CURSO DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA UNE-ISO/IEC 27000

INTECO-CERT

Junio 2010

ÍNDICE

1. CONCEPTOS BÁSICOS SOBRE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información cuenta con numerosos vocablos que no son de uso cotidiano y que dificultan a veces el entendimiento de los conceptos. Vamos a clarificar en primer lugar estos términos para que los distintos aspectos que se van a tratar sean fácilmente comprensibles.

Las secciones de este capítulo son:

- Conceptos básicos.

1.1. CONCEPTOS BÁSICOS

1.1.1. ¿Qué entendemos por seguridad de la información?

Para comprender qué es la seguridad de la información, en primer lugar, debemos conocer que la información en este área es referida a los activos de información (es decir, los datos por supuesto, pero también los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, trasmitir y destruir la información), que tienen un valor para la organización.

En las complejas organizaciones de hoy en día, se recogen, gestionan y transmiten multitud de datos a través de diferentes medios, a mucha gente, y todas las acciones relacionadas con ello pueden necesitar protección.

No se debe confundir la seguridad de la información con la seguridad informática ya que la seguridad de la información abarca muchas más áreas mientras que la seguridad informática se encarga de la protección de las infraestructuras TIC que soportan el negocio. Por tanto la seguridad de la información abarca la seguridad informática.

La seguridad de la información, por tanto, se puede definir como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.

Estos tres parámetros básicos de la seguridad se definen como:

- **Confidencialidad:** A la información solo pueden acceder las personas autorizadas para ello.
- **Integridad:** La información ha de estar completa y correcta en todo momento.
- **Disponibilidad:** La información estará lista para acceder a ella o utilizarse cuando se necesita.

Figura 1. Parámetros básicos de la seguridad de la información

Dependiendo de los modelos utilizados o de las necesidades del negocio, también son parámetros a tener en cuenta:

- **Autenticidad:** La información es lo que dice ser o el transmisor de la información es quién dice ser.

- **Trazabilidad:** Poder asegurar en todo momento quién hizo qué y cuándo lo hizo.

En cualquier organización existen datos de clientes o usuarios, esta información necesita protección:

- Si accediera a ella alguien de la competencia podría utilizarla para conseguir beneficios económicos, o bien denunciar a la organización ante la Agencia de Protección de Datos para que se le impusiera una multa si se demuestra que se vulneró la Ley de Protección de Datos de Carácter Personal, o publicarla en la prensa para dañar la imagen de la organización. Un fallo de confidencialidad puede ser tremendamente dañino.

- Si la información se corrompe, se podrían enviar cartas o facturas erróneas a los clientes, con la confusión y las quejas de los afectados que acarrearía, más el trabajo y el tiempo que habría que emplear para corregir los errores y restaurar a su estado correcto la información. Que la información permanezca Íntegra en todo momento es más importante de lo que a primera vista pueda parecer.

- Si el equipo en el que reside esta información se estropea y no se puede acceder a ella, simplemente no se puede funcionar, no se puede dar servicio, lo que implica que se deja de ganar dinero y en casos extremos se puede perder, si el cliente decide marcharse y adquirir el servicio en otro proveedor. Un fallo de disponibilidad tiene siempre un impacto económico directo en la organización, por leve que sea, ya que se deja de trabajar, hay una parte de la organización que ha parado, por lo que ha dejado de generar beneficio.

1.1.2. ¿Qué entendemos por seguridad de la información?

Un fallo de seguridad es cualquier incidente que la compromete, es decir que pone en peligro cualquiera de los parámetros con los que se valora la seguridad: la confidencialidad, la disponibilidad o la integridad de la información. Con la actual complejidad de los sistemas de información, con una economía y un comercio que se basan en intercambios y comunicaciones a lo largo y ancho del mundo, con un número creciente de usuarios que no sólo se conectan desde dentro sino también desde fuera de la organización, es fácil hacerse una idea del reto que presenta evitar que sucedan cosas como:

- Fallos en las comunicaciones.
- Fallos en el suministro eléctrico.
- Fallos humanos de usuarios internos, usuarios externos, administradores, programadores, etc.
- Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc. que inundan la red.
- Accesos no autorizados a los sistemas o la información.
- Incumplimiento de una ley o un reglamento.

Los fallos de seguridad son ocasionados muchas veces por la errónea percepción de que si la seguridad física está razonablemente asegurada, no tiene por qué haber problemas. O que protegiendo únicamente las aplicaciones y las bases de datos ya está garantizada la seguridad. Con esos supuestos se dejan desprotegidas muchas áreas de la organización, muchos activos de información que pueden ser fácilmente dañados o destruidos, ya que no se han tenido en cuenta todos los aspectos de la seguridad de la información: la seguridad física, la seguridad lógica y las medidas organizativas.

1.1.3. ¿Qué son los Sistemas de Gestión de la Seguridad de la Información (SGSI)?

Hasta ahora lo más común ha sido ir parcheando los agujeros de seguridad con medidas puntuales, descoordinadas y poco proporcionadas al riesgo que reducen. Se trata de medidas cuya implantación y efectividad no son llevadas a cabo y controladas de manera planificada. El resultado es obvio, se siguen manteniendo altos niveles de riesgo frente a las amenazas.

Todos estos incidentes que amenazan la seguridad de la información requieren, cada día más, de sistemas de gestión acordes con el valor de la propia información y de los sistemas informáticos que los tratan. Las directrices, procedimientos y controles de seguridad que se utilizan para gestionar esta seguridad es lo que conocemos por Sistema de Gestión de Seguridad de la Información o SGSI.

De una manera más estricta, un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que comprende:

- la política.
- la estructura organizativa.
- los procedimientos.
- los procesos y
- los recursos necesarios,

para implantar la gestión de la seguridad de la información.

Con un sistema de gestión de seguridad de la información nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas encaminadas a reducir paulatinamente los riesgos a los que la organización se enfrente.

A pesar de lo que puede parecer en un principio, la definición e implantación de un SGSI no debería ser ni un coste ni un esfuerzo relevantes, máxime teniendo en cuenta los beneficios que conlleva. Un SGSI debe ajustarse tanto a los requisitos del negocio como a los recursos disponibles y debe solucionar los problemas que tiene planteados el negocio pero siempre dentro de lo razonable en cuanto a esfuerzos y costes.

Como cualquier sistema de gestión, el SGSI debe ayudar a conseguir los objetivos de la organización, no convertirse en un impedimento para ello.

Un SGSI contiene en primer lugar, las pautas que se van a seguir en la organización para garantizar la seguridad de la información y las responsabilidades de cada cual al respecto.

El SGSI recoge los objetivos que se pretenden obtener y los medios con que se va a contar para ello. Para determinar ambas cosas, se realiza un análisis de riesgos que da la medida de hasta qué punto los activos están expuestos a que les ocurran fallos de seguridad y cuál sería el impacto en caso de que lleguen a ocurrir.

Con esa información se establece el punto de partida, cual es el estado en el que está la seguridad y se decide cual se pretende conseguir, así como cual es el objetivo para un periodo de tiempo determinado. A partir de ahí, se deciden las acciones a tomar para reducir esos riesgos al nivel que se decidido que sea el objetivo. Por ejemplo, si se ha averiguado que un determinado servidor es un activo expuesto a un gran riesgo y debe estar funcionando 24 horas al día, para reducir el riesgo de que se pare, puede ser necesario instalar un SAI o incluso una línea alternativa de suministro eléctrico, realizar un mantenimiento exhaustivo mensual, instalar un equipo duplicado de manera que si falla uno el otro siga funcionando, etc.

Las acciones que se tomen deben documentarse dentro del SGSI, mediante procedimientos y planes para su ejecución.

Por tanto definiremos un Sistema de Gestión de Seguridad de la información (SGSI) como la manera en la que una organización **conoce** los **riesgos** a los que está sometida su **información** y los **gestiona** mediante una **sistemática** definida, documentada y conocida por todos, **que se revisa y mejora constantemente**.

2. LA SEGURIDAD Y SU JUSTIFICACIÓN DESDE EL PUNTO DE VISTA DEL NEGOCIO

Los motivos por los que la seguridad debe formar parte de la agenda de cualquier organización, independientemente de su sector económico o de su tamaño, son muchos y variados, algunos de los cuales se pueden leer en la prensa con mucha frecuencia: fraudes electrónicos, casos de phishing en la banca, filtraciones no deseadas de información o de datos personales, cortes en las comunicaciones, etc.

Los perjuicios que ocasionan los incidentes de seguridad son, cuando menos, incómodos y en muchos casos económicamente gravosos: paradas de producción, pérdidas de clientes, pérdida de reputación, etc.

Según el último Estudio sobre sector de la seguridad TIC en España del INTECO, más del 77% de las PYMES han tenido incidencias de seguridad: troyanos informáticos (77,3%), virus (42,7%) y recepción de correo no deseado (41,3%).

Para decirlo de una manera breve, ¿se puede permitir la organización no proteger su información?

En respuesta a esta pregunta en este módulo se van a ver los siguientes contenidos:

- Importancia de la seguridad para el negocio.
- Beneficios.

2.1. IMPORTANCIA DE LA SEGURIDAD PARA EL NEGOCIO

En un país en el que todavía hacen falta planes de concienciación y campañas de promoción para informatizar a las PYMES, y la implantación de las medidas de seguridad establecidas por la LOPD dista mucho aún de haber sido llevada a cabo en el 100%, ¿qué puede impulsar a una organización a implantar un Sistema de Gestión de Seguridad de la Información?

Las PYMES tienen que enfrentarse como siempre a las limitaciones de presupuesto, y a la falta de conocimientos y de concienciación a la hora de afrontar nuevos retos. El hecho de que la seguridad de la información tenga un importante componente tecnológico agrava estas limitaciones, ya que se percibe como un área extraña que se deja en manos de expertos, habitualmente ajenos y que no conocen el negocio y las implicaciones que tiene su trabajo en dicho negocio.

La seguridad de la información sin embargo, es un tema directamente relacionado con la supervivencia del negocio y con el aseguramiento de los ingresos. Para un banco sería dramático que le fallaran sus sistemas informáticos por unos minutos, pero tienen la capacidad de evitarlo, y en su caso, de solucionarlo. Para una PYME, un simple fallo de energía de unas horas puede ocasionar un trastorno importante, en muchos casos con repercusiones económicas, ya que se podría parar la actividad y se perderían encargos o ventas. En caso de desastre (incendio o robo, no hace falta pensar en ataques terroristas o huracanes) puede significar incluso el cierre a corto plazo del negocio.

Puesto que, a pesar de nuestro retraso tecnológico, hoy el ordenador ya ha sustituido a la máquina de escribir y el correo electrónico se impone al tradicional, los problemas asociados a estos avances también han llegado. Nuevas tecnologías (informática móvil, redes inalámbricas, memorias USB, etc.) van incorporándose progresivamente a los negocios debido a sus evidentes ventajas, pero llevan

aparejados riesgos que no se consideran. Si además la empresa tiene empleados, su negocio corre un riesgo aún mayor.

Como se mencionaba en la Introducción, al menos el 77 % de las empresas ha tenido algún incidente de seguridad relevante. Es decir, que el riesgo existe, y no es en absoluto despreciable. Además hay que tener en cuenta que, a pesar de que los ataques a sistemas informáticos reciben en muchos casos una tremenda publicidad, existe un considerable porcentaje de incidentes con origen interno, es decir, ocasionados por algún empleado y que, a pesar de no contar habitualmente con una gran difusión, son potencialmente más dañinos por el conocimiento de primera mano que tienen los que los generan. Es decir, pueden entrar en los sistemas con facilidad, saben dónde está la información más útil o que puede ser utilizada para hacer daño a la organización, o simplemente sacan información que en caso de pérdida o filtración puede ocasionar problemas.

Los incidentes, desde una simple infección por virus a una venta de información interna a la competencia o a un desastre como el incendio del Windsor, tienen un coste económico directo que hay que valorar: tiempos de parada, activos dañados o perdidos, cese del lucro entrante, sanciones administrativas o contractuales, etc. Los costes indirectos pueden ser incluso más graves: pérdidas de clientes a medio plazo, pérdida de reputación, etc.

El cumplimiento de la legislación (principalmente la LOPD) está propagando la idea de que la información debe ser protegida so pena de incurrir en faltas que se pagan con multas bastante elevadas. Ya que el principio es el mismo, detectar qué es importante (para la LOPD los datos personales, para la organización el fichero de clientes, por ejemplo), se podría aprovechar esta preocupación para extender la protección al resto de los activos de información de la empresa.

Siempre existe el, por supuesto justificado, temor de los costes de afrontar este tipo de proyectos. Hay que tener muy presente que ninguna ley ni norma va a exigir un nivel de seguridad por encima de los que las necesidades y los recursos disponibles en la organización requiera, porque lógicamente, las necesidades de seguridad (y el presupuesto, no lo vamos a negar) de la asesoría que lleva la contabilidad no son comparables a las de la Agencia Espacial Europea, por ejemplo.

Contar con un sistema de gestión permite ordenar las actividades de la organización y dirigirlas hacia el objetivo que la empresa busca. Esto a veces se ve como un impedimento para el desarrollo de las actividades de la organización, como un obstáculo que impide reaccionar con la rapidez que requieren los tiempos y las particularidades del sector económico en el que se encuentre la organización. Sin embargo, lo que se pretende con un sistema de gestión es precisamente evitar que tengamos que reaccionar ante hechos que podrían haber sido previstos y gestionados adecuadamente antes de que llegaran a ser un problema. Evitar problemas es una manera muy barata de ahorrar costes. Como tantos otros aspectos de la gestión de cualquier organización, la clave está en adoptar una solución proporcionada a las necesidades del negocio.

2.2. BENEFICIOS

Existen numerosas e importantes razones para afrontar el desarrollo y la implantación de un Sistema de Gestión de la Seguridad:

- **Reducción de costes.** Esta debería ser una de las principales motivaciones para llevar a cabo la implantación de un SGSI, ya que incide directamente sobre la rentabilidad económica de una organización. No suele serlo porque lo que se ve en un principio es el coste del mismo, sin embargo, en un breve plazo, se puede observar como el SGSI evita varias situaciones que suponen un coste, a veces importante. Al detectar los principales focos de fallos y errores, y eliminarlos o reducirlos hasta donde es posible, se evitan costosos incidentes de seguridad, que hasta entonces se asumían como cosas que pasan. A veces se evitan incidentes que hubieran ocurrido de no haber tomado las medidas a tiempo, y eso es difícil de cuantificar, pero no por ello es menos real. A veces los beneficios surgen de manera imprevista, como la reducción de primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados.

- **Optimizar los recursos y las inversiones en tecnología.** Con un SGSI las decisiones se tomarán en base a información fiable sobre el estado de los sistemas de información y a los objetivos de la organización. Habrá una motivación de negocio detrás de estas decisiones, por lo que la dirección podrá comprenderlas y apoyarlas de manera más consciente. La organización dejará de depender exclusivamente de la experiencia o pericia del responsable de informática, o más peligroso aún, del proveedor habitual de informática, a la hora de valorar las distintas opciones de compra.

- **Protección del negocio.** Con un SGSI en marcha se evitan interrupciones en el flujo de ingresos, ya que se está asegurando de una manera eficaz la disponibilidad de los activos de información y, por lo tanto, de los servicios que la organización ofrece. Esto en cuanto a la actividad cotidiana, pero también se está preparado para recuperarse ante incidentes más o menos graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el negocio a largo plazo.

- **Mejora de la competitividad.** Cualquier mejora en la gestión de la organización redunda en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza de los clientes en nuestro negocio, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

- **Cumplimiento legal y reglamentario.** Cada vez son más numerosas las leyes, reglamentos y normativas que tienen implicaciones en la seguridad de la información. Gestionando de manera coordinada la seguridad tenemos un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

- **Mantener y mejorar la imagen corporativa.** Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y

servicios. Debido a la exposición de cualquier organización a un fallo de seguridad que pueda acabar en la prensa, este punto puede ser un catalizador de esfuerzos, ya que nadie quiere que su marca quede asociada a un problema de seguridad o una multa por incumplimiento, por las repercusiones que acarrea.

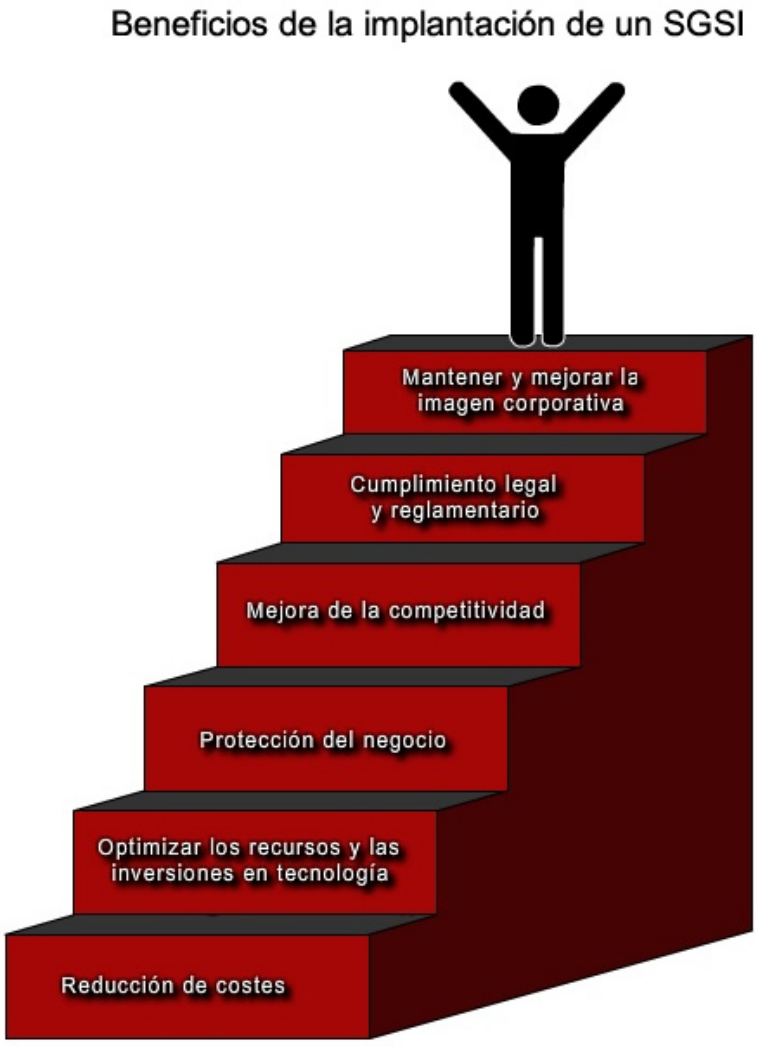

Figura 2. Beneficios de la implantación de un SGSI

Según uno de los últimos estudios llevados a cabo, los costes asociados a los incidentes de seguridad van aumentando progresivamente. En Estados Unidos, país donde se llevó a cabo el estudio, en el año 2008 se estimó el coste de un incidente por cada registro comprometido en unos $202, mientras que en año anterior era de $197.

Más cerca geográficamente hablando, está un estudio británico según el cual el porcentaje de empresas pequeñas (<50 personas) que tuvieron un incidente de seguridad el pasado año fue del 45%, con un coste medio del peor de ellos entre 11.600 y 23.200 euros. Según este mismo estudio el 72% de la empresas medianas (>250 personas), se vieron afectadas por incidentes que les costaron de 100.000 a 200.000 euros de media para el peor de ellos.

Si tenemos en cuenta que el número y la gravedad de los incidentes no hace más que crecer, es fácil hacerse una idea del problema económico que puede suponer hasta el más aparentemente fácil de resolver y por qué cada vez es más necesario evitar que ocurran, es decir, implantar un Sistema de Gestión de Seguridad de la Información.

3. MARCO LEGAL Y JURÍDICO DE LA SEGURIDAD. NORMATIVAS DE SEGURIDAD.

Desde la publicación del la Ley Orgánica de Protección de Datos de Carácter Personal en el año 1999 hasta la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos del año 2007, hay una serie de leyes que, de una manera u otra, están relacionadas con la seguridad de la información, además de numerosas regulaciones sectoriales en diversos ámbitos: financiero, telecomunicaciones, agrario, etc.

- Los contenidos de este módulo son:
- Legislación española.
- Regulaciones sectoriales.
- Delitos tecnológicos.

3.1. LEGISLACIÓN ESPAÑOLA

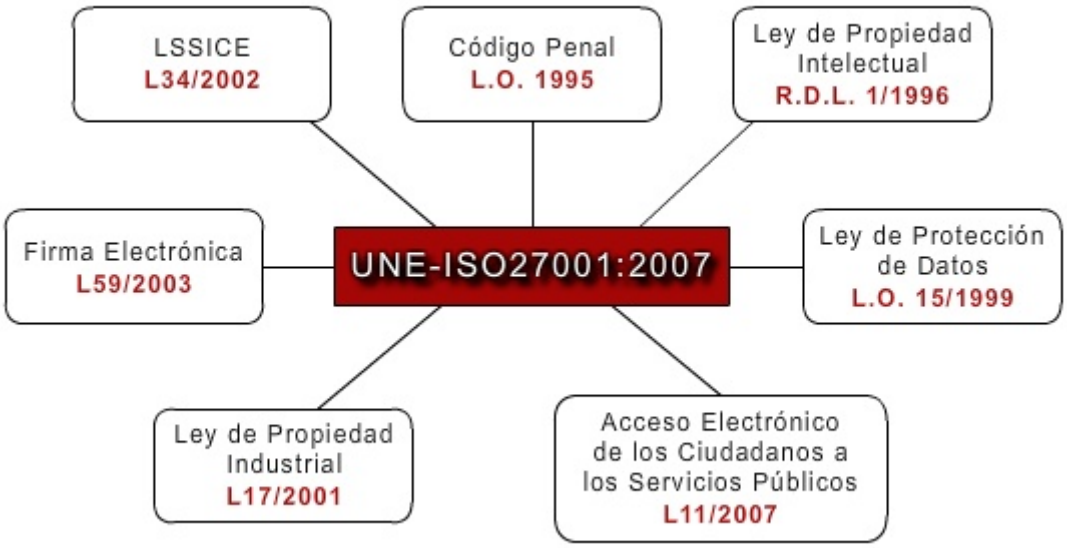

Figura 3. Esquema legislación y UNE-ISO27001:2007

3.1.1. Ley Orgánica 15/99 de Protección de Datos de Carácter Personal

Esta ley se complementa con el reglamento estipulado en el Real Decreto RD 1720/2007.

El objetivo de esta Ley es garantizar y proteger, en lo concerniente al tratamiento de los datos personales (automatizados o no), las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

Los derechos recogidos en la LOPD son:

- Las personas de las que se almacena datos de carácter personal, tienen una serie de derechos amparados por esta ley:
  - **Derecho de información:** Cuando alguien proporciona sus datos debe ser informado de que van a ser almacenados.
  - **Derecho de acceso, cancelación, rectificación y oposición:** La persona puede ver la información que se dispone de él, puede cambiar esos datos para que sean correctos y exactos, cancelar la información que se almacene de él y oponerse a que se almacene.

3.1.2. Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI)

Esta Ley se encarga de regular las obligaciones de los prestadores de servicios y los servicios que prestan. Entre las obligaciones que estipula la Ley están:

- Los prestadores de servicios deben facilitar sus datos de contacto.
- Deben colaborar con las autoridades, reteniendo los datos de conexión y tráfico durante 12 meses.
- Los que albergan datos proporcionados por un cliente, no serán responsables por la información almacenada a petición del destinatario, siempre que:
  - No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
  - Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Cuando transmitan información de terceros, los proveedores de servicio no tendrán responsabilidad al respecto si:

- No modifican la información.
- Permiten el acceso a ella sólo a los destinatarios autorizados
- Actualizan correctamente la información.
- No utilizan su posición con el fin de obtener datos sobre la utilización de la información, y
- Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto sepan que ha sido retirada del lugar de la red en que se encontraba, o que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

3.1.3. Ley 32/2003, general de telecomunicaciones

El objeto de esta ley es la regulación de las telecomunicaciones. Entre los objetivos de esta Ley están:

- Fomentar la competencia.
- Garantizar el cumplimiento de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas.
- Promover el desarrollo del sector de las telecomunicaciones.
- Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones.
- Defender los intereses de los usuarios.
- Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.
- Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.
- Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

3.1.4. Ley 59/2003 de firma electrónica

Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel, por lo que tanto su generación como su utilización deben ser cuidadosamente controladas para evitar problemas.

3.1.5. R.D.L, 1/1996 Ley de Propiedad Intelectual

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor y le da la plena disposición y el derecho exclusivo a la explotación de la obra. Las obras pueden estar expresadas en cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro como:

- Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, etc.
- Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.

- Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia.
- Las obras fotográficas.
- Los programas de ordenador.

Al amparo de esta Ley, las organizaciones protegen su conocimiento y las obliga a respetar el de las demás. El otro punto relevante en el ámbito de la seguridad de la información es la obligación de contar únicamente con software original (propietario o libre), ya que la utilización de software sin licencia sería una infracción de la Ley.

3.1.6. Ley 17/2001 de Propiedad Industrial

Es la que regula los derechos sobre:

- Las marcas.
- Los nombres comerciales.

El organismo que se encarga de mantener el registro de marcas es la Oficina de Patentes y Marcas. Para tener derechos de propiedad sobre una marca hay que registrarla en dicha Oficina.

3.1.7. Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos

Los puntos más destacables de la Ley son:

- Los ciudadanos verán reconocidos nuevos derechos en sus relaciones con las administraciones públicas.
- Se creará la figura del Defensor del Usuario.
- Los trámites y gestiones podrán hacerse desde cualquier lugar, en cualquier momento.
- La administración será más fácil, más ágil y más eficaz.
- Los ciudadanos pasan a tomar la iniciativa en sus relaciones con la administración.

Contará con un Esquema Nacional de Seguridad y otro de Interoperabilidad, para que los servicios ofrecidos cuenten con un mínimo nivel de seguridad y las distintas administraciones puedan comunicarse con fluidez.

3.2. REGULACIONES SECTORIALES

3.2.1. Agricultura

En el sector agrícola encontramos el Reglamento (CE) No 465/2005 de la Comisión de 22 de marzo de 2005 sobre la Seguridad de la Información de los Sistemas de Información de los Organismos Pagadores.

Este reglamento establece que los organismos pagadores deberán basar la seguridad de sus sistemas de información en los criterios establecidos en una versión aplicable de una de las normas siguientes, que gozan de aceptación internacional:

- Organización Internacional de Normalización 17799/Norma británica 7799: Code of practice for Information Security Management (ISO/IEC 27002).
- Bundesamt fuer Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch (IT Protection Manual).
- Information Systems Audit and Control Foundation: objetivos de control en el ámbito de la información y las tecnologías afines (COBIT).

Las medidas de seguridad deberán estar adaptadas a la estructura administrativa, al personal y al entorno tecnológico de cada organismo pagador. El esfuerzo financiero y tecnológico deberá ser proporcional a los riesgos reales.

3.2.2. Banca

3.2.2.1. Basilea II

El Comité de Basilea fue creado en 1974. Actualmente lo componen representantes de los bancos centrales de Bélgica, Canadá, Francia, Alemania, Italia, Japón, Luxemburgo, Países Bajos, España, Suecia, Suiza, Reino Unido y EEUU.

La directiva Basilea II pretende alinear el cálculo de los requerimientos de capital de los bancos con las mejores y más avanzadas prácticas de gestión de los riesgos (riesgo de mercado, riesgo de crédito y riesgo operacional) para contribuir a una mayor estabilidad del sistema financiero internacional, de manera que en función del resultado del análisis de riesgos se fijen los requerimientos de capital mínimo, adecuados a las características y circunstancias de cada entidad. Esta directiva exige transparencia en la información facilitada por la entidad, por lo que los mecanismos de generación y transmisión de la información deben ser seguros.

3.2.2.2. MIFID

La Directiva sobre Mercados de Instrumentos Financieros, conocida por sus siglas en inglés como MIFID(Markets in Financial Instruments Directive), introducirá un mercado único y un régimen regulatorio común para los servicios financieros en los 27 estados miembros de la Unión Europea.

Establece la necesidad de que las entidades adopten medidas razonables para garantizar la continuidad y la regularidad de la realización de los servicios y actividades de inversión. A tal fin, se deben emplear sistemas, recursos y procedimientos adecuados y proporcionados.

3.2.3. Seguros

Dentro del sector asegurador se encuentra el proyecto Solvencia II, que tiene como objetivo revisar el marco europeo de supervisión prudencial de las compañías de seguros.

Solvencia II debe servir para dinamizar y sistematizar de una manera más homogénea y rigurosa el cálculo, medición y la gestión de riesgos dentro de las compañías aseguradoras, y a partir de ahí facilitar la aplicación de un modelo de gestión global más eficiente.

3.3. DELITOS TECNOLÓGICOS

3.3.1. Definición y tipos de delitos tecnológicos

Con la expresión delito tecnológico se define a todo acto ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

La clasificación de dichos delitos que hace la Brigada de Investigación Tecnológica, la Unidad de la Policía Nacional destinada a responder a los retos que plantean las nuevas formas de delincuencia es:

- Ataques que se producen contra el derecho a la intimidad. Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal).

- Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor. Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal).

- Falsificación de documentos. Entendiendo documento como todo soporte material que exprese o incorpore datos, aunque se extiende también a la falsificación de moneda y a las tarjetas de débito y crédito. También pertenece a este grupo la fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.(Artículos 386 y siguientes del Código Penal).

- Sabotajes informáticos. Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 264 y otros del Código Penal).

- Fraudes informáticos. Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal).

- Amenazas. Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal).

- Calumnias e injurias. Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal).

- Pornografía infantil. Existen varios delitos en este epígrafe:

    - La inducción, promoción, favorecimiento o facilitación de la prostitución de una persona menor de edad o incapaz. (artículo 187)

    - La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (artículo 189).

    - La facilitación de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (artículo 189).

    - La posesión de dicho material para la realización de dichas conductas.(artículo 189).

Hay que tener en cuenta que además nuestro Código Penal recoge directivas europeas y establece penas importantes por comportamientos tales como las del Artículo 197, penas de prisión de seis meses a dos años para quien por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o las recogidas en el Artículo 264:

- Pena de prisión de seis meses a dos años por intromisión en datos o programas sin autorización.

- Pena de prisión de seis meses a tres años por obstaculizar o interrumpir el funcionamiento de un sistema de información ajeno.

- Se impondrán penas superiores y, en todo caso, la pena de multa proporcional al perjuicio ocasionado, cuando se comete el delito en el marco de una organización criminal o se hayan ocasionado daños de especial gravedad o afectado a los intereses generales.

3.3.2. Convenio sobre ciberdelincuencia

El "Convenio sobre Ciberdelincuencia" del Consejo de Europa, se firmó el 23 de noviembre del 2001 en Budapest. Siguiendo dicho convenio, en nuestro Código Penal se recogen los siguientes delitos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en los datos que ocasionen daños, borrado, alteración o supresión de estos.
- Abuso de dispositivos que faciliten la comisión de delitos.
- Delitos informáticos.
- Falsificación informática que produzca la alteración, borrado o supresión de datos informáticos que ocasionen datos no auténticos.
- Fraudes informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con la pornografía infantil.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

3.3.3. Decisión marco 2005/222/JAI

Esta decisión del Consejo de Europa del 24 de febrero de 2005 es relativa a los ataques contra los sistemas de información. Establece que deben sancionarse los siguientes hechos:

- Acceso ilegal a los sistemas de información.
- Intromisión ilegal en los sistemas de información que introduzcan, transmitan, dañen, borren, deterioren, alteren, supriman o hagan inaccesibles datos informáticos.
- Intromisión ilegal en los datos, para borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información.
- La inducción a los delitos o la tentativa de cometerlos y la complicidad con ellos también son sancionables como infracciones penales.

4. ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se da un repaso en este módulo a los principales estándares aceptados por la industria en el área de la seguridad de la información, las Normas ISO 27001 e ISO 27002, explicando los objetivos y los requisitos contenidos en estas dos normas.

El contenido de este módulo es:

- La organización ISO.
- Estándares en Seguridad de la Información: Las Normas ISO 27000.
- La Norma ISO 27001.
- La Norma ISO 27002.

4.1. LA ORGANIZACIÓN ISO

ISO (Organización Internacional de Estándares) es una organización especializada en el desarrollo y difusión de los estándares a nivel mundial.

Los miembros de ISO, son organismos nacionales que participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (International Electrotechnical Commission), la organización que a nivel mundial prepara y publica estándares en el campo de la electrotecnología. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1).

Los borradores de estas Normas Internacionales son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

4.2. LA FAMILIA DE LAS NORMAS ISO

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Muchos de ellos no están aún publicados, pero la estructura ya está definida:

- ISO/IEC27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.
- UNE-ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005), publicada en el año 2007. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la

información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen.

- ISO/IEC27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, publicada en el año 2005. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- ISO/IEC27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases

- ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

- ISO/IEC27005:2008 Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.

- ISO/IEC27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información. Publicada en el año 2007. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios.

- ISO/IEC27007. Guía para la realización de las auditorías de un SGSI.

- ISO/IEC27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002. Contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la Norma ISO27001 y conseguir un nivel de seguridad aceptable.

- EN ISO27799. Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC27002 (ISO27799:2008). Vigente en nuestro país ya que ha sido ratificada por AENOR en agosto de 2008. Como en la anterior, es una guía sectorial que da cabida a los requisitos específicos de entorno sanitario.

4.3. LA NORMA ISO 27001

4.3.1. Orígenes

La Norma fue publicada como Norma Española en el año 2007, pero tiene una larga historia antes de llegar a este punto.

Ya en el año 1995 el British Standard Institute (BSI) publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.

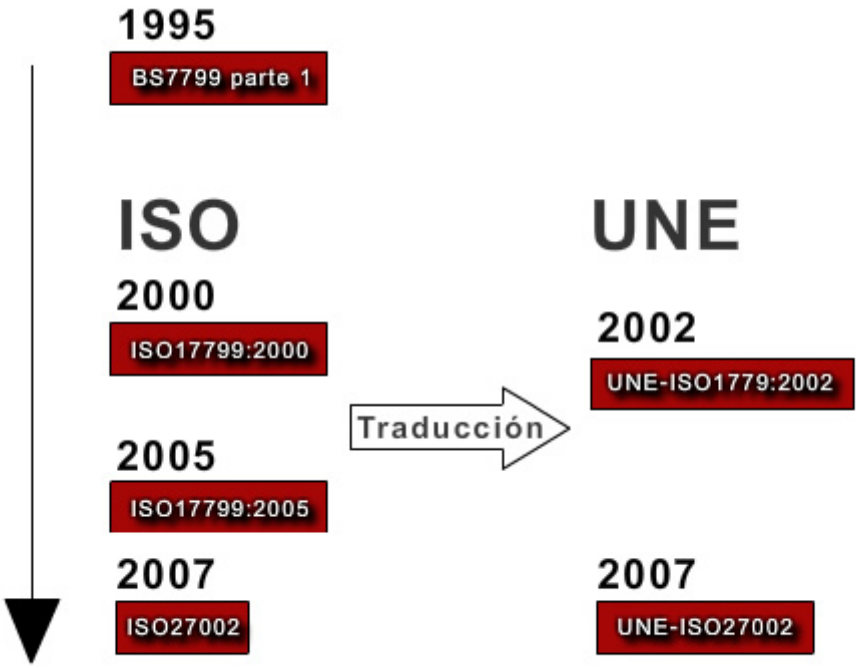

Figura 4. Evolución de la norma

A la vista de la gran aceptación de esta Norma, en 1998, el BSI publica la norma BS7799-2, Especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2001. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799.

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2, sin que haya un equivalente ISO.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27002 y en octubre de 2007 la norma ISO 27001 se adopta como UNE. Con la publicación de la UNE-ISO/IEC 27001, dejó de estar vigente la UNE 71502 y las empresas nacionales se certifican ahora únicamente con esta nueva norma (UNE-ISO/IEC 27001).

4.3.2. Contenido de la UNE-ISO/IEC 27001

La norma UNE-ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización.

Como otras Normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

Asimismo está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La Norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para

transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua.

La Norma recoge:

Los componentes del SGSI, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.

- Cómo se debe diseñar e implantar el SGSI.
- Define los controles de seguridad a considerar. Se requiere que se escojan los controles del Anexo A, que recoge todos los controles detallados en la Norma ISO/IEC 27002.
- Cómo debe realizarse la revisión y mejora del SGSI.

La ISO 27001 adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización.

4.4. LA NORMA ISO 27002

Esta norma contiene 11 capítulos de controles de seguridad que contienen un total de 133 controles de seguridad. Puede servir de guía práctica para la gestión de la seguridad de la información. No es una norma certificable.

Los objetivos de control contemplados en la Norma son:

1. Política de seguridad. Cuenta con dos controles: Documento de Política de seguridad y Revisión del Sistema.
2. Organización de la seguridad de la información, tienen 11 controles: Compromiso de la Dirección, Identificación de riesgos relacionados con terceras partes.
3. Gestión de activos, con 5 controles: Utilización aceptable de los activos, etiquetado y tratamiento de la Información
4. Seguridad ligada a los Recursos Humanos con 9 controles: Análisis y selección, Retirada de los derechos de acceso.
5. Seguridad física y del entorno tiene 13 controles: Controles físicos de entrada, emplazamiento y protección de los equipos.
6. Gestión de comunicaciones y operaciones, con 32 controles es el capítulo más extenso y más técnico: Gestión de la Capacidad, Protección frente a código malicioso, Copias de seguridad, Registro de fallos

7. Control de acceso, cuenta con 25 controles: Gestión de contraseñas de usuarios Autenticación de usuarios para conexiones externas, Aislamiento de sistemas sensibles.

8. Adquisición, desarrollo y mantenimiento de SI, tiene 16 controles: Validación de datos de entrada, Control de acceso al código fuente de los programas, control de vulnerabilidades técnicas

9. Gestión de incidentes de seguridad de la información, con sólo 5 controles: Informes de eventos de seguridad, Recogida de pruebas, es sin embargo uno de los aspectos claves en la gestión de la seguridad de la información.

10. Gestión de la continuidad del negocio, también con 5 controles: Evaluación de riesgos y continuidad del negocio Prueba, Mantenimiento y re-evaluación de los planes de continuidad. Es uno de los requisitos fundamentales para cualquier SGSI.

11. Conformidad, tienen 10 controles: Identificación de la legislación aplicable, Controles de auditoría de los sistemas de información.

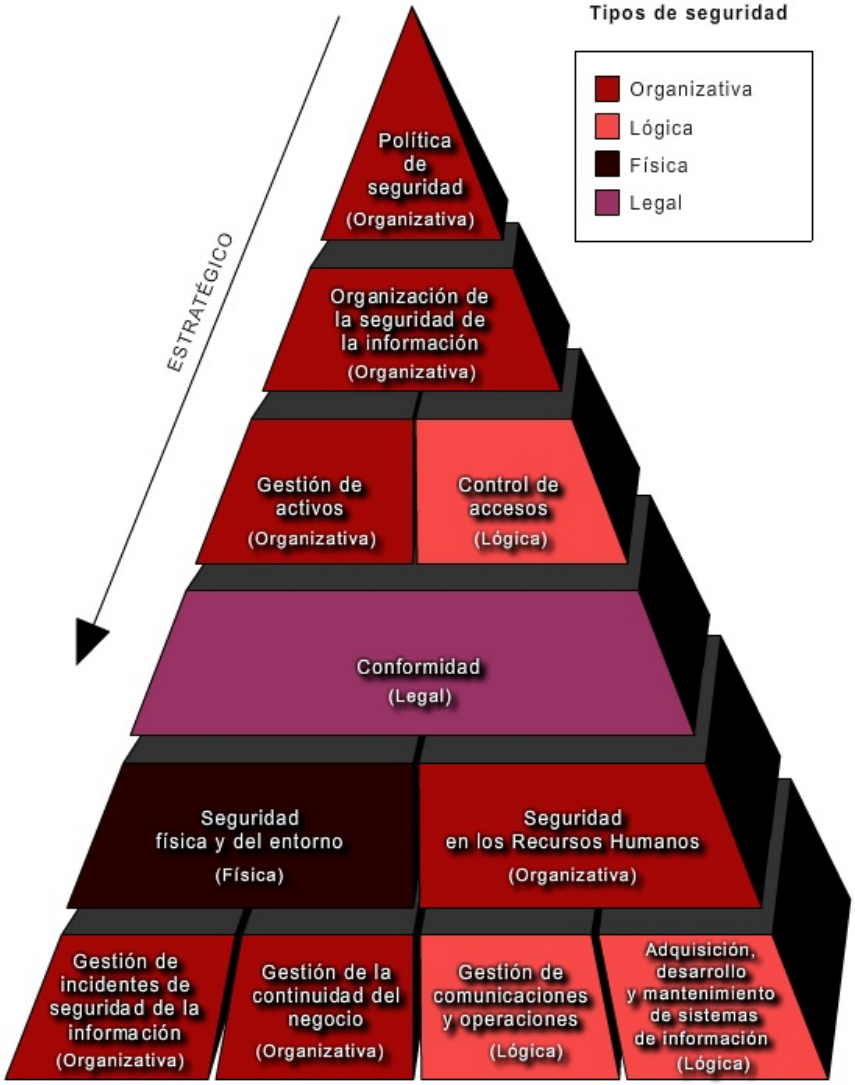

Figura 5. Objetivos de control

La Norma contiene explicaciones exhaustivas de cómo se puede implantar cada uno de los controles, pero hay que tener en cuenta que no es una norma preceptiva sino informativa, por lo que la información que da puede y debe ser adaptada a las necesidades y situación específica de la organización. Debe evitarse caer en el error de tratar de seguir al pie de la letra las indicaciones que se dan, ya que pueden ser excesivamente complejas e innecesarias para muchas organizaciones.

5. IMPLANTACIÓN DE UN SGSI

En este módulo se explica brevemente cuáles son las tareas y la documentación que deben realizarse para dar cumplimiento a los requisitos expresados por la Norma ISO 27001, de manera que se articule un SGSI adecuado para la organización, cubriendo sus necesidades y expectativas en materia de seguridad de la información.

El contenido de este módulo abarca:

- Aspectos Generales.
- Tareas a realizar.

5.1. ASPECTOS GENERALES

La primera consideración importante que tiene que hacerse a la hora de abordar la implantación de un SGSI es restringirse a un ámbito manejable y reducido. No es necesario ni aconsejable, muchas veces ni siquiera viable, el abarcar toda la organización o gran parte de ella si no se cuentan con los recursos materiales y humanos. Entendiendo que la implantación es sólo la primera parte, después el SGSI debe mantenerse y eso requiere también de una cierta dedicación.

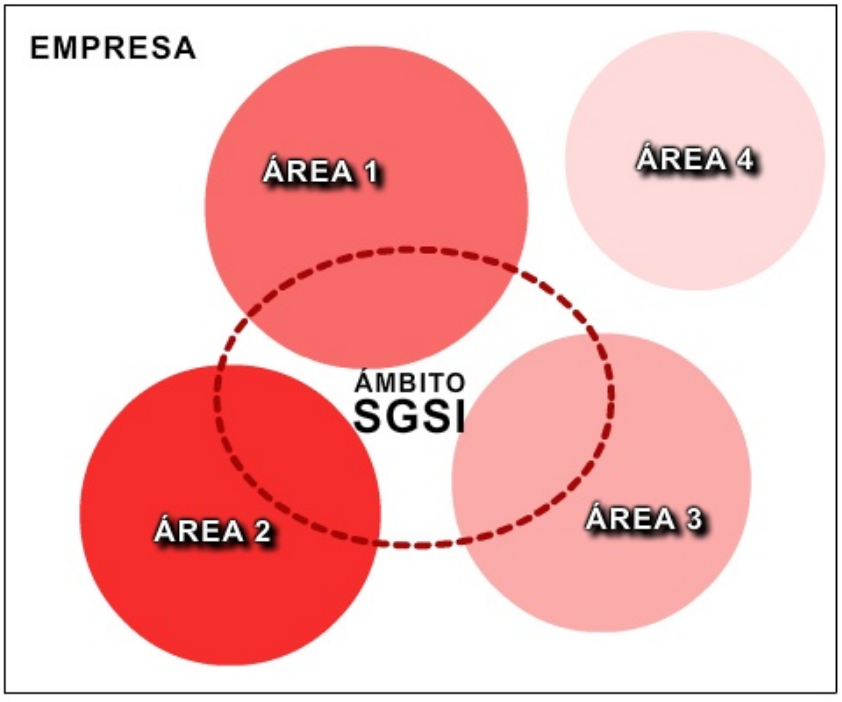

Figura 6. Ámbito SGSI

Sería deseable que todo el personal involucrado entendiera el proceso de implantación y tuviera evidencia de que se cuenta con el apoyo de la dirección para realizar el diseño e implantación del SGSI.

Plantearse la certificación como objetivo puede ayudar a darle visibilidad y credibilidad al proyecto, ya que plantea una meta concreta y clara.

La implantación de un sistema de Gestión de la Seguridad de la Información en una empresa suele oscilar entre 6 meses y 1 año. Todo depende del ámbito, el tamaño y complejidad de la organización. Se recomienda que el proceso de implantación no supere el año, ya que un alargamiento elevado puede causar que todo el trabajo realizado al principio del proyecto quede obsoleto antes de llegar a su finalización.

Para conseguir el éxito en la implantación de un SGSI según la norma ISO 27001 es muy importante intentar no complicar el proyecto, optando siempre por escoger la solución más sencilla de implantar y mantener.

5.2. TAREAS A REALIZAR

5.2.1. Fase Plan

Figura 7. Ciclo PDCA. Fase "Plan"

Planificar y diseñar el SGSI según la Norma UNE/ISO-IEC 27001 implica:

- Establecer alcance del SGSI. Es el primer paso. Hay que decidir qué parte de la organización va a ser protegida. Evidentemente puede ser la organización completa, pero es perfectamente válido y muy recomendable comenzar por un área de la organización que sea relevante o importante, por ejemplo, en el caso de un banco, comenzar por el servicio de banca electrónica.

- Establecer las responsabilidades. Se asignará un responsable de seguridad, que coordine las tareas y esfuerzos en materia de seguridad. Será el que actúe como foco de todos los aspectos de seguridad de la organización y cuyas responsabilidades cubran todas las funciones de seguridad. En muchas organizaciones será necesario designar un comité de seguridad que trate y busque soluciones a los temas de seguridad, resuelva los asuntos interdisciplinarios y que apruebe directrices y normas.

- Definir política de seguridad. Este paso es fundamental. La política de la organización es la que va a sentar las bases de lo que se va a hacer, mostrará el compromiso de la dirección con el SGSI y servirá para coordinar responsabilidades y tareas.

- Realizar análisis de riesgos. El análisis de riesgos es la piedra angular de un SGSI. Es la actividad cuyo resultado nos va a dar información de dónde residen los problemas actuales o potenciales que tenemos que solucionar para alcanzar el nivel de seguridad deseado. El análisis de riesgos debe ser proporcionado a la naturaleza y valoración de los activos y de los riesgos a los que los activos están expuestos. La valoración del riesgo debe identificar las amenazas que pueden comprometer los activos, su vulnerabilidad e impacto en la organización, determinando el nivel del riesgo.

- Seleccionar los controles. Una vez que se sabe dónde están los puntos débiles en la gestión de la seguridad, se escogen los controles necesarios para eliminarlos o al menos, reducir la probabilidad de que ocurran algún incidente o el impacto que tendría en caso de que algo ocurriera. En principio los controles se escogerán de los detallados en el Anexo A de la Norma.

- Establecer el plan de seguridad. Debido a que serán numerosas las actuaciones que se pretenderá realizar, debe establecerse un plan con los plazos, los recursos y las prioridades a la hora de ejecutarlas.

5.2.2. Fase Do (Hacer)

Figura 8. Ciclo PDCA. Fase "Do" (Hacer)

En esta fase debe llevarse a efecto el plan de seguridad planteado en la fase anterior. Algunas medidas de corte técnico requerirán poca documentación, pero otras más de índole organizativa, como son el caso de la gestión de la documentación o de los recursos humanos, necesitan ser documentadas.

Los principales documentos a generar son:

- Política de seguridad. Con las líneas generales que la organización desea seguir en seguridad.
- Inventario de activos. Con la descripción de los activos de información de la organización y su valoración para la misma.
- Análisis de riesgos. Con los valores de riesgo de cada uno de los activos.
- Documento de aplicabilidad. En el que se recoge para cada control del Anexo A de la Norma UNE/ISO-IEC 27001 si se aplica o no y la justificación para esa decisión.
- Procedimientos. Con la descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI.
- Registros. Son las evidencias de que se han realizado las tareas definidas para el SGSI. Son muy importantes de cara a poder medir la eficacia de las medidas implantadas así como a

justificar las labores realizas frente a las auditorías del sistema (tanto internas como externas).

Una tarea importante dentro de esta fase es la formación. Desde luego la formación e información continua al personal dentro del proyecto debe comenzar con el mismo, pero en esta fase hay que involucrar a todos aquellos que se vean afectados por el SGSI tanto de forma directa como indirecta, es decir, todos, ya que todo el mundo tiene alguna responsabilidad si maneja información en cualquier forma o soporte.

Mantener informado a todo el mundo de lo que se está haciendo, del por qué y cuáles son los objetivos que se pretende conseguir es primordial para lograr la colaboración de todos y reducir en la medida de lo posible la resistencia al cambio.

5.2.3. Fase Check (Comprobar)

Figura 9. Ciclo PDCA. Fase "Check" (Comprobar)

Una vez puesto en marcha el plan de seguridad, se debe revisar periódicamente de manera que se detecten posibles desviaciones. Pueden haberse producido retrasos en las acciones a tomar o bien haber surgido problemas que no fueron previstos y que hay que solucionar para continuar con el plan.

Otra de las comprobaciones que se realizan dentro del SGSI es la auditoría interna. Tiene por objeto la medida y evaluación de la eficacia de otros controles, mediante la auditoría se determinar si los objetivos de los controles, los controles, los procesos y los procedimientos:

- Están conformes con los requisitos de la Norma UNE/ISO-IEC 27001.
- Están conformes con la legislación y regulaciones aplicables.

- Están conformes con los requisitos de seguridad identificados.
- Están implementados y mantenidos de manera efectiva.
- Dan el resultado esperado.

Si se detectan no conformidades, deben tomarse las acciones oportunas para corregirlas.

Una no conformidad es el incumplimiento de un requisito, que en el caso que nos ocupa puede ser un requisito de la Norma, una norma interna de la organización, un requisito contractual o legal, etc.

La otra actividad de seguimiento o comprobación contemplada dentro de la Norma es la Revisión del SGSI por parte de la dirección. El objetivo es que la dirección se asegure de que el SGSI continúa siendo adecuado, apropiado y efectivo. Esta revisión es una herramienta muy potente para la identificación de oportunidades de mejora.

Existen muchas formas en que la alta dirección puede revisar el SGSI como, por ejemplo, recibir y revisar un informe generado por el representante de la dirección u otro personal, la comunicación electrónica como parte de reuniones regulares de la dirección en donde también se discutan aspectos tales como objetivos.

5.2.4. Fase Act (Actuar)

Figura 10. Ciclo PDCA. Fase "Act" (Actuar)

Cuando mediante cualquiera de las actividades de comprobación realizadas o incluso durante la operativa habitual del SGSI se descubren no conformidades, reales o potenciales, deben tomarse medidas para solucionarlas. Hay tres maneras para ello:

- Adoptar acciones correctoras. Estas acciones son las que se toman para corregir una no-conformidad significativa con los requisitos del Sistema de Gestión de Seguridad de la Información. Las decisiones de qué hacer y cómo deben estar basadas en una identificación precisa de la causa del problema para evitar malgastar recursos simplemente arreglando provisionalmente un incidente que volverá a repetirse si no se ataca la causa que lo originó.

- Adoptar acciones preventivas. Son aquellas que se toman para prevenir que ocurra algo no deseado. La gran ventaja de estas acciones es que evidentemente es más eficaz y sencillo prevenir los problemas que solucionarlos. De todos modos es fundamental también en este caso determinar cuál es la posible fuente de problemas con el objeto de eliminarla.

- Definir acciones de mejora. Las acciones de mejora no surgen de la necesidad de solucionar un problema sino de la dinámica del sistema de gestión, que impulsa a refinar procesos y superar objetivos continuamente. Son acciones encaminadas a hacer mejor las cosas de una manera más eficaz y eficiente, consiguiendo los resultados esperados con menos esfuerzo.

6. DEFINICIÓN DE LAS POLÍTICAS, ORGANIZACIÓN, ALCANCE DEL SISTEMA DE GESTION Y CONCIENCIACIÓN

En este módulo se desglosan de manera detallada los primeros pasos que deben llevarse a cabo para desarrollar un SGSI de acuerdo con la Norma UNE/ISO-IEC 27001: cómo se debe definir una Política de Seguridad coherente, cuales son las principales responsabilidades que deben asignarse internamente, cómo debe definirse el alcance del Sistema y de qué manera debe llevarse a cabo una labor de concienciación que permita posteriormente implantar un SGSI eficaz.

El contenido de este módulo es:

- Alcance del SGSI.
- Política de Seguridad.
- Organización de la seguridad.
- Concienciación.

6.1. ALCANCE DEL SGSI

Para comenzar a diseñar el SGSI en primer lugar hay que decidir qué se quiere proteger, es decir, el alcance que se le va a dar al sistema.

Según lo especificado por la Norma UNE/ISO-IEC 27001, los límites del SGSI deben estar definidos en términos de las características de la organización, localización, activos y tecnologías. Esto significa que hay que considerar qué parte de la organización va a quedar protegida por el SGSI, si es que no se pretende abarcarla toda.

Que el SGSI comprenda toda la organización o no depende sobre todo del tamaño de la misma. En una gran empresa es raro que se intente hacer un SGSI de estas características porque el esfuerzo y los recursos que habría que dedicarle al proyecto serían muy elevados debido a la gran cantidad de personal involucrado y a la complejidad de las actividades que se realizan. Lo más habitual en este tipo de organizaciones es escoger un departamento o servicio relevante dentro de la misma y diseñar e implantar un SGSI con ese alcance reducido. Una vez completado el proyecto satisfactoriamente, se va extendiendo paulatinamente el sistema al resto de la organización, normalmente a lo largo de varias fases y en un periodo de tiempo importante.

En una organización pequeña sin embargo es más factible preparar un SGSI que abarque toda la organización, ya que su menor tamaño y el limitado número de actividades que se realizan lo permiten. A pesar de ello hay que valorar cuidadosamente los recursos que van a ser necesarios para poner en marcha y mantener el SGSI y considerar si esta opción es posible o es más realista escoger un alcance más reducido para empezar.

No se debe olvidar que la implantación de este tipo de sistemas debe ayudar a los procesos propios de la empresa y no debe interferir en su desarrollo para que se lleven a cabo de la mejor manera posible, aunque inevitablemente la organización verá modificados algunos de sus hábitos sobre todo a nivel de gestión y del personal involucrado.

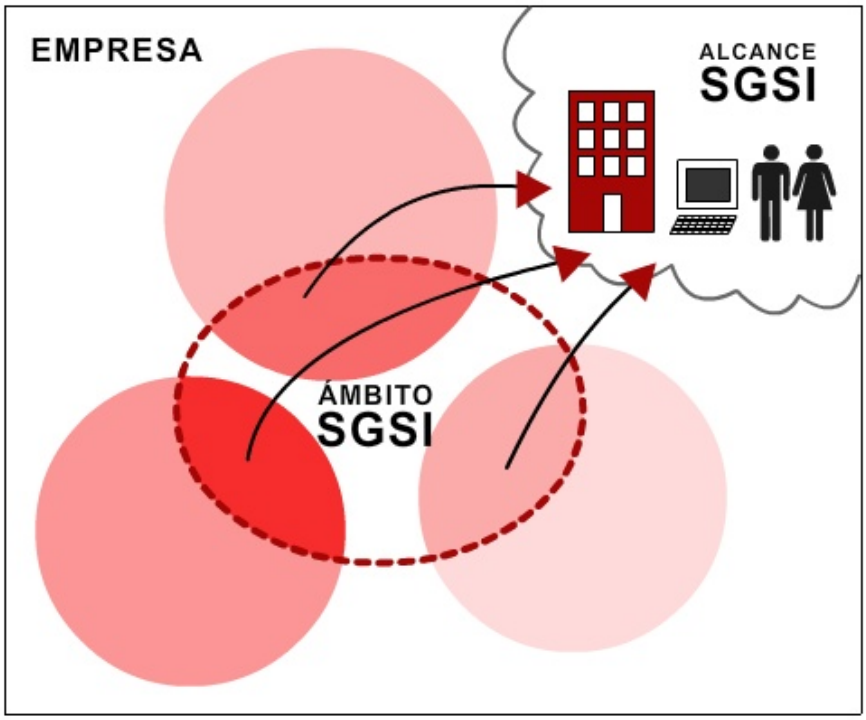

Figura 11. Alcance del SGSI

Una vez decidido si el alcance va a ser toda la organización o sólo una parte de ella, hay que definir claramente este alcance. Para ello deben enumerarse:

- Las localizaciones físicas incluidas: oficinas, sedes, fábricas, delegaciones, etc. De manera que queden claros los límites físicos del SGSI.

- Las actividades de la organización: servicios y productos que suministra, actividades internas, etc. Es aquí donde es importante detallar exactamente qué queda dentro del alcance y qué queda excluido, por ejemplo, si la organización proporciona servicios de asesoría legal y fiscal, y se ha decidido que sólo se van a considerar dentro del alcance los de asesoría fiscal. Hay que tener en cuenta que no sería lógico excluir por ejemplo el departamento de informática, ya que no se puede obviar que este departamento es el que manipula y gestiona probablemente toda la información. Aunque este servicio estuviera subcontratado, hay que tener los mecanismos para poder gestionarlo con seguridad y el SGSI debe incluir los controles necesarios para ello.

- Las tecnologías utilizadas: tipos de equipos informáticos, redes, comunicaciones, etc. En general esta parte queda documentada con un mapa esquemático de la red de la organización. No es necesario que muestre mucho detalle, pero sí que para cualquiera que tenga acceso a la documentación pueda hacerse una idea cabal de qué elementos constituyen la red informática de la organización y como están dispuestos.

La definición del Alcance es, por tanto, uno de los puntos críticos en la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que su correcta definición hará que las tareas de implantación y los responsables estén correctamente determinados y que, de esta manera, dichas tareas así como el mantenimiento del sistema estén acordes con los recursos disponibles y las necesidades de la organización.

6.2. POLITICA DE SEGURIDAD

El objetivo de la Política de Seguridad es dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo a los requisitos del negocio y la legislación aplicable. Es el punto de partida del diseño del SGSI, a partir del cual se desarrollan las actuaciones necesarias para implantar el SGSI. Es un requisito de la Norma UNE/ISO-IEC 27001 contar con este documento, y los controles asociados están en el primer objetivo de control, Política de Seguridad de la Información.

La Política de Seguridad la define la Dirección, estableciendo en ella de forma clara las líneas de actuación en esta área, que deben estar alineadas con los objetivos de negocio. La Política es también una manifestación expresa del apoyo y compromiso de la Dirección con la seguridad de la información. El Documento que recoja la Política de Seguridad debe ser aprobado por la Dirección, publicado y comunicado a todos los empleados y terceras partes, tiene que ser del dominio público las intenciones y objetivos de la organización. Esto es fundamental para que el personal perciba la importancia del asunto y sea consciente de que no es una comunicación más dentro de la organización, sino que debe ser tenida en cuenta y puesta en práctica.

La Política debe ser un documento legible y comprensible para toda la audiencia a la que va dirigido, lo cual es más fácil de conseguir si es corto y preciso, enfocado a describir qué se quiere proteger en la organización y por qué.

Figura 12. Jerarquía

Además de la declaración de principios, debe recogerse, en el mismo documento o en otro, una breve explicación de las políticas, principios, normas y requisitos de cumplimiento más importantes para la organización, como por ejemplo:

- Definición de las responsabilidades en materia de gestión de la seguridad de la información de cada puesto y descripción de las posibles consecuencias en caso de no observar estas responsabilidades.
- Cómo se deben comunicar las incidencias de seguridad de la información para que puedan ser gestionadas adecuadamente.
- Cómo se va llevar a cabo el cumplimiento de los requisitos legales, reglamentarios y contractuales.
- Cuáles son las responsabilidades y tareas de cada uno en cuanto a la continuidad del negocio.
- Las referencias a documentación que pueda sustentar la política; por ejemplo, normas, instrucciones y procedimientos detallados para poder ejecutar tareas específicas o las reglas de seguridad que los usuarios deben cumplir.

Esta política de seguridad de la información debe ser comunicada a todos los miembros de la empresa, y estar disponible para todos aquellos a los que va dirigida. El objetivo es asegurarse que la plantilla conoce y comprende los problemas asociados a la seguridad de la información y que asumen y son conscientes de sus responsabilidades en este tema. Debe transmitirse el mensaje claro de que la seguridad es un asunto de todos y no solo de la dirección o del responsable de seguridad.

La política de seguridad de la información se debería revisar a intervalos planificados, aunque lo recomendable es que sea al menos anualmente, o en el caso de que se produzcan cambios importantes, para que se ajuste en todo momento a las necesidades y contexto de la organización. Por ejemplo:

1. Después de incidentes de seguridad (sobre todo de aquellos que sean considerados como graves).

2. Después de una auditoría / revisión del sistema que no haya tenido éxito (evidentemente esto es porque falla el SGSI y no está acorde con la normativa).

3. Frente a cambios que afecten a la estructura de la organización: nuevos servicios o eliminación de alguno de ellos, cambios en el contexto económico, cambios en el sector, etc.

6.3. ORGANIZACIÓN DE LA SEGURIDAD

El segundo dominio de actuación de la norma ISO 27001 se corresponde con los aspectos organizativos de la seguridad de la información y trata tanto la organización interna como la relación de la empresa con terceras partes (clientes, subcontratas, etc.)

Es por ello que el diseño e implantación de un SGSI y su posterior mantenimiento implica describir nuevas funciones dentro de la organización para hacerse cargo de las nuevas actividades. En algunos casos se añadirán responsabilidades a puestos ya definidos y en otros se tratará de perfiles completamente nuevos aunque en organizaciones de pequeño tamaño probablemente serán asumidos por personas de la plantilla y no necesariamente por personal nuevo.

Hay dos funciones principales:

- Un responsable de seguridad, que será el que coordine las tareas y esfuerzos en materia de seguridad. Esta persona centralizará todos los aspectos de seguridad de la organización y sus responsabilidades cubrirán todas las funciones de seguridad.

- Integrantes del comité de seguridad. Los participantes de este comité son los que tratan los problemas de seguridad y las no conformidades, discuten y deciden las soluciones a los mismos, Identifican cambios significativos y como deben ser gestionados, valoran si los controles implantados son suficientes y coordinan la implantación de los nuevos, resuelven los asuntos interdisciplinarios, revisan y aprueban directrices y normas, proponen objetivos a la dirección y revisan con ella la marcha de los mismos. Si la organización es muy pequeña puede no existir este comité y es el propio responsable de seguridad el que asume estas funciones. Pero en la medida de lo posible deberían colaborar todas las áreas de la organización de manera que todas las decisiones fueran lo más informadas y consensuadas posible.

Sin embargo la gestión y operación de un SGSI requiere la colaboración de todo el personal, por lo que deben definirse y asignarse todas las responsabilidades relativas a la seguridad de la información. Esto evitará lagunas de seguridad, ya que todos los aspectos quedarán bajo la responsabilidad de alguien. Como parte de este proceso puede hacerse uso de los acuerdos de confidencialidad. En algunas organizaciones se exige a la plantilla que firmen acuerdos sobre el mantenimiento de la confidencialidad de la información a la que tienen acceso, incluyendo incluso en este tipo de documentos la Política de Seguridad. De esta manera queda asegurado que todo el personal conoce las normas y ha aceptado seguirlas.

Sin ser exhaustivos, las principales responsabilidades de los roles más habituales que se encuentran en cualquier organización son:

Figura 13. Organización de la seguridad de un SGSI

- **Dirección.**

La Dirección tiene varias de las responsabilidades clave en la puesta en marcha y funcionamiento del SGSI. Es la Dirección la que debe:

- Aprobar la Política y los objetivos de seguridad.
- Aprobar los riesgos residuales, aquellos que quedan tras la aplicación de controles de seguridad y que en ese momento no se pueden reducir más, por lo que la organización debe asumirlos.
- Aprobar los planes de formación y auditorías.
- Realizar la revisión del SGSI.

- Demostrar su compromiso con la seguridad de la información para promover una cultura efectiva dentro de la organización.

- **Responsable de Sistemas.**

Tiene entre sus obligaciones:

- Llevar a cabo las actividades de gestión del SGSI actuando en coordinación con el responsable de seguridad.

- Administrar y gestionar las cuentas de los usuarios y los privilegios de acceso de cada uno de ellos.

- Asegurarse de que sólo las personas autorizadas a tener acceso a la información y los sistemas cuentan con él.

- Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la organización.

- Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.

- **Propietario de activos.**

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Definir si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.

- Definir quienes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.

- Informar al Responsable de Seguridad de la Información cuando detecte cualquier incidencia para tratarla y corregirla.

- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.

- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

Personal. En general, cualquier integrante de la plantilla deberá:

- Conocer y comprender la Política de Seguridad y los procedimientos que apliquen a su trabajo.

- Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad.

- Comunicar las incidencias de seguridad que detecte mediante el canal establecido para ello.

Terceras partes. Cualquier entidad externa a la organización que de alguna manera tenga acceso a los activos de información de la misma (clientes, usuarios, contratistas, etc.) debería:

- Conocer la Política de Seguridad y entender su impacto en las relaciones con la organización.

- Cumplir lo estipulado en los contratos respecto a la seguridad de la información de los activos con los que trabajan.

- Comunicar las incidencias de seguridad que detecten.

6.4. CONCIENCIACIÓN

Esta es una parte crucial de un proyecto de implantación de un SGSI. Aunque todo el proceso de diseño y desarrollo del sistema se haya hecho cuidadosamente, escogiendo las mejores soluciones y las implementaciones más prácticas y adecuadas, todo puede fallar de manera estrepitosa si no se consigue que el personal se involucre para que el sistema funcione. Es imprescindible para obtener el nivel de seguridad que se persigue que todo el personal sea consciente de la trascendencia y de la importancia de las actividades de seguridad de la información y como sus propias tareas contribuyen a conseguir los objetivos del SGSI.

Desde el arranque del proyecto hay que llevar a cabo acciones de divulgación, para que todo el personal, aunque no participe directamente, sepa qué se está haciendo y por qué. Dar difusión a las tareas de diseño y desarrollo del SGSI permite a la plantilla ir haciéndose a la idea de los cambios que se avecinan de una manera transparente. No hacerlo puede dar lugar a suspicacias, ya que el SGSI puede ser percibido como un mecanismo de control por parte de la dirección. Por supuesto que lo es, pero no está dirigido al personal sino a la seguridad de la información que hay que observar para poder funcionar eficazmente en un entorno digital como este en el que nos movemos.

Esta parte de concienciación, debe ser complementada con formación. Por muy mentalizada que se haya conseguido que esté la plantilla, no servirá de mucho si no se les han dado los medios para

poder ejecutar sus tareas de manera segura. Es necesario que el personal al que se le han asignado responsabilidades definidas en el SGSI sea competente para llevar a cabo sus tareas. Habrá algunos puntos en los que ya se cuente con las competencias necesarias, pero cuando no sea así, hay que formar al personal.

Realizar un plan de formación razonable pasa por determinar cuáles son las necesidades de formación. Debe realizarse un análisis de las competencias necesarias y de las existentes para detectar las carencias. Con esa información se pueden planificar las acciones formativas necesarias para cubrirlas. Hay que decidir también quién va a recibir la formación y escoger el mejor momento para que puedan recibirla, aunque una formación básica en los aspectos fundamentales de la seguridad de la información y en el SGSI de la organización deben recibirla todos los empleados.

Volviendo al tema de los recursos, también aquí hay que ser cuidadosos y contar con los recursos disponibles en ese momento para elaborar un plan que sea viable. Las acciones formativas no tienen por qué reducirse a cursos externos, presenciales y habitualmente costosos. Hay que valorar las numerosas alternativas que hoy en día están disponibles, comenzando por la formación en línea, que no requiere desplazamientos ni estancias fuera del lugar de residencia, y cuyo coste es reducido en muchos casos. También se puede buscar internamente a alguien que cuente con el conocimiento que se busca y que pueda formar al resto de las personas que lo necesitan. La asistencia a conferencias o jornadas de difusión son otros tipos de acciones que puede perfectamente formar parte del plan de formación.

Tras la planificación, hay que asegurarse de que el plan va cumpliéndose y las acciones van realizándose. Se debe llevar algún tipo de registro para que quede evidencias de esta ejecución. Tras un periodo de tiempo razonable, se debe realizar una evaluación acerca de la eficacia de las acciones tomadas. Se trata de verificar si han servido para el propósito con el que se planificaron.

Dependiendo de las circunstancias, puede darse el caso de que sea más práctico contratar a una persona que cuente con las competencias que necesita la organización en ese momento. Si es así, la información sobre el perfil de la personal a contratar y el detalle de las cualificaciones o habilidades que se requieren debe comunicarse a quien se encargue de esta tarea.

Con todas estas actuaciones se creará en la empresa una cultura de seguridad que conllevará el asumir las labores relativas a la seguridad de la información como parte del día a día y como un todo en la organización.

7. LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Se explica en este tema cómo deben abordarse la elaboración de un inventario de activos que recoja los principales activos de información de la organización, y cómo deben valorarse esos activos en función de su relevancia para la misma y del impacto que ocasionaría un fallo de seguridad en ellos.

El contenido de este módulo es:

- Identificación de los activos de información.
- Inventario de activos.
- Valoración de los activos.

7.1. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Figura 14. Activos de la información

Para facilitar el manejo y mantenimiento del inventario los activos se pueden distinguir diferentes categorías de los mismos:

- **Datos:** Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.
- **Aplicaciones:** El software que se utiliza para la gestión de la información.
- **Personal:** En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.
- **Servicios:** Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).
- **Tecnología:** Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)
- **Instalaciones:** lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)
- **Equipamiento auxiliar:** En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hayan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.)

Cada uno de los activos que se identifiquen debe contar con un responsable, que será su propietario. Esta persona se hará cargo de mantener la seguridad del activo, aunque no necesariamente será la que gestione el día a día del mismo.

Por ejemplo, puede existir una activo que sea la base de clientes, cuyo propietario sea el Director Comercial, sin embargo serán los comerciales de la organización los usuarios del mismo y el responsable de sistemas el encargado del mantenimiento de la base de datos.

Pero el propietario decide quién accede y quién no a la información, si es necesario aplicarle alguna medida de seguridad o existe algún riesgo que deba ser tenido en cuenta, si le aplica la LOPD y por tanto deben implantarse las medidas de seguridad exigidas por la Ley, etc.

7.2. INVENTARIO DE LOS ACTIVOS

El inventario de activos que se va a utilizar para la gestión de la seguridad no debería duplicar otros inventarios, pero sí que debe recoger los activos más importantes e identificarlos de manera clara y sin ambigüedades.

Figura 15. Inventario de activos

El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre. Esta información como mínimo es:

- **Identificación del activo:** un código para ordenar y localizar los activos.
- **Tipo de activo:** a qué categoría de las anteriormente mencionadas pertenece el activo.
- **Descripción:** una breve descripción del activo para identificarlo sin ambigüedades.
- **Propietario:** quien es la persona a cargo del activo.
- **Localización:** dónde está físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.

El inventario de activos no es recomendable que sea demasiado exhaustivo. Desglosar los activos hasta el nivel de registro o de elemento de un equipo informático no es probable que vaya a proporcionar información relevante en cuanto a las amenazas y los riesgos a los que debe hacer frente la organización y además complicará enormemente la realización del análisis de riesgos, ya que cuantos más activos haya más laborioso será el mismo.

El inventario deberá recoger los activos que realmente tengan un peso específico y sean significativos para la organización, agrupando aquellos que, por ser similares, tenga sentido hacerlo. Por ejemplo, si hay treinta PCs de parecidas características técnicas y en la misma ubicación física, pueden agruparse en un único activo, denominado por ejemplo “equipo informático”.

En el caso de que hubiera veinte PCs y diez portátiles, si los portátiles no salieran nunca y los treinta equipos permanecieran siempre en la misma ubicación, también se podría asumir que constituyen un único activo pero si los portátiles se utilizan fuera de las instalaciones de la organización, ya no se podrían agrupar los treinta equipos, ya que las circunstancias en las que se utilizarían los equipos son

distintas, por lo que habría que distinguir dos activos, por ejemplo “Equipo informático fijo” para los PCs y “Equipo informático móvil” para los portátiles.

En algunos casos, la complejidad de la organización, de sus procesos o de su contexto, puede hacer necesario el desarrollar un árbol de dependencias entre activos. El concepto es que algunos activos dependen de otros, en uno o más parámetros de seguridad.

Identificar y documentar estas dependencias constituye un árbol de dependencias, que dará una idea más exacta del valor de cada activo. Por ejemplo, una aplicación alojada en un servidor, depende este servidor para ejecutarse, para estar disponible. Si el servidor tiene una avería o un error de configuración, la aplicación podría ver afectada su disponibilidad. Por lo tanto el valor del servidor puede considerarse que sea no sólo el que tiene en si mismo, sino también el que tiene por permitir el correcto funcionamiento de la aplicación.

7.3. VALORACIÓN DE LOS ACTIVOS

Una vez identificados los activos, el siguiente paso a realizar es valorarlos. Es decir, hay que estimar qué valor tienen para la organización, cual es su importancia para la misma.

Para calcular este valor, se considera cual puede ser el daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

Esta valoración se hará de acuerdo con una escala que puede ser cuantitativa o cualitativa. Si es posible valorar económicamente los activos, se utiliza la escala cuantitativa. En la mayoría de los casos, no es posible o va a suponer un esfuerzo excesivo, por lo que utilizan escalas cualitativas como por ejemplo: bajo, medio, alto o bien un rango numérico, por ejemplo de 0 a 10

Con independencia de la escala utilizada, los aspectos a considerar pueden ser los daños como resultado de:

- Violación de legislación aplicable.
- Reducción del rendimiento de la actividad.
- Efecto negativo en la reputación.
- Pérdidas económicas.
- Trastornos en el negocio.

La valoración debe ser lo más objetiva posible, por lo que en el proceso deben estar involucradas todas las áreas de la organización, aunque no participen en otras partes del proyecto y de esta manera obtener una imagen realista de los activos de la organización.

Es útil definir con anterioridad unos parámetros para que todos los participantes valoren de acuerdo a unos criterios comunes, y se obtengan valores coherentes. Un ejemplo de la definición de estos parámetros podría ser la siguiente:

- **Disponibilidad.** Para valorar este criterio debe responderse a la pregunta de cuál sería la importancia o el trastorno que tendría el que el activo no estuviera disponible. Si consideramos como ejemplo una escala de 0 a 3 se podría valorar como sigue:

Tabla 1. DISPONIBILIDAD

Valor	Criterio
0	No aplica / No es relevante
1	Debe estar disponible al menos el 10% del tiempo
2	Debe estar disponible al menos el 50% del tiempo
3	Debe estar disponible al menos el 99% del tiempo

Por ejemplo, la disponibilidad de un servidor central sería de 3, siguiendo estos criterios.

- **Integridad.** Para valorar este criterio la pregunta a responder será qué importancia tendría que el activo fuera alterado sin autorización ni control. Una posible escala es:

Tabla 2. INTEGRIDAD

Valor	Criterio
0	No aplica / No es relevante
1	No es relevante los errores que tenga o la información que falte
2	Tiene que estar correcto y completo al menos en un 50%
3	Tiene que estar correcto y completo al menos en un 95%

Siguiendo con el ejemplo del servidor central, debe mantenerse en todo momento funcionando correctamente, se le asigna el valor 3.

- **Confidencialidad.** En este caso la pregunta a responder para ponderar adecuadamente este criterio será cuál es la importancia que tendría que al activo se accediera de manera no autorizada. La escala en este caso podría ser:

Tabla 3. CONFIDENCIALIDAD

Valor	Criterio
0	No aplica / No es relevante
1	Daños muy bajos, el incidente no trascendería del área afectada
2	Los daños serían relevantes, el incidente implicaría a otras áreas
3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas

Dependiendo de la organización y su contexto, el valor del servidor podría ser incluso 3 si la dependencia de esa máquina es muy grande y el simple acceso físico al servidor sería un trastorno para la organización.

También debe decidirse cómo se va a calcular el valor total de los activos, bien como una suma de los valores que se han asignado a cada uno de los parámetros valorados, bien el mayor de dichos valores, la media de los mismos, etc.

Los criterios para medir el valor del activo deben ser claros, fáciles de comprender por todos los participantes en la valoración y homogéneos, para que se puedan comparar los valores al final del proceso. De esta manera se sabrá cuales son los principales activos de la organización, y por lo tanto aquellos que necesitan de una particular atención.

La valoración de los activos deben realizarla un grupo de personas que sean lo suficientemente representativas como para aportar entre todos una visión razonablemente objetiva de la organización. Por supuesto deben ser personas que conozcan bien la organización. Si se van a hacer las valoraciones mediante reuniones de trabajo, el grupo no debería ser excesivamente numeroso para que las reuniones no se alarguen demasiado. Si se van a utilizar cuestionarios o entrevistas, se puede involucrar a más personas, siempre teniendo en cuenta el coste asociado a ello.

8. ANÁLISIS Y VALORACIÓN DE LOS RIESGOS. METODOLOGÍAS

Uno de los puntos clave de todo SGSI es el análisis de riesgos. En este módulo además de explicar detalladamente en qué consiste y cómo debe llevarse a cabo para cumplir con lo establecido por la Norma se describirán las principales metodologías que existen en el mercado.

Los contenidos de este módulo comprenden:

- Conceptos básicos.
- Realización del análisis de riesgos.
- Metodologías.

8.1. CONCEPTOS BÁSICOS DE UN ANÁLISIS DE RIESGOS

En primer lugar conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Figura 16. Esquema de gestión de riesgos

Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

- **Amenaza:** Es la causa potencial de un daño a un activo.
- **Vulnerabilidad:** Debilidad de un activo que puede ser aprovechada por una amenaza.
- **Impacto:** Consecuencias de que la amenaza ocurra.
- **Riesgo intrínseco:** Cálculo del daño probable a un activo si se encontrara desprotegido.
- **Salvaguarda:** Medida técnica u organizativa que ayuda a paliar el riesgo.
- **Riesgo residual:** Riesgo remanente tras la aplicación de salvaguardas.

El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es relativamente sencillo calcular con cuantos recursos se cuenta (económicos, humanos, técnicos…) pero no es tan fácil saber a ciencia cierta cuáles son las necesidades de seguridad.

Es aquí donde se muestra imprescindible la realización de un análisis de riesgos. Hacerlo permite averiguar cuáles son los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información ya será posible tomar decisiones bien fundamentadas acerca de qué medidas de seguridad deben implantarse.

Por tanto, un aspecto de gran importancia a la hora de realizar la implantación de un SGSI es tener en cuenta que la inversión en seguridad tiene que ser proporcional al riesgo.

La información es generada y tratada por el personal tanto interno como externo, mediante los equipos de tratamiento de la información existentes en la organización y está situada en las instalaciones, por lo hay que considerar todos los riesgos relacionados con estos aspectos.

8.2. REALIZACIÓN DEL ANÁLISIS DE RIESGOS

8.2.1. Preparación del análisis de riesgos

Para realizar un análisis de riesgos se parte del inventario de activos. Si es razonablemente reducido, puede decidirse hacer el análisis sobre todos los activos que contiene. Si el inventario es extenso, es recomendable escoger un grupo relevante y manejable de activos, bien los que tengan más valor, los que se consideren estratégicos o todos aquellos que se considere que se pueden analizar con los recursos disponibles. Se puede tomar cualquier criterio que se estime oportuno para poder abordar el análisis de riesgos en la confianza de que los resultados van a ser útiles.

Figura 17. Preparación del análisis de riesgos

Hay que tener en cuenta que la realización de un análisis de riesgos es un proceso laborioso. Para cada activo se van a valorar todas las amenazas que pueden afectarle, la vulnerabilidad cada una de las amenaza y el impacto que causaría la amenaza en caso de ocurrir. Con todos esos datos, se calcula el valor del riesgo para ese activo.

Independientemente de la metodología que se utilice, el análisis de riesgos debe ser objetivo y conseguir resultados repetibles en la medida de lo posible, por lo que deberían participar en él todas las áreas de la organización que estén dentro del alcance del SGSI. De esta manera quedarán plasmados varios puntos de vista y la subjetividad, que es inevitable, quedará reducida. Además contar con la colaboración de varias personas ayuda a promover el desarrollo del SGSI como una herramienta útil para toda la organización y no sólo para la dirección o el área que se encarga del proyecto. Se puede abordar el análisis de riesgos con varios enfoques dependiendo del grado de profundidad con el que se quiera o pueda realizar el análisis:

- **Enfoque de Mínimos:** Se escoge un conjunto mínimo de activos y se hace un análisis conjunto, de manera que se emplean una cantidad mínima de recursos, consumiendo poco tiempo y por lo tanto tiene el coste es menor. Este enfoque tienen el inconveniente de que si se escoge un nivel básico de seguridad muy alto, puede requerir recursos excesivos al implantarlo para todos los activos y por el contrario, si es muy bajo, los activos con más riesgos pueden no quedar adecuadamente protegidos. Debido a la falta de detalle en el análisis, puede ser difícil actualizar los controles o añadir otros según vayan cambiando los activos y sistemas.

- **Enfoque informal:** Con este enfoque, no se necesita formación especial para realizarlo ni necesita de tantos recursos de tiempo y personal como el análisis detallado. Las

desventajas de este informe son que al no estar basado en métodos estructurados, puede suceder que se pasen por altos áreas de riesgos o amenazas importantes y al depender de las personas que lo realizan, el análisis puede resultar con cierto grado de subjetividad. Si no se argumenta bien la selección de controles, puede ser difícil justificar después el gasto en su implantación.

- **Enfoque detallado:** Con este enfoque se consigue una idea muy exacta y objetiva de los riesgos a los que se enfrenta la organización. Se puede decidir un nivel de seguridad apropiado para cada activo y de esa manera escoger los controles con precisión. Es el enfoque que más recursos necesita en tiempo, personal y dinero para llevarlo a cabo de una manera efectiva.

- **Enfoque combinado:** Con un enfoque de alto nivel al principio, permite determinar cuáles son los activos en los que habrá que invertir más antes de utilizar muchos recursos en el análisis. Por ello ahorra recursos al tratar antes y de manera más exhaustiva los riesgos más importantes mientras que al resto de los riesgos sólo se les aplica un nivel básico de seguridad, con lo que consigue un nivel de seguridad razonable en la organización con recursos ajustados. Es el enfoque más eficaz en cuanto a costes y a adaptabilidad a empresas con recursos limitados. Hay que tener en cuenta que si el análisis de alto nivel es erróneo puede que queden algunos activos críticos a los que no se realice un análisis detallado.

8.2.2. Identificar amenazas

Como ya se ha visto anteriormente, podríamos denominar amenaza a un evento o incidente provocado por una entidad natural, humana o artificial que, aprovechando una o varias vulnerabilidades de un activo, pone en peligro la confidencialidad, la integridad o la disponibilidad de ese activo. Dicho de otro modo, una amenaza explota la vulnerabilidad del activo.

Atendiendo a su origen, existen dos tipos de amenazas:

- **Externas:** Son las causadas por alguien (hackers, proveedores, clientes, etc.) o algo que no pertenece a la organización. Ejemplos de amenazas de este tipo son los virus y las tormentas.

- **Internas:** Estas amenazas son causadas por alguien que pertenece a la organización, por ejemplo errores de usuario o errores de configuración.

Las amenazas también pueden dividirse en dos grupos según la intencionalidad del ataque en deliberadas y accidentales:

- **Deliberadas:** Cuando existe una intención de provocar un daño, por ejemplo un ataque de denegación de servicio o la ingeniería social.

- **Accidentales:** Cuando no existe tal intención de perjudicar, por ejemplo averías o las derivadas de desastres naturales: terremotos, inundaciones, fuego, etc.

Para valorar las amenazas en su justa medida hay que tener en cuenta cual sería el impacto en caso de que ocurrieran y a cual o cuáles son los parámetros de seguridad que afectaría, si a la confidencialidad, la integridad o la disponibilidad.

8.2.3. Identificación de vulnerabilidades

Tal y como hemos comentado anteriormente, una vulnerabilidad es toda aquella circunstancia o característica de un activo que permite la materialización de ataques que comprometen la confidencialidad, integridad o disponibilidad del mismo. Por ejemplo, un equipo será vulnerable a los virus si no tiene un programa antivirus instalado.

Hay que identificar las debilidades en el entorno de la Organización y valorar cómo de vulnerable es el activo en una escala razonable (alto-medio-bajo, de 1 a 5, etc.).

Hay que tener en cuenta que la presencia de una vulnerabilidad por si misma no causa daño. Para que se produzca este daño debe existir una amenaza que pueda explotarla.

Algunos ejemplos de vulnerabilidades son:

- La ausencia de copias de seguridad, que compromete la disponibilidad de los activos.
- Tener usuarios sin formación adecuada, que compromete la confidencialidad, la integridad y la disponibilidad de los activos, ya que pueden filtrar información o cometer errores sin ser conscientes del fallo.
- Ausencia de control de cambios, que compromete la integridad y la disponibilidad de los activos.

8.2.4. Ejecución del análisis

Con el equipo de trabajo asignado para ello y la metodología escogida, se llevará a cabo el análisis de riesgos. Los participantes tendrán que valorar las amenazas y las vulnerabilidades que afectan a los activos escogidos para el análisis y el impacto que ocasionaría que alguna de las amenazas realmente ocurriera, sobre la base de su conocimiento y experiencia dentro de la organización.

Como ejemplo de metodología de Análisis de Riesgos (muy resumida) utilizaremos como referencia las siguientes tablas:

Estimación de la probabilidad de ocurrencia de una amenaza sobre cada activo:

Tabla 4. PROBABILIDADES

Probabilidad de ocurrencia de la amenaza	Guía

Baja	Una media de una vez cada 5 años
Media	Una media de una vez al año
Alta	Una media de 3 veces al año
Muy alta	Una media de una vez al mes

Estimación de la vulnerabilidad de cada activo, es decir, la facilidad de las amenazas para causar daños en el mismo.

Tabla 5. VULNERABILIDAD

Vulnerabilidad	Guía
Baja	Difícil que ocurra el peor escenario posible (Prob.< 33%)
Media	Probable que ocurra el peor escenario posible (33% > Prob.< 66%)
Alta	Casi seguro que ocurra el peor escenario posible (Prob.> 66%)

La siguiente tabla se utilizará para calcular el nivel de riesgo, valorando el impacto que tendría en un activo la ocurrencia de una amenaza:

Tabla 6. NIVEL DE RIESGO

Amenaza		Baja			Media			Alta			Muy alta		
Vulnerabilidad		B	M	A	B	M	A	B	M	A	B	M	A
Impacto	0	1	1	1	1	1	2	1	2	2	2	2	3
	1	1	2	2	2	2	3	3	3	3	3	3	4
	2	2	2	3	2	3	3	3	3	4	3	4	4
	3	2	3	3	3	3	4	3	4	4	4	4	5
	4	3	3	4	3	4	4	4	4	5	4	5	5

	5	3	4	4	4	4	5	4	5	5	5	5	6
	6	4	4	5	4	5	5	5	5	6	5	6	6
	7	4	5	5	5	5	6	5	6	6	6	6	7
	8	5	5	6	5	6	6	6	7	7	8	8	9
	9	6	6	7	7	8	8	8	9	9	9	10	10

Tomemos como ejemplo un activo, portátiles, cuya valoración ha resultado ser 8 y cuyas principales amenazas se considera que son:

- Robo.
- Errores de los usuarios.
- Divulgación de información.
- Acceso no autorizado.

Por lo que el nivel de riesgo será:

Amenaza	Impacto (Valor del activo)	Probabilidad de la Amenaza	Vulnerabilidad	Nivel de riesgo
Fuego	8	Baja	Alta	6
Errores de usuarios	8	Alta	Media	7
Divulgación de información	8	Media	Media	6
Acceso no autorizado	8	Muy Alta	Alta	9
			Total	28

El valor de riesgo para este activo es la suma de los valores individuales de cada amenaza, por lo que es 28.

De este modo obtendríamos el riesgo de todos los activos que se han incluido en el Análisis de Riesgos y podríamos realizar las medidas oportunas para mitigarlos (o realizar el tratamiento escogido en cada caso).

8.2.5. Documentar el análisis de riesgos

Independientemente de la metodología o la herramienta informática que se utilice para la realización del análisis de riesgos, el resultado debería ser una lista de los riesgos correspondientes a los posibles impactos en caso de que se materialicen las amenazas a las que están expuestos los activos.

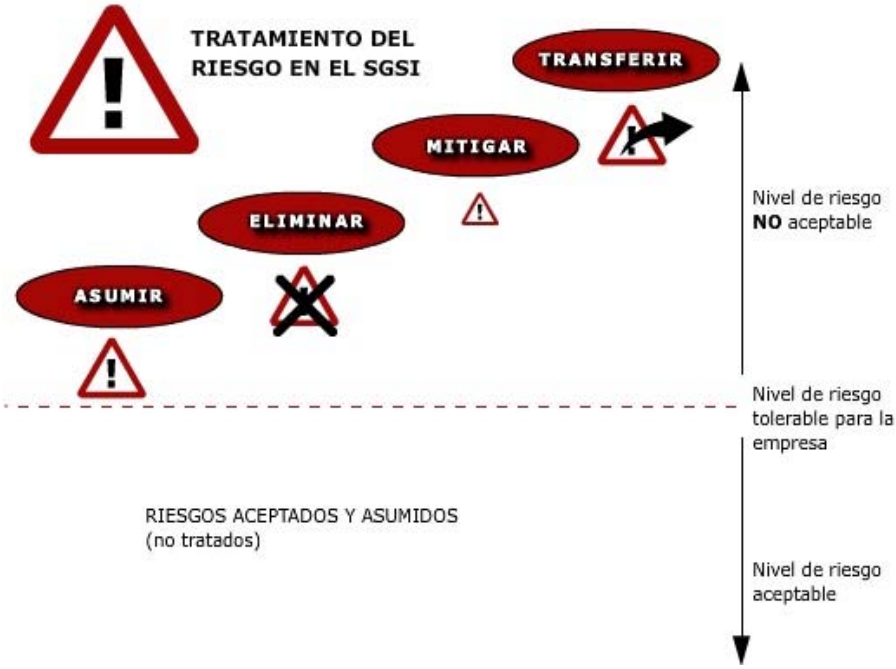

Figura 18. Tratamiento del riesgo

Esto permite categorizar los riesgos e identificar cuáles deberían ser tratados primero o más exhaustivamente. Se debe escoger, a la vista de los resultados, cual es el nivel de riesgo que la organización está dispuesta a tolerar, de manera que por debajo de ese nivel el riesgo es aceptable y por encima no lo será y se tomará alguna decisión al respecto.

Hay cuatro tipos de decisiones para tratar los riesgos que se consideran no aceptables:

- **Transferirlo:** El riesgo se traspasa a otra organización, por ejemplo mediante un seguro.
- **Eliminarlo:** Se elimina el riesgo, que normalmente sólo se puede hacer eliminando el activo que lo genera, por ello esta opción no suele ser viable.
- **Mitigarlo:** Es decir, reducir el riesgo, normalmente aplicando controles de seguridad. Es una de las opciones más habituales.

- **Asumirlo:** Otra opción común es aceptar que no se puede hacer nada y por lo tanto se asume ese riesgo.

Toda esta información debe quedar documentada para justificar las acciones que se van a tomar para conseguir el nivel de seguridad que la organización quiere alcanzar y como referencia para posteriores análisis.

8.3. METODOLOGÍAS

Existen numerosas metodologías disponibles para la realización de análisis de riesgos, ya que es una labor que requiere de bastante dedicación y con una metodología estructurada se facilita la tarea, sobre todo si existe una herramienta que simplifique todo el proceso.

La organización debe escoger aquella que se ajuste a sus necesidades, y si considera varias opciones, inclinarse por la más sencilla. Hay que tener en cuenta que el análisis de riesgos debe revisarse periódicamente, por lo que si se hace con una metodología complicada, esta labor necesitará de una dedicación excesiva.

A continuación se detallarán algunas de las metodologías más reconocidas:

- **Análisis holandés A&K.:** Es método de análisis de riesgos, del que hay publicado un manual, que ha sido desarrollado por el Ministerio de Asuntos Internos de Holanda, y se usa en el gobierno y a menudo en empresas holandesas.

- **CRAMM:** Es un método de análisis de riesgos desarrollado por el gobierno británico y cuenta con una herramienta, ya que es un método difícil de usar sin ella. Está basado en las mejores prácticas de la administración pública británica, por lo que es más adecuado para organizaciones grandes, tanto públicas como privadas.

- **EBIOS:** Es un juego de guías mas una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado no sólo de Francia sino en otros países. La metodología EBIOS consta de un ciclo de cinco fases:

  - Fase 1. Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.

  - Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.

  - Fases 4 y 5, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

- **IT-GRUNDSCHUTZ (Manual de protección básica de TI):** Desarrollado en Alemania por la Oficina Federal de la Seguridad de la Información (BSI en sus siglas alemanas). Este manual proporciona un método para establecer un SGSI en cualquier organización, con

recomendaciones técnicas para su implantación. El proceso de seguridad de TI propuesto por esta metodología sigue los siguientes pasos:

- Iniciar el proceso.
- Definir los objetivos de seguridad y el contexto de la organización.
- Establecer la organización para la seguridad de TI.
- Proporcionar recursos.
- Crear el concepto de la seguridad de TI.
- Análisis de la estructura de TI.
- Evaluación de los requisitos de protección.
- Modelado.
- Comprobación de la seguridad de TI.
- Planificación e implantación.
- Mantenimiento, seguimiento y mejora del proceso.
- La metodología incluye listas de amenazas y controles de seguridad que se pueden ajustar a las necesidades de cada organización.

- **MAGERIT:** Desarrollado por el Ministerio de Administraciones Públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión realmente efectivos. Cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas. Cuenta con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información que tiene dos versiones, una completa para grandes organizaciones y otra simplificada para las pequeñas.

- **Manual de Seguridad de TI Austriaco:** Consta de dos partes, en la primera se describe el proceso de la gestión de la seguridad de TI, incluyendo el análisis de riesgos y la segunda es un compendio de 230 medidas de seguridad. Es conforme con la Norma ISO/IEC IS 13335 y en parte con la ISO 27002.

- **MARION – MEHARI:** El primigenio MARION (Método de Análisis de Riesgos por Niveles), basado en una metodología de auditoría, permitía estimar el nivel de riesgos de TI de una organización. Sustituido por MEHARI, este método de análisis de riesgo cuenta con un

modelo de evaluación de riesgos y módulos de componentes y procesos. Con MEHARI se detectan vulnerabilidades mediante auditorías y se analizan situaciones de riesgo.

- **Métodos ISF para la evaluación y gestión de riesgos:** El Information Security Forum. (ISF) es una importante asociación internacional. Su Estándar de Buenas Prácticas es un conjunto de principios y objetivos para la seguridad de la información con buenas prácticas asociadas a los mismos. El Estándar cubre la gestión de la seguridad a nivel corporativo, las aplicaciones críticas del negocio, las instalaciones de los sistemas de información, las redes y el desarrollo de sistemas. El Estándar contiene:

  - FIRM, una metodología para el seguimiento y control del riesgo. o Una herramienta para la gestión del riesgo. o SARA, otra metodología para analizar el riesgo en sistemas críticos. o SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.

  - SARA, otra metodología para analizar el riesgo en sistemas críticos.

  - Una herramienta para la gestión del riesgo

  - SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.

- **Norma ISO/IEC IS 27005:** La Norma habla de la gestión de los riesgos de la seguridad de la información de manera genérica, utilizando para ello el modelo PDCA, y en sus anexos se pueden encontrar enfoques para la realización de análisis de riesgos, así como un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.

- **OCTAVE:** (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®), desarrollado en EEUU por el SEI, en un una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados.

- **SP800-30 NIST Risk Management Guide for Information Technology Systems:** Desarrollado por el NIST estadounidense, es una guía detallada de las consideraciones que deben hacerse para llevar a cabo una evaluación y una gestión de riesgos orientada a la seguridad de los sistemas de información.

9. GESTIÓN Y TRATAMIENTO DE LOS RIESGOS. SELECCIÓN DE LOS CONTROLES

Este apartado describirá en qué consiste la gestión de riesgos, cómo se deben escoger los controles, se darán recomendaciones para la selección y se explicará la manera de documentar esta selección.

Los puntos a tratar son:

- Gestión del Riesgo.
- Mitigación del Riesgo.
- Documentar la Gestión del Riesgo.

9.1.1. GESTIÓN DEL RIESGO

La gestión de esos riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados. La gestión de los riesgos tiene como objetivo reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización.

Una vez que conocemos los riesgos de la organización y decidido el tratamiento que se le va a dar para cada uno de los activos, se deben tomar acciones en consecuencia. Los cuatro tipos de tratamiento requieren de acciones de distinta naturaleza:

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.
- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.
- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No caben más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos **jamás podrá ignorarlos**, puesto que, de este modo, no estaría vigilando que no se convirtiesen en riesgos que la organización no es capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a un incidente de seguridad.

Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. El nivel de riesgo resultante de este segundo análisis es el **riesgo residual**. Este se define como el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad apropiadas

En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección.

9.2. MITIGACIÓN DEL RIESGO

En el caso de se decida mitigar el riesgo, los pasos a seguir son:

Figura 19. Mitigación del riesgo

1. **Seleccionar** los **controles** apropiados para los riesgos a los que se quiere hacer frente, en principio del Catálogo de Buenas Prácticas de la ISO/IEC 27002 (133 controles posibles), pero pueden añadirse otros que la organización considere necesario.

2. **Implantar** los **controles** para lo que deben desarrollarse procedimientos. Aunque sean controles tecnológicos deben desarrollarse para su instalación, uso y mantenimiento.

3. **Verificar** que los **controles** están correctamente implantados.

4. Establecer **indicadores** para saber en qué medida la implantación de los controles seleccionados reduce el riesgo a un nivel aceptable.

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos.

Existen dos grandes grupos de controles. Por un lado los **técnicos**, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, y por otro los **organizativos** que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

Es muy importante conseguir un conjunto de controles que contenga controles de los dos tipos, ya que muchas medidas técnicas no pueden impedir que los usuarios de los sistemas cometan errores o dañen intencionadamente los activos y, al contrario, emitir muchas normas internas puede ser inútil si no hay una mínima seguridad técnica implantada.

Por ejemplo, el estudio del uso de ordenadores portátiles para trabajos fuera de las instalaciones de la organización puede haber determinado que existe un riesgo alto de robo para los portátiles. Se pueden escoger varios controles para mitigar este riesgo. Uno de ellos será diseñar unas normas de utilización de este tipo de activos, que obligue a los usuarios a no dejar sus portátiles desatendidos y a no dejarlos a la vista en el coche. Con este control es probable que se reduzca la probabilidad de robo, sin embargo la posibilidad todavía existe. Así que es necesario tomar otras medidas como el cifrado del disco duro y un proceso de autenticación de usuario, que servirán para reducir el daño a la confidencialidad que se produciría si el equipo es robado.

La combinación de las medidas técnicas y organizativas consigue un nivel de seguridad razonable con unos recursos limitados para el escenario de riesgo que se trataba de mitigar.

Otra clasificación que se puede hacer de los controles para facilitar su selección es la de controles **preventivos** y **correctivos**. Los controles de tipo preventivo son aquellos que sirven para evitar incidentes de seguridad no deseados mientras que los correctivos son aquellos que se pondrán en marcha ante la ocurrencia de fallos o incidentes de seguridad.

Por ejemplo, para prevenir accesos no autorizados a una red se crean cuentas de usuario y se otorgan privilegios a estos usuarios, diferenciando aquellos que sí pueden acceder de los que no. En el caso de que ocurriera un acceso no autorizado, por ejemplo, un empleado que ha cambiado de departamento y conserva sus antiguos privilegios de los que hace uso, lógicamente primero hay que ser capaces de detectarlo y una vez detectado, esos privilegios deberían ser automáticamente eliminados.

Muchos controles están interrelacionados, por lo que hay que tener en cuenta estas dependencias para que no queden lagunas de seguridad que puedan suponer nuevas vulnerabilidades.

Hay que tener en cuenta que la implantación de un control requiere de ciertos recursos y su mantenimiento también. Por lo tanto hay que valorar al escoger un control, si se cuenta con dinero y mano de obra suficientes tanto para ponerlos en marcha como para gestionarlos.

Esto significa que hay que considerar varios factores y restricciones a la hora de seleccionar un control, ya que puede darse el caso de que a pesar de cubrir un riesgo detectado, no se puede o no debe ser aplicado, como por ejemplo:

- El mencionado **coste de la implementación y el mantenimiento del control**. Por ejemplo, se escoge el control 11.6.1 Restricción del acceso a la información y para implantarlo se decide instalar un firewall. Esta decisión tiene el coste de su compra, más el de su instalación, configuración y gestión.

- La **disponibilidad del control**. Puede ser necesario instalar un firewall pero si el modelo específico necesario para la organización tiene un plazo de entrega muy largo, puede ser necesario optar por alguna otra medida al menos temporalmente.

- **Ayuda** que hay que otorgar a los **usuarios** para desempeñar su función. Siguiendo con el ejemplo del firewall, hay que considerar que el responsable de su gestión dentro de la organización debe saber hacerlo. Si no es así, habrá que valorar darle formación o bien subcontratar el servicio. Además los usuarios de la red verán probablemente restringidos sus privilegios de acceso, por lo que habrá que informar de la nueva situación y buscar soluciones alternativas si surge algún problema.

- **Controles** que ya existen y sólo hace falta **modificarlos**. Si se diera el caso de que ya existe un firewall en la organización realizando las funciones requeridas por el control, quizás se pueda solucionar el problema con un cambio en la configuración o con una actualización del software. También podría suceder que ya hay aplicados otros controles que mitigan el mismo riesgo, y añadir otro resulte excesivo o demasiado costoso.

- Su **aplicabilidad** de acuerdo con los riesgos detectados. En cualquier caso, si no hay un riesgo claro en la organización respecto a los accesos a la información, la aplicación del control 11.6.1 no estaría justificada.

No todos los controles deben ser seleccionados, pero los hay que siempre deben ser implantados si no lo están ya y son aquellos que constituyen un requisito de la Norma UNE/ISO-IEC 27001 tales como la Política de Seguridad o las auditorías internas.

Seleccionados los controles pertinentes, debe definirse los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos, como por ejemplo la gestión de los recursos humanos. Pero incluso los de corte tecnológico pueden ser susceptibles de necesitar documentación, como por ejemplo la realización de copias de seguridad.

Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Hay que contar también que si la organización no tiene procesos muy complejos puede ser posible que varios controles puedan agruparse en un único procedimiento. No es necesario ni recomendable, desarrollar un procedimiento para cada control. La cantidad de documentación generada puede hacer francamente difícil que se logren gestionar correctamente los controles. Por otro lado, los procedimientos deben ser lo más breves y claros posible. No deben incluir demasiadas instrucciones ni particularidades de la tarea a realizar. El objetivo del procedimiento es contar con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

Una vez puestos en marcha, debe comprobarse periódicamente que los controles funcionan como se esperaba. Si no es así, deberán tomarse las acciones necesarias para corregir esa situación.

Una herramienta fundamental del SGSI es la verificación de la eficacia de los controles implantados. Para ello deben establecerse objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los resultados de manera que se sepa si el control realmente protege los activos hasta el punto que la organización necesita.

Por ejemplo, se detecta el riesgo de que los puestos de usuarios se infecten de virus, por lo que se determina aplicar el control 10.4.1, Controles contra el código malicioso. Para implantar este control se decide instalar en todos los puestos un antivirus actualizable automáticamente a diario. Se prepara la compra de la aplicación, se valoran distintas opciones, se compra la que se considera más apropiada y el responsable de sistemas se encarga de instalarla en todos los puestos. Se ha hecho un gasto para la compra del material y otro de mano de obra del responsable de sistemas, para los que he necesario presentar una justificación. Esta justificación vendrá dada por la reducción de las infecciones de virus en los puestos y la consiguiente reducción de horas de trabajo perdidas solucionando estas incidencias. Si hasta la instalación del antivirus teníamos 4 infecciones mensuales, en las que se empleaban 6 horas de trabajo, los objetivos pueden declararse como sigue:

- Reducir el Nº de infecciones /mes a 2
- Reducir el Nº de horas empleadas en repararlas/mes a 3

Se establece que semanalmente el responsable de sistemas comprobará el número de infecciones y registrará el tiempo empleado en su resolución, reportando los resultados mensualmente. Los registros de los tres meses siguientes son:

1. Mes 1. Nº de infecciones 0. Horas empleadas en reparación. 0
2. Mes 2. Nº de infecciones 3. Horas empleadas en la reparación: 3
3. Mes 3. Nº de infecciones 1. Horas empleadas en la reparación: 2

De estos datos podemos inferir que más o menos se está consiguiendo el objetivo, y en cualquier caso ha habido una reducción significativa de las pérdidas en términos de costes de horas de trabajo que originaban las infecciones, que justifican sobradamente la inversión en la compra e instalación del antivirus.

9.3. DOCUMENTAR LA GESTIÓN DE RIESGOS

La documentación de la gestión de riesgos se realiza mediante la Declaración de Aplicabilidad también conocida por sus siglas en inglés SOA ("Statement Of Applicability"). Este documento, requerido por la Norma UNE/ISO-IEC 27001, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados.

Este documento registra todo lo que se ha realizado y se va a realizar en el futuro inmediato para que la seguridad de la información de la organización llegue al nivel que se haya estimado apropiado para sus necesidades y recursos. La declaración de aplicabilidad debe incluir los 133 controles del Anexo A de la Norma, mas los controles adicionales a los de la Norma que la organización hubiera estimado conveniente aplicar. Para cada uno de los controles debe reflejarse en este documento:

- Si está implantado actualmente en la organización, con una breve descripción de cómo se aplica.
- Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.
- Si no se va a implantar, y entonces hay que exponer los motivos que han llevado a esta decisión. Las exclusiones deben justificarse adecuadamente.

El principal objetivo de este documento es que, al tener que repasar todos y cada uno de los controles, se hace una comprobación de que no se ha pasado por alto ningún control por error o descuido, que podría ser útil o necesario para la gestión de la seguridad de la información.

Este documento constituye de alguna manera un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué va a consistir el sistema de seguridad, detallando cada uno de los controles que se tiene la intención de aplicar de manera explícita.

Sólo insistir en que no es necesario seleccionar todos los objetivos ni todos los controles asociados a cada uno de los objetivos. Deben escogerse los objetivos y controles apropiados a las circunstancias, es decir, aquellos que se considera que cubren los requisitos de seguridad de la organización y son viables.

Una vez que está claro que se va a hacer, debe prepararse un plan para la realización de todo lo que se ha decidido hacer. Este plan, que la Norma denomina **Plan de Tratamiento de Riesgos**, contempla todo las acciones necesarias tanto para implantar el SGSI y gestionarlo como para la puesta en marcha de los controles escogidos.

El plan tiene que contar con los recursos materiales, técnicos y humanos necesarios para que pueda ser llevado a cabo con ciertas garantías de éxito. Debe ser revisado a intervalos regulares para comprobar que no se producen desviaciones. Estas pueden ser de plazo porque no hay recursos para ejecutarlas o han resultado ser más difíciles de ejecutar de lo que se preveía en un principio o también de que no se llevan a cabo las acciones planificadas sino otras, normalmente porque se han tomado decisiones sobre la marcha para solventar problemas no previstos.

Dentro de este plan pueden quedar recogidos los objetivos definidos para medir la eficacia de los controles, estableciendo asimismo el mecanismo de recogida y análisis.

El avance en la consecución de los objetivos suele ser unos de los puntos que se tratan en el Comité de Seguridad, ya que es en este Comité donde se deciden los objetivos y se modifican según sea necesario.

10. SEGUIMIENTO, MONITORIZACIÓN Y REGISTRO DE LAS OPERACIONES DEL SISTEMA

Una vez que está en marcha el SGSI es fundamental hacer un seguimiento de cómo funciona y cómo va evolucionando el sistema. En primer lugar para corregir las posibles desviaciones sobre lo planificado y previsto y en segundo lugar, aunque igual de importante, detectar oportunidades de mejora del sistema, ya que el objetivo último de implantar un sistema de gestión de este tipo es el mejorar continuamente, hacer cada vez más con los limitados recursos disponibles.

En este modulo se da una visión general de las actividades que comprende este seguimiento.

El contenido de este módulo es:

- Revisión del SGSI.
- Auditoría interna.
- Acciones correctoras y preventivas.
- Plan de tratamiento del riesgo.

10.1. REVISIÓN DEL SGSI

Uno de los requisitos más relevantes de la Norma UNE/ISO-IEC 27001 es la revisión que la dirección de la organización debe realizar con una cierta periodicidad, como mínimo anual, al Sistema de Gestión de Seguridad de la Información. Esta revisión tiene como objetivo asegurarse de que el SGSI es en todo momento adecuado, apropiado y efectivo para los propósitos y contexto de la organización.

La importancia que tiene este requisito queda patente por la minuciosa descripción que se hace en la norma de la información que debe recogerse y evaluarse y de los resultados que deben quedan documentados. Es importante tener en cuenta que una acción que no se documenta y no queda registrada a ojos del sistema no estaría completa ya que no se podría medir y, por tanto, mejorar si fuese preciso.

Figura 20. Ciclo PDCA. Fase "Check"

Esta revisión forma parte de la fase Check (comprobar) del ciclo de mejora continua, y es una herramienta magnífica para el análisis y la adopción consensuada de oportunidades de mejora, ya que se contemplan todos los aspectos y la marcha del SGSI, por lo que se tiene una visión general de todo y se pueden detectar los puntos débiles y discutir sobre cómo mejorarlos.

Existen muchas formas en que la alta dirección puede revisar el SGSI como, por ejemplo, recibir y revisar un informe generado por el representante de la dirección u otro personal, o incluir los temas pertinentes en la agenda de reuniones regulares de la dirección.

10.1.1. Entradas a la revisión

Existen muchas fuentes de las que se pueden recoger datos e información útiles para realizar la revisión por la dirección:

- Las **auditorías** llevadas a cabo en la organización. No sólo las auditorías internas del SGSI son útiles aquí, sino también otras auditorías tales como la de la LOPD, auditorías de clientes, de otras normas de gestión, etc. Todas ellas pueden aportar información sobre los puntos fuertes y débiles del SGSI y poner en evidencia oportunidades de mejora. Hay que tener en cuenta que muchas veces los requisitos de las distintas normas y reglamentos se solapan, por lo se pueden llegar a cubrir varios puntos débiles con una acción que valga para todos, con el consiguiente ahorro de recursos. Por ejemplo, muchos de los requisitos de la LOPD se pueden cubrir con controles del SGSI, y parte de los requisitos de un sistema de gestión según la Norma ISO 9001 son comunes con los de la Norma ISO 27001, como la realización

de auditorías internas, por lo que se puede llevar a cabo una única auditoría que contemple los requisitos de ambas normas.

- Las **anteriores revisiones** del SGSI y las acciones derivadas del mismo, son el punto de partida, dónde estaba el SGSI y qué es lo que se ha hecho al respecto desde entonces. Analizar qué se decidió hacer y hasta donde se ha avanzado, proporciona información muy valiosa sobre qué se puede hacer para continuar mejorando y progresando. Estudiar por qué no se han llevado a cabo todas las acciones planificadas servirá para detectar puntos débiles y obliga a determinar nuevas medidas.

- **Comentarios** de las partes interesadas. A lo largo de la actividad cotidiana de la organización, tanto clientes, como usuarios, proveedores, público, cualquiera que entra en contacto con ella puede emitir algún comentario que puede ser útil para diseñar alguna acción de mejora. Debe existir algún mecanismo, aunque sea informal para incorporar esta información al sistema.

- **Técnicas, productos o procedimientos**, que podrían ser usados en la organización para mejorar el funcionamiento y la efectividad del SGSI. La información necesaria para este punto probablemente vendrá en primer lugar del responsable de sistemas, pero también las distintas personas involucradas en tareas que necesiten mejoras pueden aportar ideas al respecto.

- El **estado** de las **acciones preventivas y correctoras**. Hay que analizar las acciones, que son la medida de cómo se desarrolla la actividad cotidiana del SGSI, estudiando cuantas se han abierto, por qué motivo, si se han ido cerrando en plazo, si ha habido problemas con alguna de ellas, etc. Con esa información se extraerán conclusiones importantes para la mejora del SGSI.

- Las **vulnerabilidades** o **amenazas** que no se han tratado adecuadamente en análisis de riesgos anteriores. Es decir, si se han detectado nuevas amenazas o ha habido cambios que necesiten revisar las anteriormente consideradas, o bien valorar si riesgos que no se trataron por cualquier motivo antes, ahora necesitan de tratamiento.

- La **evaluación de los objetivos**. Uno de los principales puntos de esta revisión es comprobar si se han conseguido los objetivos marcados en un principio. Cuando se diseña el SGSI, se marcan unos objetivos, para los que habrá que definir unas métricas que permitan evaluar hasta qué punto se han alcanzado los objetivos. Esta información es la que indica si el SGSI funciona o no, si es eficaz o no. A la luz de esta información se podrá decidir si hay que modificar los objetivos o qué acciones tomar para alcanzarlos.

- **Cambios en la organización**. Cambios por ejemplo en la infraestructura informática por ejemplo, que afectaría de manera directa y clara al SGSI, ya que las medidas de seguridad aplicadas en los anteriores sistemas de información pueden no ser válidas o suficientes para los nuevos sistemas. Pero también cambios en el personal, que requieran reajustar los

privilegios en el acceso a la información, en los servicios que la organización ofrece, que pueden plantear nuevos requisitos de seguridad, etc.

Todas las ideas, razonamientos y decisiones que hayan surgido al revisar el SGSI deben **documentarse**, como por ejemplo:

- Mejoras de la efectividad del SGSI, es decir, qué se va a hacer para mejorar el SGSI: se van a implantar más controles, se van a mejorar los ya implantados, se van a transferir riesgos, etc.

- Actualización de la evaluación y gestión de riesgos. Hay que documentar los cambios que se hayan producido en el análisis y gestión de los riesgos y los motivos que los han motivado.

- Modificación de procedimientos y controles que afectan a la seguridad de la información, según sea necesario, para responder a incidentes internos o externos que puedan impactar en el SGSI, incluyendo cambios en:

  - Requisitos de negocio, de seguridad o legales.

  - Procesos de negocio que tengan efecto en los requisitos de negocio existentes.

  - Obligaciones contractuales.

  - Cambios en el nivel de riesgo aceptable.

  - Necesidades de recursos.

- Mejoras en la manera de medir la efectividad de los controles. Al revisar los indicadores y métricas que se utilizan debe comprobarse si siguen siendo útiles, eliminando aquellos que no lo sean y diseñando nuevos indicadores más eficaces a la hora de suministrar información relevante.

10.2. AUDITORÍA INTERNA

Podemos definir auditoría como una actividad independiente que tiene lugar dentro de la organización y que está encaminada a la revisión de operaciones con la finalidad de prestar un servicio a la dirección, ya que en realidad es un control de dirección El objetivo de una auditoría es determinar si los objetivos de los controles, los controles, los procesos y los procedimientos están conformes con los requisitos de la Norma en la que se audite el sistema, los requisitos legales y reglamentarios, los requisitos de la organización (contractuales, de seguridad, internos, etc.). Además de esto, la auditoría verifica si el SGSI se mantiene de manera efectiva y se obtienen los resultados esperados. Es decir, si el sistema dice lo que hace y hace lo que dice.

La planificación de la auditoría debe hacerse al menos anualmente, ya que es importante realizar una revisión al sistema completo a lo largo del año, decidiendo no solo las fechas en las que se va a realizar, sino si el alcance va a ser global o parcial y en este último caso, las áreas y procesos que van a ser auditados en cada una de las auditorías.

Una vez hecho esto, se puede comenzar a preparar la auditoría en sí, decidir los criterios de auditoría, el método que se va a utilizar e informar a los afectados por la auditoría con tiempo suficiente para que se puedan preparar.

Los auditores designados para la realización de la auditoría prepararán una lista de comprobación que incluirá datos como el alcance de la auditoría, las actividades a auditar, los documentos aplicables tales como las normas aplicables y la política de seguridad, documentos de referencia como los informes de otras auditorías o la revisión del sistema, además de la fecha prevista de realización.

Esta lista será la guía de trabajo para la ejecución de la auditoría, que revisará las actividades y las evidencias de que se realizan según los requisitos y los controles aplicables.

Una vez hechas las comprobaciones, se redacta y entrega a dirección y a los afectados el informe de resultados, identificando las no conformidades detectadas, es decir, las desviaciones o los incumplimientos de la Norma de referencia de la auditoría o de las normas internas de la organización. Con esta información se deben tomar las medidas oportunas para solucionarlas, identificando las causas de las no conformidades y eliminándolas.

El objetivo siempre será detectar problemas con los procesos y procedimientos nunca con el personal encargado de ejecutarlos, para poder mejorar continuamente.

Las personas que asuman el rol de auditor Interno tienen que poseer la necesaria preparación profesional en las metodologías que hay que emplear, los conocimientos generales (tanto del ambiente empresarial como del SGSI) y contar con el carisma personal para tener credibilidad y el respaldo de la dirección. Es muy importante que sean personas que tengan independencia en relación con las actividades involucradas. Los resultados de una auditoría realizada por alguien que realiza o controla el trabajo auditado estarán probablemente sesgados, por lo que debe evitarse esta situación.

10.3. ACCIONES CORRECTORAS Y PREVENTIVAS

Cuando se producen no conformidades, es decir, cuando hay un incumplimiento de un requisito, bien de la Norma bien de las pautas internas, se deben toman acciones encaminadas a resolver esa situación no deseada. Las acciones contempladas por la Norma se dividen en:

- Acciones correctoras.
- Acciones preventivas.
- Acciones de mejora.

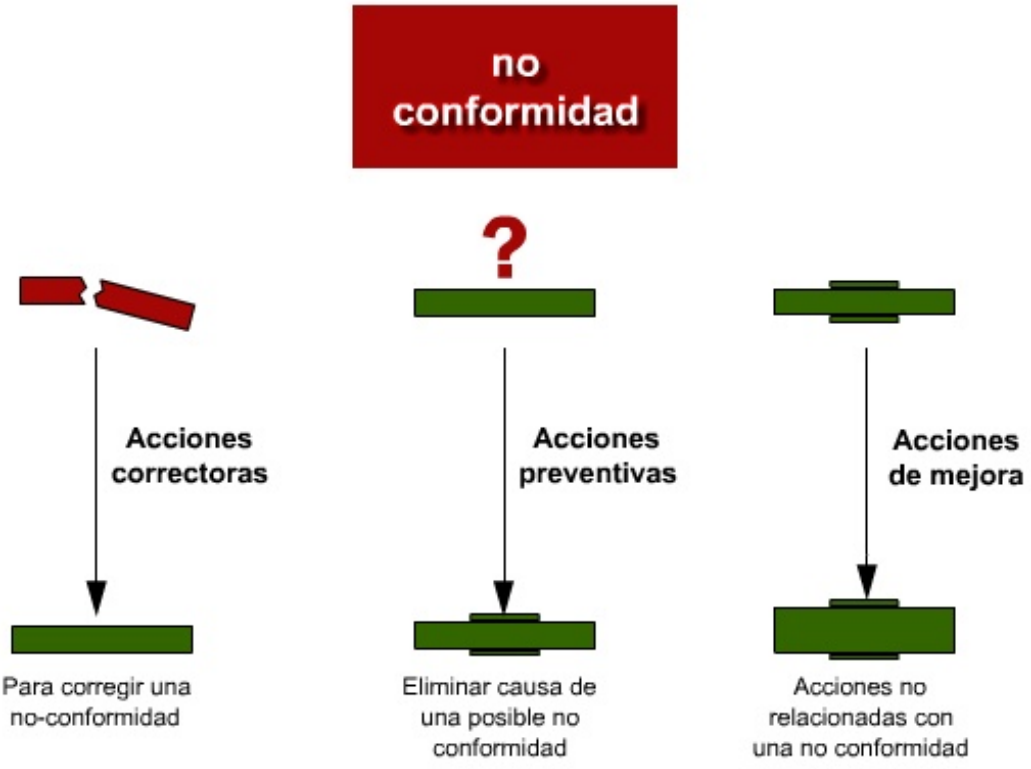

Figura 21. Acciones

Las acciones **correctoras** son las que se toman para corregir una no-conformidad significativa con los requisitos del Sistema de Gestión de Seguridad de la Información. Se pueden detectar no conformidades durante cualquiera de las auditorías y revisiones a las que se somete el SGSI, al analizar los registros de incidencias, ya las que sean graves o se reiteradas en el tiempo constituyen no conformidades, o durante la operativa habitual del SGSI.

Localizado un problema debe determinarse la relación causa-efecto para determinar el curso de acción. Las acciones correctivas tienen como objetivo la eliminación de la causa origen del problema para evitar que éste se pueda repetir en el futuro. Solucionar momentáneamente el incidente no es una acción correctora completa. Evidente es necesario restablecer el servicio u operación que se haya visto afectada por el incidente, pero debe descubrirse el por qué del mismo.

Esta tarea de investigación a veces puede resultar muy laboriosa ya que hay causas más evidentes y fáciles de localizar que otras. Incluso puede suceder que la causa última del problema no se puede ser solventada con los medios disponibles o sin causar un impacto excesivo en la organización, sin embargo es necesaria su detección para ser evaluada y estudiada por parte de los diferentes comités de seguridad que serán los que, en última instancia, tomarán la resolución de las acciones a llevar a cabo.

Las acciones **preventivas** como su propio nombre indica, son aquellas que se toman para eliminar la causa de una posible no conformidad, es decir, se actúa antes de que ocurra. En una acción preventiva se determina la posible fuente de problemas antes de se haya materializado ninguno, con el objeto de eliminarla y evitar que se produzca.

Como fuentes de información para el establecimiento de acciones preventivas son, entre otras, los resultados de las auditorías internas y externas, los resultados de los análisis de datos, los registros de gestión, el personal, las mediciones y métricas, etc.

Habitualmente tanto las acciones correctoras como las preventivas se discuten y analizan, dentro del Comité de Seguridad.

En ambos casos, para abrir una acción es necesario recoger todos los datos e información relativos al problema a tratar. A partir de ahí se trata de determinar el origen del problema y las primeras acciones a tomar, los responsables de ejecutar estas acciones y los plazos para ello. Se hace un seguimiento de la acción hasta que se hayan completado todas las acciones planificadas. Para cerrar una acción debe verificarse que se ha resuelto satisfactoriamente, es decir que ha sido efectiva.

Cuando se deciden acciones que no están relacionadas con una no conformidad éstas se denominan acciones de **mejora**. Pueden venir de sugerencias del personal, de la revisión del SGSI, etc. Estas acciones suponen un cambio positivo en la manera de afrontar una tarea o procesos de manera que se mejoren la operativa, los resultados o ambas.

No se debe olvidar que el SGSI se basa en un ciclo de mejora continua por lo que es importante que en cada ciclo del proceso se sigan implantando medidas que mejoren el mismo.

10.4. PLAN DE TRATAMIENTO DEL RIESGO

La Norma estipula que se debe preparar un plan que contenga las acciones que se van a realizar para gestionar el riesgo. Este plan constituye el marco para la implantación del SGSI

Además de las acciones necesarias para implementar los controles seleccionados para cumplir los objetivos de los controles, el plan contendrá los responsables, recursos y plazos asignados para la ejecución de las mismas. La amplitud del plan depende del alcance de los trabajos y los objetivos. Para la estimación de recursos y plazos deberán evaluarse varias opciones, teniendo en cuenta los riesgos y las oportunidades.

El objetivo de este plan es definir el alcance de los trabajos a realizar, así como el de evaluar la viabilidad de los objetivos del proyecto con los recursos disponibles.

De manera regular, el responsable del plan debe controlar e informar del progreso del proyecto para que si se producen desviaciones, se puedan definir de manera oportuna las acciones para corregirlas.

10.4.1. Objetivos e indicadores

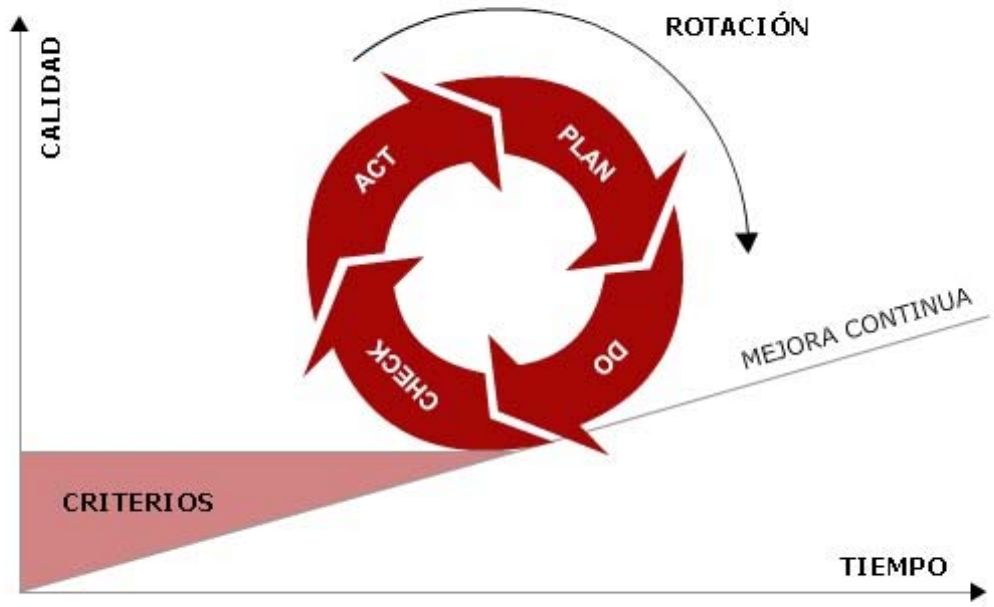

Figura 22. Objetivos e indicadores

La **mejora continua** es una actividad recurrente para aumentar la capacidad para cumplir los requisitos. Para poder medir esta mejora se establecen objetivos y se identifican oportunidades de mejora y, a su vez, estos objetivos para ser útiles, deben formularse de forma clara, inequívoca y mensurable.

Una vez establecidos los objetivos, se deberían establecer indicadores de rendimiento para medir el grado de cumplimiento de los objetivos. Los indicadores son la manera de medir los objetivos. La información se recogerá a partir de los registros del sistema reflejados en cada uno de los documentos, por ejemplo, logs de accesos, registros de incidencias, etc.

Se pueden establecer métricas en cuanto a cualquier parámetro relevante, por ejemplo la disponibilidad o la confidencialidad. Los valores de los parámetros que componen los objetivos (indicadores y métricas) tienen que recogerse de manera objetiva y regularmente para poder evaluar el progreso apropiadamente, por ejemplo:

- Objetivo: Aumentar un 20% la disponibilidad.
- Indicador: % de disponibilidad de los sistemas.
- Métricas: Nº de horas de parada/ Nº de horas de funcionamiento.

Los valores recogidos se van comparando en el tiempo con los objetivos marcados, para analizar las diferencias con los mismos y tomar las medidas oportunas cuando no se alcanzan.

Cuando la organización adquiere cierta experiencia en el manejo de métricas, puede encontrar útil desarrollar un cuadro de mando. Un cuadro de mando consiste en la gestión de un conjunto de indicadores que sean representativos del funcionamiento de la organización y sirvan para tomar decisiones al respecto. Estos indicadores tienen que cubrir los aspectos económicos de la organización (ventas, cuota de mercado, beneficios, etc.), los del cliente (satisfacción del cliente, valoración de servicios), el rendimiento de los procesos (costes internos, indicadores de seguridad, de calidad, de medioambiente) y por último indicadores sobre el aprendizaje y el crecimiento de la organización (formación, satisfacción del personal, indicadores de innovación).

11. GESTION DE CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad de negocio consta de varias tareas encaminadas a la obtención de un plan de continuidad eficaz y viable que permita a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. La manera de gestionar esta área tan delicada de la organización de detalla en este módulo, cuyos contenidos son:

- Qué es la continuidad del negocio.
- Gestionar la continuidad del negocio.

11.1. ¿QUÉ ES LA CONTINUIDAD DEL NEGOCIO?

La continuidad del negocio se define como la capacidad de una organización de reaccionar ante incidentes e interrupciones del negocio, de manera que sus procesos críticos no dejen de ejecutarse.

Gestionar la continuidad del negocio es el proceso de identificar las amenazas que pueden ocasionar interrupciones en la organización y planificar las acciones necesarias para que, si llegan a ocurrir, se minimice el impacto y se pueda llevar a cabo la recuperación de los procesos en un plazo determinado de tiempo.

La gestión de la continuidad del negocio es una pieza clave dentro de la gestión de la seguridad, ya que no contar con esta herramienta hace que la organización sea extremadamente vulnerable a incidentes graves. Carecer de la capacidad de recuperarse ante un evento de estas características, fuego, ataque terrorista, cortes de suministro, etc., puede tener consecuencias muy graves para la organización, pudiendo llegar a suponer la desaparición de la organización y su salida del mercado.

Por todo esto, los planes de continuidad de negocio ayudarán a las empresas a:

- Mantener el nivel de servicio en los límites definidos.
- Establecer un período de recuperación mínimo que garantice la continuidad de negocio.
- Recuperar la situación inicial antes de cualquier incidente de seguridad.
- Analizar los resultados y los motivos de los incidentes para aprender de ellos y evitar que se vuelvan a producir.
- Evitar que las actividades de la empresa se interrumpan o, en caso de hacerlo, que el tiempo de inactividad sea lo mínimo posible.

11.2. GESTIONAR LA CONTINUIDAD DEL NEGOCIO

Una gestión de la continuidad del negocio coherente se realiza también con un enfoque basado en el ciclo PDCA.

Planificar. Definir la política y los objetivos que se pretenden alcanzar, así como el alcance que se le va a dar los planes de continuidad del negocio. Realizar el Análisis de Impacto en el Negocio (conocido por sus siglas en inglés BIA “Business Impact Analysis”).

Hacer. Desarrollar los planes y procedimientos necesarios para ejecutar la política y los objetivos.

Comprobar. Revisar los resultados obtenidos y si se han cumplido los objetivos.

Actuar. Tomar las acciones necesarias para corregir las desviaciones detectadas en la fase anterior.

Figura 23. Ciclo de mantenimiento y mejora continua

En un proyecto de implantación de un SGSI según la Norma UNE/ISO-IEC 27001, hay que valorar la aplicación o no de cada uno de los controles relacionados con la continuidad del negocio, que conforman un grupo de cinco controles dentro de un único objetivo que se corresponde con los aspectos de seguridad de la información en la gestión de la continuidad de negocio.

Aunque no es obligatorio aplicar los cinco es muy difícil no hacerlo, ya que están tan directamente relacionados que no son realmente independientes unos de otros. Para hacer un plan de continuidad es necesario contar un análisis de impacto en el negocio (BIA) y es imprescindible probarlo, con lo cual ya tendremos estructurado un proceso de gestión de la continuidad.

11.2.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

En algunas organizaciones se cuenta con planes de continuidad parciales, como planes de contingencia para los sistemas de información o los planes de emergencia requeridos por la Ley. En este caso, se trata de que todos aquellos activos críticos identificados en el SGSI queden protegidos ante desastres. Es decir, incluir en el SGSI el proceso por el que se controla la continuidad del negocio en la organización.

Si no existe todavía, y se escoge este control, deberá crearse, normalmente definiendo el procedimiento que se va a seguir.

Un proceso de continuidad tendrá en cuenta los riesgos a los que están expuestos los procesos y activos críticos de la organización, si los controles preventivos son suficientes o hace falta aplicar más y contendrá los planes necesarios para afrontar casos de desastre.

11.2.2. Continuidad del negocio y evaluación de riesgos

Este control es la identificación de los eventos que provocan interrupciones en los procesos de negocio, así como la probabilidad y los efectos de dichas interrupciones y sus consecuencias con respecto a la seguridad de la información.

Para poder llevar a cabo una evaluación apropiada de las necesidades en continuidad del negocio debe formarse un grupo de trabajo. Este grupo debe estar liderado por un responsable del plan y formado por los líderes de las áreas que se desean cubrir con dicho plan.

La elaboración del Plan de Continuidad de Negocio (PCN) ha de desarrollarse con la continua supervisión por parte de la dirección ya que durante la elaboración y/o ejecución de éste, deberán comprometerse recursos y aprobarse procedimientos especiales que requieran un nivel de autorización superior.

Como primera tarea, el grupo de trabajo debe identificar cuáles son las funciones críticas de la organización, aquellos elementos de la organización o funciones que puedan ser críticos ante cualquier eventualidad o desastre, y jerarquizarlos por orden de importancia dentro de la organización. Aunque sea expresado crudamente, de lo que se trata es de dilucidar de qué vive la organización, cual es su fuente de ingresos determinando de esta manera los procesos críticos, que serán aquellos por los que la organización puede recibir estos ingresos.

Resulta evidente que la participación de varias o todas las áreas de la organización es la única manera de garantizar un nivel razonable de objetividad, puesto que si la participación es muy reducida es probable que los resultados sean sesgados y la información obtenida tenga poco valor.

Tras la concreción de cuáles son los procesos y activos a proteger y en qué orden de prioridad, se definen y documentan posibles escenarios que podrían suceder para cada elemento o función crítica. Hay multitud de escenarios que pueden considerarse. Pueden ser de problemas con el hardware (destrucción del CPD), problemas con el software (infección generalizada de virus), de telecomunicaciones (fallos de la conexión a Internet), de personal (falta de personal debida a una epidemia). También deben incluirse escenarios provocados por incendios, desastres naturales, y cualquier otro daño de origen físico que pudiera provocar la pérdida masiva de información.

La siguiente tarea es analizar, dentro de cada uno de estos escenarios, el impacto del desastre en cada función crítica (Business Impact Analisys, BIA). Este análisis es una de las principales fases del PCN, ya que permite identificar los riesgos asociados a las funciones críticas de la organización y el impacto en una escala de tiempos que producirían esos riesgos. Esta información permite establecer prioridades a la hora de plantear la estrategia de recuperación.

A la hora de realizar el BIA, se establecen prioridades como por ejemplo:

- Evitar pérdidas de vida.

- Reanudar las operaciones lo antes posible.
- Proteger el medio ambiente.
- Lograr las conexiones con los principales clientes y proveedores.
- Mantener la confianza en la empresa.

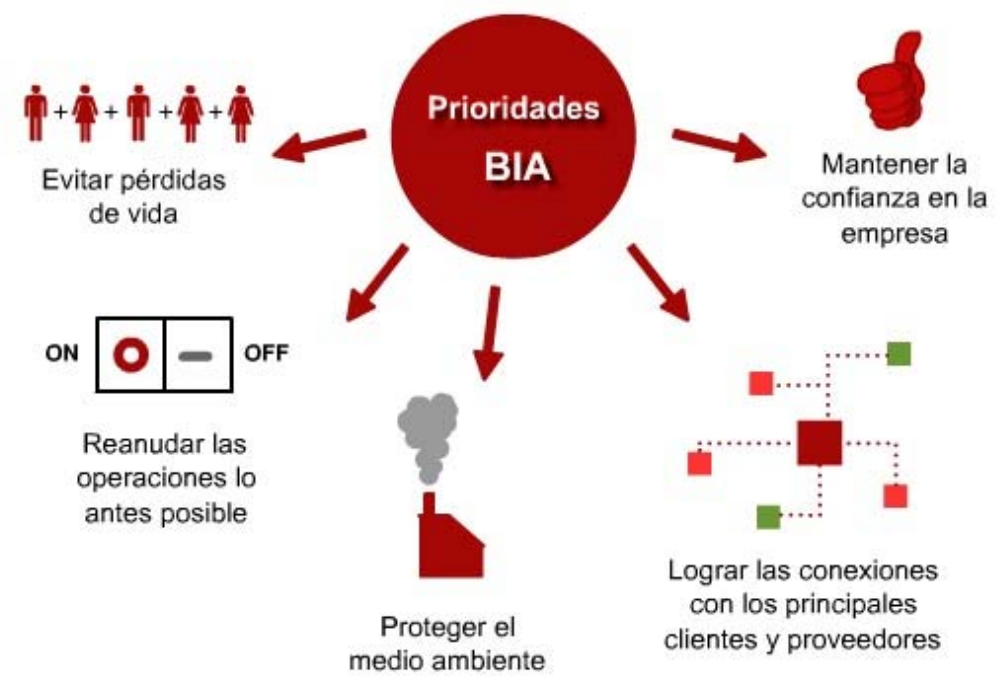

Figura 24. Prioridades del BIA

En resumen, se trata de un análisis de riesgos enfocado específicamente a valorar el impacto de incidentes que comprometen la continuidad del negocio teniendo en cuenta que este impacto será mayor cuanto más dure el incidente. Los pasos a seguir para realizarlo son los habituales de un análisis de riesgos:

- Se identifican los procesos críticos de negocio.
- Se identifican los eventos que pueden provocar interrupciones en los procesos de negocio de la organización, p. ej. fallos de los equipos, errores humanos, robos, incendios, desastres naturales y actos terroristas.
- Se evalúan los riesgos para determinar la probabilidad y los efectos de dichas interrupciones en cuanto a tiempo, escala de daños y período de recuperación. Por ejemplo, un corte de electricidad no tiene la misma repercusión si dura cinco minutos, que sería una incidencia

menor, que si dura cinco horas, que ya puede ser un trastorno o que si dura cinco días, que probablemente sea un problema muy serio. Evidentemente las soluciones a tomar serán distintas en función del impacto en el tiempo que supondría.

Los resultados de este análisis proporcionan la información necesaria, perfilando cuales son las necesidades de continuidad de la organización que se deben cubrir. De esta manera se cuenta con información sólida en la que basarse para decidir cuál tiene que ser la estrategia de continuidad de negocio, ya que quedarán en evidencia cuáles son los procesos más críticos y por qué, por lo que se pueden definir acciones apropiadas para recuperarlos al nivel que se considere aceptable.

Es importante definir los mínimos niveles de servicio aceptables para cada problema que se pueda plantear, ya que la complejidad de las soluciones y el consiguiente coste, quedarán determinados por hasta qué punto se van a restablecer las funciones y servicios. Es importante que dicho nivel se consensue con cada uno de los responsables de las áreas que puedan verse afectadas ya que son los que mejor conocen los diferentes procesos.

De esta manera será más fácil acotar las diferentes alternativas para solucionar cada uno de los problemas detectados y evaluarlas en función de la capacidad de la organización de implantarlas y mantenerlas. Las posibles soluciones para recuperar las actividades pasan por:

- La definición e implementación de procesos manuales, para suplir a los procesos automatizados mientras dura la incidencia.
- La contratación de tareas críticas a terceros, de manera que sean ellos los que garanticen el suministro del servicio o producto.
- Diferir las tareas críticas por un tiempo determinado.

Por ejemplo, si tenemos unas instalaciones situadas a la orilla de un río, para las que el análisis de impacto en el negocio ha arrojado un valor de riesgo alto para inundaciones, los problemas que una inundación presenta variarán en función de la duración y la severidad de la misma. En este sentido, por ejemplo, se ha determinado que si dura más de un día se mantendrá activo el proceso de comunicación con los clientes y el de correo electrónico interno al menos.

Teniendo en cuenta esta información, se presentan varias opciones que se podrán utilizar dependiendo del caso: realizar obras para contar con zonas protegidas y evitar daños en caso de inundaciones leves, transferir estos procesos críticos a otras ubicaciones o subcontratarlos, buscar ubicaciones alternativas para trabajar en caso de inundaciones graves, contar con proveedores de comunicaciones que puedan instalar unos servicios mínimos en otra ubicación o incluso en los domicilios de los empleados, etc.

El PCN debe incluir la composición del equipo de emergencias que será responsable poner en marcha el PCN cuando proceda y de organizar al resto del personal según lo definido para que la organización pueda recuperarse de un incidente.

11.2.3. Desarrollo e implantación de planes de continuidad.

Deben desarrollarse e implementarse planes para mantener o restaurar las actividades y garantizar la disponibilidad de la información en el nivel y la escala temporal requeridos después de una

interrupción o un fallo de los procesos críticos de negocio. Los planes de continuidad del negocio deberían incluir quienes son los responsables de cada tarea, cuales son las pérdidas tolerables de información y servicios y la identificación de los procedimientos que permitan la recuperación y restauración de las actividades.

Para elaborar este plan, se necesita la información recogida en el análisis de impacto en el negocio (BIA). Es necesario documentar el plan, que tendrá que incluir los objetivos, plazos, recursos asignados, costes estimados, responsables, método de seguimiento y plan de pruebas que se va a realizar para verificar que el plan es viable y correcto.

Es necesario que el plan sea validado por los responsables de las áreas involucradas. De igual manera hay que tener en cuenta las posibles consecuencias jurídicas que pudiesen derivarse de las actuaciones contempladas en él.

Un plan de continuidad contempla las siguientes fases:

- **Fase de Notificación ó Detección:** Debe instruirse al personal para que informen en caso de que detecten cualquier incidencia grave mediante un canal de comunicación claro y preciso.

- **Fase de activación:** El Responsable asignado para la tarea deberá valorar si la incidencia que ha sido reportada es motivo suficiente para activar el Plan de Continuidad.

  - Si no es necesario activar dicho plan, pueden tomarse acciones encaminadas a solventar la emergencia rápidamente, documentando qué se ha hecho y quien lo ha hecho.

  - En casos graves, puede ser necesario poner en marcha un **Plan de Emergencia**, que puede incluir un **Plan de Evacuación**.

  - Si no hay peligro para las personas, pero la incidencia es grave se pondrá en marcha el Plan de Continuidad.

Los criterios para decidir si la incidencia es grave o no deberán esta definidos de antemano. El Plan de Continuidad tiene que incluir instrucciones claras y precisas, y si es necesario la referencia a procedimientos relevantes, para que puedan ser ejecutadas sin dilación en cuanto se active.

Es muy importante aquí definir los canales de comunicación, quién debe informar a quién, quién está al cargo y las responsabilidades de cada uno. En particular es esencial que esté claro quién puede hablar con los medios de comunicación, ya que en casos de desastre, unas declaraciones poco afortunadas de alguien pueden dañar aún más la reputación de la organización.

En esta fase las acciones tienen como objetivo salir de la situación de emergencia lo antes posible y con los daños mínimos.

- **Fase de recuperación:** En esta fase se trata de volver a poner en funcionamiento los sistemas y servicios, en una ubicación alternativa si fuera necesario, y de reparar el daño que hayan sufrido en la ubicación original.

- **Fase de restablecimiento:** En esta fase se recogen las actividades necesarias para restaurar los sistemas y servicios en su ubicación original o en una nueva si no fuera posible volver a la anterior.

Una vez completado el plan, debe darse una formación adecuada para el personal sobre los procesos y procedimientos definidos para que todo el mundo esté coordinado y sepa cómo actuar en caso de incidencia.

11.2.4. Marco para la planificación de la continuidad del negocio

Se debería mantener un único marco de referencia para los planes de continuidad del negocio para asegurar que todos los planes son consistentes, para dirigir de una manera coherente los requisitos de seguridad de la información y para identificar prioridades para las pruebas y el mantenimiento.

Es decir, debe existir una **metodología** para la definición de los planes de continuidad de manera que haya homogeneidad en varios aspectos claves:

- Condiciones de activación de los planes de emergencia.
- Procedimientos de emergencia.
- Medios para evitar que la imagen de la empresa resulte dañada.
- Procedimientos de vuelta a la normalidad en el menor tiempo posible.
- La concienciación y formación del personal para que sea capaz de gestionar con eficacia estos planes de emergencia en caso de crisis.
- Un calendario de pruebas que garanticen la viabilidad de estos procedimientos.

11.2.5. Pruebas y mantenimiento de los planes de continuidad del negocio

Los planes de continuidad del negocio deberían probarse y actualizarse periódicamente para garantizar que están al día y que son efectivos.

Debe realizarse un calendario de pruebas, intentando que entorpezcan lo menos posible la operativa diaria.

La ejecución de las pruebas tiene como objetivos comprobar que:

- El personal sabe cuáles son sus tareas y está capacitado para realizarlas.
- El plan está completo, que no faltan datos o instrucciones.
- El plan es viable, que se puede realizar con los plazos y recursos asignados.
- El plan está actualizado.

Los resultados de las pruebas deben documentarse, de manera que el plan se pueda corregir o mejorar teniendo en cuenta lo que se ha detectado durante la realización de las pruebas.

Existen varias técnicas para la realización de pruebas. Se pueden realizar pruebas de sobremesa de varios escenarios, hacer simulaciones, pruebas de recuperación técnica, ensayos generales, etc. Hay que escoger para cada escenario la prueba o grupo de ellas más fáciles de llevar a cabo.

Por ejemplo, para el caso de un corte del suministro eléctrico y su impacto sobre un servidor, una prueba habitual es la comprobación del funcionamiento del SAI. Si se ha estipulado que el SAI mantenga alimentado el servidor durante 10 minutos y si el suministro eléctrico no se restablece en ese periodo que lo apague, se hace la prueba de cortar la electricidad durante varios periodos de tiempo para ver si el SAI se comporta como se espera. Si todo sucede según lo planificado, la prueba es satisfactoria y si no así, deben averiguarse la causa y solucionarlo.

Periódicamente el plan debe ser revisado para incluir aquellos cambios en la organización que puedan requerir ajustes en el mismo, o mejoras que se vayan diseñando. Por ejemplo, cambios en el organigrama que requieran de una modificación en las responsabilidades asignadas o cambios en la infraestructura de TI, una sustitución de un servidor obsoleto requerirá como mínimo de cambios en el inventario de activos, en los controles aplicados y en los datos que habrá que incluir en el plan para el contacto con los proveedores.

La respuesta de la recuperación será tan exitosa como la última prueba de recuperación efectuada, si la prueba no fue bien no se puede esperar que, si estamos frente a un incidente, vaya mejor, ya que en estas situaciones suelen también influir factores externos como el estrés y la presión que no ayudarán a mejorar la respuesta. Es por esto que es muy importante tener los planes bien probados y todo el personal conocedor de las acciones que tendrá que realizar, no dejando puntos abiertos a la improvisación.

12. PROCESO DE CERTIFICACIÓN

Una vez implantado el SGSI, con todo el trabajo que ello implica, puede darse el caso de que la organización decida mostrar sus logros a sus clientes, a sus proveedores, al público en general. Para ello lo que se hace es certificar el sistema.

En este módulo se hace un repaso de en qué consiste esta certificación, cómo se desarrolla y los beneficios que comporta. Los contenidos del módulo son:

- ¿Qué significa obtener la Certificación en la Norma UNE/ISO-IEC 27001?
- ¿Quién certifica?
- Proceso de certificación.

12.1. ¿QUÉ SIGNIFICA OBTENER LA NORMA UNE/ISO-IEC 27001?

Certificar un SGSI según la Norma UNE/ISO-IEC 27001 significa obtener un "Documento" que reconoce y avala la correcta adecuación del Sistema de Gestión de Seguridad de la Información conforme a esta norma de referencia.

Las motivaciones para intentar obtener la certificación provienen de muchas fuentes, y probablemente cada área de la organización tenga sus propios motivos para implicarse en una tarea de esta índole. El motivo más claro y generalizado es el prestigio que otorga una certificación a la organización, ya que es una evidencia clara y objetiva de que la gestión se está realizando de manera ordenada y eficaz, siguiendo buenas prácticas internacionales con el objetivo de ser cada día un poco mejores. Con la certificación se formaliza y acredita la buena gestión de la seguridad de la información.

Otros importantes motivos son mejorar la confianza de clientes y proveedores en los productos y servicios de la organización, el cumplimiento de objetivos empresariales o alimentar el proceso de mejora continua, proporcionar visibilidad al área de sistemas, e incluso servir de canal de comunicación entre esta área y el resto de la organización, que en ocasiones parecen existir ajenas las unas de las otras.

Lo que aporta la certificación es avalar la adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un SGSI según la Norma UNE/ISO-IEC 27001, siendo ésta la norma más importante que existe ahora mismo en cuanto a la implantación de controles que permitan establecer un marco de gestión de la seguridad de la información para las organizaciones.

La certificación aumenta el valor comercial de la organización siendo un factor de diferenciación en el mercado muy significativo, ya que el número de organizaciones certificadas según esta Norma todavía es muy reducido en comparación con la certificación en otras Normas de gestión que llevan muchos más años implantadas en el mercado.

Esta certificación va apareciendo como requisito o como aspecto que se valorará positivamente en pliegos de contratación pública y privada, ya que las grandes empresas y la administración van mejorando su gestión en esta área y una manera de asegurarse es exigiendo a sus proveedores que cuenten con un SGSI.

Es muy importante reseñar que certificar un SGSI no es certificar la seguridad de la organización ni las medidas de seguridad implantadas. Lo que se está certificando es la gestión de un sistema, en este caso de seguridad, es decir, cómo se está gestionando la seguridad de la información.

12.2. ¿QUIÉN CERTIFICA?

Pueden certificar las entidades de certificación acreditadas. En el caso de nuestro país, el organismo que acredita es ENAC (Entidad Nacional de Acreditación), que está designado por la Administración para establecer y mantener el sistema de acreditación a nivel nacional, de acuerdo a normas internacionales, siguiendo en todo momento las políticas y recomendaciones establecidas por la Unión Europea. En otros países existen organismos similares tales como UKAS en Gran Bretaña, COFRAC en Francia o JISC en Japón.

Las organizaciones que deseen suministrar servicios de certificación tienen que cumplir una serie de criterios para poder hacerlo, en este caso los recogidos en la Norma UNE/EN ISO/IEC 17021, Evaluación de la conformidad, que fija los requisitos para los organismos que realizan la auditoria y la certificación de sistemas de gestión. Esta norma recoge los requisitos en cuanto a competencia, coherencia e imparcialidad de las auditorías y la certificación de los sistemas de gestión de cualquier tipo y de las organizaciones que son proveedoras de estas actividades.

La acreditación es el procedimiento mediante el cual una entidad de acreditación reconoce formalmente que una organización es competente para la realización de una determinada actividad de evaluación de la conformidad. Las entidades de acreditación se encargan de verificar y evaluar los requisitos que deben cumplirse, y si es así, las organizaciones auditadas pasan a estar acreditadas para certificar y quedan registradas como tales en las entidades de acreditación.

La realización de las auditorías de un SGSI se rige por la Norma ISO/IEC 27006, que determina los requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información.

Cualquier empresa acreditada puede realizar auditorías de certificación dentro de su ámbito de actuación, es decir, una empresa acreditada por ENAC puede certificar en otros países y empresas acreditadas por UKAS o JISC pueden certificar aquí siempre y cuando así lo especifique en su certificado de acreditación, puesto que todas se rigen por los mismos principios y han sido acreditadas según los mismos criterios.

12.3. PROCESO DE CERTIFICACIÓN

El proceso de certificación se inicia mediante la petición de oferta a una entidad acreditada para que lleve a cabo la certificación.

Para la realización de la oferta y el cálculo del número de días de auditoría y auditores necesarios para llevar a cabo la certificación, normalmente la organización debe suministrar algunos datos a la entidad certificadora, que suele suministrar un cuestionario con la información que se necesita a la organización que ha pedido la oferta.

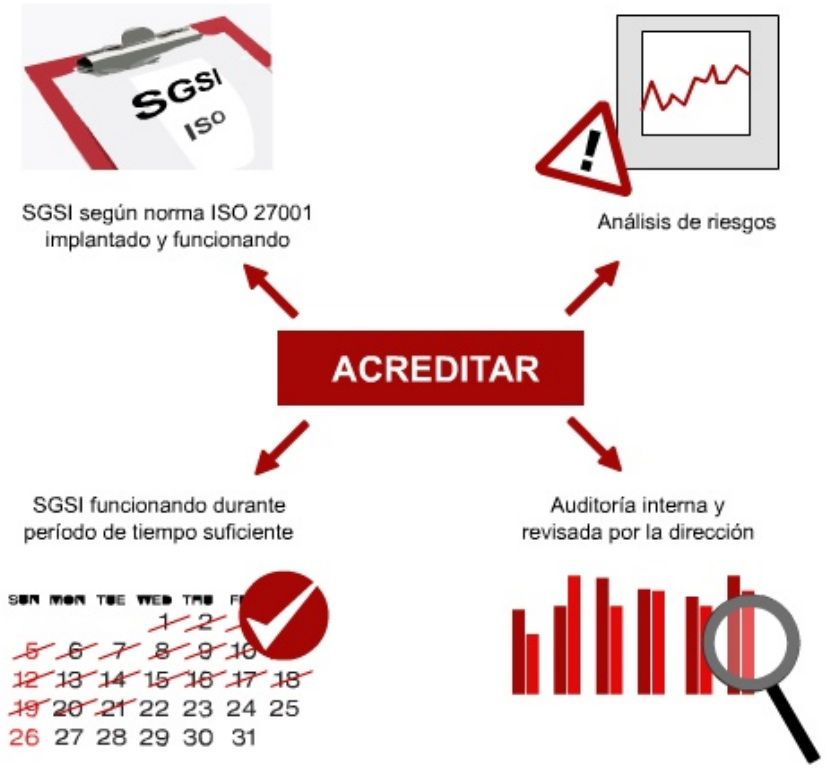

Figura 25. Proceso de certificación

El objetivo de ese cuestionario es que la organización acredite un cierto nivel de cumplimiento de la Norma. En particular es necesario contar con:

- Un SGSI según la norma ISO 27001 implantado y funcionando.
- El análisis de riesgos.
- Haber realizado la auditoría interna y la revisión por la dirección.
- Evidencias del funcionamiento del SGSI durante un período de tiempo suficiente para que el sistema esté probado.

Por supuesto, la organización debe contar con recursos económicos y personal de la empresa para atender a las demandas de la entidad de certificación.

Si la entidad certificadora considera que la organización está lista para afrontar una auditoría de certificación con ciertas garantías de éxito, se prepara y envía una oferta. En caso de que se acepte,

se pasa a planificar la auditoría de certificación. Esta auditoría es el requisito indispensable para acceder a la certificación y poder utilizar el sello de certificación junto al de la propia empresa

La duración de la auditoría de certificación depende fundamentalmente del número de personal que está dentro del alcance del SGSI y dura un mínimo de 5 días de auditoría para un alcance que incluya hasta 10 personas, aunque esta duración puede verse reducida a 3 días en función de las características del sistema a auditar y el contexto de la organización.

La auditoría suele constar de dos fases:

1. Fase 1. Durante esta fase, los auditores deben revisar la documentación del SGSI para comprobar si la organización cuenta con un sistema lo suficientemente maduro y completo como para superar la Fase 2. En esta fase los auditores repasan la política y el alcance del SGSI, el análisis de riesgos, la selección de controles y los procedimientos. Con los hallazgos que realicen, los auditores preparan un informe de la Fase I. En este informe se recogen las no conformidades halladas, con indicación de su gravedad. Hay tres clases de hallazgos:

    - Las no conformidades mayores, son aquellas que indican un incumplimiento de un requisito de la Norma o del mismo SGSI, y el auditor considera que pone en peligro la seguridad de la información de la organización. Estas no conformidades deben estar completamente resueltas antes de emprender la Fase 2.

    - Las no conformidades menores, son incumplimientos parciales o menores de la Norma o de alguna de las reglas internas. Estas no conformidades deben estar como mínimo en fase de resolución antes de llegar a la Fase 2.

    - Observaciones, u oportunidades de mejoras. Los auditores también pueden emitir observaciones encaminadas a mejorar el sistema, basadas en su experiencia y conocimientos. Estas observaciones no necesitan ser tratadas de momento, pero en sucesivas auditorías los auditores pueden revisar su estado y decidir que han pasado a ser no conformidades si la situación ha empeorado.

2. Fase 2. En esta fase los auditores deben confirmar que la organización cumple con sus políticas, objetivos y procedimientos y que el SGSI es eficaz. Para todo ello se realizaran pruebas de cumplimiento, es decir, se buscarán evidencias del cumplimiento de las normas establecidas por la organización, por ejemplo:

    - Prueba del Registro de los ficheros ante la Agencia Española de Protección de Datos, para verificar que se cumple con la LOPD.

    - Prueba de los controles de acceso implantados, para comprobar que se siguen los procedimientos de autenticación de la organización.

    - Revisión de los registros de incidencias, para comprobar cómo se gestionan.

Con las no conformidades halladas, los auditores preparan un nuevo informe. Las no conformidades menores no impiden obtener el certificado, pero deben abrirse acciones correctoras por parte de la organización para solucionarlas. En caso de que se detectara una no conformidad mayor, la entidad certificadora no otorgará el certificado. Por ejemplo que no se hubiera realizado un Proceso de Análisis y Gestión de Riesgos. También puede ocurrir que se estipule la realización de una auditoría extraordinaria para dar tiempo a que se solucione el problema.

Una vez superada la auditoría de certificación y en su caso, la auditoría extraordinaria, se obtiene el certificado, que es válido para 3 años, aunque está sujeto a la realización de una auditoria de seguimiento cada año. Es decir, anualmente los auditores realizarán una auditoría, menos exhaustiva que la de certificación y de duración más reducida, para comprobar que se siguen cumpliendo los requisitos.

Una vez pasados los 3 años, en los que se habrá realizado una auditoría de certificación y dos de seguimiento, se lleva a cabo la Auditoria de renovación, en la que de nuevo se audita el SGSI completo, y vuelve a comenzar el ciclo de tres años.