Seguridad y auditoría de la información

PID_00248481

Santiago Codolà Vilahur

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Índice

1. Información y seguridad

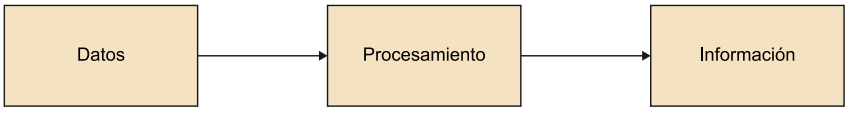
1.1. El valor de la información

En el entorno empresarial, en muchas ocasiones, se utilizan los términos *datos* e *información* como sinónimos; si bien son muy diferentes y aunque relacionados, es necesario establecer estos conceptos.

Así, los **datos** son «grupos de símbolos no aleatorios que se erigen en representación de algo (cantidades, objetos, acciones, etc.)». Los datos se constituyen a partir de caracteres; pueden ser la combinación de letras, números o símbolos que conforman una palabra, cifra o imagen que se refiere a algo. Los datos describen hechos empíricos, sucesos y entidades. Pero los datos aisladamente pueden no contener información humanamente relevante; por ejemplo, el código 840280985G por sí solo no aporta información, necesitamos saber a qué se refiere este código o palabra: puede ser un número de documento de identidad o el identificador de un producto, en el primer caso necesitamos saber a quién se refiere, y en el segundo qué producto representa.

Los datos son la materia prima imprescindible para conseguir información; para ello es necesario que exista un proceso de elaboración que sea capaz de manejar los datos y convertirlos en información. Los datos se convierten en información cuando son útiles para algún propósito, y una vez que son procesados obtienen un significado, un propósito y una utilidad, es decir, cuando a los datos se les agrega algo más (inteligencia) se convierten en información.

Figura 1.



Un dato se convierte en información si es capaz de contestar a una pregunta o solucionar un problema de información; es decir, la información se vincula a «los datos que hacen falta para tomar decisiones».

La diferencia entre dato e información no reside en el contenido del conjunto de caracteres dado, más bien reside en su utilidad para la toma de una decisión.

En definitiva, los datos, para convertiste en información, han de detentar una serie de características:

- **Utilidad**. Deben servir en el proceso de la toma de decisiones, influyendo en las acciones que se adopten.
- **Relevancia**. Si el dato no es relevante no servirá para responder a una pregunta o proporcionar conocimiento sobre algo.
- **Ser interpretables**. Si los datos carecen de un significado, si no se puede interpretar su sentido, no servirán para el proceso de toma de decisiones.
- **Ser perceptibles**. Si el dato no se percibe, porque no llega al destinatario o porque llega muy difuminado entre una gran cantidad de otros datos, el usuario no podrá procesarlo.

La **información** es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje, y por tanto ejerce algún tipo de influencia sobre nuestras acciones, ya que puede intervenir en el proceso de toma de decisiones o se pueden utilizar para reducir el nivel de incertidumbre o la realización de cálculos. Sin embargo, hay que considerar que el mismo conjunto de caracteres puede ser un dato o una información para individuos diferentes, de manera similar al hecho de que lo que es materia prima para una empresa puede ser el producto final para otra. Por ejemplo, para un despacho de abogados, un informe pericial es parte de su materia prima, que se utilizará y combinará dentro de un determinado un proceso judicial que es su producto final, mientras que para quien ha realizado el informe, este ya es el producto final. Algo similar ocurre con los datos y la información, ya que aquello que consideramos información en un nivel de la empresa puede ser solo un dato en otro.

La información se utiliza en la mayoría de las ramas científicas como piedra angular sobre la que fundamentar la toma de decisiones. Aparece así un término impreciso, amplio y moldeable en función del entorno en el que se utilice; se desarrolla esta situación hasta tal punto que en numerosos casos se obvia su definición por considerar que algo tan común y próximo a todas las facetas de nuestra vida no necesita demostración. En realidad, nos encontramos ante un concepto que puede ser abordado desde numerosos ángulos y diversas perspectivas (lingüística, comunicación, matemáticas, ciencias sociales, informática, etc.).

En general, se asimila información a «todo aquello que reduce la incertidumbre». Esta es una visión muy amplia que enuncia un problema causa-efecto que no se corresponde exactamente con la realidad, ya que no solo reduce la incertidumbre sino que la puede ampliar; más bien habría que decir «todo aquello que varía la incertidumbre». La información es la diferencia entre un estado de incertidumbre y otro inmediatamente posterior, que puede acercarnos a la realidad o alejarnos de ella, sabiendo que la incertidumbre es la carencia de conocimiento o ausencia de información acerca de un área de interés.

La teoría económica nos dice que la tierra, el trabajo y el capital han sido, tradicionalmente, los recursos económicos fundamentales; sin embargo, cada vez con un mayor reconocimiento, la información se ha establecido en cuarto lugar como recurso estratégico decisivo dada su enorme importancia económica.

De hecho, nadie duda de que la información es poder, por lo que cada vez son más las organizaciones que emplean una parte importante de sus medios para obtenerla y controlarla.

La información cobra aún más importancia en aquellos momentos de caos, incertidumbre, desequilibrios y ajustes, y llega a ser tanto o más valiosa que los recursos materiales, humanos y financieros con los que cuenta la empresa. Esto se debe a que la empresa para poder ser competitiva en una economía cada vez más globalizada debe ser capaz de obtener, seleccionar, procesar y aplicar correctamente la información relevante para afrontar cada problema.

La información es un elemento básico en la empresa, de ahí que las empresas, frente a circunstancias tales como la expansión y diversificación de actividades o la constante variación de los empleados en plantilla, sientan la necesidad de estructurar y formalizar sus sistemas de información, a través de su nivel directivo. Y todo ello porque la información es la materia prima imprescindible en todas y cada una de las fases que conlleva una toma de decisiones, entendiendo por esto el proceso dirigido a la selección y ejecución de una acción que resuelve un problema y permite la ejecución de unos objetivos establecidos. La información constituye, pues, un recurso estratégico, lo mismo que los recursos humanos, financieros, tecnológicos o comerciales.

La información es un recurso que cuenta con una serie de características peculiares que la diferencian de otros recursos existentes en la empresa. Estas características son:

- **Transportabilidad**: se puede transportar instantáneamente de un lugar a otro del mundo.
- **Es ilimitada**: el hombre no consume información, sino que la crea constantemente; los recursos de información son inagotables.
- **Subjetividad**: es difícil asignar un valor objetivo a la información. El valor de la información depende de quién la use; se lo asigna el sujeto de acuerdo con sus necesidades concretas en un determinado momento: el sujeto suele percibir el valor de una información como el coste de disponer de ella. La evolución en el tiempo del valor de la información es difícilmente previsible, puede tener un valor extraordinario hoy y no tener ninguno mañana.

1.2. Flujos de información

La irrupción de las nuevas tecnologías ha significado pasar de unos datos e información discretos, en muchas ocasiones costosos de obtener y que afectaban a partes específicas de una organización, a un flujo constante y creciente que afecta a todas las partes, desde la alta dirección al recepcionista. Ahora la dificultad radica en gestionar el flujo de información debido a la velocidad con la que se genera, filtrar e identificar la que se necesita, en el momento adecuado; ello le da pertinencia a la información.

Lo ideal sería que una organización fuera capaz de identificar, captar, clasificar y analizar una gran cantidad de información útil (de mercado, financiera, económica, tecnológica, regulatoria, etc.) y hacerla llegar a las personas adecuadas para generar conclusiones e implementar acciones que respondan de manera óptima a las condiciones del mercado.

En toda organización suelen coexistir tres tipos básicos de flujos de información, y cuanto mayor es la habilidad de la organización para manejar dichos flujos, más importancia adquieren los activos intangibles que se basan en esos flujos.

Por un lado, obtienen información del entorno con el fin de determinar qué productos necesita el mercado y qué tecnologías existen para cubrirlos, es lo que denominamos **información ambiental o externa**.

Por otro lado, la propia organización genera internamente información, que surge del procesamiento de la información ambiental y la derivada de las relaciones en la organización, es la que llamamos **información interna**.

Y por último, dan a conocer los productos y servicios que la empresa realiza, lo que se denomina **información corporativa**.

Veámoslo más detenidamente:

1) Información ambiental o externa. Es la información que entra en una organización procedente del entorno. Es esencial para poder tener éxito en los mercados actuales, y fundamentalmente debe buscar:

- Capacidad de respuesta a las necesidades del mercado. La organización obtiene información procedente del entorno con el fin de determinar estrategias, como por ejemplo qué productos necesita el mercado.
- Adquisición de habilidades tecnológicas. La organización obtiene información procedente del entorno con el fin de determinar qué tecnologías existen, el correcto funcionamiento de las funciones de I+D y la formación; y aumentar la habilidad tecnológica de la organización.

Las organizaciones necesitan información sobre dos entornos muy distintos: entorno inmediato y entorno remoto. Para informarse de cada uno de estos dos entornos existen **fuentes informales** de información (no se registran en ninguna parte y se basan en relaciones personales) y **fuentes formales** (registradas en papel, medio electrónico o en cualquier tipo de soporte físico).

- **Entorno inmediato**. Constituido por aquellos elementos con los que una organización debe tratar a diario: clientes, proveedores, distribuidores, competidores, fuentes de financiación y reguladores.
- **Entorno remoto.** Aquel al que la organización no se ha de enfrentar a diario, pero del que debe monitorizar la información con el fin de identificar los cambios y tendencias que exijan una adaptación de las estrategias de la organización a medio y largo plazo. Es un contexto más amplio: el clima político, la situación económica, las tendencias sociales y las innovaciones tecnológicas. Cada día el entorno remoto se hace más inmediato gracias a las TIC.

2) Información interna. La organización va asimilando y procesando toda esa información externa a la vez que la recibe, y la une a la información interna generada por la propia organización, lo que la ayuda a desarrollar los productos y servicios que posteriormente ofrece a sus clientes. En toda organización cabe distinguir dos grandes tipos de información interna:

- Las organizaciones generan una gran cantidad de **información operacional**, información que resulta del propio funcionamiento rutinario de la organización (listas de clientes, catálogos de productos, listados del inventario en almacén, registros contables, datos numéricos de control de la maquinaria), y que suele ser **formal** y fácilmente almacenable en algún tipo de registro físico.
- Las organizaciones generan conocimientos como resultado de la asimilación o digestión de información interna y externa y de la explotación de las capacidades creativas de sus miembros (se diseñan nuevos productos, se mejoran los procesos, se optimizan los mecanismos de gestión, etc.). La organización aprende y su conocimiento se acumula en forma de *know how*. Esta información es básicamente **informal** y se almacena en la experiencia de las personas.

3) Información corporativa. Así denominamos la salida de la información desde una organización hacia el exterior. Toda organización que quiera sobrevivir debe esforzarse en emitir hacia su entorno un mensaje diferenciado que le permita ser claramente percibible por parte de los consumidores. Existen dos tipos principales de mensajes:

- Una organización puede llevar a cabo acciones **directas** de comunicación: lanzar una campaña publicitaria, explotar su imagen a través de acciones de patrocinio, iniciar un proceso de I+D con el fin de generar un producto

muy concreto; en este caso, la información que se emite al entorno está contenida en el producto en forma de tecnología aplicada.

- Una organización puede llevar a cabo acciones **indirectas** de comunicación, a través de la ruta operacional: una organización que cuide la calidad de sus productos, está, quizás sin saberlo, esparciendo información por el entorno, ya que al satisfacer a sus clientes con productos de calidad consigue imagen de marca y un prestigio que los mismos clientes se encargan de difundir entre sus conocidos.

1.3. El valor de la información

Tal como se ha citado anteriormente, una de las características de la información es la subjetividad, en el sentido de que la información no tiene un valor absoluto: el valor se lo asigna el sujeto que la utiliza de acuerdo con sus necesidades concretas en un determinado momento.

Por tanto, este valor vendrá determinado por según cómo afecten al usuario las propiedades que califican la estructura interna de la información:

- **Significado** (semántica). Del significado extraído de una información, cada individuo evalúa las consecuencias posibles y adecúa sus actitudes y acciones de manera acorde a las consecuencias previsibles que se deducen del significado de la información. Esto se refiere a qué reglas debe seguir el individuo o el sistema experto para modificar sus expectativas futuras sobre cada posible alternativa.
- **Importancia** (relativa al receptor). Es decir, si trata sobre alguna cuestión importante. La importancia de la información para un receptor se referirá a en qué grado cambia la actitud o la conducta de los individuos. En las sociedades modernas, los individuos obtienen de los medios de comunicación masiva gran cantidad de información, pero una gran parte de la misma es poco importante para ellos, porque altera de manera muy poco significativa la conducta de los mismos. Esto se refiere al grado cuantitativo en que deben alterarse las expectativas futuras. A veces se sabe que un hecho hace más o menos probables algunas cosas; la importancia tiene que ver con cuánto menos probables serán unas alternativas respecto a las otras.
- **Vigencia** (en la dimensión espacio-tiempo). Se refiere a si la información está actualizada o desfasada. En la práctica la vigencia de una información es difícil de evaluar, ya que en general acceder a una información no permite conocer de inmediato si dicha información tiene o no vigencia.
- **Validez** (relativa al emisor). Se evalúa si el emisor es fiable o puede proporcionar información no válida (falsa). Tiene que ver si los indicios deben ser considerados en la revaluación de expectativas o deben ser ignorados por no ser indicios fiables.

El análisis de estas propiedades de la información y de su contenido es lo que determina que el usuario de la información tome, de manera más coherente, sus decisiones. Consecuentemente, se puede establecer que la información tiene valor porque nos ayuda a tomar decisiones.

A partir de esta valoración cualitativa y bastante intuitiva de la información, a nivel empresarial se puede precisar una valoración más cuantitativa. Un principio que se puede aplicar es definir que el valor de la información para la toma de una decisión determinada es igual a la pérdida producida por tomar la decisión errónea (la decisión contraria a la que se tomaría si se tuviera la información perfecta), por la probabilidad de que dicha pérdida se produzca. Es decir, lo máximo que una organización está dispuesta a pagar por una información es lo que podría dejar de ganar si tuviera la información perfecta multiplicado por la probabilidad de esa pérdida.

Pero al igual que una información tiene un valor para una organización que la ha obtenido, cuando esta se refiere a personas también tiene un valor, más cualitativo (confidencialidad, seguridad, reputación, etc.), mucho más difícil de cuantificar para la persona a la que corresponde; se puede considerar que este valor se ha cedido temporalmente a una organización asumiendo que no habrá deterioro ni pérdida en este valor.

En cualquier caso, cuantificada o no, la información es un activo (intangible y volátil) más de una organización y como tal hay que resguardarla y protegerse de su deterioro, desaparición o robo; con el agravante de que la organización actúa como depositaria de un valor de terceros sobre el cual, en caso de mal uso o deterioro, se pueden exigir responsabilidades.

2. Nociones básicas de seguridad de la información

2.1. Definición

Cuando se habla de seguridad en el ámbito de las TIC a menudo se confunden los conceptos de *seguridad de la información* y *seguridad informática*. Y aunque ambos son realmente importantes y similares, hay diferencias entre ellos.

Cuando aplicamos el término de seguridad a la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger. Así pues podemos definir la **seguridad de la información** como:

> Conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su información.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de clientes, proveedores de la organización o empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información y reducen el espacio ocupado, pero, sobre todo, facilitan su análisis y procesado. Se gana en «espacio», acceso, rapidez en el procesado de la información y mejoras en la presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca «por el camino»; si es más fácil acceder a ella, también es más fácil modificar su contenido; etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información también han ido cambiando y evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación del ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.

En lo referente al término de **seguridad informática** también existen también diferentes definiciones. De ellas nos quedamos con la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC):

> "La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, y puede, además, abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio."

O dicho en otras palabras, la seguridad informática se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan una empresa.

Como vemos, el término *seguridad de la información* es más amplio ya que engloba otros aspectos relacionados con la seguridad más allá de los puramente tecnológicos.

2.2. Bases de la seguridad de la información

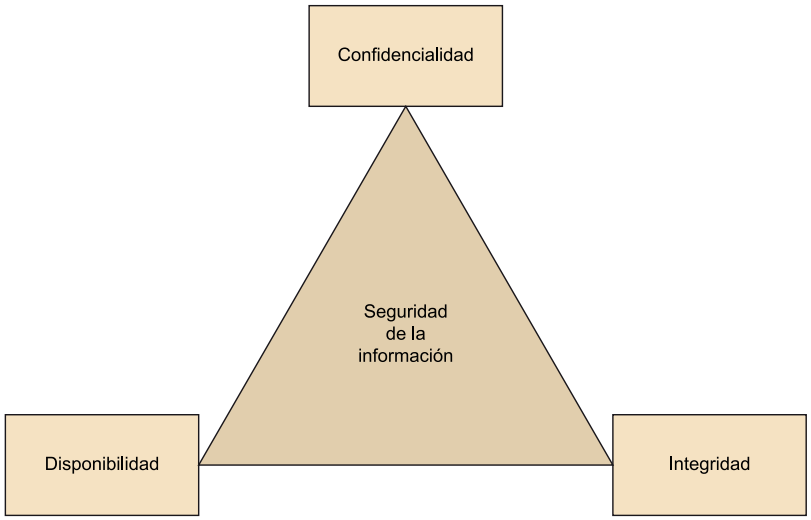
En general, la información será segura si podemos garantizar tres parámetros conocidos por las siglas CID (CIA en inglés):

Confidencialidad: implica el acceso a la información por parte únicamente de quienes están autorizados; es decir, el acceso a la información es solo mediante autorización y de forma controlada.

Integridad: conlleva el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso, lo que implica modificación de la información solo mediante autorización.

Disponibilidad: entraña el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran, lo que significa que la información debe permanecer accesible mediante autorización.

Figura 2.



2.2.1. Confidencialidad

En general el término *confidencial* hace referencia a «que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas».

En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es la del ejército de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Por otra parte, a menudo determinadas empresas desarrollan diseños que deben proteger de sus competidores. La sostenibilidad de la empresa, así como su posicionamiento en el mercado, pueden depender de forma directa de la implementación de estos diseños y, por ese motivo, se deben proteger mediante mecanismos de control de acceso que aseguren la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida; en función del tipo de mecanismo de encriptación utilizado, la clave puede o debe viajar por la red y puede ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

2.2.2. Integridad

En general, el término *integridad* hace referencia a la cualidad de *íntegro* e indica «que no carece de ninguna de sus partes», y relativo a una persona, «recta, proba, intachable».

En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información. La integridad hace referencia a:

- la integridad de los datos (el volumen de la información)
- la integridad del origen (la fuente de los datos, llamada *autenticación*)

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a la exactitud, credibilidad y confianza que las personas ponen en la información.

A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos. Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

2.2.3. Disponibilidad

En general, el término disponibilidad hace referencia a una cualidad de *disponible* y dicho de una cosa, «que se puede disponer libremente de ella o que está lista para usarse o utilizarse».

En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas o controladas del acceso a la información.

En términos de seguridad de información, «una información está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos determinados». Es decir, una información es disponible si permite no estar disponible.

Y una información no disponible es tan malo como no tener información. No sirve.

Como resumen, se puede concluir que la seguridad de la información consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

Dependiendo del entorno de trabajo y sus necesidades se puede dar prioridad a un aspecto de la seguridad o a otro. En entornos militares suele ser siempre prioritaria la confidencialidad de la información frente a la disponibilidad. Aunque alguien pueda acceder a la información o incluso pueda eliminarla no podrá conocer su contenido, y reponer esa información será tan sencillo como recuperar una copia de seguridad (si las cosas se están haciendo bien).

En entornos bancarios es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.

2.3. Estándares para la gestión de la seguridad de la información

Como hemos visto, la información es un valioso activo del que depende el buen funcionamiento de una organización. Esta información se puede ver afectada por diferentes riesgos y amenazas; por tanto mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos de negocio.

Por esa razón, desde tiempos inmemoriales las organizaciones han puesto los medios necesarios para evitar el robo y manipulación de sus datos confidenciales. Estos medios se centran en la aplicación de un proceso sistemático de análisis de riesgos.

El análisis de riesgos, en el contexto de la seguridad de la información, es un proceso sistemático para hacer una estimación del nivel de riesgo al cual están expuestas las diferentes partes (activos) que están involucradas en los sistemas de información o los hacen funcionar.

Difícilmente se pueden tomar decisiones sobre seguridad de la información sin saber qué tenemos que proteger, de qué peligros nos tenemos que proteger, ni cuáles pueden ser las consecuencias en caso de que se produzca un incidente de seguridad.

Este proceso intenta identificar los peligros (amenazas), es decir, concretar qué incidentes (voluntarios o accidentales) pueden afectar los datos/información o su valor. También se evalúa la probabilidad de que las amenazas se materialicen y hasta qué punto afectarían los sistemas y los datos (impacto).

Las medidas de seguridad implantadas son salvaguardas que pueden reducir la probabilidad de que suceda el incidente o pueden disminuir los efectos negativos en caso de que se produjera el incidente. Cuando se habla de gestionar el riesgo, lo que se quiere hacer es reducir el nivel de riesgo que existe y esto se consigue implantando nuevas salvaguardas o mejorando las existentes.

La plasmación práctica de este proceso sistemático para poder estar preparados ante cualquier imprevisto y actuar con rapidez y eficacia conlleva implantar un sistema de gestión de seguridad de la información (SGSI), gracias al cual se pueden analizar los posibles riesgos, establecer las medidas de seguridad necesarias y disponer de controles que permitan evaluar la eficacia de esas medidas. De este modo, se pueden anticipar los posibles problemas y prepararse en el caso de cualquier contingencia.

Para llevar a cabo todo el proceso de una manera más sencilla se dispone de la familia de normas internacionales ISO/IEC 27000. Las más importantes son:

- La norma ISO/IEC 27000, que recoge los términos y definiciones empleados en el resto de normas de la serie. Con ello se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de las mismas. Además, incluye una visión general de la familia de normas en esta área, una introducción a los sistemas de gestión de seguridad de la información y una descripción del ciclo de mejora continua.
- La norma ISO/IEC 27001, que es la norma principal de la serie. Se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad. La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización. Esta es la norma que se aplica para la certificación de los sistemas de gestión de seguridad de la información de las empresas que lo deseen.
- La norma ISO/IEC 27002, una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización. Para ello, describe 11 dominios (es decir, áreas de actuación), 39 objetivos de control o aspectos a asegurar den-

tro de cada área y 133 controles o mecanismos para asegurar los distintos objetivos de control.

En cuanto al proceso específico del análisis de riesgos, en España se utiliza bastante ampliamente la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) creada por el Consejo Superior de Administración Electrónica.

2.4. Principios para la implantación de un SGSI

La implantación de un sistema de gestión de seguridad de la información es una decisión estratégica que debe involucrar a toda la organización, que debe ser apoyada y dirigida desde la dirección y que requiere dedicar tiempo y recursos.

Su diseño dependerá de los objetivos y necesidades de la organización, así como de su estructura. Estos elementos son los que van a definir el alcance de la implantación del sistema, es decir, las áreas que van a verse involucradas en el cambio. En ocasiones, no es necesario un sistema que implique a toda la organización, puede ser que sea solo necesario en un departamento, una sede en concreto o un área de negocio.

El objetivo de un SGSI es proteger la información; al implantarlo, la organización obtiene los siguientes beneficios:

- Se obtiene una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello se consigue reducir las amenazas hasta alcanzar un nivel asumible por la organización. De este modo, si se produce una incidencia, los daños se minimizan y la continuidad del negocio está asegurada.
- Se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.
- La seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización.
- La organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

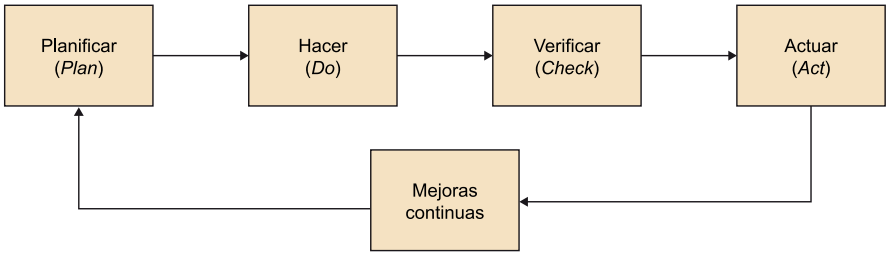
En cualquier caso, un SGSI no ha de considerarse una situación estática, al contrario, dada la rápida y dispar evolución del elemento a gestionar, la información y su seguridad, ese elemento ha de estar en continua evolución. Por ello, en su implantación, a partir de una fase inicial de identificación de

los activos de información que deben ser protegidos y en qué grado, se aplica el modelo PDCA, un modelo dividido en cuatro fases en el que finalizada la última y analizados sus resultados se vuelve a comenzar de nuevo la primera.

Las siglas PDCA corresponden a los términos en inglés *plan*, *do*, *check*, *act* (planificar, hacer, verificar, actuar).

Con ello se plasma que la gestión de la seguridad es un proceso que nunca termina, ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad; y en consecuencia se debe estar siempre alerta.

Figura 3.



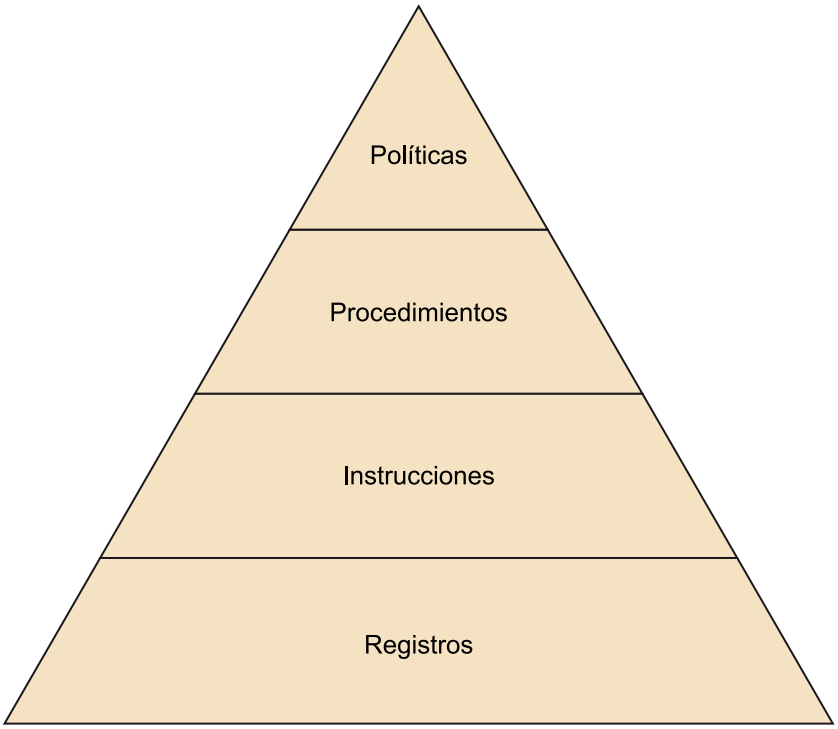
- La primera fase del Modelo PDCA para la implantación del sistema es la fase de **planificar** (*plan*). Durante esta fase se realiza un estudio de la situación de la organización desde el punto de vista de la seguridad, para estimar las medidas que se van a implantar en función de las necesidades detectadas. No toda la información de la que se dispone tiene el mismo valor o está sometida a los mismos riesgos. Por ello, es importante realizar un análisis de riesgos que valore los activos de información y vulnerabilidades a las que están expuestos. Así mismo, es necesaria una gestión de dichos riesgos para reducirlos en la medida de lo posible. Con el resultado obtenido en el análisis y la gestión de riesgos se establecen unos controles adecuados que permitan minimizar los riesgos.
- En la fase de **hacer** (*do*) del modelo PDCA se lleva a cabo la implantación de los controles de seguridad seleccionados en la fase anterior. Estos controles se refieren a los controles más técnicos, así como a la documentación necesaria. Esta fase también requiere un tiempo de concienciación y formación para dar a conocer al personal de la empresa qué se está haciendo y por qué.
- La tercera fase es la fase de **verificar** (*check*). En esta fase se evalúa la eficacia y el éxito de los controles implantados. Por ello, es muy importante contar con registros e indicadores que provengan de estos controles.
- El modelo PDCA se completa con la fase de **actuar** (*act*), durante la cual se llevarán a cabo las labores de mantenimiento del sistema. Si durante la fase anterior de verificar se ha detectado algún punto débil, este es el

momento de mejorarlo o corregirlo y definir y aplicar medidas correctoras, medidas preventivas y medidas de mejora según convenga.

Al finalizar las cuatro fases, se toman los resultados de la última y se comienza nuevamente la primera.

La continua evaluación del sistema de gestión de seguridad de la información debe estar documentada, para lo que se utilizarán los cuatro tipos distintos de documentación que se representan en esta estructura piramidal:

Figura 4.



- En la cúspide se encuentran las **políticas** que sientan las bases de la seguridad. Indican las líneas generales para conseguir los objetivos de la organización sin entrar en detalles técnicos. Toda la organización debe conocer estas `políticas.
- En un segundo nivel se sitúan los **procedimientos** que desarrollan los objetivos marcados por las políticas. En los procedimientos aparecen detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las políticas. Los procedimientos deben ser conocidos por aquellas personas que lo requieran para el desarrollo de sus funciones.
- En el tercer escalón aparecen las **instrucciones** que constituyen el desarrollo de los procedimientos. En las instrucciones se describen los comandos técnicos que se deben realizar para la ejecución de los procedimientos.
- En el último escalón se hallan los **registros**, que evidencian la efectiva implantación del sistema y el cumplimiento de los requisitos. Entre estos

registros se incluyen indicadores y métricas de seguridad que permitan evaluar la consecuencia de los objetivos de seguridad establecidos.

3. Seguridad técnica y Seguridad jurídica

Existen muchas definiciones del término *seguridad*. Simplificando, y en general, podemos definir la seguridad como «característica que aplicada a un ente indica que este está libre de todo peligro, daño o riesgo».

Cuando hablamos de información estamos ante un ente que implica dos sujetos: la tecnología que la sustenta y el individuo al que hace referencia. Por tanto, en el caso de un individuo, el concepto de seguridad se traduce como la certidumbre de que su información y derechos están a salvo de ataques violentos e indebidos y, en el peor de los casos, de efectuarse, se harán cesar con premura y los daños le serán resarcidos. En el caso de la tecnología, la seguridad se traduce en que los componentes que la conforman están libres de todo peligro, daño y riesgo; y en el caso de ataque se actúa rápidamente para evitarlos y restituir los daños.

En cuanto a la seguridad jurídica, el concepto alude a la certeza, el orden, la firmeza y la confianza en el ordenamiento legal, tanto en las relaciones jurídicas entre particulares como en las relaciones entre el ciudadano y la Administración.

Parece obvio que la seguridad jurídica en el mundo virtual (intrínsecamente intangible) no puede lograrse del mismo modo y a través de los mismos instrumentos que la seguridad proveniente del mundo preinformático (sustentado en lo tangible), un tema que adquiere nuevas tonalidades a la luz de la nueva realidad. Por ejemplo, en el caso de los negocios, la forma exigida para los contratos, la registración pública, la certificación de las firmas y otros institutos no son medios de seguridad apropiados cuando los contratos se celebran a distancia, entre ausentes, sin escritos y hasta de forma anónima; o para la información cuando las medidas de salvaguarda física son inoperantes cuando la información está en soporte intangible o en algo tan etéreo como «la nube».

Al inicio del uso de los ordenadores y primeras redes de comunicaciones, estas eran puramente para uso interno de las organizaciones y se utilizaban como soporte de comunicación de datos puntuales o envío interno de correo electrónico. En estas condiciones, la seguridad no recibía mucha atención. La «democratización» de la informática y su combinación con las telecomunicaciones ha conducido a la llamada «sociedad de la información». La información ha acontecido uno de los motores de nuestra sociedad (un activo para las empresas y administraciones públicas), con lo que la información se ha convertido en un bien de gran valor y ha dejado de servir solo para un fin

concreto y en un momento concreto, puesto que han desaparecido conceptos como tiempo y espacio en relación a la desaparición del concepto de olvido de la información.

Actualmente los datos se recogen incluso antes de nuestro nacimiento (datos médicos), y continúan acumulándose a lo largo de toda nuestra vida. En cada una de las fases de nuestro desarrollo como personas (escuela, universidad, trabajo, salud, aficiones, lecturas, compras, créditos…) se van recogiendo datos que con las herramientas oportunas pueden permitir un conocimiento de nosotros incluso mejor del que haríamos nosotros mismos. Ante esto, la información se convierte en una nueva forma de poder para quien la pueda recoger y tratar. Ante esta situación, garantizar la seguridad de la información y de las redes se convierte en un problema potencial de grandes proporciones.

Los problemas de seguridad de la información, tanto en sí misma como de los medios utilizados para acceder a ella o compartirla, como ya apuntado en el subapartado «Bases de la seguridad de la información», pueden dividirse en cuatro áreas interrelacionadas: secreto, validación de identificación, no repudio y control de integridad. El secreto tiene que ver con mantener la información fuera de las manos de usuarios no autorizados. Esto es lo que normalmente viene a la mente cuando la gente piensa en la seguridad de las redes. La validación de identificación se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios. El no repudio se encarga de las firmas. Por último, el control de integridad se asegura de que un mensaje recibido realmente es el enviado, y no algo que un adversario malicioso modifica en el camino o cocina por su propia cuenta; es decir, que no se altera en su integridad.

En esta situación, lo que la seguridad jurídica reclama es certeza, estabilidad y razonabilidad, en cuyo alcance deben converger tanto las soluciones normativas como las tecnológicas implicadas en la seguridad técnica de la información.

En este sentido, merece mención especial la consideración de la seguridad en su relación con el derecho a la intimidad (y su nuevo rostro actual: el derecho a la protección de los datos personales), el cual nace como una herramienta para proteger al ciudadano ante esta nueva realidad. Sin embargo, no hay que olvidar que no hay derechos absolutos y, por lo tanto, habrá otros derechos y bienes que también tendrán que ser protegidos.

El reconocimiento explícito de este derecho es relativamente reciente y muestra una evolución que puede examinarse a través de ciclos sucesivos, sentidos diferentes y enfoques diversos, en cuyo marco procede ubicar la protección jurídica actual de los datos personales en general y en el sector de las TIC en particular.

Inicialmente el derecho a la intimidad apuntó básicamente a una protección contra la publicidad de actos o datos personales puestos en conocimiento del público sin noticia o permiso de la persona afectada. Posteriormente, dicho concepto se extendió para abarcar el derecho de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y con qué extensión puede ser comunicada a terceros la información acerca de ellos. Las TIC han replanteado la cuestión del derecho a la intimidad en atención al riesgo que para la persona implica la estructuración de grandes bancos de datos de carácter personal, y particularmente la potencialidad del entrecruzamiento de información contenida en ellos.

Frente al «poder informático» de quienes pueden acumular informaciones sobre cada persona en cantidad ilimitada, y memorizarla, usarla y transferirla como una mercancía, el derecho a la intimidad se configura como una nueva forma de libertad personal, ya no caracterizada negativamente como la posibilidad de refutar o evitar el uso de datos referidos a cada uno, sino positivamente como la potestad de ejercer un poder de control sobre las informaciones referidas a la propia persona. Consiste en lo que ha dado en llamarse *libertad informática*, consistente en el derecho de autotutela de la propia identidad informática, es decir, el derecho de vigilar los datos personales incluidos en archivos automatizados, de preservar la propia identidad informática o, lo que es lo mismo, de consentir, controlar y rectificar los datos informativos concernientes a la propia personalidad. Al derecho de informar y de ser informado se ha agregado el derecho de proteger la libertad de la información como un bien personal, que constituye un nuevo derecho fundamental, propio de la tercera generación, que tiene por finalidad el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente.

Muchas veces, los datos personales son facilitados voluntariamente por el propio titular de los mismos para acceder gratuitamente a algún servicio o para la obtención onerosa de un bien a través de internet sin tener conciencia de que pueden ser utilizados para fines diferentes de aquellos para los que fueron recabados. Pero otras veces los datos del internauta son proporcionados por este de manera completamente involuntaria ya que, una vez que los datos salen de su ordenador, el internauta desconoce la ruta que siguen hacia su destino, en qué puntos intermedios se almacenan temporalmente y quién puede acceder a ellos, copiarlos, modificarlos y utilizarlos para cualquier finalidad diferente de aquella para la que fueron entregados.

Queda claro que los servicios TIC constituyen un ámbito específico y peculiar para la protección de los datos personales por dos razones principales: por un lado, porque las crecientes interoperatividad y extensión de estos servicios constituyen por sí mismas un factor de riesgo para la seguridad de la gestión de la información en general y de los datos relacionados con la intimidad en particular; y por otro lado, porque el proceso de comunicación requiere

determinar e identificar los puntos de terminación de la red entre los que se produce la comunicación, unos puntos que por su eventual identificación con personas pueden alcanzar la consideración de datos personales.

En cualquier caso, lo que persigue la seguridad jurídica es la de facilitar al ciudadano los medios que garanticen el cumplimiento de las normativas y preservación de su derecho a la intimidad basándose en la seguridad (tanto física como lógica), la confidencialidad y el consentimiento del ciudadano para el tratamiento de sus datos.

Bibliografía

Delpiazzo, C. E. (2007). «El principio de seguridad jurídica en el mundo virtual». *Revista de Derecho* (año VI, n.º 11).

Instituto Nacional de Tecnologías de Comunicación (INTECO) (2011). *Guía de apoyo Implantación de un SGSI en la empresa* [Recurso en línea]. <https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>

Marí, J.; San José, C.; Miralles, R. M.; Ferreres, J. (2010). *El dret a la protecció de dades de caràcter personal. Autoritat catalana de protecció de dades* [Recurso en línea]. Escola d'Administració Pública de Catalunya. <http://virtual.eapc.cat/pluginfile.php/110864/mod_resource/content/1/dret_prot_dad/inici.html>

Martínez, F. «Tema 1: El subsistema de la Información de la Empresa. Universidad de Huelva». *Gestión de los Recursos de Información* [Recurso en línea]. <http://www.uhu.es/francisco.martinez/gri/_private/TEMA%201GRI.doc>

Martínez Musiño, C. (2010). «El valor de la información, su administración y alcance en las organizaciones». *Revista mexicana de ciencias de la información* (vol. 1, n.º 2, págs. 10-20).

Mifsud, E. (2012). *Introducción a la seguridad informática* [Recurso en línea]. Ministerio de Educación, Cultura y Deporte. <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>