SEGURIDAD DE LA INFORMACIÓN

La información es el principal activo de muchas organizaciones por lo que es necesario protegerla adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio.

En la actualidad, la mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, encuadrados dentro de lo que se conoce como sistemas de información. Estos sistemas de información están sujetos a riesgos e inseguridades internos y externos a la organización.

El objetivo de las organizaciones es disminuir los riesgos sin necesidad de realizar fuertes inversiones en software y sin contar con una gran estructura de personal. Para ello es necesario conocer y afrontar los riesgos a los que se somete la información, contemplar procedimientos adecuados y planificar e implantar controles de seguridad.

Existen varias herramientas para gestionar la seguridad de la información, obligatorias como la Ley Orgánica de Protección de Datos de Carácter Personal, (LOPD), y voluntarias como los Sistemas de Gestión de Seguridad de la Información.

LOPD

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

Todo Responsable, ya sea del Fichero o de Seguridad, debe evaluar qué medidas de protección debe incorporar para obtener el nivel de seguridad deseado, de acuerdo a la información que se gestione en su organización. No obstante, existen medidas que toda organización está obligada a cumplir.

El Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre) establece tres niveles de seguridad para los ficheros, en función de los datos contenidos en ellos:

- Básico: todos los ficheros o tratamiento de datos con carácter personal.
- Medio: ficheros con datos relativos a la comisión de infracciones administrativas, Hacienda Pública, Servicios financieros, así como los ficheros sobre solvencia patrimonial y de crédito.
- Alto: ficheros con datos sobre ideología, religión, creencias, origen racial, salud o vida sexual, los recabados para fines policiales sin consentimiento del afectado, y aquellos que contengan datos derivados de actos de violencia de género.

Además, a la hora del tratamiento de los datos hay que aplicar medidas de seguridad técnica y organizativas en función del nivel y según establece el reglamento. Sin entrar a analizar en detalle las implicaciones de cada medida, la idea que subyace en la ley es la necesidad de implantar en las organizaciones, y en la sociedad, en general, una cultura compartida de la protección de la información.

Sistema de Gestión de Seguridad de la Información, (SGSI)

Un SGSI, según la definición recogida en la norma UNE-EN ISO 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Es decir, a partir de la aplicación de un sistema de gestión en una organización, se comienza a trabajar de manera más sistemática y controlada sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja.

Para establecer y gestionar un SGSI se utiliza el ciclo PDCA (o ciclo de Deming), propio de los sistemas de gestión de la calidad. Esta metodología permite establecer la mejora continua en organizaciones de todos los sectores.

Conseguir la seguridad total en una organización es imposible, sin embargo mediante el proceso de mejora continua del sistema de gestión de seguridad se puede obtener un nivel de seguridad altamente satisfactorio, reduciendo al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si se produjesen.

Para la implantación de los SGSI, ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) han desarrollado la serie de normas ISO 27000. Esta familia incluye normas sobre requisitos, gestión del riesgo, métricas y mediciones, así como una guía de implementación, que a continuación detallamos.

UNE-ISO/IEC 27001

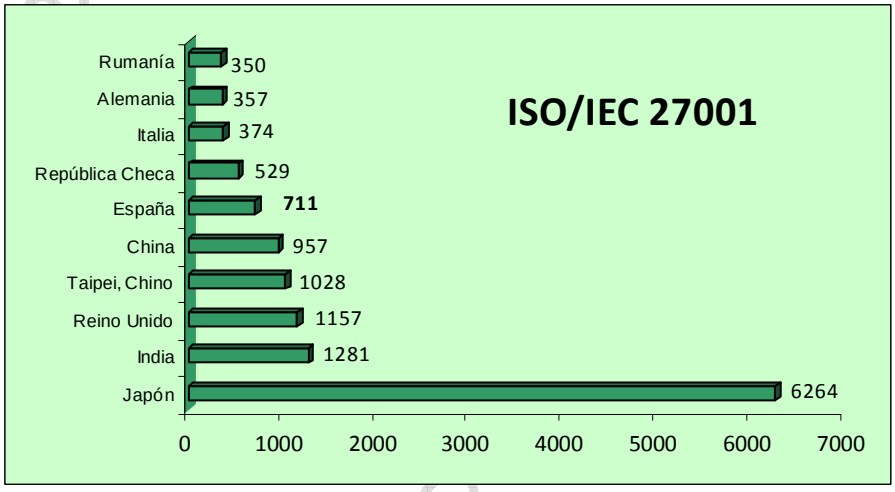
ISO e IEC desarrollaron en 2005 la norma ISO/IEC 27001 a partir de la norma BS 7799. Fue traducida posteriormente al español por AENOR (Asociación Española de Normalización), convirtiéndola en *UNE-ISO/IEC 27001:2007 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.*

Esta norma aplica una aproximación por procesos para la gestión de la seguridad, según el modelo PDCA, enfatizando la importancia de los siguientes aspectos:

- Comprensión de los requisitos de seguridad de la organización. Necesidad de establecer una política y unos objetivos.
- Implementar controles para gestionar los riesgos en el contexto del negocio.
- Monitorizar el rendimiento del SGSI.
- Mejora continua basada en la medición de los objetivos.

Esta norma es certificable y ha tenido una fuerte implantación en los últimos años en todo el mundo, especialmente en Japón, India y Reino Unido. En la siguiente gráfica se pueden observar los 10 países que poseen más certificados bajo la norma ISO/IEC 27001 a nivel mundial en el año 2010.

Nº de certificados ISO/IEC 27001 en 2010 a nivel mundial. Fuente: ISO Survey



La norma UNE-ISO/IEC 27001:2007 indica en su Anexo A, de forma resumida, los objetivos de control y controles que desarrolla más detalladamente la norma UNE-ISO/IEC 27002.

UNE-ISO/IEC 27002

La norma *UNE-ISO/IEC 27002:2009 Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información*, tiene como origen la norma ISO 17799 y no es certificable.

UNE-ISO/IEC 27002 establece las directrices y principios generales para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información, mediante objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y controles (medidas a tomar).

La elección de los controles debe relacionarse con lo detectado en un análisis previo de riesgos, y el grado de implementación se llevará a cabo de acuerdo a los requisitos de seguridad identificados y a los recursos disponibles, para alcanzar un equilibrio razonable entre seguridad y coste.

ISO/IEC 27004

La norma *ISO/IEC 27004 Mediciones para la gestión de la seguridad de la información*, es una norma no certificable. Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de sus controles. Su misión es desarrollar todos los aspectos que deben ser considerados para poder "medir" el cumplimiento de la Norma ISO 27001 en una organización.

La idea de medición es muy amplia y en definitiva, va desde la medición más simple hasta la combinación de varios niveles o instancias para poder ofrecer datos que lleven a un verdadero "cuadro de mando de la seguridad", que sería el objetivo último de todo SGSI. A partir de éste, los diferentes niveles jerárquicos de la organización podrán acceder a la información de seguridad que les hace falta conocer y, basándose en esta, adoptar las decisiones correspondientes.

Los objetivos de estas mediciones son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del SGSI, incluyendo continuas mejoras.
- Proveer estados de seguridad que guíen las revisiones del SGSI, facilitando mejoras a la seguridad y nuevas entradas para auditar.
- Comunicar valores de seguridad a la organización.
- Servir como entradas al plan de análisis y tratamiento de riesgos.
- Comparar los logros obtenidos en periodos de tiempo concretos y en áreas de negocio similares.

ISO/IEC 27006

ISO/IEC 27006:2011 Tecnologías de la información. Técnicas de seguridad. Requisitos para las entidades que proporcionan auditorías y certificación de sistemas de seguridad de la información, esta norma ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. El objeto de esta norma es apoyar la acreditación de las entidades que realizan esta certificación.

ISO/IEC 27035

ISO / IEC 27035:2011 Tecnología de la información - Técnicas de seguridad - Gestión de incidencias de seguridad de la información, es el nuevo estándar publicado por ISO en el último mes de 2011, como se puede leer en el Boletín nº 107 de la AEC, para ayudar a las organizaciones a mejorar la gestión de los incidentes relativos a la seguridad de la información.

Los controles de seguridad existentes pueden fallar, no se han aplicado bien o simplemente no son perfectos. Una gestión de incidencias eficaz implica aplicar controles detectivos y correctivos dirigidos a minimizar los impactos adversos, reunir pruebas (si aplica) y “aprender las lecciones” en términos de la mejora de la gestión de la seguridad o de un SGSI.

ISO/IEC 27035 establece un enfoque estructurado y planificado para:

- Detectar, informar y evaluar los incidentes de seguridad de información.
- Responder a incidentes y gestionar incidentes de seguridad de la información.
- Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información.
- Mejorar continuamente la seguridad de la información como resultado de la gestión de la información obtenida sobre incidentes y vulnerabilidades.