Seguridad y auditoría de la información

Guía de la asignatura

PID_00269892

Amadeu Albós Raya

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Amadeu Albós Raya

Ingeniero informático por la Universitat Oberta de Catalunya.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Helena Rifà (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

La irrupción de las tecnologías de la información y la comunicación (TIC) en todos los ámbitos de la vida cotidiana y el volumen de datos, información y conocimiento que se ha derivado de este hecho han provocado que la seguridad de la información se haya convertido en un factor de especial importancia tanto en el ámbito personal como en el profesional.

Si bien las problemáticas de seguridad son diferentes en cada entorno por su propia idiosincrasia, sí que presentan aspectos comunes que es imprescindible conocer para protegerse adecuadamente de los riesgos y prevenir posibles incidentes.

La seguridad de la información va más allá de la simple definición de *confianza* en el conjunto ordenado de datos. El alcance de este término es bastante más amplio e incluye medidas tanto preventivas como reactivas en las organizaciones y los sistemas informáticos, que deben permitir salvaguardar y proteger la información garantizando sus principios básicos de seguridad y privacidad de conformidad con la Ley general de protección de datos (LGPD).

En esta asignatura nos centraremos en todos aquellos aspectos que facilitan trabajar y transferir la información de manera segura y de acuerdo con la LGPD. Haremos un repaso de las tecnologías y metodologías que deben permitir gestionar y controlar que la información se mantiene de manera segura dentro de los parámetros fijados por la organización, y también cómo el establecimiento de políticas y la realización de auditorías ayudan al buen gobierno de la seguridad. Plasmaremos así los dos ejes principales de la asignatura: la planificación y la implantación, por un lado, y la auditoría y el análisis, por otro.

Objetivos

Los objetivos principales que se quieren lograr con esta asignatura son los siguientes:

1. Conocer los conceptos generales que se aplican a la seguridad de la información.

2. Conocer los sistemas de información y entender los mecanismos de seguridad principales para protegerlos y detectar incidentes.

3. Conocer los procesos de implantación y de auditoría de la seguridad de la información, así como las normativas y los estándares.

4. Conocer los mecanismos de gobierno de la seguridad dentro de la organización.

1. Seguridad, privacidad y protección de la información

1.1. Presentación

De un tiempo a esta parte, el mundo de las comunicaciones vive una revolución en prácticamente todos los ámbitos. La cantidad de datos que se generan, transfieren y procesan hoy en día no para de crecer y genera la necesidad de dar el valor y la protección que corresponde a la información que resulta de ello.

Más allá del cumplimiento legal en cuanto a la recogida y al tratamiento de datos, la información también puede presentar características de privacidad, sensibilidad o restricción en determinados contextos, lo que la puede poner en el punto de mira de los atacantes, ya sea para conseguirla, modificarla o destruirla.

La progresión de los riesgos y de las amenazas que afectan a los sistemas de información y, por extensión, de los contenidos que estos procesan, no hacen sino justificar la necesidad de establecer mecanismos de protección para minimizar el impacto y las posibles consecuencias para la organización en caso de que se produzca un incidente de seguridad.

1.2. Objetivos

Los objetivos que se pretenden lograr son los siguientes:

- Conocer el valor de la información y la necesidad de protegerla en contextos determinados.
- Conocer las implicaciones de romper la cadena de seguridad de la información.
- Identificar contextos con requisitos de seguridad de la información.
- Conocer el estado actual de los ataques informáticos a escala mundial.
- Identificar el papel de la tecnología en la evolución de la ciberdelincuencia.

1.3. Contenidos

Los contenidos que se desarrollarán son los siguientes:

- Concepto de información, flujo y ciclo de vida de la información.
- Propiedades de seguridad de la información: confidencialidad, integridad y disponibilidad.
- Legislación en torno a la privacidad de la información.

- Medidas básicas de seguridad informática.

1.4. Guía de estudio

El tratamiento de datos es una realidad que hace mucho tiempo que está presente en nuestra sociedad, pero con la informatización de casi todas las situaciones de la vida cotidiana dicho tratamiento ha dado un importante paso hacia adelante.

El concepto de **información** como resultado del procesamiento de datos es esencial para comprender la ayuda que ofrecen las tecnologías de la información y la comunicación. En este sentido, tanto el contexto de interpretación de los datos como las características de utilidad, relevancia, interpretación y percepción que deben presentar son básicos para entender que **la información es todo aquello que reduce la incertidumbre**.

Figura 1. El proceso de los datos (contexto, interpretación, etc.)

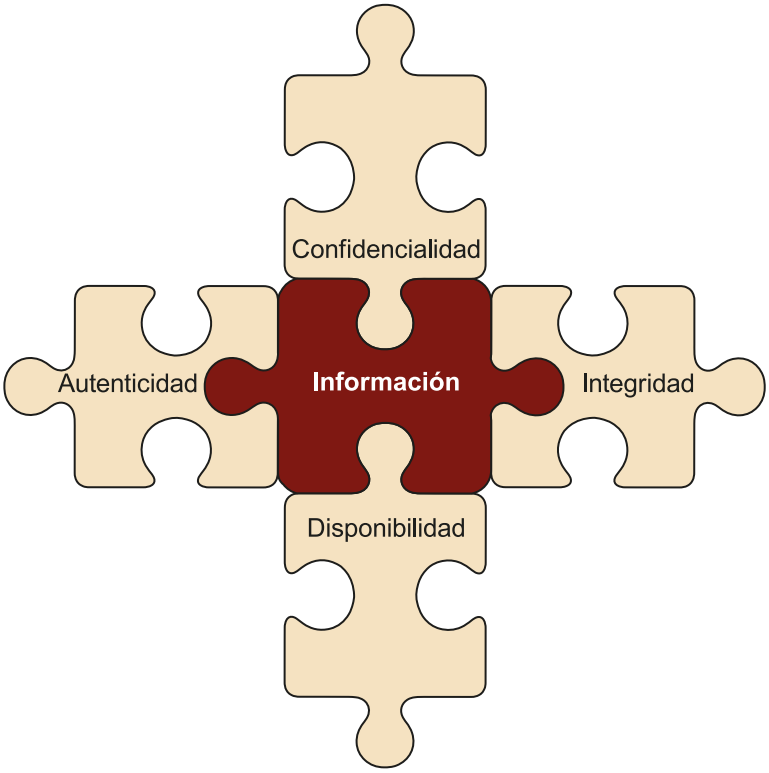
De hecho, hoy en día, la información es un recurso estratégico para cualquier organización. Gracias a la información se puede conocer el estado de las entidades a las que hace referencia, se pueden tomar decisiones adecuadas y coherentes con este estado o incluso se puede obtener conocimiento con el procesamiento masivo de diversos tipos de información, lo que resulta fundamental en la estrategia de cualquier organización.

Pero hay informaciones de muchos tipos y no todas requieren la misma consideración. Los **flujos de información** que posee la organización serán uno de los puntos de partida para valorar cuál es la información que trata una organización, qué valor tiene y cómo de necesario es protegerla ante situaciones diversas (por ejemplo, la pérdida, la exposición o el robo de datos). Valorar estos aspectos nos hará otorgar significado, importancia, vigencia y validez a la información para así poder determinar con exactitud qué implicaciones tiene esta para la organización.

El **sistema de información** es el apoyo por excelencia a la hora de procesar los datos. Su digitalización no solo facilita el tratamiento, sino que el coste de la copia, la modificación o la transmisión es ínfimo en términos absolutos, lo que por sí mismo ya supone un riesgo si no se mantiene bajo control.

De hecho, las **propiedades de seguridad de la información**, esto es, la **confidencialidad**, la **integridad** y la **disponibilidad** (adicionalmente también la **autenticidad**) se deben poder garantizar en cualquier circunstancia, tanto si la información se está transfiriendo, como si está almacenada o en tratamiento.

Figura 2. Propiedades de seguridad de la información: confidencialidad, integridad, disponibilidad (y autenticidad)



En este sentido, la normativa ISO/IEC 27000 tiene como objetivo establecer un marco de apoyo y de buenas prácticas para desarrollar un **sistema de gestión de la seguridad de la información** (SGSI) que permita garantizar su seguridad, reducir los riesgos inherentes a su tratamiento, ahorrar costes orientando y complementando correctamente las medidas, garantizar la gestión activa de la seguridad y cumplir con la legislación vigente. Todo esto permitirá sustentar tanto la seguridad técnica como la jurídica de dicha información.

Esto implica, además, que la seguridad de la información no es un resultado, sino un proceso iterativo ordenado en fases de **planificación**, **implantación**, **verificación** y **actuación** (PDCA, de la sigla en inglés de *plan, do, check, act*). Como se señala en la Ley general de protección de datos (LGPD) y en el Reglamento general de protección de datos (RGPD), el enfoque sobre los riesgos y la responsabilidad proactiva son los ejes principales para garantizar la seguridad de la información.

Este planteamiento requiere el **análisis previo** de la organización antes de establecer **controles físicos**, **técnicos** y **organizativos**. Algunos de los controles más habituales son los siguientes:

- las copias de seguridad,
- el control de acceso a la información,
- las limitaciones en la utilización de aplicaciones,
- el control de los dispositivos externos,
- el cifrado de datos,
- los protocolos de eliminación de información, o
- el control de la contratación de servicios en la nube.

1.5. Materiales

Los materiales de estudio de esta actividad son los siguientes:

- Seguridad y auditoría de la información.
- Protección de la información (https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf).

2. Fundamentos de seguridad informática

2.1. Presentación

La simplicidad, la inmediatez y la ubicuidad con las que hoy en día se pueden explotar las tecnologías de la información y la comunicación son, sin ningún tipo de duda, una parte de los factores que han llevado a su omnipresencia actual.

Pero esta accesibilidad de los servicios a todos los públicos esconde la complejidad de muchas soluciones técnicas y la transmisión constante de todo tipo de información en todas direcciones, realidades que ponen de manifiesto la necesidad de combinar varias medidas para asegurar que el sistema de información garantiza las propiedades de seguridad en toda circunstancia, desde los aspectos físicos y arquitecturales del sistema hasta la transmisión de datos y la explotación de los servicios por parte de los usuarios.

De hecho, todas estas medidas de seguridad van encaminadas a proteger el sistema de la multitud de riesgos y amenazas a las que está sometido, y a minimizar el impacto que puedan tener los ataques o incidentes de seguridad, en caso de que se produzcan.

2.2. Objetivos

Los objetivos que se pretenden lograr son los siguientes:

- Conocer los mecanismos de seguridad informática más habituales.
- Conocer los mecanismos de cifrado más utilizados en la actualidad.
- Identificar la complementariedad de los diferentes mecanismos de seguridad.
- Identificar contextos de aplicación de cifrado como elemento de seguridad.
- Comprender la evolución de la seguridad informática y la necesidad de actualización.

2.3. Contenidos

Los contenidos que se desarrollarán son los siguientes:

- El sistema de información, los componentes y el funcionamiento.
- La seguridad física y perimetral de los sistemas de información.

- La seguridad de los servicios y las comunicaciones de los sistemas de información.

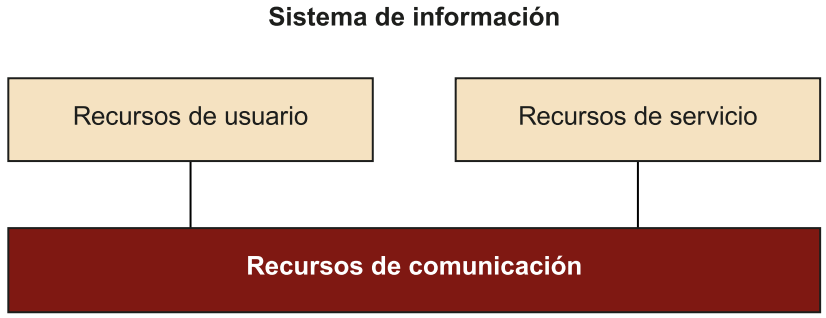
2.4. Guía de estudio

Si bien no es estrictamente necesario utilizar la tecnología para procesar los datos, hoy en día difícilmente se puede prescindir de ella para realizar cualquier tarea, por simple que esta sea.

El **sistema de información** representa la base para el tratamiento de información y está formado por la combinación coherente de recursos humanos, materiales y lógicos. Estos recursos se estructuran funcionalmente en **infraestructura**, **servicios** y **comunicaciones**.

Los recursos de usuario, de servicios y de comunicaciones son los componentes esenciales de su infraestructura y permiten realizar las tareas, comunicar los nodos y explotar los servicios, ya sean locales, remotos o híbridos, que son los que combinan ambas características.

Figura 3. La infraestructura del sistema de información está formada por recursos de usuario, de servicio y de comunicaciones

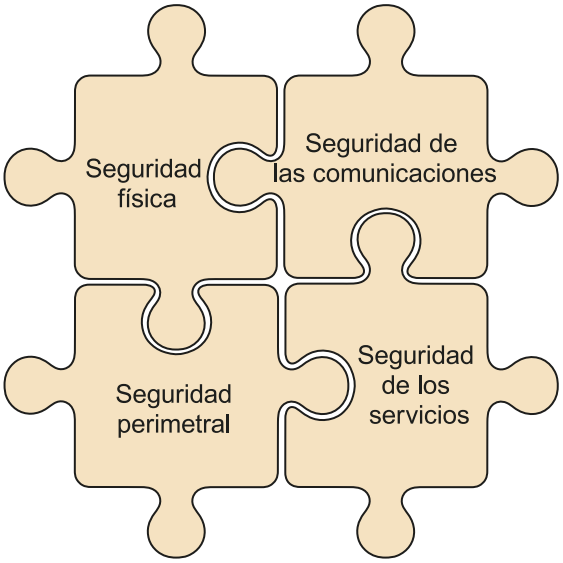


Todos estos componentes deben estar integrados perfectamente en el sistema de información para cumplir estos objetivos, lo que requiere un **diseño** y una **operativa** bien definida. En cuanto a la **infraestructura**, los segmentos de red cableada e inalámbrica y el direccionamiento físico y lógico de los nodos se complementan con protocolos de asignación de direcciones y de resolución de nombres para completar su funcionamiento. Por otro lado, los **servicios**, el diseño y la operativa se fundamentan en paradigmas de comunicación y protocolos de conexión que garantizan el intercambio correcto de datos entre los extremos, lo que supone estandarizar tanto el acceso como la comunicación del servicio.

La seguridad del sistema requiere asegurar todos los componentes anteriores, pero también debe hacer frente a la evolución imparable de la tecnología y de los requisitos de las organizaciones, así como a unos riesgos y amenazas que no dejan de crecer cada día.

La seguridad del sistema debe empezar por la **protección física** de los recursos contra accesos indebidos, riesgos naturales o el fallo de cualquiera de los soportes, sin olvidar que cada recurso de la infraestructura necesitará la protección adecuada de acuerdo con las características que posea y la función que realice.

Figura 4. La seguridad del sistema de información se basa en la seguridad física, perimetral, de los servicios y de las comunicaciones



En este sentido, los **recursos de usuario** deben garantizar que no suponen un riesgo de seguridad para el sistema, tanto desde el punto de vista de la configuración como de su utilización por parte del usuario. Los **recursos de servicios** necesitan garantías de funcionamiento tanto del hardware como del software, sin perder de vista que tienen acceso directo a la información que almacenan (aunque esta puede estar ubicada en otros recursos). Finalmente, los **recursos de comunicación** pueden presentar problemas de funcionamiento físico, pero también requieren que la configuración sea segura. Un caso especial de dispositivos es la internet de las cosas, que por su propia casuística puede requerir actuaciones específicas tanto desde el punto de vista funcional como desde el operativo.

Todos los recursos del sistema se comunican a través de una **red informática** que expone tanto los dispositivos conectados como la información que circula a través de ellos, por lo que se requieren medidas determinadas para garantizar su seguridad, como, por ejemplo:

- la segmentación de la red (sea esta física o virtual) para aislar zonas con requisitos de seguridad específicos,

- la parametrización de las redes inalámbricas,

- la implantación de cortafuegos que garanticen el filtrado de las comunicaciones con internet,

- las redes privadas virtuales para conectar al sistema todos aquellos usuarios y sistemas remotos de manera segura,

- el uso de herramientas de detección y protección contra intrusos para monitorizar el sistema y controlar los posibles ataques, o

- la creación de zonas desmilitarizadas para publicar servicios en internet con garantías de seguridad tanto para estos servicios como para el sistema local.

La implementación de medidas de seguridad de infraestructura no debe olvidar la necesidad de asegurar los **servicios** y las **comunicaciones** que operan en ella, procesando una información que debe mantener las propiedades de seguridad con mecanismos concretos:

- la **confidencialidad** se garantiza por medio del cifrado de clave privada o pública, esta última con la ayuda de la infraestructura de clave pública y las autoridades de certificación,

- la **integridad** se verifica con funciones resumen de los datos y se puede aplicar tanto al contenido como a la fuente de los datos, y

- la **disponibilidad** se garantiza sobre todo con medidas de infraestructura, pero también con la implantación de políticas y controles de autorización.

Buena parte de las medidas de seguridad se basan en garantizar que la acción que realiza cada usuario es legítima, lo que requiere un proceso de **autenticación del usuario**, que puede estar basado en la combinación de múltiples factores que el usuario conoce o posee (de hecho, cuanto más factores exija el sistema, más garantías obtendrá de la identidad del usuario). Pero no es suficiente saber quién es el usuario que interactúa con el sistema, hace falta además un proceso de **autorización del usuario** para poder realizar las acciones que pretende llevar a cabo, porque no todos los usuarios deben poder realizar las mismas tareas o acceder a la misma información. Los **gestores de identidad** permiten centralizar estas funciones de autenticación y de autorización del sistema, además de otras funciones de gestión y administración.

Por su parte, las soluciones que prestan las funcionalidades de los **servicios** deben ser robustas, verificadas y proceder de proveedores contrastados, de manera que incorporen las medidas de seguridad actuales y no presenten vulnerabilidades.

No se puede completar este escenario sin garantizar que las **comunicaciones** cierren la cadena de seguridad entre los extremos (por defecto, los datos viajan por la red en claro, sin cifrar), puesto que pueden ser el objeto de ataques pasivos (escucha de comunicaciones) y activos (denegación de servicio, interceptación de datos, etc.). El **cifrado** permite garantizar la confidencialidad y la integridad de los datos transmitidos (no así la disponibilidad, que se debe asegurar sobre todo con medios de infraestructura) gracias a protocolos como el *transport layer security* (TLS), uno de los más utilizados para incorporar funciones de seguridad en todo tipo de protocolos (por ejemplo, en la mayoría de protocolos de aplicación del modelo TCP/IP).

Como en todo sistema de información, el **usuario** es un factor clave para completar las medidas de seguridad implantadas, y la mejor forma de integrarlo es mediante la formación y la promoción de una cultura en torno a la seguridad de la información. Este planteamiento también ayuda a asegurar los contenidos de los documentos o mensajes con los que dicho usuario trabaja a diario, utilizando los mecanismos de cifrado, firma digital o incluso la esteganografía.

2.5. Materiales

Los materiales de estudio de esta actividad son los siguientes:

- Fundamentos de seguridad informática.

3. Gestión y auditoría de la seguridad de la información

3.1. Presentación

Hoy en día es relativamente fácil implementar mecanismos de seguridad, dada la diversidad de soluciones que ofrece el mercado, pero, como en otros aspectos de la informática, no tiene sentido la implantación de medidas si no se hace antes un proceso metódico que formalice desde la identificación de necesidades hasta la revisión periódica.

La normativa ISO/IEC 27000 (y siguientes) estructura la comprensión, el planteamiento y el despliegue de los mecanismos de seguridad de manera lógica y ordenada, así como también la revisión, la comprobación y la auditoría de todos estos elementos para verificar que son coherentes con la estrategia definida y actúan de acuerdo con las previsiones.

En este sentido, todas las actuaciones en materia de seguridad informática se materializan en el sistema de gestión de la seguridad de la información (SGSI), que es el medio para garantizar la seguridad de la información de la organización.

3.2. Objetivos

Los objetivos que se pretenden lograr son los siguientes:

- Conocer la normativa ISO/IEC 27000 y su aplicabilidad.
- Conocer el proceso de auditoría de la seguridad en las organizaciones.
- Cohesionar aspectos normativos y de auditoría en contextos determinados.

3.3. Contenidos

Los contenidos que se desarrollarán son los siguientes:

- La normativa ISO/IEC 27000, características, estructura y ciclo de vida.
- La auditoría de seguridad de la información, principios, características y proceso.

3.4. Guía de estudio

En ocasiones se puede tener la impresión de que la implantación (o incluso la actualización o la mejora) de una solución de seguridad es suficiente para proteger la organización. Esta visión de la seguridad como un producto donde la simple instalación resuelve una problemática (como lo haría una solución de ofimática o una herramienta de cooperación) no se ajusta a la realidad.

La seguridad de la información no es un producto, sino un proceso, y el **SGSI** aporta un enfoque sistemático para enfrentarse al reto de asegurar la información en todo tipo de organizaciones.

La familia de estándares ISO/IEC 27000 son un conjunto de normativas que pretenden dar un marco conceptual, metódico, estructurado y práctico para implantar un SGSI en una organización. En especial, el estándar **ISO/IEC 27002** es una guía de buenas prácticas del sector para desarrollar normas de seguridad, prácticas de gestión y la confianza en la relación con terceros.

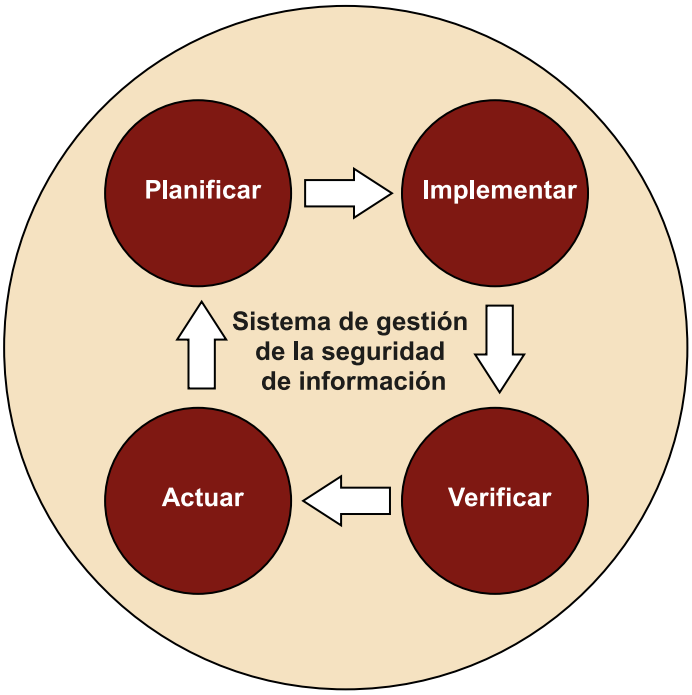
Uno de los aspectos relevantes de la norma ISO/IEC 27002 son los **dominios de seguridad**, que recogen los objetivos de control y los controles de seguridad que se deben aplicar para lograr el objetivo definido. Por ejemplo, hay dominios para la seguridad física y del entorno, para la gestión de incidentes, para el control de acceso o para la gestión de la continuidad del negocio (entre muchos otros). Cabe tener en cuenta que la implementación de la norma requiere la aplicación de la legislación en vigor por un lado y la contextualización con la organización en la que se implanta, por otro.

Los **principios de un SGSI** se basan en los siguientes aspectos:

- Definir una política general que enmarcará todas las actuaciones.
- Planificar la seguridad necesaria para la organización (desde la identificación de los requisitos hasta la preparación de los planes).
- Implantar y operar todos los elementos de seguridad del sistema.
- Analizar el rendimiento con la monitorización y las auditorías para detectar disfunciones.
- Establecer mejoras (preventivas, correctivas o continuas).
- Revisar el sistema para asegurar la adecuación y el cumplimiento de los objetivos.

Todas estas fases del SGSI son una aplicación del ciclo de Deming al área de seguridad, que consiste en un ciclo iterativo de planificación (*plan*), implementación (*do*), verificación (*check*) y actuación (*act*).

Figura 5. Ciclo de Deming aplicado a la seguridad de la información (*plan, do, check, act*)



De este modo, el SGSI permite lograr un conjunto de beneficios concretos:

- Obtener una visión única de la seguridad en la organización.
- La implicación de los actores que intervienen en la seguridad.
- La gestión global y activa de manera que se unifica la implementación de la seguridad.
- El control y seguimiento con la realización de auditorías.
- La mejora continua de todos los elementos de la cadena de seguridad a partir de las disfunciones detectadas.
- La optimización de recursos para garantizar la complementariedad de las medidas implantadas.

Como se puede ver, el **proceso de auditoría** es esencial para completar el ciclo de mejora de la seguridad, ya sea para el cumplimiento de la legalidad, para el control de algunos aspectos específicos o para la revisión de la conformidad con las buenas prácticas del sector. Para que sea plenamente efectiva, la auditoría se debe ceñir a unos principios de integridad y profesionalidad, así como también de presentación justa e imparcial. Para conseguirlo, la auditoría debe ser independiente de la organización, debe estar enfocada plenamente en la busca de pruebas o evidencias que demuestren la realidad y guardar la confidencialidad de los resultados obtenidos.

Hay varios tipos de auditorías, si bien la diferenciación más extendida es entre interna y externa. La **auditoría interna** puede ser realizada por la propia organización o por un proveedor de servicios de consultoría, y la **auditoría externa** siempre será realizada por un organismo externo (y diferente, si procede, del proveedor de servicios de consultoría que se pueda tener contratado).

La realización de auditorías busca la conformidad del sistema, el cumplimiento de la legislación, la eficacia de las medidas implantadas y la detección de áreas de mejora. Para lograr estos objetivos, ha de establecerse un **programa** o un **ciclo de auditoría**, de manera que la continuidad lleve a una mejora constante y sostenible a lo largo del tiempo.

Realizar el proceso de auditoría supone desde la planificación previa de los aspectos que se deben revisar hasta el seguimiento de la corrección (o mejora) de las no conformidades actuales, pasando por el trabajo de campo centrado en la realización de pruebas y obtención de evidencias, y en la realización del informe que contrasta el planteamiento con las evidencias encontradas.

Seguramente, el trabajo de campo y la obtención de evidencias son los aspectos más destacables del proceso de auditoría. El primero porque se centra en la realización de pruebas de cumplimiento de los controles, y el segundo porque determina con resultados fiables si la realidad de la seguridad de la información coincide con la prevista, lo que conducirá a los resultados de la auditoría en forma de conformidades, no conformidades, observaciones o posibilidades de mejora.

3.5. Materiales

Los materiales de estudio de esta actividad son los siguientes:

- Implantación de un sistema de gestión de la seguridad de la información (hasta el sexto apartado, incluido).
- Introducción a la auditoría TIC y de seguridad TIC (apartados del 1 al 4, ambos incluidos).

4. Gobierno de la seguridad

4.1. Presentación

La seguridad de la información, como cualquier otro proceso, requiere la estructuración de las funciones y la asignación de los recursos necesarios para cumplir con los objetivos. Esta necesidad no tiene una única respuesta, ya que las organizaciones pueden presentar diversas características, y se deberá valorar la idiosincrasia de cada una de ellas para encontrar el planteamiento que más se adapte a cada caso.

Como en otras áreas, también existen modelos de gestión, normativas y estándares que facilitan el análisis, el diseño, la implantación, la auditoría y la mejora continua de la seguridad de la información en una organización. Además de retomar las buenas prácticas del sector materializadas en modelos y normativas, el buen gobierno de la seguridad también puede recibir el apoyo de consultores y profesionales especializados en la materia, así como de los organismos de control de emergencias de seguridad.

4.2. Objetivos

Los objetivos que se pretenden lograr son los siguientes:

- Comprender los modelos, las normas y los organismos de apoyo que enmarcan la seguridad de la información.
- Justificar el planteamiento y la implantación de políticas de seguridad de la información.
- Desarrollar el buen gobierno de la seguridad de la información a través de políticas coherentes y cohesionadas.

4.3. Contenidos

Los contenidos que se desarrollarán son los siguientes:

- Modelos y estándares de gestión de la seguridad, organismos externos de apoyo.
- Implementación del SGSI.
- El gobierno de la seguridad a través del desarrollo de políticas de seguridad.

4.4. Guía de estudio

La gestión de la seguridad en una organización comporta un gran número de tareas que combinan aspectos técnicos, organizativos y jurídicos. Si bien inicialmente se pueden priorizar algunas de estas tareas, con el paso del tiempo habrá que dedicar esfuerzos para cumplirlas todas.

Se puede afrontar la gestión de la seguridad bajo varias perspectivas o modelos de gestión. La **gestión** puede ser **interna** cuando el personal de la organización realiza las tareas, **externa** cuando se externaliza el proceso como servicio, o **mixta** si la realización de las tareas se reparte entre el personal interno y un servicio subcontratado.

En cualquier caso, la gestión de la seguridad deberá iniciarse considerando los siguientes aspectos:

- El objeto de negocio de la organización para facilitar la contextualización.
- La situación inicial de la organización para valorar el estado y la eficiencia de las medidas implementadas.
- El análisis de riesgos para poder identificar los riesgos a los que pueden estar expuestas tanto la organización como la información que esta gestiona.
- El cumplimiento de la legalidad vigente que afecta directamente a la organización (ya sea general, sectorial, etc.).

Con estos resultados se podrán identificar las medidas que permitirán mitigar, controlar o eliminar los riesgos de seguridad a los que debe hacer frente la organización. Estos **controles de seguridad** se pueden organizar de acuerdo con la **naturaleza** (controles técnicos y organizativos), la **actuación** (reducción de la probabilidad o del impacto) o la **finalidad** (controles preventivo, de detección, correctivo o de monitorización).

Las **normativas** pueden servir de guía y de apoyo para enmarcar todas estas tareas en torno a la seguridad de la información; por ejemplo, la ISO/IEC 27001 (requisitos de sistemas de gestión de la seguridad de la información) y la ISO/IEC 27002 (código de buenas prácticas). Pero hay muchas otras, entre las que destacan ITIL (Information Technology Infrastructure Library), CMM (Capability Maturity Model) o SSE-CMM (System Security Engineering Capability Maturity Model). Se trata de herramientas que no solo se pueden utilizar para la gestión de la seguridad, sino también para la gestión general de las tecnologías de la información y la comunicación en las organizaciones.

Además del marco que ofrecen estas normativas, la gestión de la seguridad también puede tener el apoyo de organismos externos que centralizan el estado real de la seguridad a escala global y pueden ofrecer soluciones para gestionar las incidencias eventuales, como, por ejemplo, el INTECO (Instituto Nacional de Tecnologías de la Comunicación, S. A.) a través del CERT (Computer

Emergency Response Team). Otras entidades pueden ayudar a obtener certificaciones de seguridad que garanticen la conformidad de la seguridad de la organización con respecto a alguna normativa concreta.

De una forma u otra, el desarrollo de un SGSI en la organización requiere un desarrollo por etapas:

- La **planificación**, donde se definen las políticas generales de seguridad, el alcance, el análisis de riesgos y la selección de controles (entre otros aspectos).
- La **implementación**, donde se ejecuta la implantación de todas las actuaciones previstas (especialmente de los controles) y se seleccionan los indicadores de actividad.
- La **verificación**, donde se monitoriza el estado del sistema y se realizan los controles de seguimiento y las auditorías.
- La **actuación**, donde se implantan las mejoras y se ejecutan todas las acciones preventivas y correctivas que se han detectado.

Todo este desarrollo suele tomar forma documental considerando los principios del SGSI, la metodología seguida, la declaración de aplicabilidad del sistema, las políticas de seguridad de alto nivel, el plan de continuidad del negocio, los procedimientos realizados y los registros que se obtendrán (incluidas las auditorías).

Figura 6. El gobierno de la seguridad de la información se fundamenta en la planificación y la implantación de medidas de seguridad, así como en la auditoría y el análisis del cumplimiento real

De hecho, el gobierno de la seguridad de la información (y de las tecnologías de la información y la comunicación en general) se materializa con la planificación y la implantación de las medidas correspondientes, así como con el control y la auditoría.

Esto es así porque la organización debe hacer frente a los requisitos legales de seguridad, al crecimiento del capital intelectual y a la necesidad de alinear el sistema de información con los objetivos estratégicos de la organización, pero también debido a la proliferación de unas amenazas contra la seguridad que cada vez son más numerosas y sofisticadas.

Por lo tanto, la eficacia del gobierno será una realidad cuando las tecnologías de la información y la comunicación hayan sido bien planificadas y gestionadas y adecuadamente monitorizadas, lo que implica necesariamente la auditoría periódica, tanto de la seguridad del sistema de información como del proceso de gestión de la seguridad de la información.

4.5. Materiales

Los materiales de estudio de esta actividad son los siguientes:

- Introducción a la seguridad de la información (apartados 3, 5, 6 y 7).
- Introducción a la auditoría TIC y de seguridad TIC (apartados 6 y 7).
- Implantación de un sistema de gestión de la seguridad de la información (apartados del 7 al 11, ambos incluidos).

Bibliografía

Albós, A. (2019). *Fonaments de seguretat informàtica*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Codolà, S. *Seguridad y auditoría de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Estevan, R. *Introducción a la auditoría TIC y de seguridad TIC*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Introducción a la seguridad de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Implantación de un sistema de gestión de la seguridad de la información (SGSI)*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

INCIBE (2018). *Protección de la información*. Instituto Nacional de Ciberseguridad. («Protege tu empresa»). <http://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf>