona el riesgo de manera ad hoc ya veces reactiva.	Se conoce muy poco el riesgo de ciberseguridad a nivel organizativo y no se ha establecido un enfoque de gestión del riesgo de ciberseguridad en toda la organización.	Puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades.
2	RIESGO INFORMADO	Las prácticas de gestión de riesgos son aprobadas por la administración pero no pueden establecerse como políticas de toda la organización.	Se conoce el riesgo de ciberseguridad a nivel organizativo, pero no se ha establecido un enfoque a nivel de toda la organización	La organización conoce su papel en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.
3	REPETIBLE	Las prácticas de gestión de riesgos de la organización son formalmente aprobadas y expresadas como políticas.	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de la ciberseguridad.	La organización entiende sus dependencias y socios y recibe información que permite la colaboración y las decisiones de gestión basadas en el riesgo
5	ADAPTATIVO	La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos	la organización gestiona el riesgo y comparte activamente la información con los socios para garantizar que se distribuye información precisa para mejorar la ciberseguridad antes de que se produzca un evento

¿Qué es un SGSI?

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos y medidas de seguridad que se utilizan para proteger la información y garantizar su confidencialidad, integridad y disponibilidad. El SGSI se basa en un análisis de riesgos que permite evaluar los posibles riesgos para la información y tomar medidas para mitigarlos.

El SGSI se aplica a todos los aspectos de la información, incluyendo su recopilación, almacenamiento, procesamiento, transmisión y eliminación. También se ocupa de la protección de la información física, como los sistemas informáticos y los documentos impresos.

El SGSI es importante porque protege la información de la pérdida, el uso indebido o la revelación no autorizada y ayuda a garantizar la confidencialidad, integridad y disponibilidad de la información. También es importante para cumplir con las regulaciones y normativas que establecen requisitos de seguridad de la información, como la normativa HIPAA en el sector de la atención médica.

La implementación de un SGSI requiere la realización de un análisis de riesgos y la definición de políticas y procedimientos de seguridad. A continuación, se presentan algunos pasos clave para implementar un SGSI:

Identificar los objetivos y alcance del SGSI: Es necesario definir los objetivos del SGSI y el alcance de su aplicación. Esto incluye determinar qué información debe protegerse y qué medidas de seguridad deben aplicarse.

Realizar un análisis de riesgos: Es necesario evaluar los posibles riesgos para la información y determinar las medidas de seguridad necesarias para mitigarlos.

Definir políticas y procedimientos de seguridad: Es necesario establecer políticas y procedimientos de seguridad que establezcan las medidas de seguridad apropiadas para proteger la información.

Implementar medidas de seguridad: Es necesario poner en práctica las medidas de seguridad definidas en las políticas y procedimientos de seguridad. Esto puede incluir la contratación de personal de seguridad, la implementación de software de seguridad y la formación del personal en seguridad de la información.

Monitorear y evaluar el SGSI: Es necesario monitorear y evaluar continuamente el SGSI para asegurar su efectividad y hacer ajustes en caso de ser necesario.

Es importante tener en cuenta que la implementación de un SGSI es un proceso continuo y requiere una atención constante para garantizar la protección adecuada de la información.

1. Fase de evaluación

Primero que todo, debes someter a evaluación a tus sistemas e infraestructura. Tu seguridad informática siempre dependerá de la madurez de la seguridad informática y en similar medida; del modelo de infraestructura con la que cuentas.
Este diagnóstico te indicará la etapa y las medidas correctivas a tomar para corregir para darle paso a la implementación de tu SGSI bajo estándares ISO 27001.

2. Planificación
Seguido y una vez sepas con certeza qué te hace falta o qué necesitas para poner a tono tus sistemas con la norma ISO 27001; necesitas planificar y estudiar tus opciones para la implementación del SGSI. Así pues tienes estas opciones:

Auto-gestión. Es la alternativa tipo hágalo usted mismo. Vale la pena adoptarla si cuentas con el personal técnico y la documentación necesaria para mitigar el impacto del cambio; es decir, estás en un Nivel 3 o superior de Madurez de Seguridad Informática. De ser así, te ahorrará tiempo y dinero.
Contratación de un consultor. Esta alternativa es la más recomendada para empresas con un Nivel 1 de Madurez de Seguridad Informática. Con ella, cedes todo el poder de la implementación a un experto que obligatoriamente tiene que darte las respuestas que necesitas; y garantizarte todas certificaciones relacionadas.
Opción mixta. Combina las anteriores. Funciona mejor en empresas con Nivel 2 de Madurez de Seguridad Informática; y saca lo mejor de tus fortalezas y las del consultor experto en seguridad. Esta opción puede incluir tutoriales, ayuda en línea y apoyos similares.
Todas las opciones ofrecen ventajas y desventajas que te conviene medir muy bien. Lo más recomendable en este punto es hacer una matriz DOFA que recojan estas variables:

- Gasto general.
- Inversión en tiempo.
- Integridad de la documentación.
- Transferencia de Conocimiento.
- Certificaciones.

Cada una de estas variables recogen tareas y actividades que van desde la elección del personal técnico encargado; hasta la puesta en marcha de la implementación.

3. Documentación + Gantt
El tercer paso consiste en reunir toda la documentación pertinente para alimentar la base de conocimiento; y agruparla por actividades y tareas lógicas en un tiempo determinado. Con este paso, ya el proyecto comienza a materializarse en base a la planificación elegida, ajustada al tamaño de tu empresa.

4. Organización
El cuarto paso es organizar la documentación por fases de ejecución y organización del proyecto. La campana de Gantt de la fase de ejecución para la integración de SGSI bajo norma ISO 27001 es el reloj que indica el ritmo para la integración que, sin duda, debe estar bajo el mando de líderes de proyecto.
En esta etapa también se compilan los manuales para ser utilizados al momento de lanzar las campañas de concientización respecto a la implementación del SGSI bajo norma ISO 27001.

5. Presentación

Seguido, damos el quinto paso para integrar todo lo recogido en los pasos anteriores. Se presenta el proyecto factible a la alta gerencia y a los involucrados en su ejecución.

La presentación incluye alcances de la norma ISO 27001; exposición de motivos y políticas; recoge los resultados de la fase de evaluación; define el tratamiento de los riesgos detectados; declara la aplicabilidad o no de los controles; los motivos que apoyan la decisión y la forma de aplicación.

Asimismo se presentan los resultados de la medición de la eficacia de los controles para dar un panorama completo de los alcances totales de la norma.

6. Despliegue y puesta en marcha

Finalmente, el sexto y último paso comienza con la aprobación de la directiva. Una vez este cuerpo da el visto bueno, inician las campañas de concientización en forma de programas cortos en forma de programas cortos para el despliegue y puesta en marcha del proyecto.

Esto supone implementar de la misma manera los controles; procedimientos exigidos; los programas de capacitación unidos a los de concientización. El SGSI comenzará a formar parte del día día laboral.

Con ello; comenzará la emisión de registros que mantendrán informados a los auditores y agentes autorizados sobre el verdadero rendimiento de la empresa, sus empleados, y el éxito de la implementación de la Norma 27001 para tus SGSI.

Si te decantas por la opción b o c durante la fase de Planificación, tienes en nosotros un aliado ideal para llevar adelante tu implementación en SGSI bajo norma 27001.