

# MN<sub>E</sub>MO



Módulo 1

Introducción a la  
Seguridad Informática

## INTRODUCCIÓN A LA SEGURIDAD

### Contenido

¿Qué es la Seguridad Informática?.....	4
Propiedades de la Seguridad de la Información.....	4
Confidencialidad (Confidentiality).....	4
Autenticación vs Autorización .....	6
Autenticación.....	6
Autorización.....	6
Autenticación vs Autorización .....	6
Mecanismos de autorización .....	7
Riesgo, Amenaza y Vulnerabilidad.....	8
Riesgo.....	8
Amenaza.....	8
Vulnerabilidad.....	8
¿Qué es el Hacking?.....	8
Hackers de sombrero blanco (White Hat Hackers).....	9
Hackers de Sombrero Gris (Grey hats hackers).....	9
Anonymous.....	9
LulzSec.....	9
Syrian Electronic Army.....	10
Lizard Squad .....	10
Asley Madison (Julio 2015).....	11
Wannacry (Mayo 2017).....	11

Equifax (Septiembre 2017) .....	12
Diferencias entre IT y OT.....	12
Aspectos IT .....	12
Aspectos OT.....	13
Convergencia IT/OT.....	14
Introducción al Sistema de Gestión de Seguridad ISO/IEC27001:2022.....	14
Alcance .....	17
Sistemas de gestión de la seguridad de la información .....	17
Principios fundamentales.....	18
Dimensiones de la Seguridad de la Información.....	19
Órgano de dirección.....	20
Establecer, monitorizar, mantener y mejorar un SGSI.....	21
Identificar los requisitos de Seguridad de la Información. ....	22
Controles de seguridad.....	23
Controles Organizacionales: .....	27
Gestión de los riesgos en Seguridad de la Información .....	29
Mantenimiento y mejora de la efectividad del SGSI.....	31
Factores de éxito.....	31
Combinación con otros sistemas de gestión.....	32
Certificación del SGSI .....	34
Estructura de la norma .....	36
Periodo de adecuación a la norma.....	37

## ¿Qué es la Seguridad Informática?

La seguridad informática, generalmente consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió.

La seguridad informática busca la protección contra los riesgos ligados a la informática.

Los riesgos se calculan en función de varios elementos:

- Las amenazas que pesan sobre los activos a proteger.
- Las vulnerabilidades de estos activos.
- Su sensibilidad, la cual es la conjunción de diferentes factores como la confidencialidad, la integridad, la disponibilidad.

## Propiedades de la Seguridad de la Información

### Confidencialidad (Confidentiality)

El acceso a los activos del sistema está limitado a usuarios autorizados. Estamos respondiendo a la pregunta: ¿quién podrá acceder a los mismos?

La confidencialidad intenta prevenir la revelación no autorizada, intencional o no, del contenido de un mensaje o de información en general.

La pérdida de información puede producirse de muchas maneras, por ejemplo, por medio de la publicación intencional de información confidencial de una organización o por medio de un mal uso de los derechos de acceso en un sistema.

### Integridad (Integrity)

Los activos del sistema sólo pueden ser borrados o modificados por usuarios autorizados, ¿qué se podrá hacer con ella?

La integridad asegura que:

- No se realizan modificaciones de datos en un sistema por personal o procesos no autorizados.
- No se realizan modificaciones no autorizadas de datos por personal o procesos autorizados.
- Los datos son consistentes, es decir, la información interna es consistente entre sí misma y respecto de la situación real externa.

Disponibilidad (Availability)

El acceso a los activos en un tiempo razonable está garantizado para usuarios autorizados.

La información tiene que estar disponible para quienes la necesiten y cuando la necesiten, si están autorizados: ¿de qué manera, y cuando se podrá acceder a ella?

La disponibilidad asegura que el acceso a los datos o a los recursos de información por personal autorizado se produce correctamente y en tiempo. Es decir, la disponibilidad garantiza que los sistemas funcionan cuando se les necesita.

Lo contrario de la confidencialidad, integridad y la disponibilidad son la revelación, la modificación y la destrucción.



## Autenticación vs Autorización

### *Autenticación*

Es el acto o proceso de confirmar que algo (o alguien) es quien dice ser para posteriormente acceder a ciertos recursos definidos.

### *Autorización*

Es el proceso sobre el cual se establecen que tipos de recursos están permitidos o denegados para cierto usuario o grupo de usuarios concreto.

### Autenticación vs Autorización

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

- Sistemas basados en algo conocido. Ejemplo, una contraseña o un número de identificación personal (PIN).



- Sistemas basados en algo poseído. Ejemplo, una tarjeta de identidad, una tarjeta inteligente (smartcard) o tarjeta de coordenadas.
- Sistemas basados en algo que se es (característica física delante usuario o un acto involuntario del mismo): Ejemplo, verificación de voz o huellas dactilares.

La autenticación fuerte puede conseguir usando al menos 2 de los factores anteriormente descritos.

### Mecanismos de autorización

El mecanismo o el grado de autorización puede variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica.

Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización:

- **Control de Acceso Discrecional (DAC):** Es una forma de acceso a recursos basada en los propietarios y grupos a los que pertenece un objeto. El ejemplo más representativo es el mecanismo de permisos establecido por el dueño (usuario/grupo) del sujeto. Así, es el propio dueño del objeto quien determina qué usuarios y con qué privilegios acceden a sus objetos.
- **Control de Acceso Basado en Roles (RBAC):** El control de acceso basado en roles consiste en la definición de perfiles (roles) a los que se les atribuyen una serie de características que aplican sobre los permisos y acciones que pueden llevar a cabo, incluyendo el control sobre otros perfiles. Es, en cierto modo un sistema jerárquico de clases.
- **Control de Acceso Obligatorio (Mandatory Access Control, MAC):** El mecanismo MAC se basa en un "etiquetado" de todo elemento del sistema y sobre las cuales se aplicarán las políticas de control de acceso configuradas. De este modo, cualquier operación de un sujeto sobre un objeto será comprobado las etiquetas y

aplicando las políticas MAC establecidas para determinar si la operación está permitida, aún incluso cuando se hayan cumplido otros controles de seguridad.

## Riesgo, Amenaza y Vulnerabilidad

### *Riesgo*

Es la exposición a pérdida o posible daño de la información que pueda causar pérdida de dinero, tiempo y reputación entre otras.

### *Amenaza*

Es cualquier actividad que represente posible daño a su información. Las amenazas se pueden clasificar según su origen en internas y externas.

### *Vulnerabilidad*

Es una debilidad en la seguridad de la información que puede ser explotada por una amenaza; que podría ser, una debilidad en su sistema de seguridad de red, procesos, y procedimientos.

## ¿Qué es el Hacking?

Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

Hay varias clases de estos, entre las que destacan:





### Hackers de sombrero blanco (White Hat Hackers)

Este término se refiere a los expertos en seguridad informática que se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas.

### Hackers de Sombrero Gris (Grey hats hackers)

A medio camino entre uno y otro bando, los hackers en la zona gris no suelen actuar por intereses personales y suelen comunicar al resto de la comunidad hacker los hallazgos o vender los hallazgos obtenidos, así como hacer pública la información obtenida para el conocimiento de la población.

### Anonymous

"Somos Anonymous. Somos Legión. No olvidamos. No perdonamos... Espéranos".

Peculiares máscaras y han atacado a varias webs gubernamentales, alguna página corporativa o relacionada con el fundamentalismo religioso.

El grupo ha declarado la guerra a la Cienciología y ha hackeado el Pentágono, por lo que no hay que perderlos de vista.

En 2012 también atacaron MasterCard, Visa y PayPal por negarse a procesar los pagos de WikiLeaks.

Se han arrestado a varios grupos de personas pertenecientes a la organización en Estados Unidos, Inglaterra, España, Turquía, Australia y los Países Bajos.

### LulzSec

Se creó como un spin-off de Anonymous, y ya sabéis lo que dicen: "De tal palo, tal astilla".

El slogan del grupo es: "Riéndonos de tu seguridad desde 2011".

Hackearon las webs oficiales de Fox y de Sony Pictures. Además, el grupo consiguió que la página de la CIA se cayera durante varias horas.

LulzSec es bastante conocido por ridiculizar a sus víctimas después de sus ataques. Los expertos han llegado a comparar sus ataques a las bromas que circulan por la Red.

En 2012, todos los miembros de LulzSec fueron arrestados y procesados después de que su líder, Sabu, les delatara.

### Syrian Electronic Army

El Ejército Electrónico Sirio dirige sus ataques a los grupos políticos de la oposición del país para apoyar al presidente Bashar al-Assad.

Se definen a sí mismos como "un grupo de jóvenes sirios entusiastas que no pueden permanecer pasivos ante la distorsión de los hechos de las últimas revueltas en el país".

Han llegado a estar implicados en el uso de malware, phishing, spam y ataques DDoS. Además, con frecuencia, publican la bandera siria en la web de la víctima.

Son muchos los que piensan que este grupo está dirigido por el propio gobierno.

### Lizard Squad

Es el grupo de hackers más popular de los últimos tiempos es Lizard Squad.

Esta banda no sólo está detrás de las últimas caídas de Facebook, sino también de los ataques a la web de Malaysia Airlines que dirigían a los visitantes de la web a una página que decía: "Error 404: avión no encontrado".

Lizard Squad también es responsable de varios ataques a Sony y Microsoft.

Fue arrestado por las autoridades después de los ataques a Xbox y PlayStation.

## Asley Madison (Julio 2015)



## Wannacry (Mayo 2017)



El ataque sufrido en muchas empresas a partir del viernes nos ha hecho reflexionar sobre la importancia de la concienciación en ciberseguridad para tener de manera adecuada y segura nuestros sistemas. Dicho ataque ha sido categorizado como ransomware como explicábamos en el artículo de ayer y más concretamente en una de sus variantes

## Equifax (Septiembre 2017)

**Un ciberataque masivo roba los datos de 143 millones de estadounidenses**

La firma de información crediticia Equifax admitió hoy un acceso ilegal a sus bases de datos que se produjo en mayo



EFE

Nueva York - 8 SEP 2017 - 09:51 CEST



Sede de la compañía Equifax en Atlanta (EE UU). MIKE STEWART (AP)

La firma estadounidense de información sobre solvencia crediticia Equifax



## Diferencias entre IT y OT

*Aspectos IT*

- Es un sector maduro, con prácticas, normas, marcos de control y sistemas de revisión bien establecidos.
- Está centrado casi exclusivamente en la información y los sistemas que soportan los procesos de gestión de las compañías.
- Con herramientas de colaboración (correo, mensajería, voz, video, etc...)
- Con unas redes de comunicaciones internas, "externas" y de acceso a internet.
- Se utilizan protocolos de comunicaciones unificados (sobre TCP/IP).
- Con un esquema de protección de la información y las infraestructuras (seguridad lógica) que tiene más de 20 años en mejora continua.

- Basado en un “Modelo de Fortaleza” (seguridad perimetral) que ha permitido a las organizaciones ofrecer servicios internos centralizados, con transparencia, integridad, disponibilidad, confidencialidad y eficiencia.
- Con una gestión relativamente eficaz de los múltiples “agujeros” creados en los últimos años en el perímetro, para la interacción con socios, proveedores, clientes y las Administraciones Públicas.

### Aspectos OT

- Existen sistemas técnicos de diferente tamaño y complejidad.
- Controlan la operativa diaria de la industria y han estado siempre, desde sus inicios.
- Suelen estar aislados de los sistemas corporativos.
- Ejemplo de estos sistemas son los SCADA (Supervisory Control and Data Acquisition), DSS (Distributed Control System), PLCs(Programmable Logic Controller), etc..

IT	Aspecto	OT
Confidencialidad, Integridad y Disponibilidad.	Objetivo	Disponibilidad, integridad y confidencialidad.
2/3 años con la existencia de gran número de proveedores.	Ciclo de vida	10/20 años con reducido número de proveedores específicos y sectoriales.
Práctica habitual que conduce a inversión en ciberseguridad.	Evaluación cuantitativa del riesgo	Práctica realizada si es obligatoria.
Habitual e integrada en la operación.	Desarrollo de sistemas de gestión de la seguridad	No habitual y no integrada.
Común, fácil de actualizar y con políticas bien definidas y automatizadas.	Antivirus y parches	Poco habitual por la criticidad de los sistemas, complejo de desplegar y actualizar y sin políticas específicas.
Normativas genéricas	Cumplimiento normativas	Normativas específicas y/o sectoriales.
Utilización de las metodologías estándares más actuales.	Testeo y auditorías	Realización de test específicos e inexistencia de metodologías estándares.
Fácil despliegue y en ocasiones carácter obligatorio.	Respuesta a incidencias y análisis forense	Poco habitual, no realizándose análisis forense.



### *Convergencia IT/OT*

Una sola organización para alinear TI y OT manteniendo los enfoques y alcances de servicio de cada grupo:

- Gestión unificada en la ejecución de proyectos operacionales, minimiza y armoniza duplicación y/o superposición de sistemas y procesos de gestión.
- Elimina responsabilidades divididas entre IT y OT en materias de seguridad, administración, sin diluir responsabilidades de cada uno en sus respectivos segmentos de operación.
- Reduce dispersión & variedad de sistemas y tecnologías, optimiza procesos
- de soporte, servicios y repuestos.
- Enfoca y sistematiza las estructuras, estrategias y planes aplicables en cada nivel de la operación por los equipos IT y OT en sus respectivos niveles de acción y responsabilidad.
- Soporte y optimización operacional integrado desde los niveles de negocios hasta los niveles de producción.

### Introducción al Sistema de Gestión de Seguridad ISO/IEC27001:2022

Estándares dedicados a la implantación de Sistemas de Gestión de Seguridad de la Información, como es el caso de ISO/IEC 27001:2022, son inicialmente considerados por muchos de los directivos y/o plantillas de las empresas lejos de su interés y de utilidad práctica en las actividades consideradas como productivas del día a día.

Sin embargo, descuidar la atención al mantenimiento de unas mínimas garantías en la disponibilidad, confidencialidad e integridad de la información necesarias para el desarrollo de los procesos críticos de negocio avoca, tarde o temprano, a la ruina a todo tipo de organizaciones (grandes y pequeñas) en términos de productividad, de reputación, de pérdidas financieras, de pérdida de oportunidad y de competitividad en



los mercados y/o exposición a multas por incumplimiento de contratos y de la legislación relevante, tal y como podemos constatar en la prensa diaria.

Diferentes estudios señalan cifras que apuntan a que actualmente y cada día, millones de personas son víctimas de los delitos informáticos, del robo de información o de los códigos maliciosos.

El 43% de todas las violaciones de datos involucran a pequeñas y medianas empresas.

Si todavía niega las posibilidades de que su pequeña empresa se convierta en una víctima, el 61% de todas las PYMES han informado al menos un ataque cibernético durante el año anterior.

Un estudio de referencia realizado por CISCO encontró que el 40% de las pequeñas empresas que enfrentaron un ataque cibernético severo experimentaron al menos ocho horas de inactividad. Y este tiempo de inactividad representa una parte importante del costo total de una brecha de seguridad.

El estudio de CISCO mencionado anteriormente también encontró que el ransomware no se encontraba entre las tres principales amenazas cibernéticas identificadas por las pequeñas empresas. Los dueños de negocios pueden estar subestimando la amenaza del ransomware, sin embargo, los MSP no lo hacen. El 85 % de los MSP consideran que el ransomware es una de las mayores amenazas para sus clientes SMB.

El 30 % de las pequeñas empresas considera que los ataques de phishing son la mayor amenaza cibernética.

El 83% de las pequeñas y medianas empresas no están financieramente preparadas para recuperarse de un ciberataque.

A pesar de las cifras asombrosas, el 91 % de las pequeñas empresas no han adquirido un seguro de responsabilidad cibernética. Esto realmente refleja cuán inconscientes y poco

preparados están los propietarios de pequeñas empresas para lidiar con las brechas de seguridad.

Solo el 14% de las pequeñas empresas consideran que su capacidad de mitigación de riesgos y ataques cibernéticos es altamente efectiva.

El 43 % de las pymes no cuenta con ningún plan de ciberseguridad.

Una de cada cinco pequeñas empresas no utiliza la seguridad de punto final y el 52 % de las pymes no cuentan con ningún experto en seguridad de TI interno.

Fuente: Ciber Security Magazine (<https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/>)

La adopción de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica para una organización. El Sistema de Gestión de Seguridad de la Información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de Gestión de Riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.

Es importante que el Sistema de Gestión de Seguridad de la Información forme parte, y se integre junto a los procesos de la organización y la estructura general de gestión y de Seguridad de la Información. Se espera que la implementación de un Sistema de Gestión de Seguridad de la Información se aplique de acuerdo con las necesidades de la organización.

Esta Norma Internacional pueden utilizarla indistintamente partes internas y externas para evaluar la capacidad de la organización de cara a satisfacer las propias necesidades de Seguridad de la Información.



## Alcance

Esta Norma Internacional especifica los requisitos para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información, en base a un conjunto de procesos formales (requisito Cláusula 4.4 de la norma), que debemos ser capaces de planificar y controlar (requisito Cláusula 8.1 de la norma), posiblemente los requisitos más importantes de un SGSI.

Esta norma también incluye los requisitos de seguridad de la información de partes interesadas, así como los de la evaluación y tratamiento de riesgos de Seguridad de la Información adaptados a las necesidades de la organización.

Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

## Sistemas de gestión de la seguridad de la información

Un SGSI (Sistema de Gestión de Seguridad de la Información) proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio, a través de la política de seguridad de la información y los objetivos de seguridad de la información.

La base de un SGSI reside en, conociendo el contexto de la organización y los requisitos de todas las partes interesadas, evaluar los riesgos y fijar los niveles determinados como adecuados por parte de la dirección de la organización para la aceptación de un nivel de riesgo de modo que se puedan tratar y gestionar los riesgos con eficacia y eficiencia.

El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.

El Sistema de Gestión incluye el liderazgo, la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

### Principios fundamentales

En este sentido, los principios fundamentales que contribuyen a la exitosa implementación de un SGSI son:

- Entender la organización, su contexto y los elementos relevantes que podrían afectar a los objetivos del SGSI.
- Entender las necesidades y expectativas de las partes interesadas.
- El liderazgo y La asignación de responsabilidades para la Seguridad de la Información.
- La formación y concienciación en Seguridad de la Información.
- El compromiso y liderazgo de la Dirección.
- Las evaluaciones de riesgos para determinar el estado actual y las estrategias adecuadas para asumir, transferir, evitar y/o reducir el riesgo para alcanzar los niveles aceptables de riesgo.
- La seguridad incorporada como un elemento esencial de las redes y sistemas de información.
- La prevención activa y detección de incidentes de Seguridad de la Información.
- Asegurar un enfoque integral de gestión de Seguridad de la Información.
- Una reevaluación regular de la Seguridad de la Información y la aplicación de modificaciones según sea apropiada.
- Un enfoque de mejora continua.

## Dimensiones de la Seguridad de la Información

La Seguridad de la Información comprende al menos las siguientes tres dimensiones fundamentales:

- Confidencialidad.
- Disponibilidad.
- Integridad.

La confidencialidad se refiere al acceso a la información por parte únicamente de quienes estén autorizados.

La verificación y la autorización son dos de los mecanismos que se emplean para asegurar la confidencialidad de la información.

La disponibilidad se refiere al acceso a la información y los sistemas de tratamiento de esta por parte de los usuarios autorizados cuando lo requieran.

La falta de disponibilidad se manifiesta principalmente por:

- La **denegación o repudio del servicio** debido a la falta de garantías de la prestación de este, tanto por parte del prestador del servicio como del solicitante o tomador (controles de identificación fehaciente, falta de prestaciones de los equipos, congestión de líneas, entre otros posibles).
- La **pérdida de servicios** de los recursos de información por causa de catástrofes naturales o por fallos de equipos, averías, acción de virus, etc.
- La **integridad** significa un mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Respecto a esta dimensión, la información se debe preservar y poner a disposición de sus propietarios y de los usuarios autorizados de una forma precisa, completa y oportuna mediante la protección de información, datos, sistemas y otros activos informáticos contra

cambios o alteraciones en su estructura o contenido ya sean intencionados, no autorizados o casuales.

Partiendo de estas tres dimensiones fundamentales existen organizaciones que pueden necesitar de otras adicionales como, por ejemplo, la trazabilidad y la autenticidad para organismos públicos y en referencia al marco especificado por el Esquema Nacional de Seguridad o incluso, el denominado no-repudio en entornos de uso de claves de cifrado (p.ej. uso del DNI) como garantía ante la posible negación de una entidad o un usuario de que ciertas transacciones tuvieron lugar.

Estas dimensiones añadidas a las fundamentales de confidencialidad, integridad y disponibilidad significarán, en cualquier caso, una extensión opcional y particular en base a las necesidades concretas de aplicación de un SGSI que cada organización debe valorar y no un requisito fundamental del estándar ISO/IEC 27001:2022.

### Órgano de dirección

En términos de un SGSI, la gestión consiste en la supervisión y toma de decisiones necesarias para poder alcanzar los objetivos de negocio mediante la protección de los activos de información de la organización.

La gestión de la Seguridad de la Información se expresa a través de la formulación y uso de las políticas de Seguridad de la Información, objetivos, normas, procedimientos y directivas que se aplican en toda la organización y por todos los individuos vinculados con la organización.

La gestión implica el desarrollo de actividades para dirigir, controlar y aplicar mejoras a la organización de manera dinámica y continuada dentro de unas estructuras adecuadas.

Las actividades de dirección incluyen la implantación de prácticas y la adecuada gestión y supervisión de los recursos disponibles de la organización y su estructura se extiende



desde el ámbito de una única persona en organizaciones pequeñas hasta llegar a un grupo más o menos amplio de individuos en aquellas más grandes.

En relación con el estándar ISO/IEC 27001:2022 el término “órgano directivo” o “dirección” puede referirse a una persona, pero también a un grupo de personas con la suficiente autoridad y responsabilidad para dirigir y controlar una organización al nivel requerido y para el alcance de aplicación del SGSI que se haya decidido abordar.

Esto significa que ciertos responsables localizados en posiciones medias del organigrama de una empresa de tamaño medio o grande pueden considerarse como la dirección con relación a las cláusulas relevantes de ISO/IEC 27001:2022, siempre y cuando el responsable asignado tenga plena capacidad de decisión y gestión de los recursos relevantes para la implantación y mantenimiento del SGSI.

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección.

No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización.

No se debe caer en el error habitual de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama y en el que la dirección únicamente participa para la aprobación económica de las necesidades.

Se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

### Establecer, monitorizar, mantener y mejorar un SGSI

Una organización necesita llevar a cabo los siguientes pasos para el establecimiento, control, mantenimiento y mejora de su SGSI:



- Identificar las partes interesadas, sus requisitos y expectativas.
- Identificar los activos de información y sus requisitos de seguridad asociados.
- Evaluar los riesgos de Seguridad de la Información.
- Seleccionar y aplicar los controles pertinentes para gestionar los riesgos inaceptables.
- Supervisar, mantener y mejorar la eficacia de los controles de seguridad asociados con los activos de información de la organización.
- Para garantizar la protección efectiva de los activos de información del SGSI dentro de la organización de forma permanente es necesario que los cuatro pasos anteriores se repitan continuamente para estar en posición de identificar cambios en los riesgos, en las estrategias de la organización y/o en los objetivos de negocio.

#### Identificar los requisitos de Seguridad de la Información.

Es importante iniciar la identificación de los requisitos para la Seguridad de la Información partiendo de un contexto global basado en los objetivos generales, la estrategia de negocio de la organización, su tamaño y la posible distribución geográfica, entre otros.

A partir de esta información global pasamos a identificar en consecuencia los requisitos y/o expectativas de Seguridad de la Información a través de:

- La identificación de los activos de información y su valor.
- Las necesidades del negocio para el procesamiento y almacenamiento de información.
- Los requisitos legales, reglamentarios y contractuales.
- Las expectativas de las partes interesadas.

Realizar una evaluación metódica de los riesgos implica analizar:

- Las amenazas a los activos de información.

- Los factores de vulnerabilidad ante la posibilidad de que una amenaza se materialice.
- El impacto potencial de cualquier incidente de Seguridad de la Información sobre los activos de información.
- Actualmente ISO 27001:2022 únicamente menciona la necesidad de la gestión de los riesgos a través de servicios y/o productos proveídos por terceros, asociados a la pérdida de confidencialidad, integridad y disponibilidad, tras analizar las potenciales consecuencias y la probabilidad para, finalmente, cuantificar el riesgo. Adicionalmente se deberá identificar al propietario del riesgo.

El gasto en controles de seguridad pertinentes debería ser proporcional al impacto calculado para el negocio y en base a la percepción de que el riesgo se materialice.

### Controles de seguridad

Una vez que los requisitos de Seguridad de la Información han sido identificados en base a los niveles de riesgo evaluados para los activos de información se deben abordar diversas estrategias para la gestión de los riesgos no asumibles por la dirección de la organización.

Las opciones para la Gestión del Riesgo incluyen acciones como: eliminar, transferir, reducir o asumir el riesgo.

Cada acción específica relacionada con la Gestión del Riesgo debe ser registrada y acometida mediante un plan de tratamiento de los riesgos de Seguridad de la Información.

Los planes de tratamiento del riesgo son especialmente relevantes cuando se decide aplicar una selección de controles considerados como los más adecuados para asegurar que, tras su correcta implantación, los riesgos de Seguridad de la Información asociados

al plan se reducen al nivel aceptable previsto inicialmente por la propia dirección de la organización.

Para ahorrar esfuerzos y evitar omisiones que puedan originar gastos extraordinarios o ineficiencias, existe una propuesta de posibles controles a aplicar y especificados en la norma ISO/IEC 27002:2022.


Este estándar incluye adicionalmente una guía de implantación en diversos grados para cada uno de los 93 controles que recoge y que puede proporcionar una solución directa o una ayuda relevante para necesidades más específicas y según sea el caso particular de reducción del riesgo que se esté analizando.

A partir de un control específico, de un conjunto de controles pertinentes o de nuevos controles diseñados para satisfacer las necesidades específicas se cubren los requisitos de seguridad fundamentados en los criterios de aceptación de riesgos de Seguridad de Información, las opciones de tratamiento del riesgo y el enfoque de Gestión de Riesgos generales aplicados por cada organización en función de sus presupuestos.

La selección y la aplicación de los controles deben ser documentadas en una declaración de aplicabilidad que garantiza que ninguno de los 93 controles se haya podido omitir de forma intencionada o por error.

Los controles especificados en la norma ISO / IEC 27002-2022, son reconocidos como las mejores prácticas aplicables y para la mayoría de las organizaciones ya que da cabida a posibles necesidades de organizaciones de diferentes tamaños y complejidades.

De forma complementaria a este enfoque y tomando como base ISO/IEC 27002-2022, se han desarrollado normas como ISO/IEC 27011:2020 o ISO 27799:2016 que buscan orientar la aplicación de los controles recogidos en ISO/IEC 27002-2022 según el punto de vista sectorial de las telecomunicaciones y del sector sanitario respectivamente.



Del mismo modo, se han definido nuevos controles que aportan una ayuda para la consideración e implantación de los controles relacionados en el Anexo A del estándar ISO/IEC 27001:2022 según nuevos sectores de actividad relevantes.

La nueva versión de la Norma ISO/IEC 27001 publicada en Octubre de 2022, mantiene la estructura de las Cláusulas, con ligeros cambios que tratan con mayor detalle las mismas, específicamente:

#### 4 Contexto de la organización

##### 4.1 Comprensión de la organización y de su contexto

##### 4.2 Comprensión de las necesidades y expectativas de las partes interesadas

##### 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información

##### 4.4 Sistema de gestión de la seguridad de la información

#### 5 Liderazgo

##### 5.1 Liderazgo y compromiso

##### 5.2 Política

##### 5.3 Roles, responsabilidades y autoridades en la organización

#### 6 Planificación

##### 6.1. Acciones para tratar los riesgos y oportunidades:

###### 6.1.1. General

###### 6.1.2. Evaluación del riesgo para la seguridad de la información.

###### 6.1.3. Tratamiento de los riesgos de la seguridad de la información.

6.2. Objetivos de seguridad de la información y planificación para su consecución

7 Soporte

7.1 Recursos

7.2 Competencia

7.3 Concienciación

7.4 Comunicación

7.5 Información documentada:

7.5.1. General

7.5.2. Creación y actualización

7.5.3. Control de la información documentada

8 Operación

8.1 Planificación y control operacional

8.2 Apreciación de los riesgos de seguridad de la información

8.3 Tratamiento de los riesgos de seguridad de la información

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

9.2 Auditoría interna:

9.2.1. General

9.2.2. Programa de auditoría interna



9.3 Revisión por la dirección:

9.3.1. General

9.3.2. Entradas para la revisión de la gestión

9.3.3. Salidas de la revisión de la gestión

10 Mejora

10.1 Mejora continua

10.2. No conformidad y acciones correctivas. Los controles del Anexo A de la Norma ISO/IEC 27002-2022, han reagrupado los controles en cuatro dominios, y nuevos once controles:

#### Controles Organizacionales:

Se han agrupado 37 controles en este dominio, de los cuales se han definido:

5.1. Políticas de seguridad de la información

5.2. Funciones y responsabilidades en materia de seguridad de la información

5.3. Segregación de funciones

5.4. Responsabilidades de la dirección


5.5. Contacto con las autoridades

5.6. Contacto con grupos de interés especiales

5.7. Información sobre amenazas

5.8. Seguridad de la información en la gestión de proyectos



- 5.9. Inventario de la información y otros activos asociados
  - 5.10. Uso aceptable de la información y otros activos asociados
  - 5.11. Devolución de activos
  - 5.12. Clasificación de la información
  - 5.13. Etiquetado de la información
  - 5.14. Transferencia de información
  - 5.15. Control de acceso
  - 5.16. Gestión de la identidad
  - 5.17. Información de autenticación
  - 5.18. Derechos de acceso
  - 5.19. Seguridad de la información en las relaciones con los proveedores
  - 5.20. Tratamiento de la seguridad de la información en los acuerdos con los proveedores
  - 5.21. Gestión de la seguridad de la información en la cadena de suministro de las TIC
  - 5.22. Seguimiento, revisión y gestión de cambios de los servicios de los proveedores
  - 5.23. Seguridad de la información para el uso de servicios en la nube
  - 5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información
  - 5.25. Evaluación y decisión sobre los incidentes de seguridad de la información
  - 5.26. Respuesta a los incidentes de seguridad de la información
  - 5.27. Aprendizaje de los incidentes de seguridad de la información
- 

- 5.28. Recogida de pruebas
- 5.29. Seguridad de la información durante la interrupción
- 5.30. Preparación de las TIC para la continuidad de la actividad
- 5.31. Requisitos legales, reglamentarios y contractuales
- 5.32. Derechos de propiedad intelectual
- 5.33. 5.31. Protección de los registros
- 5.34. Privacidad y protección de la información personal
- 5.35. Revisión independiente de la seguridad de la información
- 5.36. Cumplimiento de las políticas, reglas y normas de seguridad de la información
- 5.37. Procedimientos operativos documentados

### Gestión de los riesgos en Seguridad de la Información

Gestionar los riesgos de Seguridad de la Información requiere de un adecuado método de evaluación y tratamiento de los riesgos.

La metodología empleada puede incluir una estimación de los costos y beneficios, los requisitos legales, aspectos sociales, económicos y ambientales, las preocupaciones de las partes interesadas en la organización, las prioridades y otras variables adicionales, según sea necesario y de interés en cada caso particular.

Los resultados de la Evaluación de Riesgos de Seguridad de la Información proporcionan una importante ayuda para determinar las decisiones de gestión más adecuadas en el tratamiento, en el uso de recursos y en las prioridades que son recomendables aplicar

para la gestión óptima de los riesgos de Seguridad de la Información en cada momento y en relación al resto de necesidades de negocio.

Uno de los resultados que más sorprende a las organizaciones cuando desarrolla las primeras evaluaciones es el comprobar que existen recursos excesivos dedicados a la protección de algunos activos de menor importancia o controles que, aunque una vez lo fueron, ya no son relevantes para la organización y mantienen un consumo y dedicación de recursos a todas luces evitables y que proporciona una fuente potencial de ahorro.

Para que una organización desarrolle su propia metodología y contemple todos los aspectos relevantes en esta tarea, existe el estándar internacional ISO/IEC 31000:2018 como ayuda más directa para acometer esta labor, y que proporciona una orientación sobre las actividades para la gestión, incluido el asesoramiento sobre la Evaluación de Riesgos, tratamiento de riesgos, aceptación del riesgo, la comunicación de riesgos, control de riesgos y revisión de los riesgos.

Es pertinente aclarar en este punto que ISO/IEC 31000:2018, así como en el caso de otros documentos relacionados con metodologías para la evaluación del riesgo en las organizaciones (Magerit, ISO 27005:2018, etc.), sirven como documento de ayuda para implementar el proceso de evaluación y tratamiento de riesgos de la seguridad de la información.

Por tanto, cada organización debe definir y formalizar la metodología que mejor se adapte a sus necesidades y recursos.

En este sentido, suele producirse el error frecuente de introducir, en la fase de implantación, metodologías más complejas y con un desarrollo más laborioso de lo que la organización puede realmente mantener condenando la posibilidad del mantenimiento a corto-medio plazo (menos de un año en muchos casos).



### Mantenimiento y mejora de la efectividad del SGSI

Una organización necesita mantener y mejorar el SGSI a través de la supervisión y la evaluación de su rendimiento y en consideración de la política de organización y los objetivos establecidos.

De forma similar a otras actividades relevantes para la organización (como las de planificación, económicas o financieras) se debe informar de los resultados de la gestión de la seguridad a la alta dirección implicada en el SGSI para su revisión.

Esta revisión del SGSI permite aportar evidencias del desarrollo de las acciones de validación, de verificación y de trazabilidad de aquellas acciones correctivas, preventivas y de mejora y en base a los registros y monitorización de las diversas áreas consideradas en el alcance de interés dentro del SGSI, incluyendo el seguimiento en el desempeño y efectividad de los controles de Seguridad de la Información que se encuentren en activo.

### Factores de éxito

Existe un gran número de factores que deben ser considerados como fundamentales para una adecuada implementación de un SGSI y permitir a una organización cumplir con sus objetivos de negocio.

A continuación, relacionamos algunos de los factores críticos de éxito más importantes a considerar:

- Obtener un entendimiento del contexto de la organización y de los elementos que pueden afectar a la seguridad de la información.
- Obtener todas las partes interesadas y los requisitos de las mismas respecto a la seguridad de la información.
- Obtener la legislación aplicable y los requisitos en materia de seguridad de la información.

- Política de seguridad, objetivos y actividades del SGSI en armonía con los correspondientes para el negocio.
- El enfoque y marco utilizados para el diseño, ejecución, supervisión, mantenimiento y mejora de la Seguridad de la Información deber ser consistente con la cultura organizacional.
- El apoyo y compromiso visible y decidido de todos los niveles de gestión con la dirección al frente.
- Obtener el conocimiento de las necesidades de protección de los activos de información en base a la aplicación de la Gestión de Riesgos de seguridad.
- Disponer de un programa eficaz en sensibilización, formación y educación en Seguridad de la Información para todos los empleados, así como otras partes que guardan relación con la organización con el objetivo de garantizar el cumplimiento de las obligaciones en materia de Seguridad de la Información y recogidas en las políticas de Seguridad de la Información, normas, etc. y que anime a actuar en consecuencia. Procesos eficientes para la comunicación y gestión de incidentes de seguridad.
- Una estrategia efectiva para la continuidad del negocio.
- Un sistema de medición establecido para evaluar el desempeño en la gestión de Seguridad de la Información y que habilite una retroalimentación de sugerencias para la mejora.

Un SGSI aumenta la probabilidad de que una organización logre la consecución de los factores críticos de éxito necesarios para proteger sus activos de información.

### Combinación con otros sistemas de gestión

Un SGSI es, en primera instancia, un Sistema de Gestión, es decir, una herramienta que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la Seguridad de la Información.



La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales.

Por ejemplo, se gestiona la calidad según ISO/IEC 9001:2015, el impacto medioambiental según ISO/IEC 14001:2015 o la prevención de riesgos laborales según OHSAS 18001.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

Las similitudes y posibilidades de integración de las normas ISO son evidentes a través de una estructura común, según indica el Anexo SL publicado por ISO. El Anexo SL describe el marco para un sistema de gestión genérico. Sin embargo, se requerirá agregarle requisitos relacionados con la disciplina específica de cada norma, para poder desarrollar sistemas de gestión completos, para, por ejemplo, la calidad, el medio ambiente, los servicios de TI, la seguridad de los alimentos, la continuidad del negocio, la seguridad de la información y la gestión de la energía. El Anexo SL contiene 10 cláusulas y cuatro apéndices. El apéndice 3 tiene tres partes: la estructura a nivel de cláusula y sub-cláusula, el texto central idéntico y los términos comunes con sus definiciones.

Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el Sistema de Gestión de Seguridad de la Información en sistemas de gestión previamente existentes en la organización a la hora de considerar una implantación inicial de un SGSI.

Para aquellos interesados en aspectos de integración de dos o varios sistemas de gestión existe la especificación pública PAS 99 como marco de referencia.

PAS 99 es la primera especificación de requisitos del mundo para sistemas de gestión integrada que se basa en los seis requisitos comunes de la guía ISO 72 (una norma para redactar normas para sistemas de gestión).

Entre las diferentes normas que se pueden utilizar con PAS 99:2012 dentro de un Sistema de Gestión integrada típico pueden incluirse las siguientes: ISO/IEC 9001:2015 (Gestión de

la calidad), ISO/IEC 14001:2015 (Gestión medioambiental), OHSAS 18001 (Salud y seguridad en el trabajo), ISO/IEC 27001:2022 (Seguridad de la Información), ISO 22000:2018 (Inocuidad de los alimentos seguridad alimentaria), ISO/IEC 20000:2018 (Gestión de servicios de TI), además de otras normas que tomen como fundamento básico de referencia el ciclo Deming o PDCA para la mejora continua.

### Certificación del SGSI

Una vez implantado el SGSI en la organización, y con un historial de registros de actividad recomendado de algunos meses, se puede afrontar la fase de auditoría y certificación de una organización y que se desarrolla de la siguiente forma:

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de esta.
- Respuesta en forma de oferta por parte de la entidad certificadora y compromiso de aceptación correspondiente.
- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.

**Pre-auditoría.** Es una fase opcional que puede realizarse a modo de auditoría previa y que aporta información sobre la situación actual y orienta mejor sobre las posibilidades de superar las fases 1 y 2 vinculantes en los tiempos inicialmente planificados.

**Fase 1 de la auditoría.** Análisis de la documentación por parte del Auditor Jefe y preparación posterior del informe en base a la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2.

La Fase 1 no necesariamente tiene que ser in situ y el informe resultante se envía junto al plan de auditoría propuesto para la Fase 2 al cliente. El periodo máximo entre la Fase 1 y Fase 2 suele estar establecido por las entidades de certificación entre 3 y 6 meses.

**Fase 2 de la auditoría.** Es la fase de detalle de la auditoría, en la que se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora.

Se realiza una revisión de las exclusiones según la declaración de aplicabilidad, de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés.

Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.

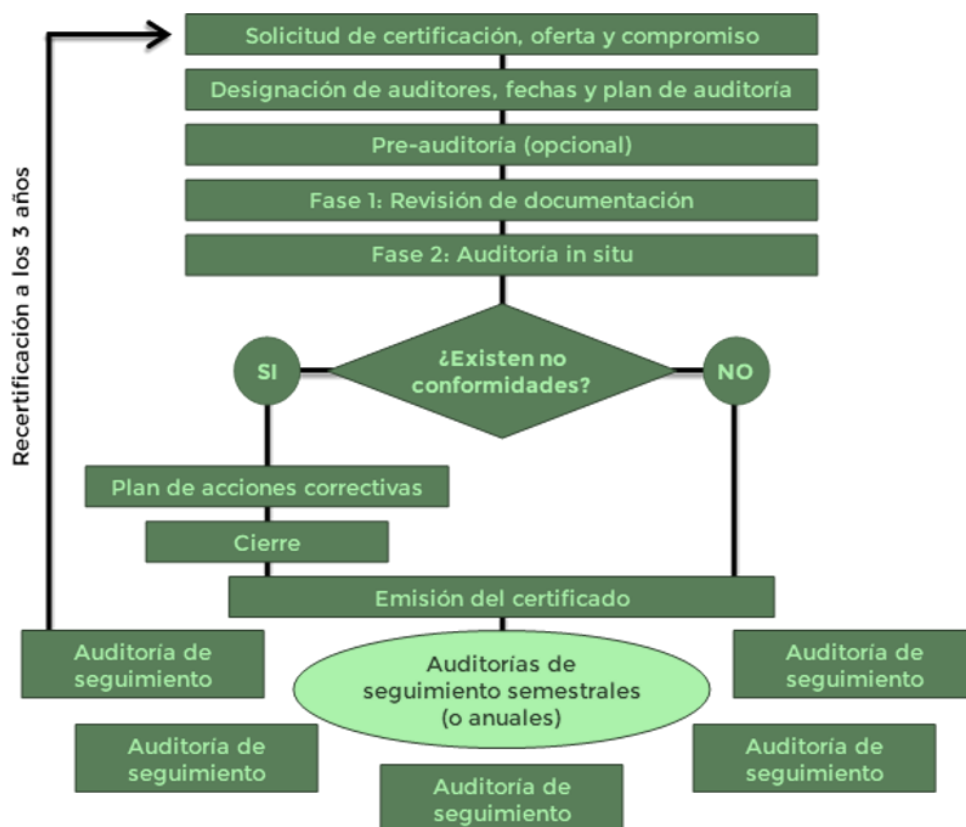
**Certificación.** En el caso de que se descubran durante la auditoría una o más No Conformidades de carácter mayor, la organización deberá implantar acciones correctivas.

Una vez verificada dicha implantación, o si directamente no se hubieran localizado No Conformidades de carácter mayor durante la Fase 2, el auditor estará en posición de emitir el informe favorable de recomendación para la certificación y la organización recibirá un certificado de su SGSI con la descripción del alcance certificado y según ISO/IEC 27001:2022.

**Auditoría de seguimiento.** Los certificados tienen una validez inicial de tres años, pero, con una frecuencia semestral o al menos anual, se debe realizar una auditoría de seguimiento por parte de la entidad de certificación con objeto de comprobar el adecuado mantenimiento de las actividades en mejora continua y de los controles apropiados en seguridad asociados.

Esta auditoría tiene una menor duración que la visita de Fase 2 inicial y sigue un programa de auditorías parciales establecido por la entidad de certificación y que se complementa en las visitas de seguimiento de modo que aquellos puntos que no se ven en una visita se acaban viendo en algún momento en las siguientes.

**Auditoría de re-certificación.** Cada tres años es necesario superar una auditoría de certificación formal completa de todos los puntos para proceder con la reemisión actualizada del certificado por un nuevo periodo de tres años.



**Figura 2.** Fases para afrontar la certificación formal de un SGSI.

### Estructura de la norma

La estructura del estándar internacional ISO 27001: 2022, se mantiene con diez cláusulas: Cláusula 4: Contexto de la Organización, Cláusula 5: Liderazgo, Cláusula 6: Planificación, Cláusula 7: Soporte, Cláusula 8: Operación, Cláusula 9: Auditorías Internas, y Cláusula 10: Mejoras, y pasa de 114 controles a 93 controles agrupados en 4 Dominios: Controles Organizativos, Controles de Personas, Controles Físicos, y Controles Tecnológicos, esto derivado de su alineación al Anexo SL de las Directivas de ISO/ IEC Parte 1, con lo cual ya no se basa en el modelo PDCA (Plan-Do-Check-Act), sino que ahora aplica la estructura de alto nivel, títulos de las sub-cláusulas, texto idéntico, términos comunes y las principales

definiciones definidas en el Anexo SL. Por lo tanto, mantiene compatibilidad con otros estándares de sistemas de gestión que también han adoptado dicho Anexo (como ISO 22301:2020 Business Continuity Management Systems — Requirements).

#### Periodo de adecuación a la norma

La norma se publicó el 1 de octubre de 2013. El periodo de actualización para las empresas que ya están certificadas en la ISO 27001: 2022, es de 3 años.