Introducción a la seguridad de la información

Silvia Garre Gui

PID_00177809

Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción

El concepto de seguridad es muy antiguo, pues desde tiempos inmemoriales los humanos han hecho esfuerzos y tomado medidas para proteger aquello que consideraban que era suyo o que tenía un valor que debía ser preservado.

En la sociedad actual uno de los principales bienes a proteger, aquel que representa un mayor valor para los negocios, es la información, y de ahí la necesidad de protegerla, ya que el mundo está cada vez más conectado, y los ataques a las infraestructuras, redes y sistemas son cada vez más sofisticados.

A lo largo de este módulo se sentarán los conceptos y pilares básicos sobre los que se asienta la gestión de la seguridad de la información, se revisarán brevemente diferentes aproximaciones de modelos de gestión, se presentará el marco normativo en torno a la seguridad de la información y, finalmente, se hablará de algunos estándares internacionalmente reconocidos en esta materia.

Objetivos

Los objetivos que persigue el presente módulo son los siguientes:

1. Entender qué se entiende por *seguridad de la información*, y su diferencia respecto del concepto de *seguridad informática*.

2. Conocer los pilares sobre los cuales se asienta la seguridad de la información: confidencialidad, integridad, disponibilidad y otros, así como los diferentes tipos de medidas de seguridad.

3. Presentar brevemente diferentes modelos de gestión adoptados hoy en día por las organizaciones.

4. Dar a conocer la principal legislación española con implicación en seguridad de la información.

5. Describir someramente los principales estándares de reconocimiento internacional, que hablan sobre seguridad de la información.

1. Qué es seguridad de la información

Como se decía en la introducción de este módulo, la información es hoy en día uno de los principales activos, si no el principal, de muchas compañías. La necesidad de proteger uno de los activos de mayor valor para la compañía ha llevado a que muchas organizaciones hayan dedicado un sinfín de recursos a este fin.

El tipo de tareas llevadas a cabo en este sentido y de medidas de seguridad implantadas han variado mucho en el tiempo. La digitalización de la información, Internet y la evolución de las nuevas tecnologías han devenido las introductoras de grandes cambios, debido a la aparición de nuevas amenazas jamás antes imaginadas.

A esto hay que añadir los nuevos modelos de gestión que se van imponiendo y que estas nuevas tecnologías están propiciando, al pasar de gestionarlo todo absolutamente de forma interna en la organización en un extremo, a contratar servicios en la nube (*cloud computing*) en el extremo opuesto.

Es importante no confundir el término *seguridad de la información*, con el término *seguridad informática*, puesto que si bien el primero engloba al segundo, no son sinónimos. La seguridad informática se ocupa únicamente de la seguridad de los sistemas de información y, por tanto, queda circunscrita al ámbito de la información automatizada, siendo por ello un término mucho más restrictivo que el de *seguridad de la información*, que se ocupa de la información **en todas sus formas** (oral, escrita, impresa, electrónica, óptica, electromagnética...) y **en cualquier momento de su ciclo de vida** (creación o captura, mantenimiento, distribución y uso, y almacenamiento, archivo y destrucción), para protegerla de cualquier amenaza que pudiera suponer pérdida o disminución del valor de la misma.

De todo ello se deduce que la seguridad de la información es una cuestión que afecta a toda la compañía, ya que toda la organización trabaja con información y que, por tanto, requiere de una gestión coordinada y transversal, lo cual comporta planificación y gestión, y no puede ser improvisado, sino que debe ser considerado como un proceso más de la compañía que interactúa con el resto de los procesos del negocio.

2. Dimensiones de la seguridad de la información

Tradicionalmente, hablar de seguridad de la información era referirse a los tres pilares básicos:

- **Confidencialidad**: sólo las personas autorizadas tienen acceso a la información sensible y/o privada.
- **Integridad**: la información y sus métodos de procesamiento son exactos y completos, y no pueden ser manipulados sin autorización.
- **Disponibilidad**: los usuarios autorizados pueden acceder a la información cuando lo necesitan.

No obstante, en los últimos tiempos se consideran también otras dimensiones de la seguridad, contempladas por la propia legislación vigente:

- **Autenticidad y no repudio**: existe garantía de la identidad de los usuarios o procesos que tratan la información, y de la autoría de una determinada acción.
- **Trazabilidad**: es posible reproducir un histórico o secuencia de acciones sobre un determinado proceso y determinar quién ha sido el autor de cada acción.

Los pilares de la seguridad de la información.

Finalmente, puede ser también útil, al trabajar en seguridad de la información, tener en consideración la **privacidad**, que garantiza que sólo las personas autorizadas tienen acceso a información de carácter personal. Es importante notar que *confidencialidad* y *privacidad*, aunque están muy relacionadas, no son sinónimos, ya que la *privacidad* se refiere únicamente a datos de carácter per-

sonal que pueden o no ser públicos, mientras que la *confidencialidad* se refiere a información, personal o no, que la compañía, por el motivo que fuere, quiere proteger de ser difundida abiertamente.

Todas las dimensiones de seguridad son relevantes y deben ser tenidas en consideración por igual, aunque dependiendo del tipo de información que se esté tratando, tendrá mayor importancia una u otra.

Ejemplo

Si el objetivo es proteger la información de nóminas de una compañía, la confidencialidad e integridad serán las dimensiones más relevantes.

Si por el contrario el objetivo es proteger una página de comercio en línea, posiblemente sean más importantes la integridad y la disponibilidad.

Si el objetivo es proteger una página a través de la cual los ciudadanos realizan trámites electrónicos con la Administración, disponibilidad, integridad y trazabilidad pasarán por delante.

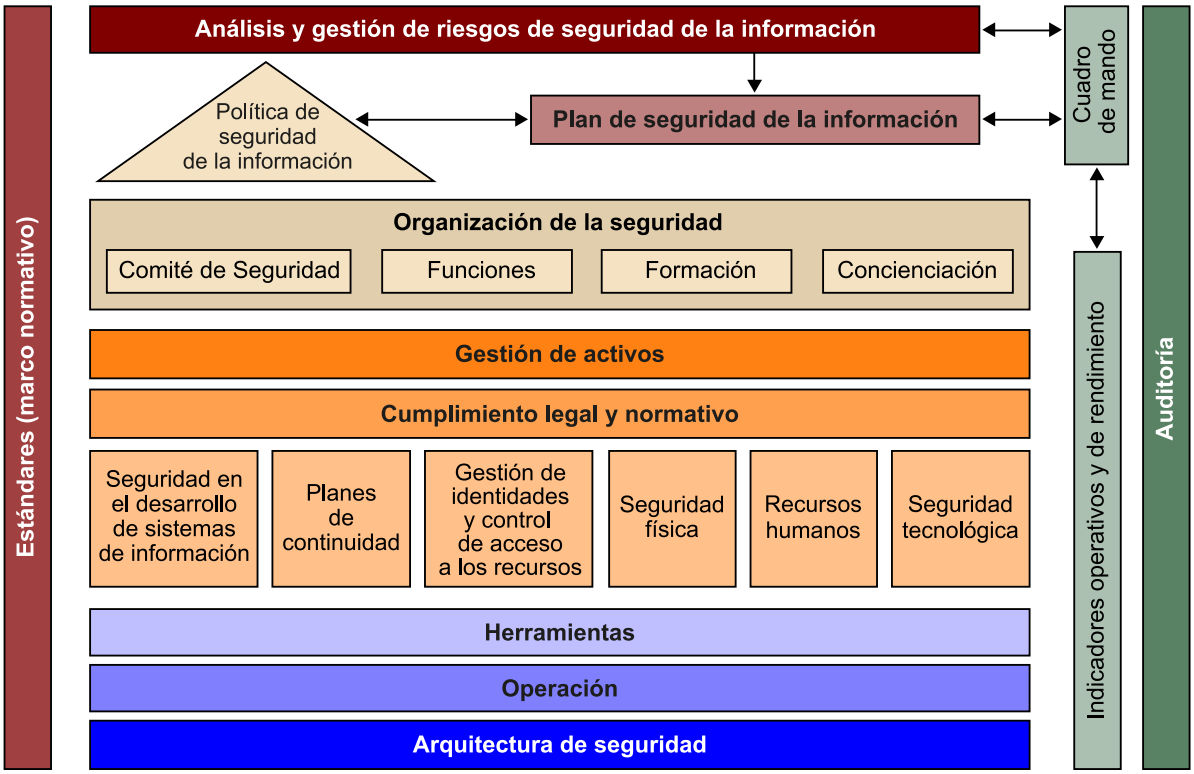
Y si el objetivo es proteger un sistema de comunicación a los ciudadanos para emergencias de carácter nacional, la disponibilidad será primordial.

3. Gestión de la seguridad de la información

La seguridad de la información es, por tanto, un proceso de la compañía que debe ser gestionado y que requiere dedicación de recursos personales y económicos, siendo indispensable una buena definición de la organización de la seguridad de la información y una buena asignación de funciones, para que ésta sea realmente eficiente y quede incorporada al día a día de la compañía.

La gestión de la seguridad de la información comporta un gran número de actividades, que en este punto enunciamos, y que se irán tratando a lo largo del curso. El siguiente esquema presenta de una forma sencilla las distintas actividades que hay que abordar en materia de seguridad de la información y que, como se puede observar, pueden ser de tipo organizativo o técnico y, en ocasiones, también jurídico.

Dependiendo del estado de madurez de la organización en cuanto al despliegue de la seguridad de la información, será necesario priorizar las actividades de una u otra forma, pero a la larga, la gestión de la seguridad requerirá de la dedicación de esfuerzos por parte de la organización a cada una de las actividades plasmadas a continuación:



El proceso de gestión de la seguridad de la información.

3.1. Modelos de gestión

Existen diferentes modelos de gestión de la seguridad de la información, todos ellos válidos. Cada organización deberá analizar cuál de dichos modelos se adapta mejor a su idiosincrasia y características.

3.1.1. Gestión interna de la seguridad

La seguridad es gestionada íntegramente por personal propio, lo cual requiere de la contratación de personal especializado.

Este modelo debe tener un responsable de seguridad de la información, a quien un equipo de trabajo, cuyo tamaño variará con la tipología de la compañía, dé soporte.

Como puntos fuertes cabe destacar el conocimiento del negocio y la implicación del personal. Como puntos débiles, el coste de contratación y la falta de flexibilidad en el dimensionamiento de los equipos.

3.1.2. Gestión externalizada de la seguridad

La compañía subcontrata una empresa externa para gestionar íntegra o parcialmente su seguridad. El personal externo puede estar ubicado internamente o realizar una gestión en remoto según las actividades subcontratadas.

Como punto fuerte cabe destacar la alta especialización, puesto que se trata de personal altamente cualificado y con experiencia, que aporta el valor de estar trabajando con otros clientes. Como punto débil, la falta de conocimiento del negocio y la posible desconfianza del personal interno.

Este modelo requiere establecer un buen contrato, en el que queden claramente definidas las responsabilidades de una y otra parte, así como los acuerdos de nivel de servicio (ANS).

Las empresas que ofrecen servicios de gestión de seguridad de la información en remoto suelen recibir el nombre de SOC o *security operations center.* Un SOC se caracteriza por disponer de:

- Avanzadas herramientas de gestión y monitorización de la seguridad de los sistemas de información.
- Avanzadas herramientas de detección de incidentes de seguridad desde un punto centralizado.
- Personal altamente especializado y conocedor de los últimos avances de la tecnología.

Habitualmente, el SOC opera monitorizando la seguridad de sus clientes 24 × 7 (24 horas, 7 días a la semana).

Las actividades más típicas de un SOC son la protección contra intrusiones y ataques externos, prestando habitualmente servicios de: análisis de actividad de cortafuegos, IDS, IPS, antivirus y en general código malicioso, así como la detección de vulnerabilidades, aunque puede ofrecer también servicios de configuración segura del hardware y del software, monitorización de la disponibilidad de sistemas, auditorías de seguridad, pruebas de penetración, asistencia técnica, etc. Además, acostumbra a tener capacidad de reacción para contener los incidentes. Obviamente, un SOC dispone de procedimientos de actuación claramente definidos y estandarizados, destacando entre otros el de escalado de incidentes al cliente.

3.1.3. Modelo mixto

Existe una organización interna en seguridad de la información, que se apoya en un equipo de personal especializado externo.

Este modelo reúne los puntos fuertes de los modelos anteriores y elimina los puntos débiles.

Es habitual que el personal interno desarrolle aquellas tareas más organizativas y menos técnicas, quedando la parte más técnica en manos de personal externo experto.

3.2. Punto de partida

Sea cual fuere el modelo de gestión escogido por la compañía, el proceso de implantación de la seguridad de la información no puede ponerse en marcha sin antes trabajar sobre los cuatro puntos siguientes:

- **Conocimiento del negocio.** La seguridad de la información debe estar al servicio del negocio, por lo cual, es imprescindible conocer la actividad del negocio y sus objetivos, con el fin de aplicar una seguridad que soporte dichos objetivos de manera eficiente y proporcional a los riesgos a mitigar. Por lo tanto, es necesario entender cuáles son los procesos de negocio que se llevan a cabo, identificando los más críticos, lo que permitirá priorizar acciones.

- **Análisis de la situación de partida.** Antes de empezar a aplicar medidas de seguridad, es importante efectuar un análisis de la situación de partida, con el fin de conocer el estado de la seguridad y su nivel de eficiencia, tanto a nivel técnico como a nivel organizativo. Ello permitirá identificar la distancia entre la situación de partida y la situación deseada y definir un plan para aproximarlas.

- **Análisis de riesgos.** Más adelante se estudiará en detalle en qué consiste el análisis de riesgos, que es uno de los fundamentos para una buena gestión de la seguridad, pero tal y como su nombre indica, el análisis de riesgos analiza cuáles son los riesgos a los que el negocio está expuesto, a partir de la valoración de cuál sería el impacto para el negocio en caso de materialización de una amenaza.

Ejemplo

Supongamos una empresa de producción de maquinaria *on-demand*, para la cual, mantener operativa la línea de producción 24 × 7 es imprescindible para cumplir con los acuerdos de nivel de servicio establecidos con sus clientes. En este caso, la disponibilidad es la dimensión más crítica del proceso y será necesario analizar de forma prioritaria qué posibles amenazas contra la disponibilidad podrían materializarse produciendo interrupciones en la producción.

Existen amplios catálogos de amenazas; algunos ejemplos de amenazas a la disponibilidad serían: inundación/incendio, corte del suministro eléctrico, baja de personal clave, caída del sistema informático de control de la producción, etc.

El riesgo será mayor, a mayor probabilidad de ocurrencia de la amenaza por un lado, y a mayor impacto sobre el negocio por el otro.

El conocimiento del riesgo al que la compañía está expuesta, o dicho de otro modo, la capacidad para trabajar en un entorno de riesgos gestionados, mejora la toma de decisiones en materia de seguridad de la información y facilita la priorización de acciones.

- **Cumplimiento legal.** Es indispensable conocer cuál es la legislación que es de aplicación a la compañía (internacional, nacional, autonómica, sectorial...), ya que esta legislación puede exigir la aplicación de ciertas medidas de seguridad que deberán ser incorporadas obligatoriamente al proceso de gestión del riesgo.

3.3. Medidas de protección

Control o salvaguarda

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

Una vez que la organización conoce cuáles son los riesgos a los que está expuesta y determina cuál es el nivel de riesgo máximo que está dispuesta a asumir, se debe proceder a seleccionar las medidas de seguridad a implantar, también denominadas controles o salvaguardas. Obviamente, en este proceso deberá regir el principio de proporcionalidad, puesto que el coste de aplicación de una medida no debe nunca exceder el coste derivado de la materialización de una amenaza.

3.4. Tipos de controles de seguridad

1) Según la naturaleza del control: técnicos y organizativos

Son medidas de seguridad técnicas, por ejemplo, un antivirus, un cortafuegos, la configuración de un sistema, un sistema de alimentación ininterrumpida, el cifrado de las comunicaciones.

Son medidas de seguridad organizativas, por ejemplo, la elaboración de políticas, normas y procedimientos, la definición de funciones de seguridad, la elaboración del plan de continuidad de negocio, la formación y concienciación.

2) Según si los controles actúan sobre la reducción de la probabilidad o reducción del impacto

Si, como hemos visto, el riesgo es una combinación de probabilidad de materialización de una amenaza e impacto sobre el negocio, podremos diferenciar dos tipos de controles: aquellos que reducen la probabilidad de ocurrencia de una amenaza, y aquellos que reducen el impacto sobre el negocio en caso de materialización de la misma.

Ejemplo

Un sistema de alimentación ininterrumpida reduce el impacto en caso de que se produzca un corte de suministro eléctrico, ya que en caso de producirse el incidente, lo que hace es mantener los sistemas críticos en marcha durante el tiempo suficiente como para conseguir un cierre ordenado. No evita la indisponibilidad del sistema, pero reduce las consecuencias que podría provocar un corte repentino.

De otro modo, un sistema de detección de incendios reducirá la probabilidad de que un incendio llegue a producirse, actuando sobre la probabilidad de materialización de la amenaza, gracias a una detección temprana.

3) Según su finalidad

Dependiendo del momento del ciclo de vida de un incidente en el que el control actúe, podemos diferenciar controles:

- **Preventivos**: actúan para que el riesgo no se materialice, reduciendo la probabilidad de ocurrencia de la amenaza.

  Ejemplo

  Los cortafuegos, ya que son una medida para prevenir la posible intrusión de un *hacker*.

- **De detección**. Detectan el incidente que se ha producido para poder reaccionar con la mayor celeridad posible.

  Ejemplo

  El IDS (sistema de detección de intrusiones o *intrusion detection system*). Este control no reduce el riesgo de acceso sin autorización a los sistemas de la organización, sino que hace saltar una alarma en caso de que suceda.

- **Correctivos**. Permiten reducir el daño y/o la recuperación de la situación normal una vez se ha producido el incidente.

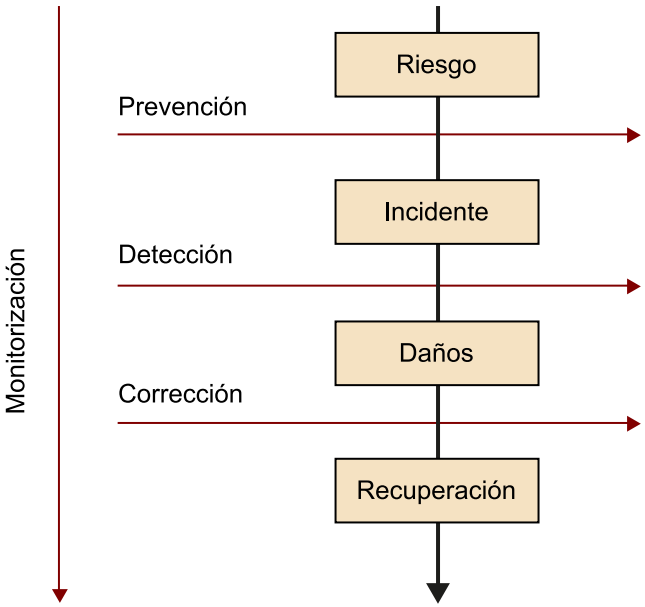
  Ejemplos

  - **Sistema de extinción de incendios y sistema de alimentación ininterrumpida**. Reduce el daño que se provocará.
  - **Copias de seguridad**. Permiten volver a la situación anterior al incidente, recuperando la información en el estado en que se encontraba.

- **De monitorización**. Permiten recoger evidencias y realizar un seguimiento para poder analizar anomalías, tendencias, conductas poco habituales o incidentes detectados.

Ejemplo

El sistema de gestión de trazas. En caso de un incidente de seguridad, se podrá analizar la causa que lo provocó, así como los pasos que se llevaron a cabo para su resolución, permitiendo introducir los cambios necesarios para evitar que vuelva a suceder.



Tipos de controles de seguridad de la información.

Aunque la mayoría de los controles tienen una finalidad básica, hay controles que pueden cubrir más de una finalidad.

Ejemplo

La implantación de una metodología de desarrollo de software podría considerarse probablemente como un control tanto preventivo, como de detección. Una metodología de este tipo debe incluir la seguridad de la información en todas sus fases: desde la toma de requerimientos, pasando por el desarrollo del código fuente para evitar determinadas vulnerabilidades típicas y acabando por la fase de pruebas. Un software nuevo no testeado para comprobar que se han cubierto todos los requerimientos de seguridad establecidos al inicio no debiera pasar nunca a producción. Ahí reside el carácter preventivo de la metodología, puesto que permite detectar deficiencias o vulnerabilidades antes de que éstas puedan ser explotadas. Por otro lado, un buen software se desarrollará con determinados controles y avisos o mensajes que pueden dar pistas de un mal funcionamiento o un mal uso. En este sentido podría considerarse una medida de detección.

4. Normativa legal en España

En realidad, la aplicación de medidas de seguridad es una cuestión opcional en una compañía, salvo en el caso de que exista una norma legal que establezca su obligatoriedad.

Es por tanto indispensable conocer cuál es la normativa legal de aplicación a la actividad desarrollada por la compañía, ya sea a nivel internacional, europeo, nacional, autonómico o local, y también a nivel sectorial (por ejemplo, existe legislación específica del sector sanitario, medioambiental...).

Se presentan a continuación algunas de las normas legales con mayor afectación general sobre la seguridad de la información en España. Cualquier profesional dedicado a la seguridad de la información debiera tener nociones sobre su contenido y haber leído como mínimo la exposición de motivos inicial. Todas ellas son consultables en el *Boletín Oficial del Estado*:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, habitualmente conocida como LOPD.

- Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la LOPD. Es en este real decreto donde se recogen las medidas de seguridad que hay que aplicar a sistemas de información automatizados y no automatizados (papel).

- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, habitualmente conocida por LAECSP, de aplicación a la Administración pública.

- Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, habitualmente conocido como ENS. Este real decreto es únicamente de aplicación a la Administración pública.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, habitualmente conocida por LSSI.

- Ley 50/2003, de 19 de diciembre, de Firma Electrónica.

- Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones y a las Redes Públicas de Comunicaciones.

5. Estándares de seguridad de la información

Existen estándares de seguridad de la información con reconocimiento a nivel internacional, aplicables a cualquier tipo de organización, independientemente de su actividad o tamaño. Dichos estándares o normas son muy buenas guías de referencia u hojas de ruta para la gestión de la seguridad de la información.

Se exponen a continuación algunos de ellos. Normalmente no son normas gratuitas y, una vez adquiridas, la autorización de uso está restringida exclusivamente a la organización que la ha adquirido:

1) Normas de la familia ISO27000. En el siguiente capítulo se hace una breve descripción de las diferentes normas de esta familia, pero cabe destacar:

- ISO 27002: Código de buenas prácticas.
- ISO 27001: Especificación de requisitos de sistemas de gestión de seguridad de la información. Es la norma certificable.

2) Normas relativas a la continuidad del negocio: norma británica BS25999.

- BS25999-1 Código de buenas prácticas.
- BS25999-2 Especificación de requisitos de un sistema de gestión de la continuidad de negocio (SGCN), basado en el código de buenas prácticas recogidas en la parte 1 de la norma. Es la norma certificable.

3) Normas relativas a la continuidad de servicios TI: BS25777.

- BS 25777-1 Código de buenas prácticas sobre cómo abordar la gestión de la continuidad de servicios de tecnologías de la información en una organización.
- BS25777-2 Requisitos para establecer, implementar, operar, supervisar, revisar, probar, mantener y mejorar un sistema de gestión de la continuidad de los servicios de tecnologías de la información y comunicación (TIC). Es la norma certificable.

4) CobIT (*control objectives for information and related technology*). CobIT es un marco de trabajo o modelo de sistema de control interno para el gobierno de las TI que se ha convertido a nivel internacional en un estándar de facto. Aporta un marco de referencia que cada organización ha de adecuar a la realidad de su negocio para establecer:

- ¿Cómo consigue la organización la información que necesita?

- ¿Cómo garantiza la contribución de TI la consecución de los objetivos de la empresa?
- ¿Cómo se gestionan los riesgos técnicos?
- ¿Cómo se protegen los recursos críticos?
- ¿Cómo controla la organización y cómo mide las TIC?

CobIT define 5 áreas de trabajo clave:

- Alineación estratégica
- Entrega de valor
- Administración de riesgos
- Administración de recursos
- Medición del desempeño

Áreas de CobIT.

5) ITIL. El acrónimo derivado del inglés *information technology infrastructure library* es un marco de trabajo para la gestión y provisión de servicios de tecnologías de la información. Es un conjunto de buenas prácticas para la planificación, provisión y soporte de los servicios TI de la compañía.

La versión actual de ITIL es la v.3., que basándose en el ciclo de vida de un servicio trabaja sobre cinco ejes básicos:

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

La versión anterior ITIL v.2. trabajaba sobre dos ejes primordiales:

- Provisión de servicios: gestión del nivel de servicio, gestión financiera de los servicios TI, gestión de la capacidad, gestión de la continuidad del servicio, gestión de la disponibilidad.
- Soporte del servicio: gestión de lanzamientos, gestión de cambios, gestión de configuraciones, gestión de problemas, gestión de incidencias.

Que se complementaban con buenas prácticas sobre:

- Gestión de la infraestructura de TI
- Gestión de la seguridad
- Perspectiva de negocio
- Gestión de aplicaciones
- Gestión de activos de software

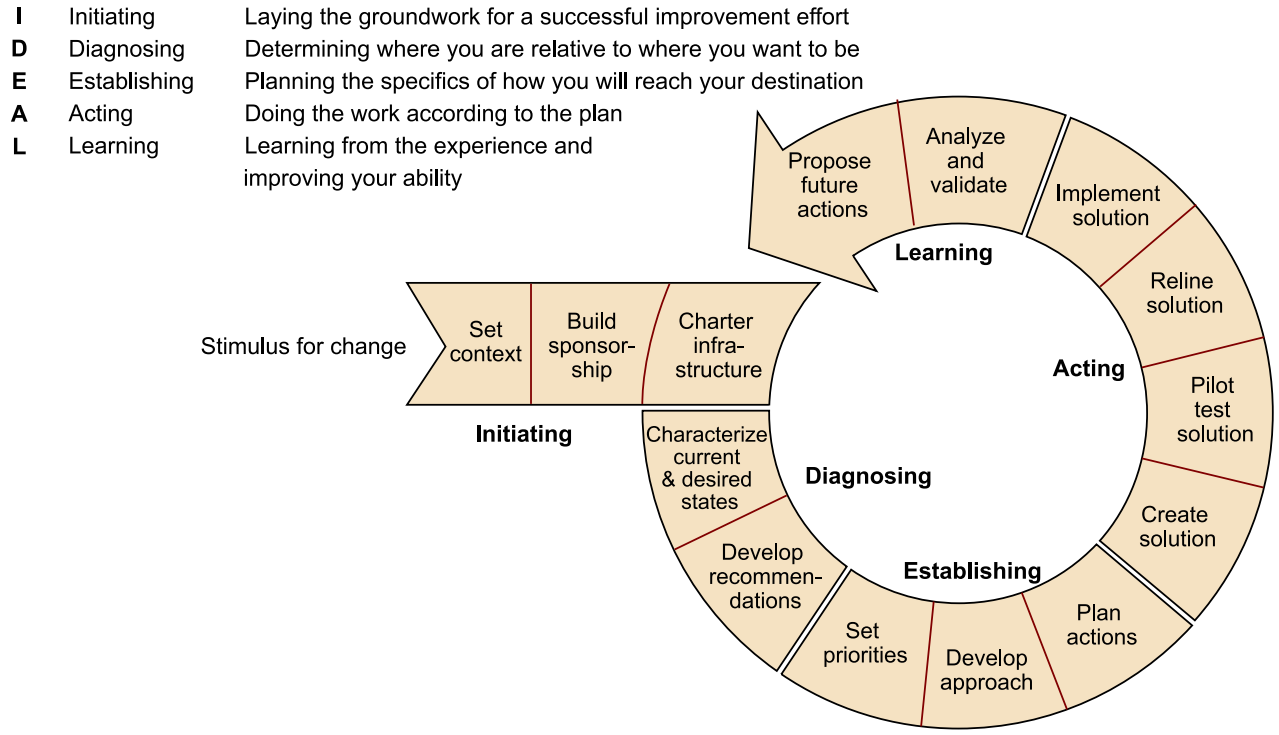
Obviamente, ésta no es una norma específica de seguridad de la información, pero es bueno conocerla en caso de que nuestra organización la haya adoptado, ya que complementa al proceso de gestión de la seguridad de la información en muchos aspectos.

6) *Capability maturity model* (CMM) y SSE – CMM. El CMMI es un marco de trabajo para la mejora de procesos, que proporciona a las organizaciones los elementos esenciales para desarrollar procesos eficientes y de calidad. Puede utilizarse para realizar la mejora de procesos en un proyecto, división o en toda una organización. Ayuda a integrar funciones de la organización tradicionalmente aisladas, establecer los objetivos de mejora de un proceso, y proporciona un punto de referencia para comparar procesos.

Es aplicable en el desarrollo de productos y servicios, en el montaje, gestión y provisión de servicios, así como en la adquisición de productos y servicios.

7) SSE-CMM o Modelo de madurez de capacidades en la ingeniería de seguridad de sistemas (*system security engineering capability maturity model*). Es un modelo derivado de CMM, que describe las características esenciales de los procesos que deben existir en una organización para asegurar una construcción segura de sistemas.

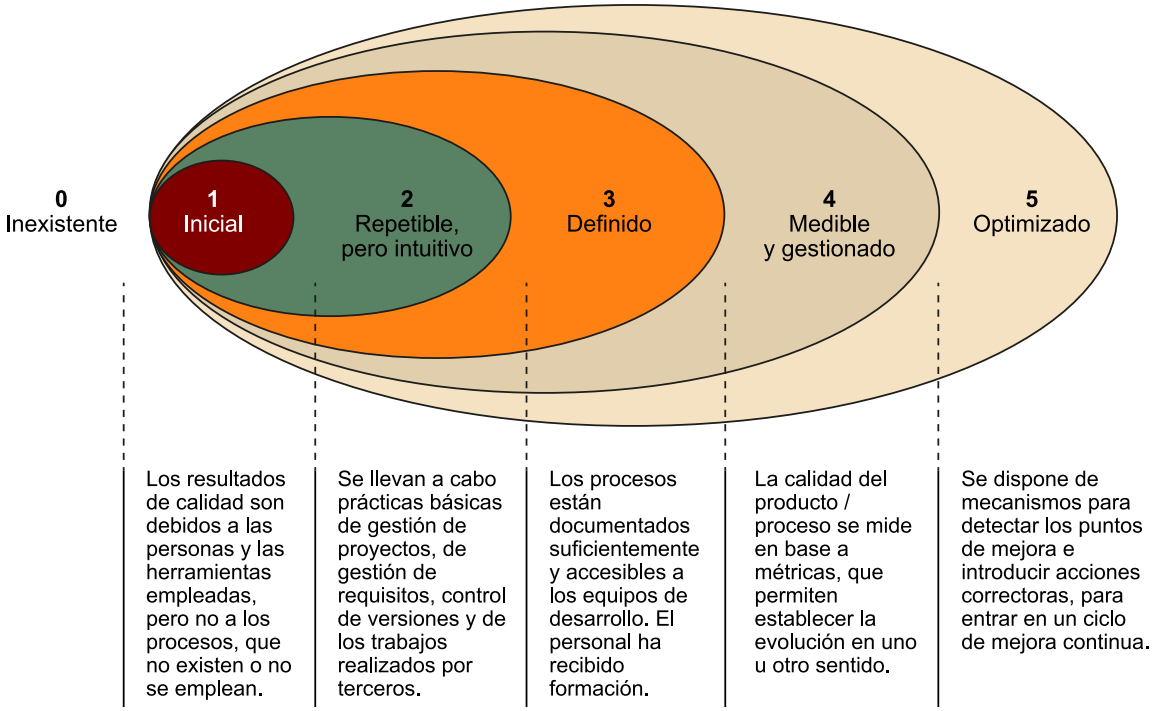
Se puede esquematizar en cinco fases de alto nivel:



Esquema del CMMI.

Se hace referencia a esta metodología de mejora de los procesos de desarrollo y mantenimiento de software en sus versiones iniciales (CMM), y de mejora en general de los procesos de una organización o proyecto en su última versión

(CMMI), no como guía para la implantación de la seguridad de la información, sino porque el concepto de madurez se utiliza habitualmente en el ámbito de la seguridad de la información, para medir el estado de la seguridad o, dicho de otro modo, para medir el grado de implantación de los controles de seguridad. Así pues, es habitual que cuando se realizan auditorías o evaluaciones internas sobre el estado de la seguridad, o el estado de implantación de alguna norma o estándar, se describa el estado a partir de la definición CMM de madurez de los controles.



Los niveles de madurez del CMM.

La aplicación del modelo de madurez permite establecer criterios objetivos para la evaluación de la eficacia de los controles gracias a la repetibilidad de la medida, permitiendo así analizar su evolución en el tiempo.

Ejemplo de aplicación del modelo de madurez a un control de seguridad de la información

Control: "Las responsabilidades en seguridad de la información están definidas".

- **0-Inexistente**: No existe una definición de responsabilidades en materia de seguridad de la información.
- **1-Inicial/existe una aproximación**: Las responsabilidades principales se asignan o asumen informalmente. Cada persona conoce su responsabilidad, pero no la de los demás.
- **2-Repetible/existe con muchas deficiencias**: Se sabe quién asume las principales funciones en materia de seguridad TIC y resto del negocio, pero las funciones de seguridad no están específicamente definidas ni documentadas, sino que se asumen individualmente como parte de otras funciones (ej: dirección de un proyecto).
- **3-Definido/existe con algunas deficiencias**: Las responsabilidades en seguridad de la información están definidas y documentadas a todos los niveles del negocio, están aprobadas y asignadas por la Dirección, se han dado a conocer y se ha realizado o planificado la capacitación de todas aquellas personas que lo requieran.

- **4-Medible y gestionado/existe y es correcto**: Las responsabilidades están definidas y documentadas a todos los niveles del negocio, están aprobadas y asignadas por la Dirección, se ha hecho difusión entre el personal y formación a aquellos que requerían conocimientos específicos, pero no se realiza una revisión anual de que todas las funciones están bien asignadas y de que los diferentes responsables desarrollan su función.

- **5-Optimizado/existe y está integrado en un ciclo de mejora continua**: Las responsabilidades están definidas y documentadas a todos los niveles del negocio, están aprobadas y asignadas por la Dirección, se ha hecho difusión entre el personal y formación a aquellos que requerían conocimientos específicos, periódicamente se revisa el desarrollo de estas funciones y existe un proceso para detectar deficiencias en la asignación y coordinación de funciones y aplicar correcciones.

En una organización con un grado de madurez bajo, puede plantearse la reducción del número de niveles de madurez, agrupando algunos de ellos.

6. Estado de la seguridad

La vertiginosa evolución de la tecnología hace difícil estar al día de toda la tecnología emergente y de la evolución de la existente.

No obstante, para un profesional de la seguridad de la información es imprescindible mantenerse al día de cuáles son las tendencias, hacia dónde evolucionan las soluciones de seguridad, cuál es el estado real de la seguridad en su sector, entorno, país..., cuáles son los incidentes de seguridad más relevantes que están teniendo lugar, etc.

Es por tanto importante mantener contacto con el mercado y los proveedores de soluciones, asistir a los eventos del mundo de la seguridad que se organizan anualmente a todos los niveles, leer prensa especializada, y consultar webs especializadas en la materia.

Entre otras muchas webs de gran interés, cabe destacar a nivel del Estado español la web del Instituto Nacional de Tecnologías de la Comunicación, S.A., conocido como INTECO, que es una sociedad mercantil estatal, con sede en León (España), adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. INTECO tiene encomendadas a través del Plan Avanza las misiones de sentar las bases de coordinación de distintas iniciativas públicas en torno a la seguridad de la información, impulsar la investigación aplicada y la formación especializada en el ámbito de la seguridad en el uso de las TIC y convertirse en el centro de referencia en seguridad de la información a nivel nacional. INTECO, a través de su CERT, ofrece soluciones reactivas a incidentes informáticos, servicios de prevención frente a posibles amenazas y servicios de información, concienciación y formación en materia de seguridad de la información, análisis del estado de la seguridad, informes de vulnerabilidades... que resultan de gran utilidad para la gestión de la seguridad. En el ámbito catalán, día a día va adquiriendo más importancia el Centro de Seguridad de la Información de Cataluña (CESICAT).

CERT (Computer Emergency Response Team)

Es un centro orientado al análisis y monitorización de la red (Internet), para la detección de vulnerabilidades y comportamientos anómalos, con el fin de alertar a la comunidad sobre amenazas e incidentes y actuar, en caso de necesidad, en coordinación con otros CERT a nivel local, nacional, o internacional.

7. Profesionales de la seguridad de la información

La gestión de la seguridad de la información requiere de una combinación de profesionales especializados que deben cubrir perfiles de gestión, de auditoría y técnicos.

Existen a nivel internacional múltiples organizaciones cuya actividad se focaliza en la seguridad de la información, y que ofrecen certificaciones de seguridad para acreditar los conocimientos, especialización y experiencia de los profesionales del sector.

Las certificaciones profesionales son un recurso muy extendido en el mundo de la seguridad de la información y son muchos los profesionales que se certifican, para lo cual puede ser preciso acreditar un mínimo de experiencia, así como mantener dicha certificación. Para ello, en muchos casos se requiere del pago de una cuota anual a la asociación certificadora, y sólo es posible manteniéndose en activo, participando en foros, seminarios, sesiones formativas..., lo cual garantiza la cualificación de sus titulares.

Se exponen a continuación los sellos de algunas de las certificaciones más habituales en el sector, pero no las únicas.

Un indicador de la importancia de la certificación profesional en seguridad de la información es el hecho de que cada vez más, la Administración pública requiera profesionales certificados en la contratación de servicios sobre la materia.

Certificaciones en seguridad de la información.