Seguridad y auditoría de la información. Guía de la asignatura

PID_00252499

Santiago Codolà Vilahur

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

Introducción

Con la irrupción de las TIC en todos los ámbitos de la vida cotidiana, y el volumen de datos, información y conocimiento que se ha derivado de ello, la seguridad de la información se ha convertido en un factor de suma importancia tanto en los negocios como en el ámbito personal.

Aunque las problemáticas de seguridad son diferentes en cada entorno, sí que tienen muchas cosas en común, y es fundamental conocer los distintos aspectos que la componen a fin de poder prevenir y protegerse adecuadamente.

La idea de *seguridad* se entiende como la ausencia de riesgo o como la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo al que se haga referencia en la seguridad. En términos generales, la seguridad se define como «el estado de bienestar que percibe y disfruta el ser humano».

Por otro lado se considera *información* a un conjunto organizado de datos que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. En este sentido amplio se puede considerar información todo aquello que genera un valor añadido al conocimiento previo.

La seguridad de la información va más allá de la simple adición de ambos conceptos: confianza en el conjunto ordenado de datos. Tiene un alcance mucho más amplio e incluye las medidas preventivas y reactivas en las organizaciones y en los sistemas tecnológicos que permiten resguardar y proteger la información, todo ello en base a garantizar los principios básicos de la seguridad de la información, que son:

- Confidencialidad: asegurar el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización; es decir, una persona solo puede acceder a la información que debe.
- Integridad: mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- Disponibilidad: la información es accesible en el momento que se requiere.

Consecuentemente ello implica que la seguridad de la información ha de actuar a todos los niveles:

- Físico: proteger la información de la destrucción física, de los desastres naturales, de las alteraciones del entorno, etc.
- Lógico: proteger el uso de los datos y su acceso ordenado y autorizado.

- Administrativo: proporcionar la gestión adecuada para la correcta aplicación de los dos ámbitos anteriores, lo cual usualmente pasa por el establecimiento de políticas y normas a implantar y seguir por las personas, instituciones y sistemas implicados en la información que se va a segurizar.

Y todo ello sin perder de vista que la actuación en cada uno de estos niveles impacta directamente en la «comodidad» de los usuarios respecto de la información. Es decir, también es obligación de la seguridad de la información alcanzar el balance adecuado entre el nivel de riesgo que se puede y/o quiere alcanzar dentro de una organización y la comodidad de los usuarios en el uso de la información: disponer de un nivel de seguridad cercano al 100 %, pero a costa de que el proceso de utilización de la información sea impracticable o altamente costoso en tiempo y gestión, no es deseable ni un objetivo planteable.

No olvidemos que en la seguridad de la información el factor humano es clave, ya que de poco sirven las medidas tecnológicas más avanzadas y las metodologías más probadas si los usuarios internos no las aplican correctamente. De ahí también la importancia del compromiso planteado entre nivel de seguridad y comodidad de uso que implica una correcta seguridad de la información.

Por tanto, la seguridad de la información se ha de plantear desde una perspectiva práctica y realista, de acuerdo con el negocio de la entidad y realidad del entorno en el que desarrolla su actividad, lo que implica asumir que:

- La tecnología evoluciona y proporciona muchos medios, pero cada vez requiere más inversión; hay más información que administrar, y la propia tecnología implica más vías para controlar.
- A nivel personal es imposible controlar toda la información que manejan las personas (lo que saben, lo que recuerdan o lo que opinan), y muchas veces son los puntos clave de la pérdida de la información, sea de manera fortuita o intencionada.

Finalmente, si de por sí ya es complicado obtener seguridad de la información en su estado pasivo (cuando está almacenada en archivos físicos o electrónicos), la situación se vuelve aún más compleja con el uso exhaustivo de las comunicaciones y funcionamiento virtual de la sociedad. Y es que, en este escenario, a la tríada de principios básicos anteriormente citados, hay que añadir un cuarto, el de la autentificación: la necesidad de identificar de manera unívoca al generador de la información, garantizar que quien comunica o actúa (accede, modifica, traspasa, etc.) sobre la información es quien dice que es y no está siendo suplantado por un tercero ajeno. Cabe destacar que la autentificación es el pilar básico para un correcto funcionamiento del mundo virtual ya que sin autentificación no se podrían llevar a cabo muchas de las acciones consideradas hoy como habituales.

La solución a todos estos parámetros implica la coordinación de actuaciones en cuatro frentes:

- Tecnología para controlar, proteger y medir el uso de la información.
- Gestión para definir cómo se ha de usar la información y cómo se ha de guardar.
- Educación para despertar y concienciar a las personas sobre la importancia de la información que manejan.
- Investigación y análisis para detectar pérdidas en la seguridad de la información, qué vulnerabilidades se presentan, cómo se pueden solventar, cuál es la situación de seguridad del entorno que rodea a la entidad; así como actualizarse adecuadamente a fin de anticiparse, en lo posible, a las nuevas situaciones.

Presentación de la asignatura

En la asignatura «Seguridad y auditoría de la información» vamos a trabajar algunos de los aspectos que se plantean en los ámbitos de actuación esbozados anteriormente. Nos centraremos en los aspectos relativos a la segurización del canal, es decir, todo aquello que nos permite trabajar sobre la información y transferirla entre los distintos usuarios de manera segura y autentificada, pero enfocándonos más en los aspectos administrativos, metodológicos y normativos que en los detalles tecnológicos. Y es que son esos aspectos administrativos, metodológicos y normativos los que han de permitir gestionar y controlar, de manera global dentro de una organización, que la información, desde una perspectiva lógica, se mantiene segura dentro de los parámetros y objetivos marcados por la organización.

El camino usual para toda organización para conseguir seguridad en su información se basa en dos vías de actuación que se van retroalimentando (y que serán el contenido central de la asignatura):

- **Planificar.** Definir, de acuerdo con los objetivos de negocio de una organización y un presupuesto acorde con ellos, un **plan de seguridad** de los sistemas de información (entendiendo el sistema de información en su sentido amplio, no solamente el tecnológico). Ligado a este plan de seguridad, y en base a su marco objetivo, establecer un **plan de contingencia**, es decir, qué hay que hacer para evitar, dentro de lo posible, que la seguridad se vea amenazada y qué hay que aplicar para atajar la amenaza; y un **plan de continuidad**, es decir, en la circunstancia desfavorable de que las amenazas no se hubieran podido atajar totalmente y la información y sus sistemas de seguridad hubieran sido afectados, cómo proceder para restituir su valor y continuar con el negocio con el mínimo de discontinuidad.
- **Auditar y Analizar.** Conocer cuál es la situación en cada momento. Ello implica, por una parte, constatar cuál es la situación real de la seguridad de la información y de todos los sistemas que la manejan (tecnológicos o no: no olvidemos el factor humano). Es decir, cómo auditar la seguridad

de los sistemas de información, y establecer su ejecución periódica y los análisis de resultados, los cuales son clave para revisar y mejorar el plan de seguridad, tanto para constatar su eficacia como para revelar sus debilidades y así plantear mejoras. Y, por otra parte, también implica que, en los momentos en que alguna circunstancia (amenaza, ataque, accidente, desastre natural, etc.) ha afectado la seguridad de los sistemas y/o información, se debe realizar un análisis exhaustivo de las consecuencias derivadas, evaluar el nivel de los daños recibidos e identificar al máximo las causas. Esta identificación de las causas debe permitir actuar en lo posible para corregirlas; recabar responsabilidades y compensaciones por los daños sufridos, si corresponde; y, cómo no, revisar y actualizar el plan de seguridad de información.

Adicionalmente a estos dos ejes centrales, en la asignatura también se trabajarán los aspectos conceptuales, tecnológicos y normativos, al nivel necesario para la comprensión de la problemática de la seguridad, su alcance e implicación en el entorno de toda organización, pero sin entrar en detalles especializados y específicos que son objeto de otras asignaturas. En este sentido, se han incluidos apartados para:

- Establecer los **conceptos generales** que se aplican a la seguridad de la información y los diferentes tipos de seguridad relacionados con ella.
- Tipificar lo que significa la **intrusión en los sistemas de información**, los ataques informáticos, y conocer cómo actúan y cómo evolucionan.
- Describir los principales componentes de los sistemas de información y su relación con la seguridad informática, explicar las **medidas generales de seguridad** y criterios generales a aplicar para segurizarlos, los cuales son los que se van a establecer y revisar en los ejes centrales de planificación y auditoría.
- Plantear a nivel conceptual qué es la **criptografía** y su importancia para la seguridad de la información y autentificación de los usuarios que intervienen en su comunicación y manejo, presentando su evolución a lo largo del tiempo y su complejidad actual para garantizar la seguridad de la información, y qué nivel de seguridad representan.
- Presentar las **normativas** para la correcta implantación de la seguridad de la información de acuerdo con los organismos oficiales, tanto en sus aspecto metodológico como de ámbito jurídico legal, principalmente por su impacto en la «propiedad e integridad» de las personas y organizaciones.

Desarrollo y contenido de la asignatura

La asignatura se ha estructurado en 7 módulos que permiten al estudiante ordenar el aprendizaje de los distintos contenidos; aunque ello no impide que el estudiante los pueda organizar de la manera que mejor se adecúe a sus necesidades y disponibilidades, siempre y cuando cumpla con el proceso de evaluación que se establezca.

El detalle de estos módulos es el siguiente:

1) Módulo 1: Información y seguridad
   1) El valor de la información
   2) Nociones básicas de seguridad de la información
   3) Seguridad técnica y seguridad jurídica

2) Módulo 2: Gestión de la seguridad
   1) Qué es la seguridad informática
   2) Intrusión informática: explotación de vulnerabilidades
      1) Concepto de vulnerabilidad e incidente
      2) Ciclo de vida del incidente
      3) Clasificación de los ataques
         1) Según cómo actúa
         2) Según quién lo origina

      4) Explotación de vulnerabilidades. Etapas de una intrusión
         1) Recogida de información
         2) Escaneo
         3) Acceso al sistema
         4) Mantener el acceso
         5) Eliminación de huellas

   3) Tipos de seguridad
      1) Activa
      2) Pasiva

   4) Medidas básicas de seguridad
      1) Medidas físicas
      2) Medidas lógicas
      3) Criterios para un buen *password*

   5) Administración de la seguridad
   6) Seguridad de los datos
   7) Seguridad del web
   8) Seguridad de la red
   9) Seguridad del servidor
   10) Roles y entidades responsables de seguridad
      1) Certificaciones profesionales
      2) El CERT

3) Módulo 3: Criptografía
   1) Introducción y fundamentos de la criptografía
   2) Claves públicas y privadas
   3) Claves simétricas y asimétricas

4) Entidades certificadoras

4) Módulo 4: Planes de seguridad
- **1)** Riesgos de seguridad y cómo prevenirlos
- **2)** Plan director de seguridad
- **3)** Planificación de la continuidad
- **4)** Plan de contingencia

5) Módulo 5: Auditoría de sistemas de información
- **1)** Introducción a las técnicas de auditoría
- **2)** Tipos y estándares de auditorías
- **3)** Metodologías, la ejecución de la auditoría

6) Módulo 6: Análisis forense
- **1)** Ciencias forenses
- **2)** Informática forense
- **3)** Etapas del análisis forense informático
  - **1)** Identificación de la evidencia digital
  - **2)** Recogida de la evidencia digital
  - **3)** Adquisición de la evidencia digital
  - **4)** Preservación de la evidencia digital
  - **5)** Análisis de la evidencia digital
  - **6)** El informe pericial y su estructura
- **4)** Análisis e investigación de delitos informáticos. El marco legal
  - **1)** Los delitos informáticos y el Código penal
  - **2)** La investigación de los delitos informáticos

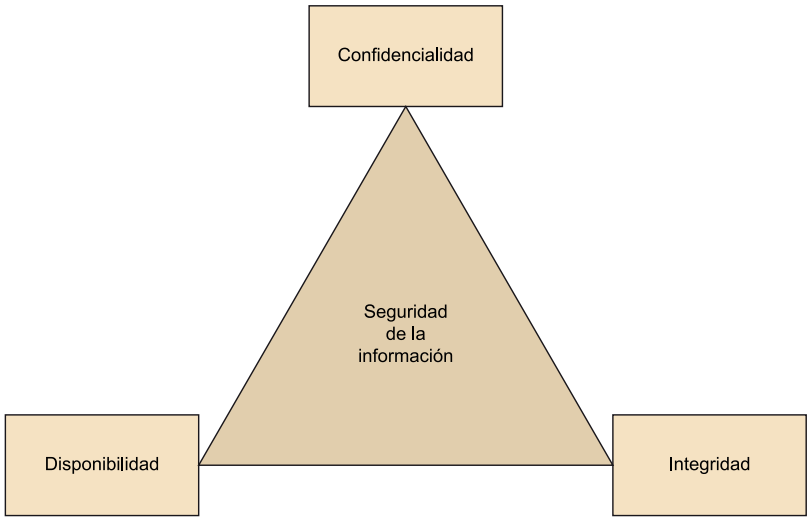
Esta estructuración es conceptual, ya que la asignatura no dispone de un material *ad hoc*: dados el objetivo no tecnológico (y de practicidad) que se persigue, la realidad actual, y la constante evolución de los temas que se trabajan, se ha considerado que, en la mayoría de los casos, su estudio será más enriquecedor utilizando libros y materiales ya existentes que se complementen con documentos y artículos relacionados disponibles en todo tipo de fuentes. Esta documentación podrá ser propuesta por el profesor durante el curso, pero también por el propio estudiante, y en todo caso el profesor ayudará a su comprensión y contraste.

1. Información y seguridad

Este primer módulo de la asignatura se dedica a presentar los conceptos de información y seguridad en las organizaciones; el flujo de información dentro y fuera de las organizaciones y los principios de seguridad que se deben aplicar.

Así pues, en primer lugar se trabajan los conceptos de **dato** y de **información**, para profundizar en cómo se generan y circulan dentro de los procesos de una organización, enriqueciéndose y evolucionando, transformándose de simples guarismos en información y conocimiento; razonando la importancia y el valor que tiene la información y lo que significa para toda organización, y por tanto su conversión en una **activo**, tangible e intangible, de la organización, que se debe proteger y evitar su uso fraudulento.

Figura 1.



A continuación se trabajarán las **características de la información** y las bases para su seguridad: **confidencialidad**, **integridad** y **disponibilidad**; y se sigue con una visión genérica de los estándares que se deben aplicar para la gestión de la seguridad de la información: la familia de normas internacionales de la serie ISO/IEC 27000 (principalmente la 27001 para la implantación de un sistema de gestión de seguridad de la Información (SGSI) y la 27002, guía de buenas prácticas para asegurar los sistemas de información de una organización). Sobre estos estándares, junto con una explicación de otras metodologías, se volverá a trabajar en el módulo 4, cuando se elabore el plan de seguridad de una organización.

La última parte del módulo se ha pensado para mostrar una visión sobre las **implicaciones tecnológicas y legales** de la seguridad de la información, donde tiene una importancia vital la autenticación de los usuarios de la información, que está generando todo el conjunto de normativas sobre la protección de datos y preservación de la intimidad en el mundo digital.

La herramienta de trabajo de este módulo es el documento disponible en los materiales de la asignatura identificado como «Módulo 1: Información y seguridad», donde el estudiante puede seguir el desarrollo de los temas de trabajo y en el que se referencian diversas fuentes a las que se puede acudir para profundizar en algunos de los aspectos presentados.

Complementariamente recomendamos, para asentar bien los conceptos que se presentan, la lectura del módulo de la UOC «Introducción a la seguridad de la información», incluido en el apartado «Bibliografía» como referencia 1, específicamente los tres primeros apartados, identificados como: «Qué es la seguridad de la información», «Dimensiones de la seguridad de la información» y «Gestión de la seguridad de la información».

Como complemento a los conceptos básicos, el resto de apartados del citado documento son también interesantes ya que presentan al lector aspectos generales relacionados con la seguridad de la información en un sentido amplio.

Con todo ello se persigue que al finalizar el módulo el estudiante alcance los siguientes objetivos:

- Saber diferenciar entre el concepto de dato e información.
- Entender los flujos de información dentro de una organización.
- Comprender que la información puede ser un activo de cualquier organización.
- Entender el concepto de seguridad de la información y sus dimensiones principales.
- Conocer a nivel general los estándares y normativas que se aplican a la seguridad de la información, así como los principios para la implantación de un SGSI.
- Ser consciente de que la seguridad de la información implica confluencia de necesidades tecnológicas y legales.

En resumen, asentar las bases para el estudio del resto de módulos.

2. Gestión de la seguridad

En el módulo «Gestión de la seguridad» se desarrolla qué implica la seguridad de la información y cómo gestionarla.

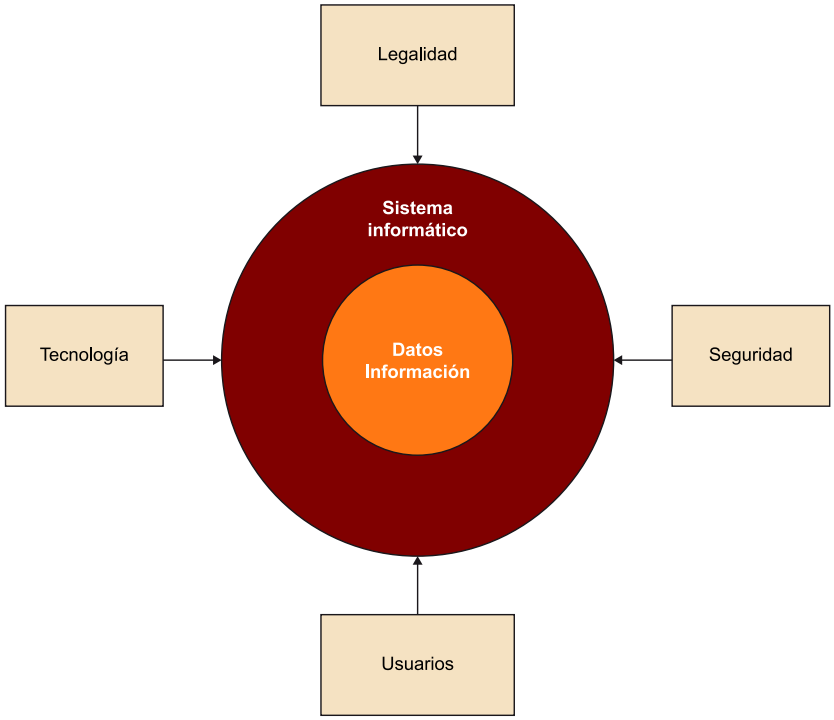
Como ya se ha apuntado en el primer módulo, hoy en día es imposible imaginarse una organización que utilice la información sin sistemas informáticos, así como también es imposible pensar en estos sistemas como elementos aislados; seguramente, están interconectados mediante una red, y muy probablemente en algún lugar también están conectados con el exterior (internet) y con variedad de accesos y dispositivos.

En el manejo de la información hay que considerar a diversos usuarios utilizando programas diferentes y mucha comunicación entre ellos (como, por ejemplo, correo electrónico); posiblemente compartiendo impresoras, protegiendo y compartiendo selectivamente información y programas. Y todo ello soportado por un conjunto de componentes de *software* y *hardware*, que hay que gestionar adecuadamente para obtener un rendimiento óptimo de todo el conjunto con el mínimo de cambios y molestias para los usuarios.

Todo este entramado se debe revestir de la seguridad adecuada para garantizar que no haya resquicios que comprometan el contenido. Así, como ya se ha visto en el módulo 1, al ser la información extremadamente valiosa, cuando se habla de seguridad y de información, es inevitable hablar de las cuestiones legales y delictivas (ciberdelito) que van asociadas: acceso no autorizado a los datos, bloqueo de servidores, *spam*, etc.

Por tanto, gestionar la seguridad de la información implica tener presente el siguiente esquema:

Figura 2.



Donde:

- **Tecnología.** La tecnología varía muy rápidamente. En cada momento tenemos que escoger la que hay en el mercado, teniendo en cuenta las necesidades que pretendemos cubrir y cómo queremos protegernos.
- **Seguridad.** La tecnología tiene que permitir el nivel de seguridad que se haya planificado y que se prevea como necesario para la organización. En cualquier caso, este nivel, como va muy ligado a la tecnología, necesita revisiones constantes.
- **Usuarios.** Los usuarios son una de las razones de ser básicas del sistema informático; son los que realmente utilizan la información, y, quizás, el eslabón más débil de seguridad.
- **Legalidad.** Como cualquier otro aspecto de la organización, todo está dentro de un marco legal que nos marca qué podemos hacer y de qué manera, y qué no podemos hacer.

Y en el centro de todos estos aspectos el **sistema informático**: las organizaciones crean constantemente grandes cantidades de datos, y lo que hacen los sistemas informáticos es procesarlos y distribuirlos entre todos los elementos de la organización para aumentar la eficacia del conjunto. El sistema informático pretende guardar la información de la organización para que posteriormente sea fácil recuperarla y de la misma manera en que se había guardado.

A partir de esta visión global, el módulo plantea el concepto de **seguridad informática**, y dado que es del todo imposible garantizar la seguridad o inviolabilidad absoluta de un sistema informático, en lugar del inalcanzable concepto de seguridad se plantea utilizar el término *fiabilidad*. Esto lleva a la considera-

ción de que un sistema informático es fiable cuando se satisfacen las mismas tres propiedades que ya se habían definido para la seguridad de la información: confidencialidad, integridad y disponibilidad (CID).

El módulo prosigue con la identificación de los elementos que pueden comprometer esta fiabilidad. Esto lleva a trabajar los conceptos de **vulnerabilidad** y, a partir de ella, a hablar de los **ataques** (**incidencias** si no hay éxito, **intrusión** si se altera alguna de las tres propiedades CID anteriormente citadas) y a analizar someramente su ciclo de vida, enumerando posibles orígenes y tipificando quién o qué actúa en dichos elementos. Ello permitirá clasificar los ataques en cuatro grandes grupos:

- **Interrupción**: ataque contra la disponibilidad en el cual un recurso del sistema se destruye o queda no disponible. Aunque usualmente son físicos, también los hay de tipo lógico.
- **Interceptación**: ataque contra la confidencialidad, en el cual un elemento no autorizado consigue el acceso a un recurso. Este tipo de ataque no se refiere únicamente a posibles usuarios que actúen como espías en la comunicación entre emisor y receptor.
- **Modificación**: ataque contra la integridad en el cual, además de conseguir el acceso no autorizado a un recurso, también se consigue modificarlo, borrarlo o alterarlo de cualquier manera.
- **Fabricación**: ataque contra la integridad en el cual un elemento consigue crear o insertar objetos falsificados en el sistema.

Y también se constatará que, si bien los actuantes en estos ataques suelen ser externos a la organización (los *hackers*), hay una parte significativa de estos ataques que tienen su origen último en las acciones (voluntarias o involuntarias) de usuarios internos. De ahí la importancia que se dará a la gestión y control de usuarios y a su educación y concienciación (dejar documentos fuera de protección, hacer copias de documentos en dispositivos transportables…) como única medida para **contrarrestar las acciones de ingeniería social**. En esta ingenieria social, elementos externos de una organización tratan de obtener la información necesaria para articular ataques de los anteriores tipos, utilizando métodos basados en el factor humano, que incluyen tanto engañar a usuarios para que suministren información sensible de la empresa o del sistema informático como hacer que el usuario acuda al atacante con esta información, aludiendo a factores de comportamiento (confianza, desconocimiento, miedo, codicia o deber moral).

Una vez identificada la tipología de los ataques y su ciclo de vida, se trabajarán los **tipos de seguridad informática** que se pueden y deben implantar: activa y pasiva. Y es que tan importante es saber cómo actuar para protegerse y afrontar los ataques como hacer una correcta previsión sobre el posible intrusismo y «educación» de los usuarios. Y en base a ellos se plantean un conjunto general de **medidas de seguridad**.

Los últimos apartados del módulo se dedican a presentar de manera descriptiva la **seguridad** de los distintos componentes que intervienen en los sistemas informáticos: usuarios, datos, red, servidores; y cómo segurizarlos, en función de los tipos de seguridad y medidas presentados en la parte inicial del módulo. Se trabajan los aspectos del qué y el cómo, sin entrar en profundidad en los detalles tecnológicos de su implementación, que quedan fuera del alcance del curso.

El módulo finaliza con una breve presentación de los **profesionales** que actúan en el ámbito de la seguridad informática, los tipos y categorías internacionales de **certificación** (CISA, *Certified Information Systems Auditor,* y CISM, *Certified Information Security Manager,* entre las más conocidas, que se suelen proponer como garantía de procedimiento en la seguridad de la información), y el rol de los **CERT** (*Computer Emergency Response Team*) en la resolución de incidencias globales de la seguridad. Estos equipos o centros de respuesta a incidentes de seguridad en tecnologías de la información se constituyen a nivel de un país o área geográfica, agrupando expertos que son los responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Es decir, un CERT estudia el estado de seguridad global de redes y ordenadores, proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de esos sistemas, coordinándose en su actuación con los otros CERT en el caso de amenazas globales.

Para trabajar este módulo no se dispone de material específico desarrollado *ad hoc* y se utilizarán partes de materiales ya desarrollados para otras asignaturas de la UOC que se corresponden con los temas que se tratan. Específicamente:

- Para los 4 apartados iniciales previstos para este módulo, «Qué es la seguridad informática», «Intrusión Informática: explotación de vulnerabilidades», «Tipos de Seguridad» y «Medidas básicas de seguridad», el estudiante se basará respectivamente en los documentos:
  - Del módulo «Administración de los datos», los dos primeros apartados: «Los datos y la organización» y «Dónde está la información» (referencia 4).
  - Todos los apartados del módulo «Gestión de los incidentes de seguridad» (referencia 2).
  - Apartado 2 (referencia 3).
  - Del módulo «Introducción a la administración de sistemas", los dos primeros apartados: «El sistema informático y la organización» y «Elementos del sistema informático» (referencia 4).

- Para el estudio de los apartados del 2.5 al 2.9, el estudiante se basará en la referencia 4, de acuerdo con el contenido de apartado, así:

  - «Administración de la seguridad», comprender el contenido del módulo «Administración de la seguridad», apartados 1, 2 y 3: «Seguridad informática», «Seguridad del entorno», «Seguridad del sistema».
  - «Seguridad de los datos», comprender el contenido del módulo «Administración de los datos», apartado 4: «Protección de la información».
  - «Seguridad de la web», comprender el contenido del módulo «Administración de la web», apartado 1: «Los servidores web y la organización» y apartado 4: «Seguridad».
  - «Seguridad de la Red», comprender el contenido del módulo «Administración de la Red», apartado 1: «Importancia de las redes» y apartado 5: «Seguridad de la red».
  - «Seguridad del servidor», comprender el contenido del módulo «Administración de servidores», apartado 9: «Seguridad de los servidores».

- Finalmente, para el apartado 2.10 (aspectos profesionales) se basará en los últimos apartados de los módulos citados anteriormente, en los que se describen las tareas y responsabilidades del administrador. Y para el apartado de comprensión del CERT, se recomienda utilizar las referencias que hay en la red. Así, a nivel introductorio para la definición y objetivos del CERT, se recomienda el artículo de la Wikipedia «Equipo de Respuesta ante Emergencias Informáticas para la definición y objetivos del CERT», y para concienciarse del nivel de actividad que implica se puede acceder al web del CERT español (CERTSI).

Con ello se persigue que al finalizar el módulo el estudiante alcance los siguientes objetivos:

- Saber que la información de la organización es muy valiosa.
- Conocer el rol del sistema informático dentro de la organización y su relación con la seguridad de la información.
- Conocer diferentes maneras de mantener la integridad de la información.
- Poder identificar las vulnerabilidades más comunes de los sistemas.
- Poder identificar posibles fuentes de ataque y conocer a nivel general cómo prevenir y atajar los ataques.
- Conocer los fundamentos de seguridad de la información y de los componentes implicados en su custodia y manipulación: servidores, red, web.
- Concienciarse sobre el rol de los usuarios en la seguridad de la información.
- Disponer de información sobre los profesionales y los centros expertos en la gestión de la seguridad.

3. Criptografía

En el apartado «Seguridad en Internet» del módulo «Internet. Funcionamiento, aplicaciones y seguridad» de la asignatura *Diseño y arquitectura de sistemas de información (DASI)* de este mismo programa, ya se han establecido los principios de la criptografía y su importancia en el mundo de internet en particular y en el de la comunicación en general.

La realidad es que, actualmente, la criptografía es omnipresente en la vida cotidiana, aunque de una manera silenciosa: desarrollos como la telefonía móvil, la televisión de pago o el comercio electrónico no serían viables sin las técnicas criptográficas.

Por ello, en este módulo repasamos y ampliamos un poco los conceptos explicados en *DASI*, en una visión más global del uso de la criptografía como elemento de seguridad de la información: no solo se aplica a la información cuando se comunica sino que también es uno de los medidas utilizadas hoy en día para protegerse del robo de información.

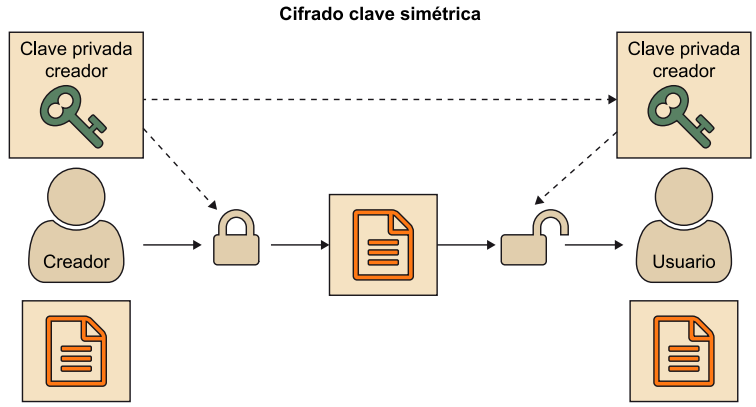
Iniciaremos el módulo con una revisión general de los conceptos básicos de la criptografía (nivel de seguridad de la clave) y se presenta su parte complementaria (o contraria) denominada criptoanálisis: ambas conjuntamente se conocen con el nombre de **criptología**. La **criptografía** se ocupa del diseño del cifrado, mientras que el **criptoanálisis** se ocupa de romper dicho cifrado. Y aunque pueda parecer que el criptoanalista es el enemigo de la seguridad, su motivación puede ser descubrir el texto que se ha cifrado o la clave que se ha utilizado para el uso no autorizado de la información, no hay que olvidar que su interés también puede ser de tipo científico-técnico enfocado en la verificación de la seguridad del cifrado; esta vertiente del criptoanálisis es esencial para la depuración de los cifrados y progreso de la criptografía.

El módulo continua con un repaso de los criptosistemas históricos y se presentan a nivel conceptual los dos grupos de que están en uso hoy en día:

- La **criptografía de clave simétrica** (también llamada criptografía de clave compartida o privada) incluye aquellos métodos de cifrado en los que el emisor y el receptor comparten una misma clave para cifrar y descifrar los mensajes. Los sistemas criptográficos más antiguos eran de este grupo, pero aún siguen vigentes y utilizándose. Los criptosistemas de clave simétrica más importantes son el *Data Encryption Standard* (DES), el estándar diseñado por IBM que el NIST (National Institute of Standards and Technology) de EE.UU. definió como estándar en el año 1977, y el *Advanced Encryption Standard* (AES), el algoritmo que sustituyó al DES en el año 2002, al haber

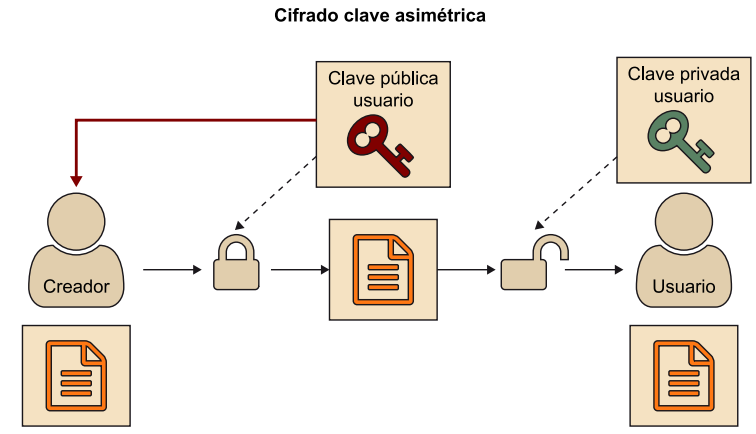
quedado aquel obsoleto debido al aumento de la potencia de cálculo de los ordenadores.

Figura 3.



- La **criptografía de clave pública** (o criptografía asimétrica) en los que la comunicación se mantiene secreta sin necesidad de transferencia de clave secreta entre el emisor y el receptor. En este método cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada. El más conocido es RSA (Rivest, Shamir y Adleman), desarrollado en 1977, el primer y más utilizado algoritmo de este tipo, válido tanto para cifrar como para firmar digitalmente.

Figura 4.



A partir de esta clasificación se trabaja, a nivel general, qué significa cada uno de los grupos y las características principales de los métodos utilizados. Se verá que cada uno tiene sus ventajas e inconvenientes y se constatará que hay algunas diferencias entre ellos:

- La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública, y se mantiene la privada para uso exclusivo del propietario.

- Sin embargo, la criptografía asimétrica, con los métodos actuales, tiene bastante desventajas respecto a la clave simétrica:
  - Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
  - Las claves deben ser de mayor tamaño que las simétricas (generalmente son cinco o más veces de mayor tamaño que las claves simétricas).
  - El mensaje cifrado ocupa más espacio que el original.

En cualquier caso el estudiante concluirá que la idoneidad de cada método depende del tipo de aplicación que se quiera realizar.

Al final se incluye, a nivel informativo, un apartado dedicado a explicar lo que son las entidades certificadoras como garantes para la generación de las claves de cifrado tanto en el ámbito de clave simétrica como asimétrica.

Como corolario final es importante que el estudiante sea consciente de que los métodos de cifrado son seguros en un contexto determinado, ya que el crecimiento exponencial de la potencia de cálculo de las nuevas generaciones de ordenadores pueden convertirlos en inseguros.

Para trabajar este módulo no se dispone de material específico *ad hoc* y se utilizarán como base parte del material desarrollado por la UOC para la asignatura «Criptografía», incluido como referencia 5 en el apartado «Bibliografía». En particular se propone la lectura a nivel conceptual, sin entrar en los detalles matemáticos que se plantean, de los siguientes apartados:

1) Para el apartado «Introducción y fundamentos de la criptografía», los contenidos del apartado «Terminología» del módulo «Introducción a la criptografía» y los apartados «Criptosistemas históricos», «Secreto perfecto y autenticidad» y «Criptoanálisis elemental» del módulo «Fundamentos de criptografía».

2) Para el tema de cifrado de clave compartida o privada, los contenidos de:

a) Módulo 3 - Cifrado de clave compartida: cifrado de flujo:
  - Capítulo 1: Requisitos de las secuencias del cifrado de flujo privada

b) Módulo 4- Cifrado de clave compartida: cifrado de bloque:
  - Capítulo 1: Estructura del cifrado de bloque
  - Capítulo 2: Criptosistemas de cifrado de bloque, visión general de los apartados:
    - 1. El estándar DES
    - 2. Criptosistema IDEA
    - 3. Propuesta AES
  - Capítulo 4: Gestión de llaves

3) Para el tema de cifrado de clave pública, los contenidos de los apartados «Conceptos preliminares» y «Fundamentos de los criptosistemas», solo los aspectos conceptuales, del módulo «Cifrado de clave pública».

4) Para la comprensión de las entidades certificadoras, los apartados «Conceptos básicos» y «Componentes de una infraestructura de clave pública» del módulo «Infraestructura de clave pública».

Con ello se persigue que al finalizar el módulo el estudiante alcance los siguientes objetivos:

- Asimilar la historia, la terminología y los supuestos de la criptografía.
- Conocer los fundamentos teóricos de la criptografía moderna.
- Comprender a nivel conceptual el funcionamiento de los sistemas de cifrado de clave privada.
- Comprender a nivel conceptual el funcionamiento de los sistemas de cifrado de clave pública.
- Comprender a nivel funcional el funcionamiento de las infraestructuras de clave pública que posibilitan la implementación de criptografía de clave pública.
- Entender el funcionamiento de los protocolos criptográficos actualmente en uso.

4. Planes de seguridad

Como ya se ha apuntado en los módulos «Información y seguridad» y «Gestión de la seguridad», la seguridad de la información es un proceso de la organización que se tiene que gestionar y que requiere dedicación de recursos personales y económicos. Es indispensable una buena definición de la organización de la seguridad de la información y una buena asignación de funciones para que esta seguridad sea realmente eficiente y quede incorporada al día a día de la entidad. La gestión de la seguridad de la información comporta un gran número de actividades que son organizativas o técnicas y, a veces, también normativas y jurídicas.

Dependiendo del estado de madurez de la organización en cuanto al despliegue de la seguridad de la información, hay que priorizar las actividades de una manera u otra, pero, a la larga, la gestión de la seguridad requiere que la organización dedique esfuerzos a cada una de las actividades.

La base para la gestión de la seguridad de la información está referenciada en la familia de normativas del ISO/IEC 27001, cuya piedra angular es el establecimiento de la política de seguridad de una organización, en relación directa con su plan estratégico de negocio, y la consecuente definición del plan de seguridad de la organización.

Así pues, a partir de esta visión general iniciaremos este módulo con una visión sobre los riesgos de seguridad y su gestión, presentando qué es un análisis de riesgos de seguridad, su justificación y su estudio, junto con una descripción general de las metodologías disponibles para realizarlos.

El análisis de riesgos es el primer paso para gestionar la seguridad, ya que antes que nada hay que identificar cuáles son los peligros de la organización. La realidad actual es que hay muchas organizaciones que son capaces de dedicar grandes recursos a su seguridad e incluso invierten dinero en hacer cambios en la seguridad de la organización. Sin embargo, si se los pregunta por qué han gastado estos recursos para protegerse de alguna manera, sus respuestas no demuestran que estas organizaciones estén muy convencidas de que con esta inversión reducirán realmente las incidencias que tienen. Por el contrario, sorprende que no estén dispuestas a usar recursos en estudiar realmente las carencias que tiene su organización; puesto que, si se analiza cuáles son esas carencias y las necesidades que se generan en la organización, la inversión posterior en seguridad será mucho más pequeña y más ajustada a la realidad de la organización. Esto es lo que supone el análisis de riesgos.

Conocida la situación, se estudiará cómo se tiene que implantar el proceso de la gestión de la seguridad de la información: cuáles son los pasos que se deben seguir, los aspectos que se tienen que tener en cuenta, los riesgos posibles y los estándares de referencia que nos ayudan a avanzar con confianza.

La parte final del módulo se dedica a trabajar una visión general de los planes de continuidad del negocio y planes de contingencia, ya que aunque se haya implantado un correcto SGSI, hay que tener en cuenta que siempre se puede llegar a dar alguna situación imposible de proteger o de evitar; hay que ser conscientes que no se podrá conseguir nunca la seguridad total.

> «El único sistema que es realmente seguro es uno que está apagado y desconectado de la red, cerrado en una caja fuerte forrada de titanio, enterrado en un búnker, rodeado de gas nervioso y custodiado por guardias armados y muy bien pagados. Incluso así, no daría la vida por eso...»
>
> Gene Spafford. Director de Computer Operations, Audit, and Security Technology (COAST), Universidad Purdue.

Para hacer frente a estas situaciones, las organizaciones necesitan crear planes de continuidad de negocio, que tienen como finalidad evitar que las actividades de negocio queden interrumpidas. Por este motivo, los planes de continuidad de negocio son imprescindibles, independientemente del tamaño de la organización. Además, estos planes de continuidad de negocio no solamente tienen el objetivo de intentar evitar las interrupciones en la actividad de negocio, sino que también intentan minimizar el tiempo de inactividad en caso de que finalmente se produzcan esas interrupciones.

Para trabajar este módulo no se dispone de material específico desarrollado *ad hoc* por la UOC y se utilizará como base parte del material desarrollado por la UOC para la asignatura «Sistema de Gestión de la Seguridad de la información» incluido como referencia 1 en el apartado «Bibliografía». En particular, se propone:

- Como enfoque general del módulo recomendamos la lectura del apartado «Gestión de la seguridad de la información» del módulo «Introducción a la seguridad de la Información».
- Para el análisis de riesgos de seguridad, se propone la lectura de los apartados «Ciclo de vida de la seguridad», «Proceso del análisis de riesgos», «Análisis de riesgos: Justificación y estudio», «Magerit», «NIST», «CRAMM» y «Octave» del módulo «Análisis de riesgos».
- Para el estudio de los planes de seguridad se propone la lectura de los apartados «Qué es un sistema de gestión de la seguridad de la información», «La familia ISO», «Introducción al SGSI» y «Planificar: establecer el SGSI» del módulo «Implantación de un sistema de Gestión de la Seguridad de la Información». Cabe decir que, aunque no vamos a trabajar con detalle todos los aspectos de la normativa, la implantación de un SGSI pasa incondicionalmente por un buen conocimiento de las normas internacionales, de forma que os recomendamos que leáis en detalle todo el apartado «ISO-

IEC 27002: código de buenas prácticas para gestionar la seguridad de la información» del mismo módulo.

- La visión sobre los planes de continuidad de negocio que se pretende alcanzar en este módulo se obtendrá a partir de la lectura de los contenidos de los apartados «Enfoques en los planes de Continuidad de negocio», «Plan de continuidad de negocio» y «Estructura de los planes de continuidad de negocio» del módulo «Planes de continuidad de negocio».

Con ello se persigue que al finalizar el módulo el estudiante alcance los siguientes objetivos:

- Presentar brevemente diferentes modelos de gestión adoptados hoy en día por las organizaciones.
- Saber en qué consiste el proceso de análisis de riesgos.
- Conocer las diferentes metodologías de análisis de riesgos.
- Ser capaces de llevar a cabo un análisis general de riesgos aplicando alguna de las metodologías presentadas.
- Disponer de una visión general del contenido de la familia 27000 de la ISO.
- Conocer las bases de los sistemas de gestión y, en concreto, del ciclo de Deming.
- Conocer las pautas para implantar un SGSI.
- Saber qué es un plan de continuidad de negocio y cuáles son los objetivos respecto a la seguridad de la información de las organizaciones.
- Identificar las fases de los planes de continuidad de negocio y la manera de implantarlas.
- Conocer la estructura y el contenido del documento del plan de continuidad.

5. Auditoría de sistemas de información

Hemos visto en los módulos anteriores que con el objetivo de reducir los incidentes de seguridad, las organizaciones tienen implantadas una serie de medidas para que si ocurren esos incidentes las consecuencias que provoquen sean mínimas. Por otro lado, las organizaciones más preocupadas por la protección de su información son conscientes de que la seguridad total no se conseguirá nunca; por eso, para tratar de conseguir esta seguridad global en una organización, también se requieren unos planes de continuidad de negocio.

Sin embargo, hay que recordar que la seguridad es un proceso vivo, no una meta que se consigue; que tiene que estar en revisión constante y que es fundamental que en todo momento las medidas de seguridad de que dispone la organización reflejen la situación actual y se adecúen al entorno en que esta se encuentra.

Por esta razón se producen cambios constantes tanto en la configuración de los sistemas de información como en el mismo entorno en que se encuentran. Así, es recomendable disponer de algún tipo de mecanismo de revisión, preferiblemente independiente, con el objetivo de que se detecten los aspectos que puedan ser más vulnerables o que no estén correctamente configurados.

Estas revisiones de la seguridad de una organización se denominan **auditorías de seguridad**. Forman parte de este ciclo vivo de la seguridad y permiten asegurar que los controles de seguridad implantados son los más adecuados y están configurados correctamente.

Cuando las auditorías de seguridad se basan en la revisión del conjunto de medidas y de su proceso de gestión ante normativas vigentes, concretamente ante la ISO/IEC 27001, nos encontramos con procesos que pretenden comprobar que se gestiona la seguridad de acuerdo con unos parámetros reconocidos por la industria; esto da como resultado las denominadas certificaciones de seguridad del SGSI.

Por otro lado, también es interesante destacar que actualmente las organizaciones se encuentran ante la obligación legal de comprobar periódicamente las medidas de seguridad implantadas para reducir los riesgos que amenazan la información. Tanto en el marco de la legislación en materia de protección de datos (en España, Ley orgánica 15/1999, de protección de datos de carácter personal, y su legislación de acompañamiento, más concretamente el Real decreto 1720/2007, del Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal), como en el marco financiero (en el ámbito europeo, los acuerdos Basilea III, actualización respecto a II el 2010, y para todas las empresas cotizadas en los Estados

Unidos, la Ley Sarbanes-Oxley), se exige hacer periódicamente revisiones del riesgo operacional y, por lo tanto, se deriva la necesidad de hacer auditorías de seguridad de los sistemas de información.

Toda esta situación que hemos comentado ha comportado el auge de la disciplina de la auditoría de sistemas de información como un derivado inicial de las auditorías de cuentas. Este protagonismo está reforzado por el entorno actual en que los sistemas de información participan cada día más en todos los procesos productivos y no solamente en los de control financiero de las instituciones. Por lo tanto, este módulo tiene por objeto presentar los conceptos fundamentales que definen las auditorías de sistemas de información, especialmente las auditorías de la seguridad de la información, y mostrar al alumnado el amplio campo que hay en esta área para su propio desarrollo profesional.

El material del módulo se organiza en varios apartados de aspectos generales de la auditoría, a partir de la definición de lo que significa: proceso ejecutado por un profesional, que tiene la característica de ser sistemático, independiente y documentado, y que busca obtener, a partir de la realización de registros, declaraciones de hechos u otra información, tangibilidades conocidas como pruebas de auditoría. Las pruebas de auditoría tienen que ser verificables, pertinentes y evaluables de manera objetiva para determinar, de acuerdo con estas, la medida en que el hecho auditado cumple unos criterios de auditoría. Estos criterios están determinados por un conjunto de políticas, procedimientos o requisitos y son usados como referencia contra la cual se compara la realidad. Las pruebas de estas diferencias entre la realidad y la referencia son lo que se entiende como constataciones de auditoría. Finalmente, el proceso concluye con el análisis de estos hallazgos para poder emitir unas conclusiones de la auditoría.

Así pues, el primer apartado ahonda en los conceptos y características que se establecen en la definición anterior.

En el segundo apartado, a partir de la identificación de los distintos actores que pueden intervenir en ellas, se trabajan los tipos de auditorías, se presentan cuáles deberían ser los objetivos, criterios y alcance de las mismas, y el esquema general de un proceso de auditoría. Dado que, de acuerdo con su definición, una característica clave de la auditoría es su referencia a un conjunto de estándares y políticas, se finaliza el apartado presentando someramente los estándares usuales que se aplican a las auditorías de seguridad de la información.

En el último apartado se introducen diferentes técnicas de auditoría y se presentan también varias herramientas, aunque, por la extensión de este curso, se tiene que considerar como una mera introducción para que el estudiante

tenga conocimiento de los diferentes tipos y técnicas, y pueda ampliar su conocimiento, en la medida que la aplicación de los conocimientos adquiridos lo requiera para su práctica profesional diaria.

Para trabajar este módulo no se dispone de material específico desarrollado *ad hoc* y se utilizará como base parte del material desarrollado por la UOC para la asignatura *Auditoría técnica y de certificación* incluido como referencia 6 en el apartado «Bibliografía». En particular se propone:

- Como enfoque general del módulo y conceptos generales recomendamos la lectura completa del apartado «Definición de auditoría» del módulo «Introducción a la auditoría TIC y de seguridad TIC».
- El segundo apartado de la asignatura lo basaremos en la lectura de los apartados «Componentes de una auditoría», «Proceso de auditoría» y «Estandarización de la tarea de auditoría» del módulo «Introducción a la auditoría TIC y de seguridad TIC».
- Finalmente, el último apartado del módulo se trabajará en base al contenido completo del módulo «Técnicas de auditorías».

Con ello se persigue que al finalizar el módulo el estudiante alcance los siguientes objetivos:

- Conocer las características que ha de presentar el auditor y el proceso de auditoría.
- Identificar los actores de una auditoría.
- Obtener una visión general de los tipos de auditoría
- Disponer de una visión global del proceso de auditoría.
- Saber que hay distintos tipos de estándares que aplican para la realización de auditorías y cuáles son sus valores.
- Obtener un conocimiento general de las técnicas de auditoría.

6. Análisis forense

En los módulos «Gestión de la seguridad» y «Planes de seguridad» se ha trabajado cómo identificar las vulnerabilidades de seguridad en los sistemas de información de una organización, identificar los riesgos que están latentes, detectar los intentos de ataques y cómo organizarse para evitar en lo posible que estos riesgos se materialicen. Sin embargo, tarde o temprano, alguien puede encontrar alguna rendija en el sistema defensivo y provocar daños o robar información (bienes intangibles) de la organización en su propio provecho; por lo que la organización deberá afrontar las consecuencias de un incidente de seguridad.

A partir de ese momento, el análisis forense se convierte en una herramienta clave: recoge información digital sobre el incidente, lo analiza y determina qué ha pasado. Este análisis tiene un doble objetivo: aprender de la situación y actuar para protegerse mejor; pero también sirve para disponer de una base sobre la que defenderse legalmente, sea para actuar legalmente contra los intrusos, sea para recabar la ejecución de pólizas de seguro que hubiera podido contratar como contingencia ante tales «accidentes». Para ello es importante utilizar metodología, aplicaciones y tecnologías que sean aceptadas en los tribunales, con el propósito de presentar este análisis como prueba en un informe pericial.

En este módulo vamos a desarrollar las líneas generales del análisis forense. Empezaremos con una presentación general de las ciencias forenses y su aplicación en el mundo de la informática, como medio para reunir pruebas en un incidente o situación tecnológica de manera ordenada y metódica y que deban tener valor probatorio para poderlas utilizar posteriormente en el ámbito procesal. Si bien hay tendencia a pensar que las pruebas informáticas se pueden crear, modificar o destruir fácilmente, y por tanto son difíciles de aportar, se tiene que considerar que, al fin y al cabo, estas pruebas son igualmente «reales», puesto que están almacenadas en apoyos físicos.

A continuación, se desarrollará el concepto de informática forense, su imbricación en la organización y el aspecto metodológico que la acompaña; y finalizaremos con una introducción al ciberdelito.

En el tercer apartado, el tema central del módulo, se trabajarán, a nivel de proceso general, las etapas por las que ha de discurrir el análisis forense informático, desde la identificación de la evidencia digital hasta la confección del informe pericial, el cual debe permitir responder a todas o a la mayoría de las preguntas clave objeto del análisis forense:

- ¿Qué ha sucedido?
- ¿Cuándo ha sucedido?

- ¿Dónde se ha cometido?
- ¿Quién lo ha hecho?
- ¿Cómo se ha llevado a cabo?
- ¿Por qué se ha cometido?

El último apartado explica de manera general diferentes tipos de jurisdicciones y su marco de actuación legal para que se vea la diferencia y algunas peculiaridades, pero sin profundizar en cada una. Hay que tener presente que este es un tema muy extenso y el objetivo de tratarlo en esta asignatura es para destacar la relevancia e implicaciones, cada vez más importantes, de los incidentes en la seguridad de la información.

En resumen, en este módulo se busca concienciar al estudiante que ante un incidente solo la informática forense nos permite averiguar lo que ha pasado y reunir las pruebas digitales de forma que, si procede, se puedan usar en términos jurídicos.

Para trabajar este módulo no se dispone de material específico desarrollado *ad hoc* y se utilizará como base parte del material desarrollado por la UOC para la asignatura *Análisis forense de sistemas de información* incluido como referencia 2 en el apartado «Bibliografía». En particular se propone:

- Como enfoque general del módulo y planteamiento de las ciencias forense recomendamos la lectura completa del apartado «Disciplinas forenses» del módulo «Conceptos básicos».
- Para el conocimiento del objeto de la informática forense utilizaremos los apartados «Marco conceptual», «La informática forense en las organizaciones» e «Informática» del módulo «Conceptos básicos».
- La comprensión de las etapas del análisis forense informático se realizará mediante la lectura de los apartados «Informática forense y prueba digital», «Securización de la escena del suceso», «Identificación de la prueba digital», «Adquisición de pruebas digitales», «Análisis de la prueba digital e investigación» y «Presentación e informe» del módulo «Fases y metodología del análisis forense».
- Para el último capítulo se utilizarán los subapartados 1, 2 y 3 del apartado «Aspectos procesales», del módulo 4 «El Peritaje: El análisis forense y el sistema legal».
- Asimismo, a nivel general de todo el módulo, se recomienda la lectura del apartado 2 del libro incluido como referencia 3.

Con los materiales de este módulo didáctico se busca aprender y desarrollar los conocimientos y habilidades siguientes:

- Comprender las ciencias forenses y cómo la informática forense se desarrolla a partir de estas ciencias.
- Saber dónde y cuándo se usa y puede ser útil la informática forense en una organización.

- Conocer cuál es el rol del experto forense.
- Conocer la definición de terminología forense básica.
- Comprender de qué manera las diferentes técnicas forenses se relacionan con los sistemas informáticos y la gestión de incidencias.
- Comprender cuál es la metodología básica de trabajo del experto forense.
- Saber aplicar esta metodología para comprender un informe pericial.
- Comprender cómo la informática forense ayuda a mantener y reforzar la seguridad del sistema informático.

7. Normativas

Como colofón a la asignatura se ha definido un módulo transversal a toda ella en el que se recogen las normativas, estándares y referencias legales que están involucradas en la seguridad de la información y que se han citado a lo largo de todo el curso.

Básicamente son las referentes a:

- Serie de normativas ISO/IEC 27000. Se puede acceder a sus características generales a través de su web pública www.iso27000.es.
- LSSI: Ley de Servicios de la Sociedad de Información de España, Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de Información y Comercio Electrónico.
- LOPD y conjunto de leyes y normativas recogidas en la publicación *Códigos electrónicos Protección de Datos de Carácter Personal* del BOE.
- Certificados digitales: se recomienda consultar la web del departamento CERES (Certificación Española de la FNMT-RCM): https://www.cert.fnmt.es.
- Certificaciones de seguridad: consultar la web de ISACA (Information Systems Audit and Control Association), en http://www.isaca.org.

Bibliografía

Arqués Soldevila, J. M.; Colobrán Huguet, M.; Iparraguirre Vilarrasa, J. (2016). *Com s'ha de fer l'informe pericial d'un delicte informàtic?* Barcelona: Editorial UOC. **Referencia 3**.

Colobrán Huguet, M.; Arqués Soldevila, J. M.; Guasch Petit, A. (2012). *Análisis forense de sistemas de información* [Recurso en línea]. <http://materials.cv.uoc.edu/daisy/Materials/PID_00146431/html5/index.html>. **Referencia 2**.

Cruz Allende, D.; Garre Gui, S. (2011). *Sistema de gestión de la seguridad de la información* [Recurso en línea]. <http://cataleg.uoc.edu/record=b1046504~S1%2Acat>. **Referencia 1**.

Domingo Ferrer, J.; Herrera Joancomartí, J.; Rifà Pous, H. (2014). *Criptografía* [Recurso en línea]. <http://cataleg.uoc.edu/record=b1047904~S1%2Acat>. **Referencia 5**.

Estevan de Quesada, R. (2017). *Auditoría técnica y de certificación* [Recurso en línea]. <http://cataleg.uoc.edu/record=b1047772~S1%2Acat>. **Referencia 6**.

Serra Ruiz, J.; Colobrán Huguet, M.; Arqués Soldevila, J. M.; Marco Galindo, E. (2012). *Administración de redes y sistemas operativos* [Recurso en línea]. <http://0-cvapp.uoc.edu.cataleg.uoc.edu/autors/MostraPDFMaterialAction.do?id=190180>. **Referencia 4**.