Implantación de un sistema de gestión de la seguridad de la información (SGSI)

Silvia Garre Gui

PID_00177811

Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción

En módulos anteriores se ha hablado de la seguridad de la información como un concepto mucho más amplio que el de seguridad informática, puesto que se centra en la protección de la información, uno de los activos más importantes de cualquier organización, frente a cualquier problema, incidente, discontinuidad, etc., independientemente del soporte en que esta información se encuentre (soporte papel, soporte digital, electromagnético...) y en cualquier momento de su ciclo de vida.

Se ha presentado también la importancia del análisis de riesgos como punto de partida para cualquier acción a acometer en materia de seguridad de la información. La máxima eficiencia se conseguirá cuando sepamos cómo estamos, a qué riesgos nos enfrentamos y cuál es el nivel de riesgo que la organización está dispuesta a asumir. Se ha visto también que el análisis de riesgos no es una acción puntual, sino que es indispensable mantenerlo actualizado en el tiempo.

Todo ello lleva a la conclusión de que la seguridad no es un producto, sino que se trata de un proceso, una actividad que debe tener continuidad en el tiempo. En concreto, se trata del proceso de mantener a la organización en un entorno de riesgo gestionado, en concreto, en el umbral de riesgo deseado, a través de un seguimiento continuo y una inversión proporcional y justificada.

En este módulo nos centraremos en estudiar cómo implantar el proceso de la gestión de la seguridad de la información, cuáles son los pasos a dar, los aspectos a tener en cuenta, los posibles riesgos, y los estándares de referencia que nos ayudan a avanzar con confianza.

Aunque dentro de este módulo se describirá el objetivo y contenido de los estándares internacionalmente reconocidos, no es objeto del mismo hacer una descripción detallada de su contenido. No obstante, la implantación de un sistema de gestión de la seguridad de la información pasa incondicionalmente por un buen conocimiento de las normas internacionales, por lo que se recomienda encarecidamente su lectura y conocimiento.

Objetivos

Los objetivos que persigue el presente módulo son:

1. Dar algunas nociones sobre los organismos que se dedican a la creación de normas.

2. Dar una visión general del contenido de la familia 27.000 de la ISO.

3. Conocer las bases de los sistemas de gestión, y en concreto del ciclo de Deming.

4. Conocer las pautas para la implantación de un sistema de gestión de la seguridad de la información.

5. Tener claro cuál es el marco documental necesario para la implantación de un SGSI.

1. Qué es un sistema de gestión de la seguridad de la información

La seguridad de la información puede ser enfocada desde diferentes puntos de vista, con diferentes objetivos y según distintas aproximaciones.

Una organización que ponga en práctica algunos controles de seguridad básicos, como un *firewall*, un antivirus, un control de acceso físico y una política de contraseñas, todo ello dirigido y gestionado desde el área de Sistemas de Información, podría considerar que está gestionando la seguridad de la información. Pero de sobras es conocido que "una cadena es tan fuerte como el más débil de sus eslabones" y por tanto, la aplicación de dichos controles de forma arbitraria, sin antes haber analizado cuáles son las principales debilidades, no es garantía de seguridad.

A estas alturas entendemos que un enfoque sistemático de la seguridad, planteado desde un análisis inicial de riesgos y alineado con la estrategia y objetivos del negocio, y entendido como un proceso independiente y no como una actividad puntual, no garantiza la seguridad de la información, pero proporciona muchos más elementos de control que permitirán minimizar la aparición de incidentes y reaccionar de la forma más adecuada y eficiente en caso de que un incidente se produzca, minimizando así su impacto.

Según el Diccionario de la Lengua de la Real Academia Española

- **Sistema**: Conjunto de elementos materiales relacionados entre sí, que constituyen un todo orgánico, generalmente sujeto a unas leyes o normas.
- **Gestionar**: Hacer diligencias conducentes al logro de un negocio o de un deseo cualquiera.

Si analizamos la definición que el diccionario hace de *sistema* y de *gestionar*, podemos concluir que un sistema de gestión es aquel conjunto de acciones relacionadas entre sí que nos permiten alcanzar un objetivo del negocio.

El desarrollo de un sistema de gestión de la seguridad de la información (SGSI) se basa principalmente en la siguiente normativa:

- ISO/IEC 27001 – Especificaciones para los sistemas de gestión de la seguridad de la información (SGSI).

- ISO/IEC 27002 – Código de buenas prácticas para la gestión de la seguridad de la información.

- ISOGuide 72 – Guía para la justificación y desarrollo de sistemas de gestión.
  Es una guía que recoge los requerimientos para cualquier sistema de gestión (sea cual sea su ámbito de aplicación).

2. Normativas internacionalmente reconocidas

Una norma o estándar es un acuerdo documentado que contiene especificaciones técnicas u otros criterios precisos que pueden ser utilizados de forma consistente, como normas, guías o definiciones de características que aseguran que los materiales, productos, procesos y servicios se ajustan a su propósito

La elaboración de normativas a nivel internacional proporciona beneficios tecnológicos, económicos y sociales, ya que:

- Proporciona eficiencia, seguridad, salubridad y calidad al desarrollo, producción y provisión de productos y servicios.
- Facilita el comercio y las relaciones internacionales.
- Facilita la compatibilidad e interoperabilidad de mercancías y productos, con especial importancia en el ámbito de las nuevas tecnologías, y redunda por tanto en una mejora de los costes.
- Proporciona soluciones a problemas comunes.
- Proporciona a los gobiernos una base técnica para legislación en materia de salud, seguridad y medioambiente.
- Permite compartir avances tecnológicos y buenas prácticas de gestión.
- Protege a los consumidores y usuarios en general en cuanto a los productos y servicios adquiridos.

Existen normas dirigidas a sectores muy concretos y también normas de carácter más transversal, pero en cualquier caso, son normas dirigidas a cualquiera que quiera aplicarlas, independientemente del tamaño de la organización donde se quieran implantar, por lo que son siempre un buen punto de partida para trabajar, dado su amplio reconocimiento y amplia validación a nivel mundial.

A continuación se presentan algunas de las organizaciones que promueven o lideran la aprobación de normas a nivel internacional y nacional.

2.1. BSI

En el campo de la seguridad de la información, la primera organización que trabajó en el establecimiento de un estándar común fue el British Standard Institute. Esta organización, fundada en 1901, fue la primera entidad nacional de normalización a nivel mundial.

Muchas de las normas internacionalmente reconocidas hoy en día parten de una norma previa del BSI: ISO 9000 (Calidad), ISO 14000 (Gestión medio ambiental), ISO/IEC 27000 (Seguridad de la Información), ISO 10002 (Gestión de reclamaciones), ISO 20000 (Gestión de servicios TI).

En materia de seguridad, cabe también destacar la OHSAS 18001 para Seguridad y Salud Laboral, así como la BS 25999 de Continuidad de Negocio.

Actualmente, el grupo BSI tiene oficinas en cerca de 100 países distintos, y ofrece básicamente tres líneas de servicio: certificación de sistemas de gestión y productos, desarrollo de estándares nacionales e internacionales y formación sobre estándares.

2.2. ISO: International Organization for Standardization

ISO (International Organization for Standardization) es el mayor desarrollador y publicador de estándares internacionales.

Se trata de una organización no gubernamental fundada en 1947, que actualmente representa a 162 países y tiene su sede central en Ginebra, Suiza.

Sus miembros pertenecen tanto al sector público como al privado, por lo que ISO facilita el consenso al proponer soluciones que representan tanto los requerimientos del negocio y la industria, como los intereses más amplios de la sociedad.

Su amplia representatividad avala su aplicabilidad a nivel internacional.

La organización promueve el desarrollo de estándares internacionales para mejorar el intercambio internacional de bienes y servicios y fomentar la cooperación a nivel intelectual, científico, tecnológico y económico.

Los estándares ISO son revisados como mínimo cada cinco años por un grupo de expertos.

El abanico de los estándares ISO va desde los sectores más tradicionales, como la agricultura o la construcción, hasta la ingeniería eléctrica y las TIC (tecnologías de la información y las comunicaciones). En estos últimos campos, ISO colabora con IEC (International Electrotechnical Commission) e ITU (International Telecommunication Union), especializadas en estos sectores. Adicio-

nalmente, ISO desarrolla también algunos estándares transversales, de aplicación a cualquier sector, como por ejemplo en temas de metodología o sistemas de gestión.

Algunos de los estándares ISO más conocidos son:

- ISO 9000: Gestión de la calidad
- ISO 14000: Gestión medioambiental
- ISO 216: Unificación de tamaños de papel
- ISO 27000: Gestión de la seguridad de la información.

Las normativas de seguridad son trabajadas en el Comité Técnico de Tecnologías de la Información (JTC1), y concretamente en el subcomité 27.

Proceso de creación de normativas internacionales

Hay tres posibles vías para la creación de las normativas:

- **Fast Track**: Existe consenso entre todos los miembros del grupo de trabajo sobre el contenido del documento resultante. En este caso, se toma una normativa existente en algún país y se adopta con carácter internacional. El proceso dura aproximadamente un año.
  Por ejemplo, ISO 27002: se adoptó la norma BS 7799.

- **Medium Track**: Los miembros del comité están de acuerdo en la esencia del documento resultante, pero no hay acuerdo en algunos aspectos concretos de carácter menor. En tal caso se inicia un proceso de discusión que dura unos tres años.

- **Slow Track**: Hay consenso en la necesidad de elaboración de una normativa, pero hay grandes diferencias en los planteamientos de los diferentes miembros del comité. En este caso se parte de cero y el proceso dura unos cinco años.
  Por ejemplo, en la ISO 27001 se partía de dos corrientes divergentes. La primera apoyaba una visión similar a la BS 7799:2 (parte 2); la segunda era más partidaria de la visión de la UNE 71502. La versión final está más próxima a esta segunda opción.

2.3. AENOR

AENOR es una entidad española dedicada al desarrollo de la normalización y la certificación en todos los sectores industriales y de servicios. Tiene como propósito contribuir a mejorar la calidad y la competitividad de las empresas, así como proteger el medio ambiente.

Fue designada para llevar a cabo estas actividades por la Orden del Ministerio de Industria y Energía, de 26 de febrero de 1986, de acuerdo con el Real Decreto 1614/1985 y reconocida como organismo de normalización y para actuar como entidad de certificación por el Real Decreto 2200/195, en desarrollo de la Ley 21/1992 de Industria.

Su presencia en los foros internacionales, europeos y americanos garantiza la participación de nuestro país en el desarrollo de la normalización, así como el reconocimiento de la certificación de AENOR.

Así pues, AENOR:

- Elabora normas técnicas españolas con la participación abierta a todas las partes interesadas, y colabora impulsando la aportación española en la elaboración de normas europeas e internacionales.

- Certifica productos, servicios y sistemas de gestión de empresas, confiriendo a los mismos un valor competitivo diferencial que contribuye a favorecer los intercambios comerciales y la cooperación internacional

3. La familia ISO 27000

Las normas ISO 27001 e ISO 27002 son las que actualmente tienen mayor difusión y aceptación a nivel internacional, por lo cual nos centraremos en ellas para trabajar sobre la implantación de los sistemas de gestión de la seguridad de la información (SGSI).

3.1. Historia de la norma

- **1995.** Primera publicación oficial de la BS 77991:1 - Código de buenas prácticas en seguridad de la información.

- **1998.** Publicación oficial de la BS7799:2 – Especificaciones de los sistemas de gestión de la seguridad de la información.

- **1999.** Publicación oficial de la BS7799. Partes 1 y 2.

- **2000.** Publicación de la primera versión de la norma ISO/IEC 17799:2000 - Código de buenas prácticas en seguridad de la información.

- **2002.** Publicación de la nueva versión de la BS7799:2 y publicación oficial por parte de AENOR de la norma UNE-ISO/IEC 17799 - Código de buenas prácticas en seguridad de la información.

- **2004.** Publicación oficial de la UNE 71502 - Especificaciones de los sistemas de gestión de seguridad de la información.

- **2005.** Publicación oficial de la ISO/IEC 17799:2005 - Código de buenas prácticas en seguridad de la información. 15/10/2005: Publicación de la ISO 27001- Especificaciones de los sistemas de gestión de la seguridad de la información.

- **2007.** 13/2/2007 Publicación de la ISO/IEC 27006:2007. 1/7/2007 - La norma ISO 17799:2005 pasa a denominarse ISO 27002:2005. 28/11/2007: Publicación de la norma ISO 27001 en España como UNE-ISO/IEC 27001:2007 (AENOR).

- **2008.** 4/6/2008 Publicación de la ISO / IEC 27005:2008.

- **2009.** 30/4/2009 Publicación de la ISO / IEC 27000:2009. 7/12/2009 Publicación de la ISO / IEC 27004:2009.

- **2010.** 1/2/2010 Publicación de la ISO-IEC 27003.

3.2. Descripción del contenido de los estándares de la familia ISO 27000

- **27000.** Presenta una revisión de los estándares de la serie 27000, incorpora una introducción a los SGSI, describe el ciclo de Deming (PDCA) y define conceptos y vocabulario que aparece en los diferentes estándares.

- **27001.** Contiene las especificaciones para la implantación de un sistema de gestión de la seguridad de la información. Tiene su origen en la BS 7799-2:2002, a la que sustituye. Es la norma certificable.

- **27002.** Es el código de buenas prácticas en la gestión de la seguridad de la información. Tiene su origen en la BS 7799 parte 1 y la ISO / IEC 17799.

- **27003.** Es una guía de implementación de SGSI, del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799:2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **27004.** Especificación de las métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" del ciclo PDCA.

- **27005.** Establece las directrices para la gestión del riesgo en materia de seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

- **27006.** Especifica los requisitos y proporciona una guía para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

- **27007.** En elaboración. Será una guía de auditoría de un SGSI.

Existen otras normas de la serie en desarrollo, de carácter más específico para un ámbito o sector. Simplemente vale la pena destacar la ISO 27799, publicada el 12 de junio del 2008. La norma define las directrices para apoyar la interpretación y aplicación de la ISO 27002 al sector sanitario. A diferencia del resto de normas, ésta no la desarrolló el subcomité JTC1 / S27, sino el comité técnico TC 215.

4. ISO/IEC 27002: Código de buenas prácticas para la gestión de la seguridad de la información

Esta norma es una base común para desarrollar:

- Normas de seguridad organizativas.
- Prácticas efectivas de gestión de la seguridad.
- La confianza en las relaciones con terceras organizaciones.

Un aspecto importante es que siempre debe aplicarse de conformidad con la legislación y reglamentos aplicables.

La norma se utiliza en diferentes organizaciones para cubrir cualquiera de los siguientes objetivos:

- Formular los requerimientos y objetivos de seguridad de la información.
- Asegurar que los riesgos de seguridad se gestionan de forma efectiva en términos de costes.
- Asegurar el cumplimiento de leyes y regulaciones.
- Implementar y gestionar los controles necesarios para asegurar que los objetivos de seguridad definidos por la organización se alcanzan.
- Definir nuevos procesos de gestión de la seguridad, o identificar y clarificar los procesos existentes.
- Conocer el estado de las actividades de gestión de la seguridad por parte de la Dirección.
- Conocer el grado de cumplimiento de políticas, directivas y estándares adoptados por la organización, por parte de auditores internos o externos.
- Establecer políticas, directivas, estándares o procedimientos de seguridad de la información en las relaciones con terceros.
- Convertir la seguridad de la información en un facilitador del negocio.
- Proporcionar información relevante sobre el estado de la seguridad de la información a clientes.

4.1. Estructura de la norma

4.1.1. Introducción

La norma consta de una primera **parte introductoria**, pero muy clarificadora sobre el concepto de seguridad de la información, por qué ésta es necesaria, cómo establecer requerimientos de seguridad, gestión de los riesgos de seguridad, selección de controles, cuál sería un buen punto de partida, cuáles son los factores críticos de éxito para la implantación de la seguridad de la información en una organización y finalmente, algunos consejos para la adaptación de la norma al desarrollo de guías o estándares propios.

Control

Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

4.1.2. Apartados

- **Apartado 1: Alcance**
  Según recoge la ISO, este estándar internacional establece guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos apuntados en este estándar proporcionan una guía general sobre los objetivos de seguridad de la información comúnmente aceptados.
  Los objetivos de control y controles de este estándar deberán ser aplicados para satisfacer los requerimientos identificados en un análisis de riesgos. El estándar se puede utilizar como una guía práctica para desarrollar estándares de seguridad organizativa y prácticas efectivas de gestión de la seguridad, y puede ayudar a crear confianza en las relaciones con terceras organizaciones.

- **Apartado 2: Glosario**
  Definición de conceptos, para el correcto entendimiento de la norma.

- **Apartado 3: Estructura del estándar**
  Descripción de cuál es la estructura de la norma y el contenido de cada uno de sus apartados.

- **Apartado 4: Análisis y gestión de riesgos**
  Finalmente, dedica un apartado completo a la necesidad del análisis y gestión del riesgo y la necesidad de llevarlo a cabo antes de tomar cualquier decisión acerca de la implantación de los controles, que más adelante la norma proporciona con gran detalle.

- **Apartados 5 al 15**
  - Cada uno de los apartados configura una sección o dominio.
  - Cada dominio recoge uno o más objetivos de control de la seguridad.
  - Cada objetivo incluye uno o más controles que pueden ser aplicados para alcanzar el objetivo de control.

La ISO 27002:2005 presenta **11 dominios, 39 objetivos de seguridad y 133 controles** además de, como ya se ha comentado, un apartado inicial sobre análisis y gestión del riesgo, el cual no incluye controles, ya que su elaboración es previa a la selección de los mismos.

Como comentario, diremos que la ISO 17799:2000 presentaba 10 dominios, 36 objetivos de control y 127 controles.

Dominios de seguridad de la ISO 27002

<table>
<tr><td colspan="5">5. Política de seguridad (1 objetivo, 2 controles)</td></tr>
<tr><td colspan="2">6. Organización de la seguridad de la información (2 objetivos, 11 controles)</td><td colspan="2">7. Gestión de activos (2 objetivos, 5 controles)</td><td rowspan="2">14. Gestión de la continuidad de negocio (1 objetivo, 5 controles)</td></tr>
<tr><td rowspan="2">8. Seguridad relativa al personal (3 objetivos, 9 controles)</td><td>9. Seguridad física y del entorno (2 objetivos, 13 controles)</td><td>10. Gestión de comunicaciones y operaciones (10 objetivos, 32 controles)</td><td>11. Control de acceso (7 objetivos, 25 controles)</td></tr>
<tr><td>13. Gestión de incidentes (2 objetivos, 5 controles)</td><td colspan="3">12. Seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información (5 objetivos, 14 controles)</td></tr>
<tr><td colspan="5">15. Conformidad (3 objetivos, 10 controles)</td></tr>
</table>

Dominios de seguridad de la ISO 27002, especificando para cada dominio el número de controles que lo componen, y el número de objetivos de control totales por dominio

4.2. Cómo interpretar la información de cada dominio

Cada uno de los dominios de la ISO, tal y como hemos comentado, contiene:

- Un mínimo de un objetivo de control a alcanzar.
- Uno o más controles que pueden ser implantados para alcanzar dicho objetivo.

La descripción de cada uno de los controles se estructura en tres partes:

- Control: definición del control específico.
- Guía de implantación: proporciona información detallada para la implantación del control.
  Se trata sólo de una guía y por tanto, no siempre será de aplicación en su totalidad; es responsabilidad de la organización analizar cuál es la mejor manera de implantar el control.
- Información adicional: proporciona información que puede ser necesario tener en consideración, como por ejemplo consideraciones legales, referencias a otros estándares...

Ejemplo de objetivo de control

9. Áreas seguras

Objetivo

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

Los recursos para el tratamiento de información crítica o sensible para la organización deberían ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debería dar protección física contra accesos no autorizados, daños e interferencias.

Dicha protección debería ser proporcional a los riesgos identificados. Se recomienda una política de puesto de trabajo despejado, y bloqueo de pantalla para reducir el riesgo de accesos no autorizados o de daños a documentos, medios y recursos de tratamiento de información.

9.1.1 Perímetro de seguridad física

Control

Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

Guía de implantación

Cuando sea apropiado, se debieran considerar e implantar las siguientes guías para los perímetros de seguridad físicos:

a) Los perímetros de seguridad debieran estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo.

b) Los perímetros de un edificio o local que contienen los medios de procesamiento de información debieran ser físicamente sólidos (es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado); las paredes externas del local debieran ser una construcción sólida y todas las puertas externas debieran estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control; por ejemplo, vallas, alarmas, relojes, etc.; las puertas y ventanas debieran quedar aseguradas cuando están desatendidas y se debiera considerar una protección externa para las ventas, particularmente en planta baja.

c) Se debiera contar con un área de recepción con un(a) recepcionista u otros medios para controlar el acceso físico al local o edificio; el acceso a los locales y edificios debieran restringirse solamente al personal autorizado.

d) Cuando sea aplicable, se debieran elaborar las barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental.

e) Todas las puertas de emergencia en un perímetro de seguridad debieran contar con alarma, debieran ser monitorizadas y probadas en conjunción con las paredes para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales; debieran operar en concordancia con el código contra-incendios local de una manera totalmente segura.

f) Se debieran instalar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales y debieran ser probados regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas debieran contar con alarma en todo momento; también se debiera proveer protección para otras áreas; por ejemplo, el centro de proceso de datos o cuarto de comunicaciones.

g) Los medios de procesamiento de información manejados por la organización debieran estar físicamente separados de aquellos manejadas por terceros.

Otra información

La protección física se puede lograr creando una o más barreras físicas alrededor de los locales de la organización y los medios de procesamiento de información. El uso de las múltiples barreras proporciona protección adicional para que el fallo de una barrera no signifique que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina con llave, o varias habitaciones rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros

adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad dentro del perímetro de seguridad.

Se debiera prestar consideración especial a la seguridad de acceso físico que se debiera dar a los edificios donde se alojan múltiples organizaciones.

La ISO en estudio, tal y como su título indica, es una guía de buenas prácticas. Con ello lo que queremos expresar es que es una buena hoja de ruta a seguir, pero no se debe considerar como una norma que se debe seguir al pie de la letra, sobre todo en lo que a las pautas de la guía de implantación se refiere, puesto que no todas ellas tienen por qué ponerse en práctica ni tampoco tienen por qué ser todas ellas aplicables a la situación concreta de la organización.

4.3. Dominios de la ISO

A continuación, se enumeran los 11 dominios de seguridad, con una breve mención de los objetivos de control de cada uno de ellos y un resumen general de su contenido.

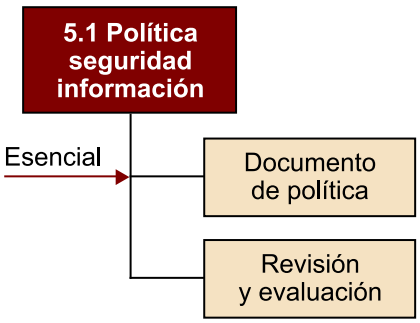
En la introducción de la norma, se especifican cuáles son los principios orientativos mínimos a cumplir para implantar la seguridad de la información. Dichos mínimos se consideran **mínimos esenciales** en la implantación de un SGSI, es decir, que es prácticamente imposible justificar que dicho control no se aplica o no entra dentro del alcance de nuestro SGSI.

Cuando se trate de un control esencial, se indicará en el gráfico a través de una flecha.

4.3.1. Política de seguridad

Se debe disponer de una normativa común de seguridad que regule las líneas maestras sobre cómo va a trabajar toda la organización en materia de seguridad. En el siguiente capítulo se aborda este dominio en mayor profundidad.

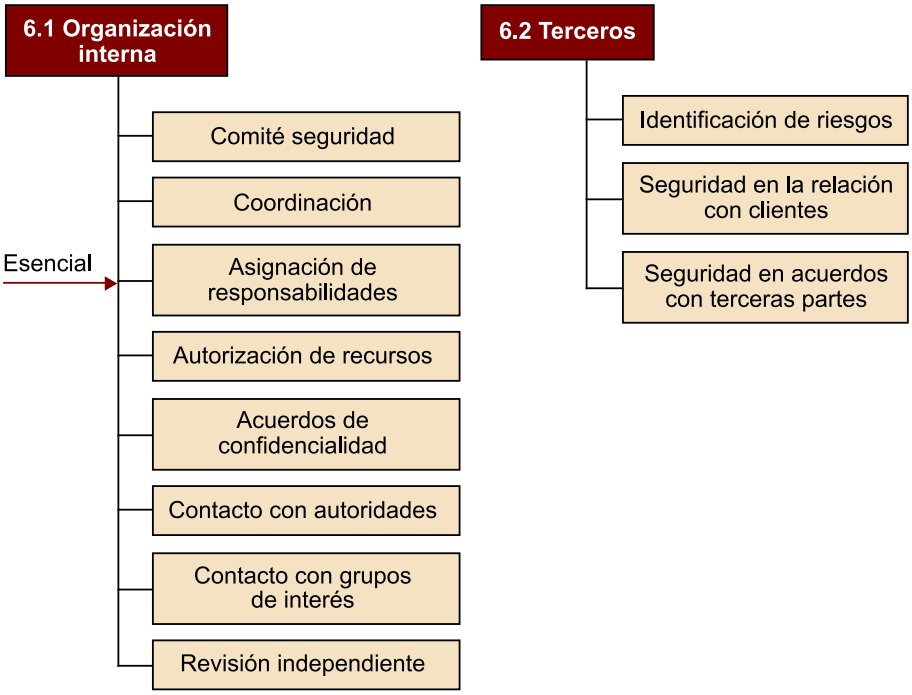
ISO 27002: Dominio sobre política de seguridad de la información



4.3.2. Organización de la seguridad de la información

Es necesario establecer una estructura organizativa y su funcionamiento tanto de forma interna como de puertas afuera. En el siguiente capítulo se aborda este dominio en mayor profundidad.

ISO 27002: Dominio sobre organización de la seguridad de la información

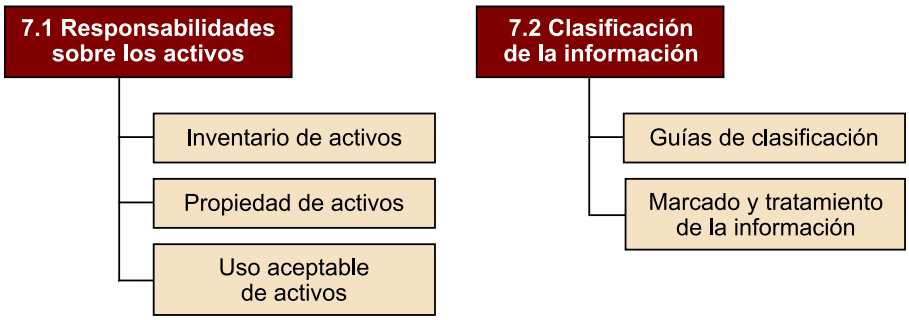


4.3.3. Gestión de activos

Para proteger la información en términos de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad, es imprescindible conocer cuáles son los activos críticos a proteger (información, software, hardware, servicios, personas...). Por tanto, es necesario hacer una identificación de los activos críticos para el desarrollo y mantenimiento de la actividad, y definir sus responsables, que son aquellas personas que decidirán sobre el uso que se puede hacer y el tipo de control que se debe ejercer sobre ellos.

En concreto, es necesario clasificar la información y definir quién es su propietario o responsable, para determinar usos, prioridades, accesos y niveles de protección necesarios en todo el ciclo de vida de la misma.

ISO 27002: Dominio sobre gestión de activos de información

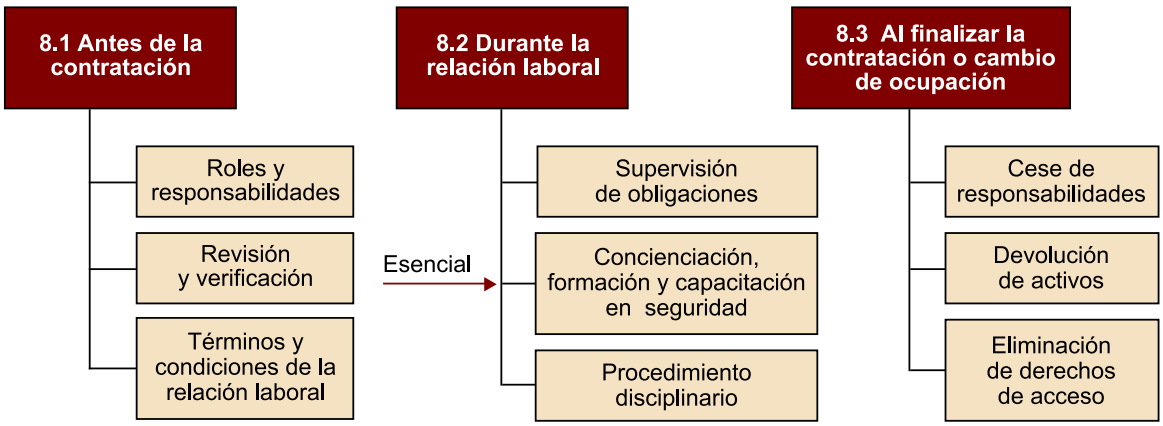


4.3.4. Seguridad relativa al personal

Todo el personal de la organización y sus colaboradores (proveedores, personal externo...) deben ser conocedores de sus responsabilidades para con la protección de la información, para garantizar su seguridad y uso correcto, con mayor importancia cuanto más confidencial o sensible sea la información a la cual tienen acceso.

Por tanto, se deberá prestar especial atención a este tema en el momento de la contratación del personal, ya sea interno o externo, estableciendo las cláusulas contractuales y los procedimientos adecuados para garantizar que el proceso de cambio de funciones, salida de la organización o terminación de contrato se realiza de forma ordenada y garantizando la recuperación por parte de la organización de información y equipos, así como la denegación de todos los derechos de accesos (físicos o lógicos) a la persona que abandona la compañía.

ISO 27002: Dominio sobre seguridad relativa al personal



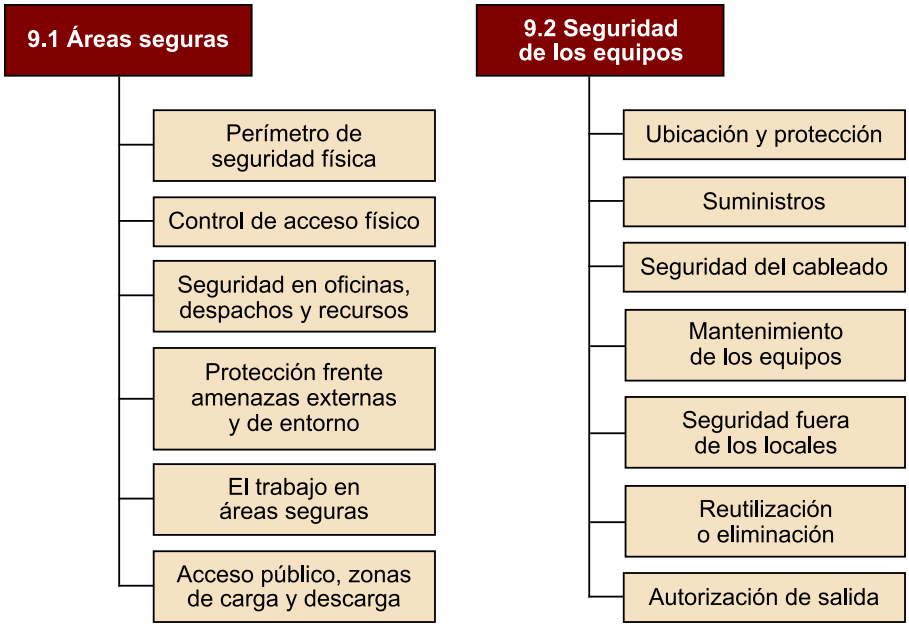
4.3.5. Seguridad física y del entorno

La información y equipos que la alojan o transmiten han de estar convenientemente protegidos para evitar accesos físicos indebidos y daños de cualquier tipo. Obviamente, el nivel de protección deberá ser proporcional a la criticidad de la información y los equipos a proteger, y dependerá obviamente de los riesgos potenciales.

Teniendo en cuenta esta premisa, se deben adoptar medidas para controlar el acceso físico a edificios y salas, y garantizar la seguridad de la información y los equipos, estableciendo, si fuera necesario, áreas seguras con controles específicos de seguridad perimetral, acceso físico, protección ante amenazas ambientales (fuego, inundación, humedad...), continuidad del suministro eléctrico, mantenimiento de equipos...

La organización también deberá definir las normas y procedimientos de uso de la información fuera de los locales habituales.

ISO 27002: Dominio sobre seguridad física y del entorno



4.3.6. Gestión de comunicaciones y operaciones

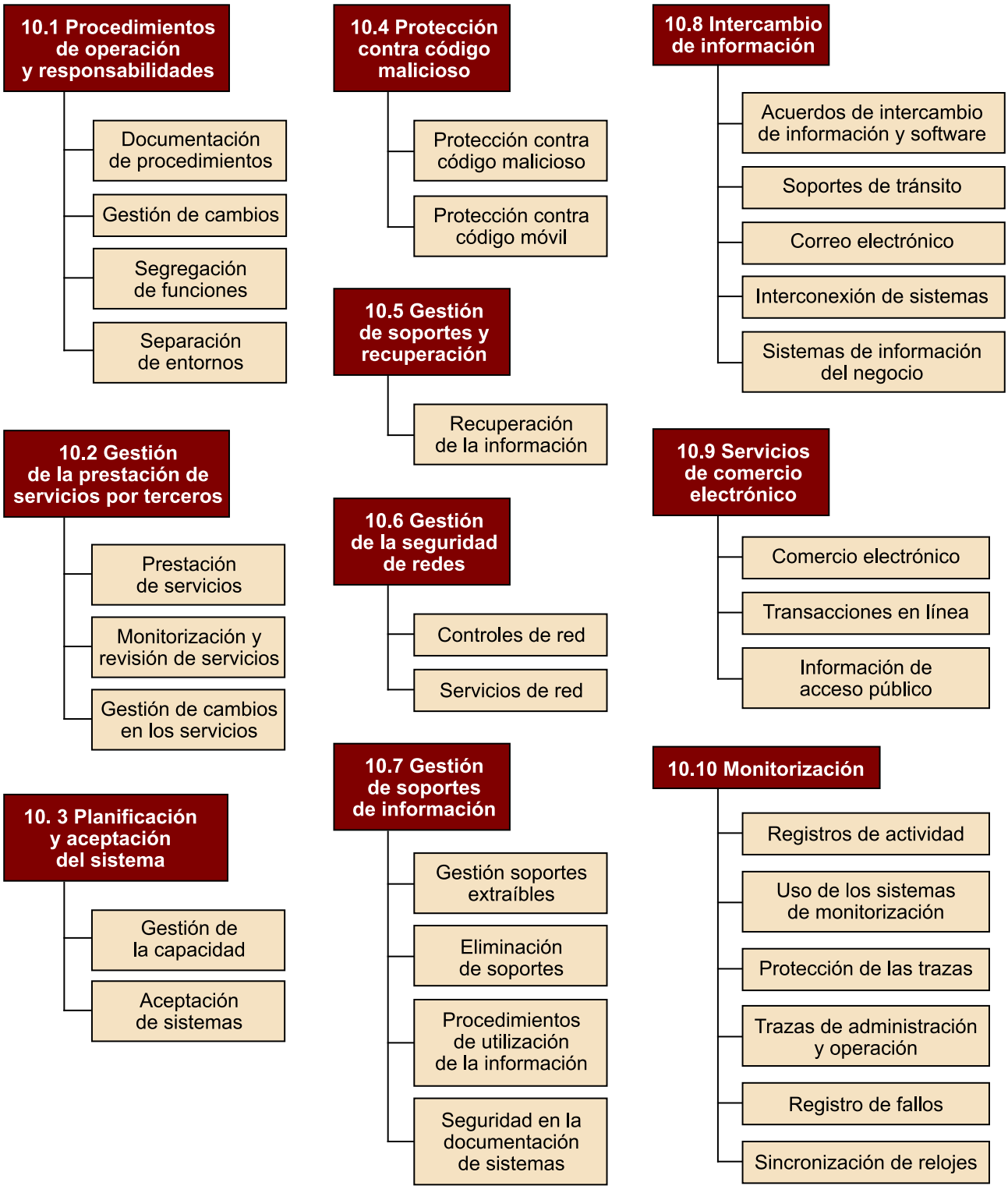
Para garantizar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información, es indispensable disponer de una correcta gestión y operación de los sistemas de información y las comunicaciones. En este sentido [10.1], las responsabilidades y procedimientos para asegurar una correcta configuración, administración y operación de los sistemas de información y las comunicaciones deberán estar claramente definidos y documentados, se deberá garantizar, siempre que sea viable, la segregación de funciones, la separación de entornos de desarrollo, prueba y producción, la gestión del cambio y [10.3] de la capacidad de los sistemas para evitar incidentes y, [10.2] en caso de participación de terceras partes en la operación, será necesario controlar el cumplimiento de los acuerdos establecidos, así como el seguimiento de las normas y procedimientos de la organización.

Asimismo, será imprescindible definir los controles necesarios para garantizar la corrección y seguridad en la operación: [10.4] protección ante software malicioso, [10.5] realización de copias de seguridad que cubran las necesidades del negocio y pruebas de restauración periódicas [10.6], gestión correcta de

redes e infraestructuras para garantizar la protección de la información y el acceso a servicios y recursos [10.7], gestión controlada de soportes que contienen información [10.8], procedimientos controlados de intercambio de información dentro y fuera de la organización y [10.9] controles específicos para garantizar la seguridad de las transacciones electrónicas cuando proceda, y la disponibilidad e integridad de la información publicada.

Finalmente, será necesario [10.10] monitorizar los sistemas para detectar cualquier acceso o uso de información o procesos no autorizados, así como registrar y gestionar las trazas de actividad de los sistemas, que permitan detectar problemas e incidentes, verificar la efectividad de los controles establecidos y dar cumplimiento a la legislación aplicable en cuanto a monitorización y gestión de trazas.

ISO 27002: Dominio sobre gestión de comunicaciones y operaciones



4.3.7. Control de acceso

El acceso a la información y a los recursos en general (aplicaciones, sistemas de procesamiento, infraestructuras de comunicación...) se deben controlar teniendo en consideración los requerimientos del negocio y de seguridad de la información.

Esto comporta la definición de criterios de acceso a la información según el principio de necesidad y la premisa de que "todo está en general prohibido, excepto aquello específicamente permitido", y teniendo en cuenta aspectos como el acceso físico y el accesos lógico en local o remoto.

Será necesario definir normas que recojan estos criterios para cada tipo de información o recurso, así como procedimientos de gestión (alta, baja y mantenimiento) del acceso de los usuarios o procesos, políticas de contraseñas, etc. y normas y códigos de buenas prácticas dirigidas a los usuarios finales sobre el buen uso de las estaciones de trabajo o de los sistemas de acceso a la información.

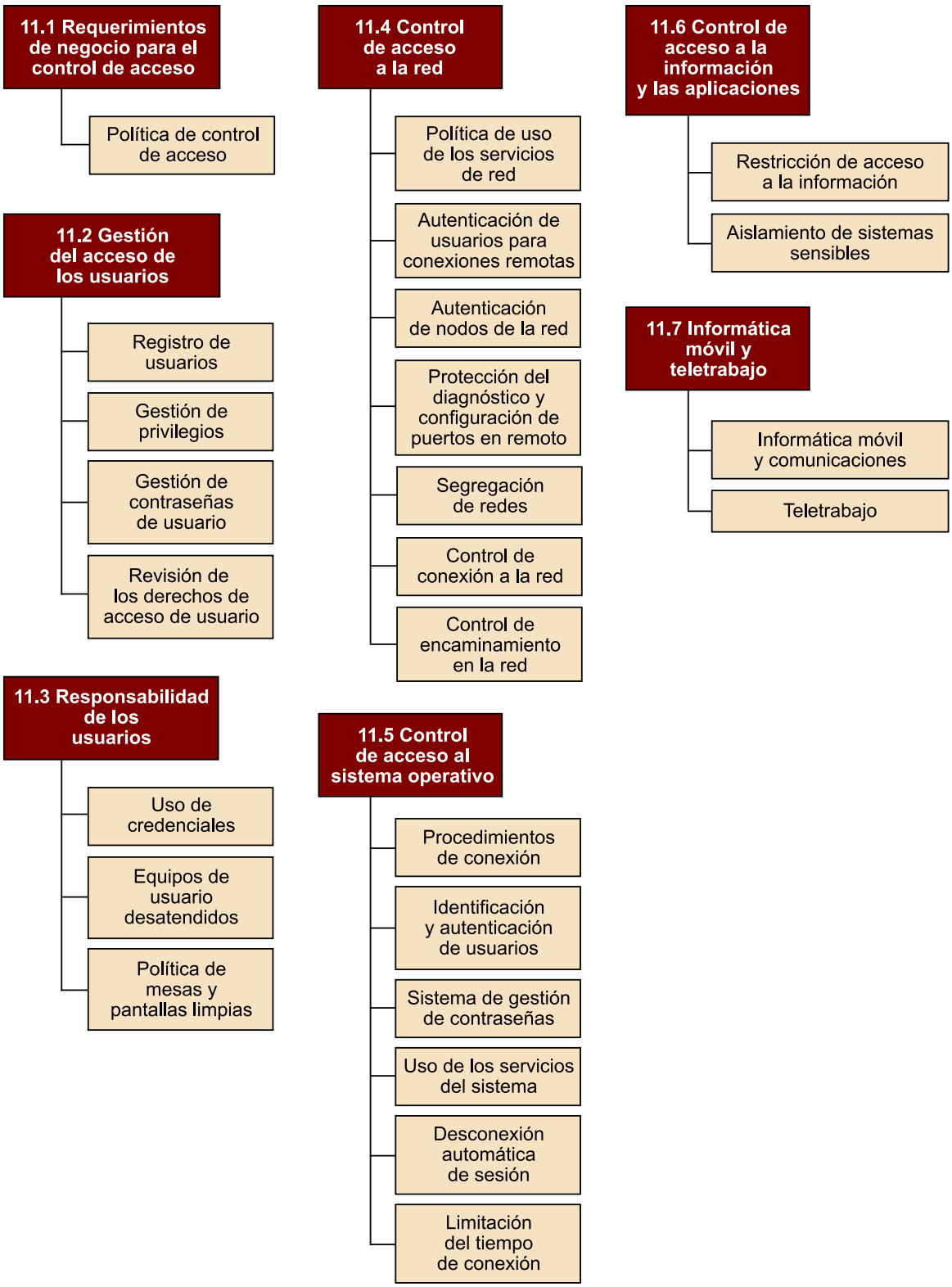
Se deberán realizar revisiones periódicas sobre los permisos y privilegios de acceso a cada recurso.

Todos los usuarios que accedan a los sistemas de información deberán estar asociados a un identificador personal y deberán pasar por un proceso de identificación, autenticación y autorización. Se evitará el uso de usuarios genéricos, excepto en el caso de imposibilidad tecnológica, que deberá ser justificada y aprobada formalmente, con el compromiso de regularización en el momento en que la imposibilidad desaparezca.

La organización debe ser capaz de conocer en todo momento quién tiene acceso a qué información y a qué recursos, así como quién accede a una determinada información o recurso.

El acceso remoto a los sistemas deberá garantizar un nivel de seguridad equivalente al de las conexiones en modo local.

ISO 27002: Dominio sobre el control de acceso



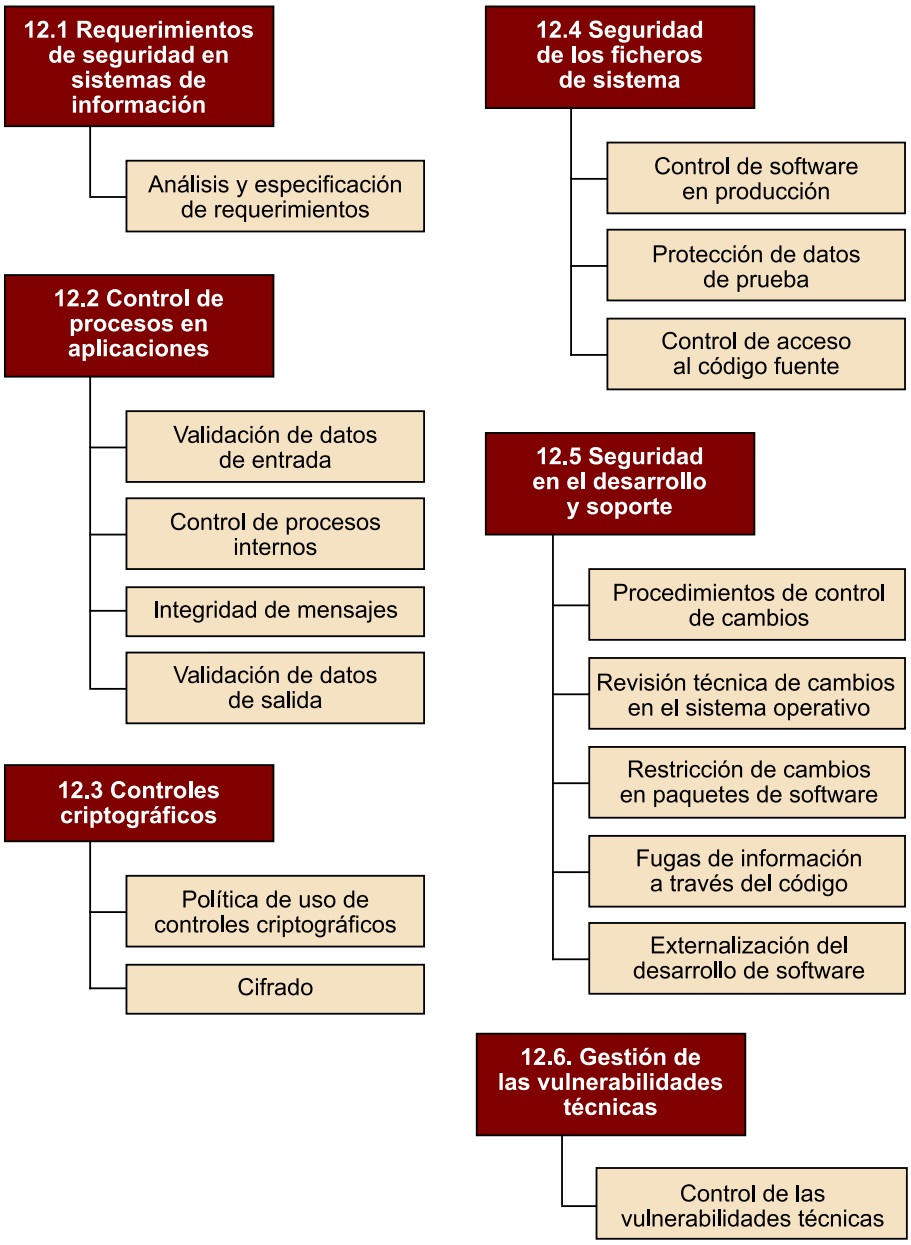
4.3.8. Seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad deber ser considerada en todo el ciclo de vida de desarrollo de sistemas: análisis de requerimientos y viabilidad, diseño, pruebas y aceptación final. Los requerimientos de seguridad deben ser identificados y acordados en la fase inicial de un proyecto, antes de iniciar el desarrollo o implantación del sistema de información.

Se deben implantar los controles necesarios para:

- Garantizar la ausencia de errores de proceso, pérdida de información, modificación no autorizada o mal uso de la información a través de las aplicaciones.
- Garantizar la confidencialidad e integridad de la información, así como la autenticidad y no refutación de acciones realizadas sobre la información.
- Proteger el software y código desarrollado.
- Garantizar el uso de las mejores prácticas en el desarrollo de código seguro.
- Generar registros o trazas de actividad.
- Establecer las medidas necesarias para garantizar la seguridad de la información en los entornos no productivos.
- Establecer los procedimientos que garanticen que cambios en el hardware o software no puedan comprometer la seguridad de la información.
- Supervisar y monitorizar los desarrollos contratados a terceras partes.
- Gestionar las vulnerabilidades técnicas de todo el software.

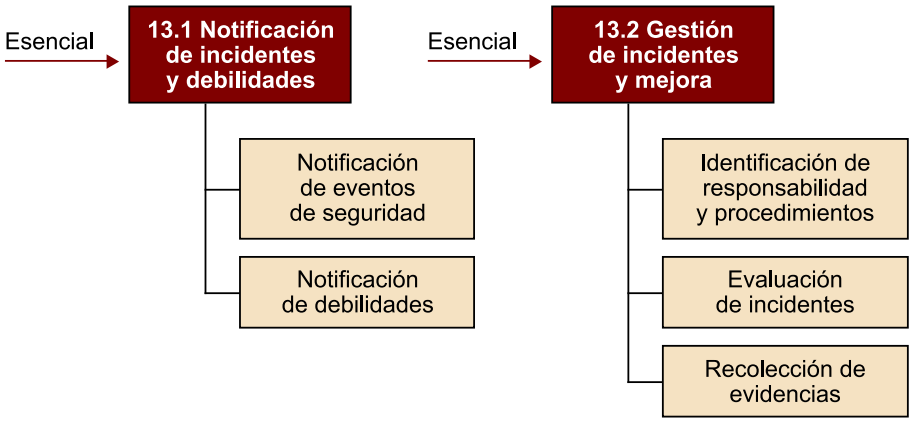
ISO 27002: Dominio sobre gestión de incidentes de seguridad de la información



4.3.9. Gestión de incidentes de seguridad de la información

Es necesario asegurar que cualquier incidente o debilidad relacionada con la seguridad de la información se comunica de forma eficiente para que se puedan tomar, a tiempo y de forma ordenada, las acciones correctivas necesarias. Para ello, es indispensable establecer y comunicar a todas las partes implicadas los procedimientos de notificación y escalado de incidentes, establecer una monitorización y seguimiento continuados de los mismos, establecer relaciones con agentes externos cuando proceda, para realizar una mejor gestión, así como recoger evidencias en la forma que el tipo de incidente requiera.

ISO 27002: Dominio sobre gestión de incidentes de seguridad de la información



4.3.10. Gestión de la continuidad de negocio

La definición de planes de continuidad de negocio tiene por objetivo proteger los procesos y actividades críticas del negocio de contingencias o desastres, y garantizar el restablecimiento del funcionamiento normal en unos plazos aceptables desde el punto de vista del negocio después de una situación de desastre.

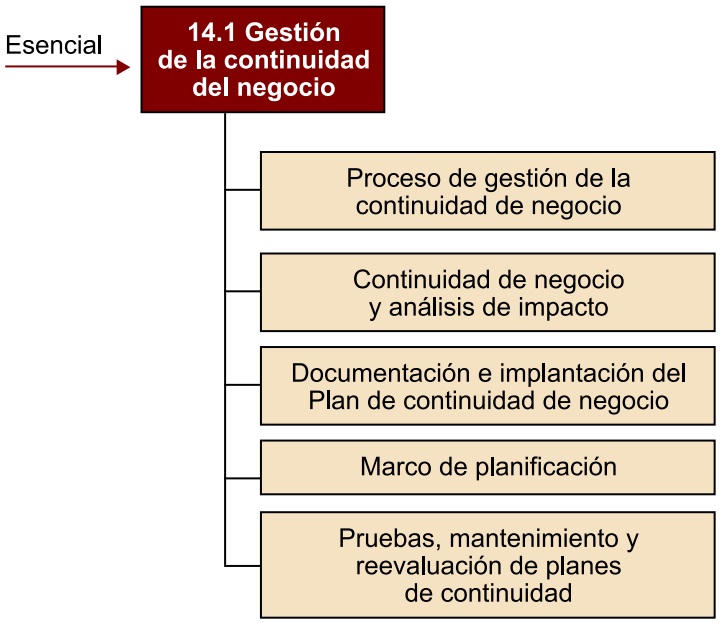
El establecimiento de un plan de continuidad pasa por el análisis de cuáles son los procesos críticos del negocio y cuál es el riesgo al que están sometidos, a través de la determinación de cuál sería el impacto en caso de que se materializase un desastre, incidente de seguridad, pérdida de servicio o, en general, pérdida de disponibilidad.

La determinación y cuantificación del riesgo permite tomar decisiones a los niveles directivos que corresponda sobre el grado de riesgo asumible, priorizar las acciones en seguridad de la información, y adoptar medidas proporcionadas, estableciendo las salvaguardas necesarias (controles técnicos, procedimientos operativos, normativas de usuario, cláusulas contractuales...) de tipo preventivo, correctivo o de detección según corresponda.

El análisis del impacto permite definir cuáles son los activos de información a proteger en función de su criticidad para el negocio, así como cuáles son los tiempos aceptables de recuperación. El plan de continuidad deberá tener en cuenta estos aspectos, así como la definición de la actuación esperada por parte de todas las partes implicadas, su formación y realización de como mínimo una prueba anual.

Se debe garantizar la actualización continuada del plan de continuidad del negocio, así como su disponibilidad en situación de crisis o emergencia.

ISO 27002: Dominio sobre gestión de la continuidad de negocio

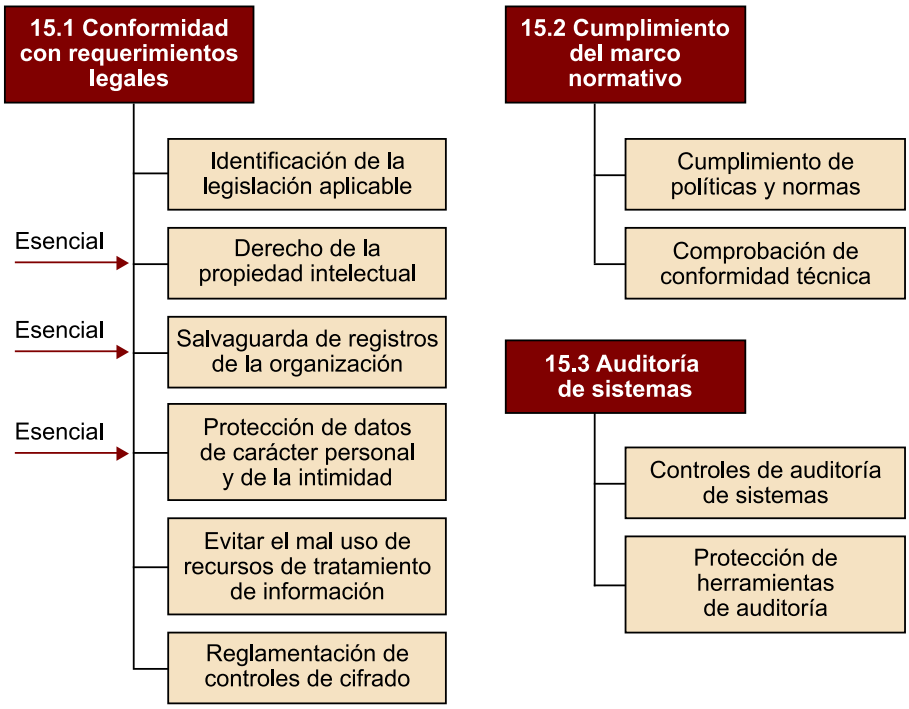


4.3.11. Conformidad

Es necesario tomar las medidas necesarias para garantizar el cumplimiento de cualquier obligación legal, estatutaria, regulatoria o contractual, así como el cumplimiento de la normativa vigente interna en materia de seguridad de la información.

Es indispensable conocer cuál es la legislación aplicable en cada caso y hacer difusión dentro de la organización. Asimismo, se debe establecer un sistema de control periódico e independiente del cumplimiento de obligaciones y, en lo que al cumplimiento de la normativa interna se refiere, establecer un sistema de autorización de excepciones cuando la causa esté justificada.

ISO 27002: Dominio sobre conformidad



5. Sistemas de gestión

Un sistema de gestión permite alcanzar los objetivos de una organización mediante:

- Una estructura organizativa donde las funciones y responsabilidades están claramente definidas y asignadas.

- Procesos y recursos necesarios para lograr los objetivos.

- Metodología de medida y de evaluación para valorar los resultados frente a los objetivos, incluyendo la realimentación de resultados para planificar las mejoras del sistema.

- Un proceso de revisión para asegurar que los problemas se corrigen y se detectan oportunidades de mejora que se implementan cuando están justificadas.

Los principios generales de cualquier sistema de gestión son los siguientes:

- Cobertura de una necesidad de mercado.
- Compatibilidad con otros sistemas de gestión.
- Facilidad de implantación.
- Posibilidad de implantación en cualquier tipo de organización.
- Basado en metodologías, prácticas o tecnologías suficientemente probadas.
- Facilidad para entenderlo, sin ambigüedades ni condicionantes culturales.
- Permite desarrollar auditorías.
- No puede especificar productos concretos, metodologías ni establecer niveles de conformidad (a pesar de que la ISO 27000 hace referencia a Magerit como metodología de análisis de riesgos).

A continuación se exponen los elementos comunes a cualquier sistema de gestión:

- Política
  Para demostrar el compromiso de la organización con los requisitos del sistema de gestión y establecer unos principios y orientación global.

- Planificación
  - Identificación de necesidades y requisitos, y análisis de elementos críticos.
  - Selección de elementos a gestionar.

  - Establecimiento de objetivos (generalmente anuales y fijados por la Dirección).
  - Identificación de recursos humanos y materiales.
  - Identificación de la estructura organizativa, funciones y responsabilidades.
  - Planificación de los procesos operativos.
  - Preparación de planes de contingencia para eventos previsibles.

- Implantación y operación
  - Control de las actividades para lograr los objetivos.
  - Gestión de recursos humanos.
  - Gestión de otros recursos.
  - Documentación y control.
  - Comunicación.
  - Relaciones con proveedores y subcontratados.

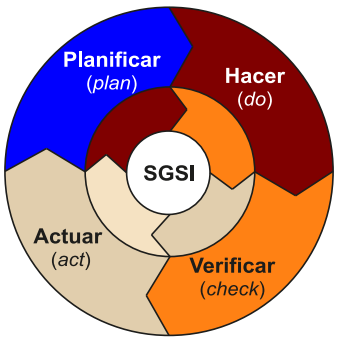
- Análisis del rendimiento
  - Monitorización y mediciones.
  - Estudio y gestión de no conformidades.
  - Auditorías del sistema de gestión.

- Mejora
  - Acciones preventivas.
  - Acciones correctivas.
  - Mejora continua.

- Revisiones de la Dirección
  - Determinar el rendimiento.
  - Asegurar su adecuación permanente.
  - Asegurar su suficiencia y efectividad.
  - Desarrollar mejoras.
  - Plantear nuevos objetivos cuando sea necesario.

Detrás de todas estas fases se halla el Ciclo de Deming, también conocido como ciclo PDCA (***P****lan* – ***D****o* – ***C****heck* – ***A****ct*), que es un proceso iterativo de calidad en cuatro fases:

- *Plan*: establecer los objetivos y procesos necesarios para conseguir los resultados esperados.
- *Do*: implantar los nuevos procesos.
- *Check*: medir los nuevos procesos y comparar los resultados obtenidos con los esperados.
- *Act*: analizar las diferencias entre los resultados obtenidos y los esperados para conocer las causas, y plantear mejoras.



Ciclo de Deming o ciclo PDCA

6. Introducción al SGSI

Sistema de gestión de la seguridad de la información (SGSI)

"Es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización."

Fuente: ISO 27001

La implantación de un SGSI comporta los siguientes beneficios:

- **Visión común**: permite definir y divulgar unas directrices básicas en materia de seguridad aprobadas por la Dirección, que sientan las bases de cualquier acción relacionada con el tratamiento de la información.

- **Implicación de la organización**: define la estructura organizativa para gestionar la seguridad de la información, identificando funciones y responsabilidades desde la alta Dirección hasta el usuario final, estableciendo los niveles de decisión necesarios, y los procedimientos de divulgación / concienciación para implicar a toda la organización.

- **Gestión global y activa**: permite gestionar la seguridad de la información según criterios comunes, procedimientos homogéneos y un vocabulario compartido, y establece los mecanismos pera garantizar la vigencia del sistema de gestión, de manera que se mantiene vivo y evoluciona, y no queda obsoleto una vez implantado.

- **Control y seguimiento**: permite disponer de una metodología de medida y evaluación de indicadores, con el fin de valorar los resultados frente a los objetivos establecidos y mantener informada a la Dirección para que pueda tomar decisiones. Asimismo, establece los mecanismos para autoevaluarse y facilita la realización de auditorías de seguridad de la información cuando corresponda.

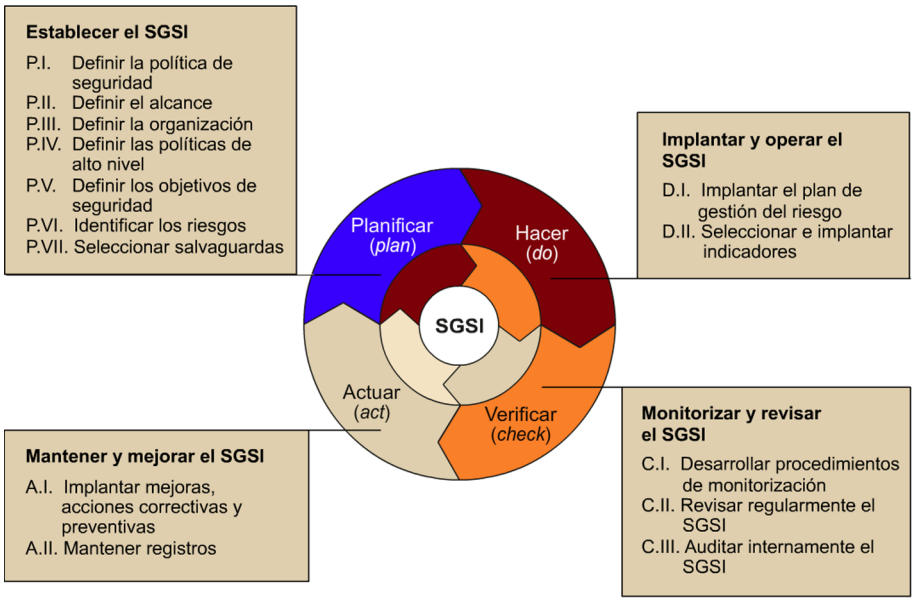
- **Mejora continua**: permite establecer un proceso para ir alcanzando los objetivos en diferentes iteraciones, de forma que el sistema de gestión se va ampliando gradualmente, y permite tener en marcha un proceso de revisión para asegurar que los problemas se detectan y corrigen, que se incorporan las lecciones aprendidas en cada nueva iteración y que se implantan mejoras justificadas, permitiendo evolucionar paso a paso.

- **Optimización de los recursos**:

- Uso racional y más controlado de la información.
- Presupuesto justificado, ajustado al riesgo real.
- Personal concienciado y formado en sus responsabilidades.
- Ahorro de tiempo, puesto que los procedimientos y criterios esenciales están claramente definidos y comunicados.
- Infraestructura ajustada a las necesidades reales del negocio.

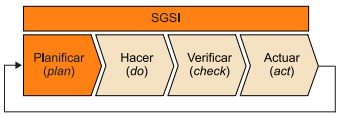
El desarrollo de un sistema de gestión de la seguridad de la información se basa en la ISO 27001 y la ISO 27002, así como en el Ciclo de Deming, para garantizar la actualización del sistema y la mejora continua, tal y como se describe en el gráfico siguiente:

Ciclo de Deming aplicado a los sistemas de gestión de seguridad de la información



7. Planificar: Establecer el SGSI

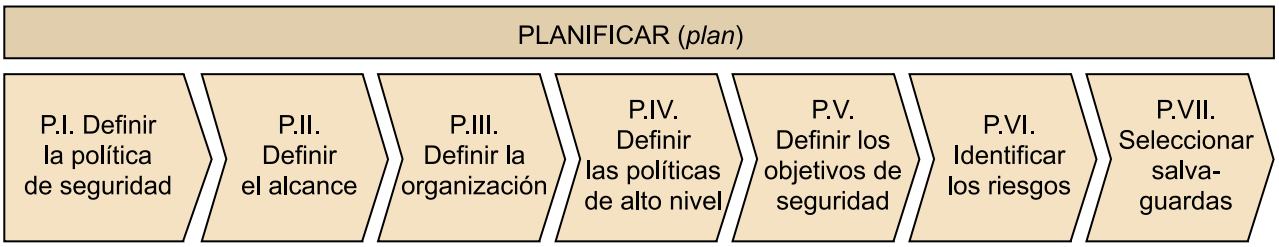
Antes de emprender acciones es necesario planificar, es decir, ver dónde estamos, adónde queremos ir, con qué medios contamos y sobre qué entorno queremos trabajar.



Planificar: primera fase del SGSI

En la imagen siguiente podemos ver cuáles son las distintas etapas que constituyen esta primera fase de planificación. A continuación revisaremos las principales características de estas etapas.

Etapas de la primera fase del SGSI: Planificar



7.1. P.I. Definir la política de seguridad de la información

La política de seguridad de la información establece los principios y líneas de actuación globales en cuestiones de seguridad de la información, alineados con los objetivos del negocio.

La política debe demostrar el compromiso de la Dirección con la seguridad de la información y se debe dar a conocer a todos los usuarios.

La política de seguridad de la información se desarrolla y concreta en políticas, normas, guías y estándares de segundo nivel.

Ved también

En el apartado "Hacer: implantar y operar el SGSI" se dan algunas pautas para la implantación de la política de seguridad de la información.

7.2. P.II. Definir el alcance

Idealmente, la seguridad de la información ha de estar gestionada en todos los ámbitos de la organización. La implantación de un sistema de gestión de la seguridad de la información es un proceso continuo de maduración y mejora, pero que habitualmente empieza abarcando los procesos más críticos de la organización, para ir englobando áreas menos críticas en fases posteriores.

Así pues, una organización podría tener implantado un SGSI para un proceso muy concreto, como por ejemplo, la producción de un determinado producto, careciendo el resto de la organización de medidas de seguridad. Si el alcance

del SGSI está claramente limitado a dicho proceso, la certificación del sistema de gestión podría ser exitosa, a pesar del mal estado de la seguridad del resto de la organización.

Por tanto, el primer paso pasa por establecer el alcance del sistema de gestión en términos de procesos, áreas organizativas, emplazamientos y activos.

Declaración de aplicabilidad

Documento que recoge la relación de controles de la ISO27002, especificando, para cada uno de ellos, si es o no de aplicación a la organización, junto con la justificación de exclusión en caso de no serlo, o una descripción de cómo se implementa en caso de serlo.

Pautas de implantación

Generalmente, y esto incluye también a la Dirección, se piensa que definir el alcance del SGSI es un ejercicio sencillo, cuando no lo es en absoluto.

- Es recomendable dedicar un tiempo a reflexionar sobre cuáles son los procesos que se quieren incluir en el sistema de gestión, para que realmente sean los **procesos más críticos**.
  Hay que pensar que implantar un sistema de gestión de la seguridad supone una dedicación de recursos y un esfuerzo importantes, y que no sólo es un proyecto de puesta en marcha, sino que mantener actualizado el SGSI implica mantener una dedicación permanente. Por este motivo es bueno tomarse el tiempo necesario para analizar hasta dónde se implantará el SGSI, y es indispensable consensuar dicho alcance con la Dirección.

- Cuando se empieza con la implantación de un SGSI, suele ser recomendable empezar por un proceso acotado y transversal. Acotado en el sentido de que suponga un alcance reducido, para empezar por algo más controlable y sobre lo cual aprender, de manera que cuando se abarquen procesos más "macro", se cuente ya con un conjunto de lecciones aprendidas que hagan más eficiente la implantación. Y transversal en el sentido de que abarque diversas áreas o departamentos de la organización, puesto que ello permitirá una implantación de todo tipo de controles (de recursos humanos, de operación, organizativos...) y permitirá sentar la base para ir ampliando el alcance del SGSI en posteriores iteraciones.

- Un aspecto importante a considerar en la definición del alcance es la inclusión o no de las actividades llevadas a cabo por terceros para la organización. En general suelen presentarse dos opciones:
  – Incluir la actividad de terceros en el propio alcance.
  – Excluir la actividad de terceros del alcance, y demostrar que se han tomado las medidas necesarias para que dicho tercero dé cumplimiento a la norma. Esta obligación debe quedar claramente recogida en el contrato con el tercero, y la organización debe reservarse el derecho a la auditoría, para analizar cuando lo crea necesario, el nivel de cumplimiento real.

- Cuando se redacta el alcance es importante ser preciso y escribir en positivo, es decir, explicar qué está incluido en el alcance, más que hacer una definición general que incluya un "excluyendo".

- El alcance suele hacer referencia a la declaración de aplicabilidad y su versión. Ésta no es más que una relación de los controles de la ISO, para cada uno de los cuales se especifica si es o no de aplicación, para lo cual será determinante el alcance escogido. En caso de decir que un control no aplica, es necesario justificar la causa.
  Cabe destacar que, por el carácter general de la norma, es bastante complicado que un control no aplique. Normalmente un mínimo del 80% de los controles es de aplicación.

A continuación se presentan algunas definiciones reales de alcance de un SGSI:

- La gestión de la seguridad de la información de las operaciones de negocio, incluyendo la consultoría de seguridad y suministro de herramientas de software de seguridad. Todo ello de acuerdo con la Declaración de Aplicabilidad Referencia 1.00.

- La implantación de un SGSI que da soporte al diseño y fabricación de equipos para los mercados militar y civil. Esto incluye el hardware, software, integración de sistemas y servicios de consultoría de acuerdo con la Declaración de aplicabilidad del SGSI Ref. 1.1.

- La gestión de la seguridad de la información en el diseño, implantación y funcionamiento de infraestructura de Microsoft.NET. De acuerdo con la declaración de aplicabilidad, versión fechada en xx/xx/xxxx.
- La gestión de la seguridad de la información que cubre todas las actividades asociadas con el CPD de Alcorcón que da soporte a los servicios de *hosting* seguro.
- Toda la información y los sistemas que la procesan para el desarrollo de software, integración y servicios de mantenimiento de las cuatro instalaciones en la India.
- El funcionamiento de un SGSI para las actividades relacionadas con el proceso de cobros y los servicios de validación asociados.
- El SGSI de Banca por Internet del Banco 123 de acuerdo con la Declaración de Aplicabilidad, versión 3.
- La gestión de la seguridad de la información que cubre todas las actividades desarrolladas por HWA Solutions, como integraciones de sistemas incluyendo la consultoría para el desarrollo de software de aplicación IT, y los servicios de gestión de redes y sistemas de la compañía.
- La gestión de la seguridad de la información en todas las actividades relacionadas con las ventas y comercialización del diseño y producción de memorias y sistemas LSI y AM LCD localizados en las plantas de producción de Göteborg y Freiburg, incluyendo los servicios proporcionados por PICSA. Esto está de acuerdo con la declaración de aplicabilidad versión 1.0.
- La gestión de la seguridad de la información de Banco Internet 123, incluyendo las operaciones bancarias y la gestión de dos centros de datos subcontratados. Esto está de acuerdo con la declaración de aplicabilidad versión 3.
- Information security management of the Information Service Center providing integrated systems management services, disaster recovery services, integrated security services, network Infra services and satellite communication services. This in accordance with the Statement of Applicability Issue 1.3.
- The information security management of the operation in the provision of commercial insurance broker services, in accordance to the Statement of Applicability Issue 3.0.
- Information security management system relating to the investigation of serious fraud. This is in accordance with the Statement of Applicability issue 1.0.

7.3. P.III. Definir la organización de la seguridad de la información

Cualquier esfuerzo para gestionar la seguridad de la información es inútil si no se asignan responsabilidades y funciones de forma clara y concreta, y no existe el soporte de la Dirección de la organización.

Cada organización deberá crear su propio esquema organizativo interno, asegurando en cualquier caso que todas las responsabilidades y funciones en materia de seguridad de la información están correctamente asignadas y garantizando, siempre que sea posible, el principio de segregación de funciones.

Ved también

En el capítulo siguiente se dan algunas pautas para la implantación de la estructura organizativa en seguridad de la información.

7.4. P.IV. Definir las políticas de alto nivel

Ved también

En el capítulo siguiente se dan algunas pautas para la implantación de un marco normativo.

Las políticas de alto nivel desarrollan la política de seguridad de la información en líneas de actuación más concretas. Las políticas de alto nivel contemplan en conjunto todas las áreas de seguridad de la información.

7.5. P.V. Definición de objetivos de seguridad de la información

Es necesario establecer objetivos concretos de seguridad de la información, que garanticen que todas las iniciativas en seguridad de la información estén coordinadas y orientadas en una misma dirección, y alineadas con los objetivos del negocio. Los objetivos de seguridad se suelen definir con carácter anual.

Obviamente, los objetivos de seguridad siempre incluirán la reducción del riesgo a niveles asumibles por la organización.

Posibles objetivos de seguridad en una entidad bancaria

- Reducción del fraude.
- Mejorar la confianza de los clientes en la banca electrónica.
- Cumplimiento legal: LOPD, Basilea II...

Pautas de implantación

- Los objetivos de seguridad se deben definir a partir de los objetivos del negocio, analizando cuál es la mejor manera de que la seguridad de la información contribuya a dichos objetivos.
- De partida, los objetivos de seguridad no se deben definir pensando en el presupuesto disponible, es decir, para contestar a la pregunta "¿qué puedo hacer?", sino que teniendo en cuenta la situación de partida, debieran responder a la pregunta "¿qué quiero hacer? o ¿cómo puedo contribuir al negocio?".
  Existen muy diferentes formas de cubrir un objetivo de seguridad, y será después, en el Plan de seguridad o Plan de gestión del riesgo, en la segunda fase del SGSI (Hacer o *Do*), cuando se determinará cómo dar cobertura a dicho objetivo o hasta qué punto es posible darle cobertura.
- Los objetivos de seguridad se deben contrastar con la Dirección para conseguir su aprobación.

7.6. P.VI. Identificación de los riesgos

Es muy importante identificar los activos de información y establecer el riesgo al que están sometidos, a partir de la determinación de cuál sería el impacto para la organización en caso de que se produjera una situación de falta de confidencialidad / privacidad, integridad o disponibilidad de dichos activos.

La determinación del riesgo real al que los activos de información están sometidos permitirá a la Dirección tomar decisiones sobre el umbral de riesgo asumible por la organización, y priorizar las acciones en materia de seguridad de la información, siempre adoptando medidas proporcionadas.

Riesgo residual

Es el riesgo remanente una vez aplicados los controles de seguridad.

Pautas de implantación

- El análisis de riesgos debe ser formal y estar documentado.
- La complejidad del análisis de riesgos dependerá de la criticidad de los activos a proteger.
- La metodología empleada debe ser coherente con la complejidad y los niveles de protección requeridos.

- El grado de profundidad con que el análisis de riesgos debe ser llevado a cabo varía en función de la madurez de la organización. Para dar los primeros pasos se recomienda hacer un análisis de alto nivel de los procesos incluidos en el alcance, con el objetivo de detectar los puntos de máximo riesgo. Más adelante, si procede, se puede realizar un análisis de mayor profundidad para los procesos incluidos en el alcance que se consideren más críticos.

- Debe cubrir todo el alcance del SGSI.

- Los riesgos cambian constantemente, por lo que debe existir una metodología y un procedimiento para su revisión y mantenimiento.

- La Dirección debe aprobar formalmente el riesgo residual, lo cual deberá quedar recogido en un documento, que constituirá un "registro" del SGSI.

7.7. P.VII. Selección de salvaguardas

Una vez identificados los riesgos que hay que mitigar (riesgos no asumibles) y los objetivos de seguridad que se desea alcanzar, se deberán seleccionar los controles o salvaguardas necesarias. Estas salvaguardas pueden ser controles técnicos, procedimientos operativos, normativas de usuario, cláusulas contractuales, etc. La selección de controles se puede hacer a partir de la ISO 27002, pero también se pueden incluir otros controles que se consideren útiles para la organización, no incluidos en la norma.

Pautas de implantación

La selección de controles se deberá realizar teniendo siempre en cuenta el principio de proporcionalidad, y deberá quedar documentado en el Documento de aplicabilidad (en inglés, *Statement of Applicability* (SoA)), o relación de controles de seguridad. Este documento recoge para cada control de la ISO si es o no de aplicación a la organización, y en caso de no serlo, la justificación. No obstante, es aconsejable incluir también para los controles que sí son de aplicación, una explicación de cómo se implementa el control (haciendo referencia a procedimientos si procede) y cuáles son los riesgos que evita. De este modo, el documento establece la relación entre el análisis de riesgos y el estado real de la seguridad, constituyéndose así en una herramienta muy útil de auditoría, ya sea interna o externa.

Las razones para la no inclusión de un control deben ser sólidas y coherentes. Generalmente los únicos motivos aplicables son:

- **Naturaleza de la organización y su actividad**.
  No entra en el alcance, o afecta a una actividad que la organización no realiza.

Ejemplo

- **Control 10.9.1. Comercio electrónico.** A una organización que no tiene comercio electrónico no le será de aplicación este control.
- **Control 7.1.5. Áreas aisladas de carga y descarga.** No será de aplicación si la organización no dispone de dichas áreas.

- **Resultado del análisis de riesgos**.
  El nivel de riesgo detectado no justifica la inversión para la mitigación.

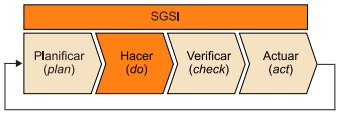
Ejemplo

- **Control 9.1.6. Acceso a zonas de carga y descarga.** No será de aplicación, si el análisis de riegos no ha detectado ningún riesgo significativo relacionado con estas zonas.

8. Hacer: implantar y operar el SGSI

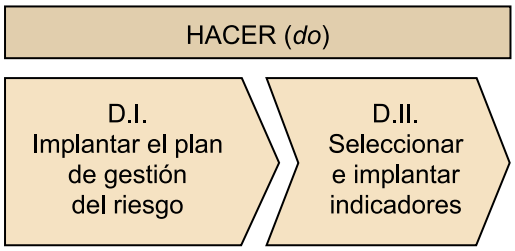
La segunda fase del SGSI se compone básicamente de dos actividades:

- Implantar el plan de gestión del riesgo
- Seleccionar e implantar indicadores



Hacer: segunda fase del SGSI

Etapas de la segunda fase del SGSI: Hacer



Una vez finalizada la fase de planificación del SGSI, se entra en la fase de implantación, que consta básicamente de dos etapas: una primera etapa de definición de cómo se va a poner en práctica aquello planificado en la fase anterior, que se concreta en un **Plan de gestión de riesgos** o **Plan de seguridad**, que una vez definido debe ser llevado a cabo, y una segunda etapa de selección de indicadores, que son los que permitirán evaluar la eficacia y eficiencia de las medidas implantadas, y en definitiva, controlar la evolución del estado de la seguridad de la información.

Es por tanto la fase de concreción, de especificación del cómo se van a poner en práctica las salvaguardas seleccionadas, cuándo se implementarán, quién será responsable y con qué presupuesto, de implementación real de dichas salvaguardas y de cómo se va a medir el éxito o fracaso de las acciones realizadas y consecuentemente, de la rentabilidad de las inversiones practicadas.

8.1. D.I. Implantación del plan de gestión del riesgo

El **Plan de gestión del riesgo** determina cómo y cuándo implantar los controles seleccionados y se concreta en el **Plan de seguridad de la información**, en ocasiones también denominado **Plan director de seguridad de la información**, que agrupa las acciones en proyectos, las prioriza definiendo acciones a corto y medio plazo (unos 3 años) y realiza una estimación de costes. El Plan de seguridad debe ser presentado a la Dirección para conseguir su aprobación y la dotación presupuestaria necesaria, paso previo al arranque de cualquier proyecto.

La implantación / revisión del Plan de continuidad de negocio acostumbra a ser parte de dicho plan de seguridad.

El **Plan de seguridad de la información** es el que describe cómo llevar a cabo el cumplimiento de los objetivos de seguridad.

Pautas de implantación

- La definición del Plan de seguridad de la información implica elaborar un plan de acción para el cumplimiento de los objetivos y, por tanto, es indispensable realizar una estimación del coste de cada uno de los proyectos antes de presentarlo a la Dirección.
- El principio de proporcionalidad debe regir como elemento conductor del plan, puesto que nunca hay que olvidar que el objetivo final no es la seguridad total, sino llevar la seguridad a los niveles que la organización puede asumir.
- Una buena propuesta de Plan de seguridad proporcional, coherente y bien justificado es, asimismo, la base para conseguir el presupuesto necesario y el apoyo de la Dirección.
- Debe estar claro a cuál o cuáles de los objetivos de seguridad definidos en la fase de planificación del SGSI contribuye cada uno de los proyectos propuestos, ya que ello facilitará la toma de decisiones por parte de la Dirección.
- En este punto es importante tener en cuenta los controles ya aplicados con anterioridad (ya sea en ciclos anteriores del SGSI, proyectos de seguridad anteriores, medidas aplicadas desde alguna unidad de la organización de forma aislada...), para estudiar si éstos siguen siendo efectivos y, por tanto, no es necesario adoptar medidas complementarias, o si éstos han perdido su efectividad y, por tanto, deben ser sustituidos.
- En este sentido, es también importante estar al día sobre el estado de la tecnología y conocer qué ofrece el mercado, puesto que la selección de una determinada tecnología para desarrollar un control puede ser un factor clave de éxito o fracaso.
- Es también importante "ser creativo". Con frecuencia se piensa que sin presupuesto, o mejor, con bajo presupuesto, no hay nada que hacer en seguridad, lo cual es totalmente falso, ya que existe un elevado número de controles puramente organizativos o bien que con sencillas herramientas se pueden implementar y dar buenos resultados.

Esta fase del "Hacer" no acaba con la definición del Plan de seguridad, sino que una vez aprobado es necesario ponerlo en práctica, según la planificación establecida. Es por tanto, una de las fases más largas del SGSI, ya que incluye el seguimiento de los diferentes subproyectos que llevarán a la implementación de las medidas de seguridad que el análisis de riesgos ha determinado como necesarias en la fase anterior.

8.2. D.II. Selección e implantación de indicadores

Para que el sistema se mantenga vivo y actualizado, es necesario evaluar su eficacia de forma continuada. Para ello, se deben establecer indicadores que permitan controlar el funcionamiento de las medidas de seguridad de la información implantadas, así como su eficacia y eficiencia, y definir los mecanismos y la periodicidad de medida de dichos indicadores.

La efectividad del SGSI está proporcionalmente relacionada con la efectividad de los controles implantados. Para disponer de información sobre la eficacia de los controles, es imprescindible implantar indicadores que nos proporcionen dicha información.

Un indicador es una medida respecto de una referencia. Todo indicador constará de ocho componentes básicos:

1) Nombre del indicador. Se debe seleccionar un nombre significativo, no excesivamente largo, que dé idea de cuál es la medición que se está realizando.

2) Descripción del indicador. Explicación del objetivo de medida de dicho indicador.

3) Control de seguridad que respalda. A qué control o controles está dando cobertura.

4) Fórmula de medición. Descripción de la fórmula aplicada para obtener la medición. Es importante que los parámetros que intervienen sean concretos y no se presten a ambigüedad.

5) Unidades de medida: las unidades de medida deben estar claramente especificadas.

6) Frecuencia de medición. Cada cuánto se debe recoger la medición. Es posible establecer una frecuencia inicial durante un período de tiempo, y una frecuencia posterior mayor (por ejemplo, quincenal los tres primeros meses, y mensual a partir del cuarto mes). En cualquier caso, la frecuencia dependerá de la variabilidad en el tiempo de la medición.

7) Cuando sea posible, valor objetivo y valor umbral, es decir y respectivamente, cuál es el valor que sería correcto para la compañía y cuál es el valor por debajo del cual se debiera levantar una alarma.

8) Responsable de la medida. Sobre quién o, preferiblemente, sobre qué cargo recae la responsabilidad de proporcionar el resultado de la medida.

Ejemplo

Supongamos el caso de que se haya instalado un sistema de autogestión de contraseñas y otro de control de privilegios de acceso en bajas laborales.

Nombre indicador	Autogestión contraseñas
Descripción	Medida de la eficacia del nuevo portal de autogestión de contraseñas
Control de seguridad	11.2.3. Gestión acceso usuarios
Fórmula de medición	N.° incidencias atendidas sobre gestión de contraseñas en el período frente al mismo valor en el período anterior
Unidades de medida	Incidencias / Incidencias
Frecuencia de medición	Mensual
Valor objetivo **Valor umbral**	Disminución del 60% < 40%
Responsable de la medida	Responsable de seguridad a partir de la información proporcionada por la herramienta de gestión de incidencias y el portal de autogestión

Nombre indicador	Control de privilegios de acceso en bajas laborales
Descripción	Control el funcionamiento del procedimiento de salida de empleados en la compañía
Control de seguridad	8.3.3. Revocación de derechos de acceso
Fórmula de medición	N.° de solicitudes de baja de acceso frente a personal (empleados, terceros, etc.) que deja la compañía
Unidades de medida	Solicitudes / personas
Frecuencia de medición	Trimestral
Valor objetivo **Valor umbral**	100% <75% (saltará la alarma si la medición es inferior al 75%)
Responsable de la medida	Responsable de seguridad a partir de formularios e información de RR. HH.

Se debe elaborar un documento que recoja todos los indicadores implantados, y la descripción de cada uno de ellos con las características que acabamos de presentar.

A la hora de seleccionar un indicador, **es importante que la medición sea fiable y repetible**, es decir, que se debe basar en **evidencias objetivas.**

Existen diferentes tipos de indicadores.

Ejemplos de indicadores

- **Indicadores de gestión**
  - Número de horas de formación impartidas.
  - Presupuesto dedicado a personal de mantenimiento de sistemas.
  - Número de empleados con responsabilidades en seguridad de la información.
  - Número de sugerencias de mejora del SGSI recibidas de los empleados.

- **Indicadores de operación**
  - Tiempo total de caída de un determinado servicio en el último mes.
  - Número de averías de equipos informáticos en el último mes.
  - Tráfico medio del *firewall*.
  - Número de intentos de penetración detectados por el IDS frente al número de intentos rechazados.
  - Número de virus detectados frente al número de incidentes por virus.

- **Indicadores de entorno**
  - Alertas por nuevo virus.
  - Tiempo medio de exposición de un sistema desde que se detecta una vulnerabilidad hasta que ésta es parcheada.
  - Alertas meteorológicas por olas de calor, tormentas eléctricas, inundaciones, ...
  - Cambios en la legislación.

Nota

La definición de indicadores dentro del ámbito del SGSI es la principal diferencia entre la ISO 27001 y la UNE 71502, y la BS 7799-2. A diferencia de las dos primeras, esta última considera que es suficiente con disponer de registros para validar la correcta implantación de la seguridad de la información en una organización, no siendo necesaria la definición de indicadores.

Pautas de implantación

- Un mismo indicador puede ser de aplicación a varios controles o incluso objetivos o secciones completas de la norma.

- Inicialmente, los indicadores se definen para la vigilancia de la implantación de los controles. Más adelante, pasan a ser indicadores de mejora continua.

- La implantación de un indicador requiere una dedicación de recursos, por lo que no se deben implantar indicadores que no sean relevantes para la organización.

- Es muy importante ser riguroso en la recogida de la información para que ésta sea fiable, representativa y comparable en el tiempo.

- Un indicador que no aporta información relevante es mejor eliminarlo.

- Un indicador adquiere la característica de "indicador" en el momento en que es comparable, es decir, que se puede conocer su evolución en el tiempo. Por ello es importante reflexionar sobre los indicadores a implantar antes de ponerlos en práctica, e intentar mantener la medida en el tiempo, para poder tener valores comparables y poder analizar si realmente se está produciendo una mejora en la seguridad de la información. No obstante, y como ya hemos dicho, si un indicador no proporciona información relevante, es mejor eliminarlo.

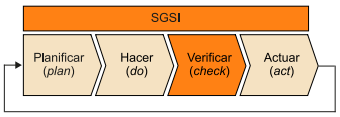
- Siempre que sea posible, se deberá automatizar la medición, por una cuestión de eficiencia (ahorro de tiempo de un recurso que se puede emplear en otras funciones) y eficacia (disminución o eliminación de errores en la medición, es decir, "repetibilidad").

- Una vez más, es indispensable aplicar siempre el principio de proporcionalidad. El esfuerzo para obtener la medición debe ser proporcional al valor de la información que proporciona.

9. Verificar: Monitorizar y revisar el SGSI

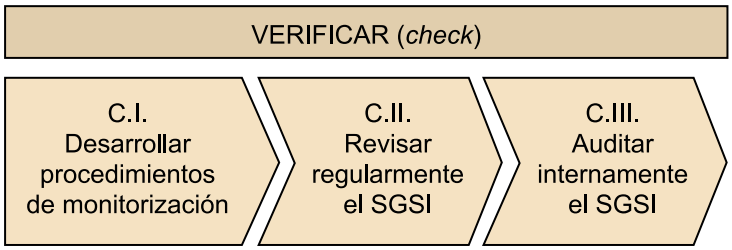
La tercera fase del SGSI se compone de 3 etapas:

- C.I Desarrollar procedimientos de monitorización
- C.II. Revisar regularmente el SGSI
- C.III. Auditar internamente el SGSI



Verificar: tercera fase del SGSI

Etapas de la tercera fase del SGSI: Verificar



Para que el sistema se mantenga vivo y actualizado, es también necesario:

- Realizar un seguimiento continuado de la evolución de los indicadores de seguridad.

- Realizar evaluaciones de seguridad de la información (del sistema de gestión, de áreas o sistemas concretos...) por parte de personal interno o externo, para detectar debilidades y poder establecer acciones correctivas, preventivas y de mejora.

- Es necesario que haya alguien velando por el mantenimiento de toda la documentación generada y por su revisión periódica, incluyendo la política de seguridad de la información, objetivos, resto del marco normativo, análisis de riesgos, indicadores, plan de continuidad del negocio, etc.

Como mínimo es necesaria una **revisión anual** del sistema de gestión global, implicando al máximo nivel directivo en la revisión de los componentes más estratégicos del sistema. Debe existir un procedimiento que describa cómo mantener actualizado el SGSI.

9.1. C.I. Desarrollar procedimientos de monitorización

Es preciso realizar un seguimiento periódico de los indicadores de seguridad de la información, para conocer su estado y evolución y, en definitiva, su eficacia; es decir, si el control contribuye a lograr el objetivo de seguridad para el que fue diseñado. Como se explicaba en el apartado anterior, siempre que sea posible y económicamente aceptable, es recomendable la automatización de los procedimientos de monitorización, para facilitar y fiabilizar la generación

de los informes del estado de la seguridad de la información y la generación de alarmas para denunciar incidencias o situaciones de seguridad deficiente que requieran de actuación urgente.

9.2. C.II. Revisión del SGSI

La Dirección debe revisar el SGSI a intervalos planificados, para ratificar su conveniencia, adecuación y eficacia. Esta revisión debe ser como mínimo anual, aunque inicialmente se recomienda una periodicidad menor.

Las revisiones de la Dirección de la organización deben:

- Contar con un procedimiento para llevarlas a cabo.
- Identificar cambios en los niveles de riesgo, nuevas amenazas y vulnerabilidades.
- Identificar cambios en la organización.
- Identificar cambios en la legislación.
- Revisar el estado del sistema y su implantación.
- Analizar el cumplimiento de los objetivos de seguridad.
- Analizar la efectividad de los controles implantados (evolución del estado de la seguridad).
- Establecer acciones preventivas, correctivas y de mejora.
- Disponer de registros que evidencien dichas revisiones.

Para conocer el estado de los controles y su evolución en el tiempo, es habitual utilizar modelos de madurez predefinidos, que introducen objetividad en la evaluación, al establecer criterios estándar fácilmente comprensibles por personal ajeno al mundo de la seguridad de la información. Tal y como se explicaba en el capítulo introductorio, es habitual utilizar el modelo CMM.

9.3. C.III. Auditorías

La comprobación de la idoneidad del diseño e implantación del SGSI se realiza a través de auditorías. Éstas pueden ser llevadas a cabo internamente, o se pueden contratar auditores externos para efectuarlas, pero en cualquier caso, los auditores deben cumplir los siguientes requisitos:

- Deben ser independientes, es decir, no pueden haber intervenido en el proceso/trabajo auditado.
- Deben estar cualificados en la materia: conocimiento del proceso de auditoría, de las normas auditadas y óptimamente, deberían tener experiencia en el campo de la seguridad de la información.

Estas auditorías se deben planificar correctamente, para poder contar con la implicación de todas las personas necesarias.

El informe de auditoría debe incluir como mínimo:

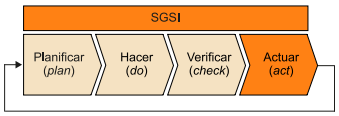
- Fecha de la auditoría.
- Nombre de los auditores.
- Alcance de la auditoría: área, departamento, proceso, auditados.
- Controles auditados.
- Conformidad del SGSI con la norma, o grado de adecuación.
- No conformidades detectadas.
- Si la auditoría no es de certificación, podrá contener además recomendaciones de mejora.

Generalmente, el informe no recoge cómo se ha auditado un control, ni tampoco las evidencias recogidas para la auditoría, que forman parte de la documentación del auditor.

10. Actuar: mantener y mejorar el SGSI

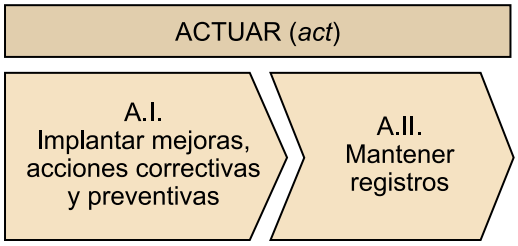
Finalmente, la cuarta y última fase del ciclo del SGSI se compone de las dos actividades siguientes:

- Implantar mejoras, acciones correctivas y preventivas
- Mantener registros



Actuar: cuarta y última fase del SGSI

Etapas de la cuarta y última fase del SGSI: Actuar



De la monitorización y la revisión del SGSI y de los resultados de las auditorías se obtendrán **propuestas de mejora y acciones correctivas y preventivas**, que se deberán planificar dentro del Plan de seguridad de la información.

Mantener el SGSI pasa también por conservar un conjunto de evidencias que prueben que políticas, procedimientos, controles e indicadores no son definiciones teóricas, sino que se están llevando a la práctica tal y como especifica el sistema. Generalmente, a estas evidencias se las denomina registros.

Los registros deben ser:

- Legibles: se deben conservar en un formato accesible / recuperable.
- Identificables: se les debe asignar una codificación o nomenclatura significativa, que permita localizarlos con relativa facilidad.
- Trazables: debe ser posible conocer la evolución de las versiones y deben preservarse de alteraciones, es decir, que se deberán proteger contra daños, deterioro, pérdida o manipulación.

Si no existen requerimientos legales específicos, los registros se suelen guardar unos tres años.

Aunque no es requisito indispensable, para obtener la certificación del SGSI es aconsejable disponer de un mínimo de 6 meses de registros.

Es indispensable desarrollar un procedimiento que especifique cómo realizar la gestión de los registros, estableciendo cómo hacer: identificación, almacenamiento, protección, recuperación y eliminación (dependiendo del tiempo de vida establecido).

Un registro puede adoptar muy diferentes formas; puede ir desde el acta de una reunión con la Dirección, pasando por una lista de asistentes a un curso de formación, hasta una extracción de trazas de un sistema.

11. Esquema documental del SGSI

Tal y como hemos visto hasta ahora, un sistema de gestión de la seguridad de la información es un conjunto de acciones coordinadas y dirigidas a mejorar la seguridad de la información de una organización, que abarca desde la fase de planificación e implantación, hasta la fase de control o verificación y actuación para la mejora, en iteraciones consecutivas que lo que persiguen es introducir a la organización en un ciclo permanente de mejora continua para, en definitiva, ir madurando el proceso de la seguridad de la información e ir haciéndolo progresivamente más eficiente.

A lo largo de la descripción de las diferentes fases, se ha ido haciendo referencia a políticas, procedimientos, revisiones, documentos, planes...

En este apartado, presentamos el esquema documental de todo SGSI, de forma ordenada. La mayoría de las entradas han sido ya referenciadas en apartados anteriores, pero en este punto se presentan de forma ordenada, con dos objetivos:

- Plasmar la coherencia de toda la documentación referenciada.

- Disponer de un índice al que se deberá dar cumplimiento para implantar un SGSI, y muy especialmente, en caso de que la organización desee superar un proceso de certificación.

Marco documental

- Principios del SGSI. (En ocasiones este apartado recibe el nombre de Manual de seguridad).
  - Política de seguridad de la información.
  - Alcance del SGSI.
  - Breve descripción de la actividad de la organización y organigrama.
  - Políticas concretas de alto nivel (se pueden describir detalladamente o simplemente hacer referencia).
  - Organización de la seguridad de la información.

  - Cómo se implanta la norma: referencia a procedimientos, manuales, instrucciones, etc.

- Metodología de análisis de riesgos y procedimientos de revisión. Metodología de gestión del riesgo y seguimiento.

- Declaración de aplicabilidad.

- Políticas de seguridad de la información de alto nivel (si no se han incluido en los Principios del SGSI).

- Políticas de seguridad de la información específicas.

- Plan de continuidad del negocio.

- Procedimientos:
  - Implantación de controles: relación de procedimientos desarrollados para implantar los controles, que especifican cómo llevar a la práctica las diferentes políticas de seguridad. Dichos procedimientos pueden estar referenciados en las propias políticas.

  - Control documental del SGSI: descripción de la lista de documentos que conforman el SGSI, dónde se ubican, cómo se revisan y versionan, cómo se codifican, etc.

  - Control de registros del SGSI: descripción de cómo se gestionan, almacenan, destruyen, etc. los registros generados por el sistema de gestión.

  - Revisión del SGSI por la Dirección (descripción de cómo llevar a cabo el proceso de revisión).

  - Gestión de indicadores (a nivel conceptual, sin entrar en el detalle de cada uno de ellos: qué es un indicador, quién los define, quién asigna la responsabilidad de la medición, a quién se reportan, *reporting* a Dirección, acciones en caso de cumplimiento reiterado de un indicador, acciones en caso de incumplimiento reiterado, etc.).

  - Formación en seguridad de la información.

  - Gestión de acciones correctivas, preventivas y de mejora. Formulario de registro de no conformidades.

  - Actualización y revisión del plan de continuidad de negocio (motivos del cambio, frecuencia de revisión, responsables, for-

mación de los implicados, etc.). Este punto puede formar parte también del propio Plan de continuidad de negocio.

- Registros.
  - Análisis de riesgos (incluyendo el inventario de activos).
  - Documento de aceptación del riesgo residual por parte de la Dirección.
  - Objetivos de seguridad de la información establecidos por la Dirección (alto nivel, más allá de la norma y del Plan de gestión del riesgo).
  - Plan de seguridad o Plan de gestión del riesgo.
  - Resultados de auditorías.
  - Lista de indicadores (fórmula de medición, responsable de la medida, frecuencia, valor objetivo del indicador, control de la ISO con que está relacionado).
  - Actas de reuniones de revisión del SGSI por la Dirección, convocatoria de reuniones, informes de revisión elaborados por el gestor de seguridad de la información.
  - Correos electrónicos enviados por la Dirección, cursos de formación, etc.
  - Formación impartida y cualificación de las personas que están dentro del alcance del SGSI.
  - Informe de no conformidades (plan de seguimiento de acciones correctivas, preventivas y de mejora, revisión de efectividad).
  - Revisiones del Plan de continuidad del negocio.
  - Formularios y documentación que pruebe el cumplimiento de los procedimientos.

Resumen

Este módulo se ha centrado en presentar la ISO 27000 de Seguridad de la Información, cuyo conocimiento es indispensable para cualquier profesional dedicado a la gestión de la seguridad de la información.

Así pues, se ha presentado en primer lugar la ISO 27002 o Guía de buenas prácticas en seguridad de la información. Esta norma establece la importancia del análisis de riesgos como punto de inicio del proceso de gestión de la seguridad de la información, para presentar a continuación once objetivos de control indispensables para hacer una gestión integral, los cuales van desde cuestiones organizativas, como la política de seguridad, el marco normativo, y aspectos de recursos humanos, como la contratación, formación o la firma de cláusulas de confidencialidad, pasando por cuestiones mucho más técnicas, como la gestión de la adquisición de productos, su desarrollo, o la operación de los sistemas y las infraestructuras TIC, para terminar hablando de la importancia del cumplimiento legal y la protección de los registros de la compañía, o la necesidad de un plan de continuidad de negocio.

Por su parte, la ISO 27001 describe la implantación de un sistema de gestión de la seguridad de la información, basado en el *Ciclo de Deming* o *Ciclo PDCA*, que plantea la gestión de la seguridad como un proceso de mejora continua, basado en la repetición cíclica de cuatro fases: **Planificar**, **Hacer**, **Verificar** y **Actuar**.

Es materialmente imposible resumir estas dos normas en unas pocas líneas, pero intentaremos concretar cuáles son los factores críticos de éxito de la implantación de un SGSI en diez puntos:

1) La política y objetivos de seguridad de la información deben estar alineados con los objetivos del negocio.

2) El enfoque para implantar la seguridad de la información debe ser consistente con la cultura de la organización.

3) Apoyo visible y compromiso de la Dirección.

4) Definición precisa y clara del alcance del SGSI.

5) Buena comprensión del análisis y de la gestión del riesgo, así como de los requerimientos de seguridad de la información.

6) Definición clara de las funciones en seguridad de la información.

7) Concienciación de la Dirección y los empleados en materia de seguridad de la información, y formación y capacitación cuando sea necesario.

8) Distribución a todos los empleados y terceras partes implicadas de la política de seguridad de la información, así como de otras normas y estándares vigentes.

9) Sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y la introducción continua de mejoras en la seguridad y su sistema de gestión.

10) Disponer de recursos humanos y técnicos, que permitan gestionar la seguridad y mantener el sistema de gestión.