1. Introducción a la Ciberseguridad

2. Estándares y Normativas de Seguridad de la Información

2.1 Introducción

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

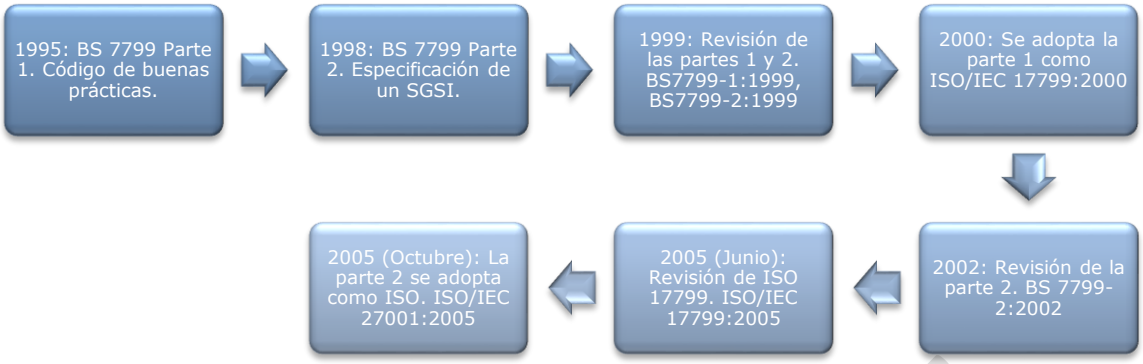
La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007.



En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

2.2 Conjunto de Normas ISO 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044 con 27799 finalizando la serie formalmente en estos momentos.

Partiendo del fundamento de que el estándar ISO/IEC 27001 indica qué **requisitos deben conformar un SGSI** pero no cómo cumplirlos, algunas de las normas que conforman la serie 27000 van orientadas precisamente a documentar **mejores prácticas** en aspectos o incluso cláusulas concretas de la norma ISO/IEC 27001 de modo que se evite reinventar la rueda con el sustancial ahorro de tiempo en la implantación.

ISO/IEC 27000:

Publicada el 1 de Mayo de 2009 y revisada con una segunda edición de 01 de Diciembre de 2012. Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del ciclo Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000.

El original en inglés y su traducción al francés pueden descargarse gratuitamente de:

http://standards.iso.org/ittf/PubliclyAvailableStandards

ISO/IEC 27001:

Publicada el 15 de Octubre de 2005. Es **la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información**. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007.

Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación para 2014.

ISO/IEC 27002:

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación de la segunda edición en Mayo de 2014.

ISO/IEC 27003:

Publicada el 01 de Febrero de 2010. No certificable. Es una **guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI** de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO/IEC 27004:

Publicada el 15 de Diciembre de 2009. No certificable. Es una **guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI** y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005:

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona **directrices para la gestión del riesgo en la seguridad de la información**. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO/IEC 27006:

Publicada en segunda edición el 1 de Diciembre de 2011 (primera edición del 1 de Marzo de 2007). Especifica los **requisitos para la acreditación de entidades de auditoría y certificación** de sistemas de gestión de seguridad de la información.

ISO/IEC 27007:

Publicada el 14 de Noviembre de 2011. No certificable. Es una **guía de auditoría de un SGSI**, como complemento a lo especificado en ISO 19011.

ISO/IEC TR 27008:

Publicada el 15 de Octubre de 2011. No certificable. Es una **guía de auditoría de los controles seleccionados** en el marco de implantación de un SGSI.

ISO/IEC 27010:

Publicada el 20 de Octubre de 2012. Consiste en una **guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores**.

En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.

ISO/IEC 27011:

Publicada el 15 de Diciembre de 2008. Es una **guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones** basada en ISO/IEC 27002.

ISO/IEC 27013:

Publicada el 15 de Octubre de 2012. Es una **guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI)**.

ISO/IEC 27014:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en **una guía de gobierno corporativo de la seguridad de la información**.

ISO/IEC TR 27015:

Publicada el 23 de Noviembre de 2012. Es **una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002**.

ISO/IEC TR 27016:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en una **guía de valoración de los aspectos financieros de la seguridad de la información**.

ISO/IEC TS 27017:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en una **guía de seguridad para Cloud Computing**.

ISO/IEC 27018:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en un **código de buenas prácticas en controles de protección de datos para servicios de computación en Cloud Computing**.

ISO/IEC TR 27019:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en **una guía con referencia a ISO/IEC 27002 para el proceso de control de sistemas específicos al sector de la industria de la energía**.

ISO/IEC 27031:

Publicada el 01 de Marzo de 2011. No certificable. Es una **guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio**. El documento toma como referencia el estándar BS 25777.

ISO/IEC 27032:

Publicada el 16 de Julio de 2012. Proporciona **orientación para la mejora del estado de seguridad cibernética**, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio.

ISO/IEC 27033:

Parcialmente desarrollada. **Norma dedicada a la seguridad en redes**, consistente en 7 partes:

- 27033-1, conceptos generales
- 27033-2, directrices de diseño e implementación de seguridad en redes
- 27033-3, escenarios de referencia de redes
- 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad
- 27033-5, aseguramiento de comunicaciones mediante VPNs

- 27033-6, convergencia IP; 27033-7, redes inalámbricas.

ISO/IEC 27034:

Parcialmente desarrollada. **Norma dedicada la seguridad en aplicaciones informáticas**, consistente en 5 partes (en su mayor parte sin previsión de publicación):

- 27034-1, conceptos generales
- 27034-2, marco normativo de la organización
- 27034-3, proceso de gestión de seguridad en aplicaciones
- 27034-4, validación de la seguridad en aplicaciones
- 27034-5, estructura de datos de protocolos y controles de seguridad de aplicaciones

ISO/IEC 27035:

Publicada el 17 de Agosto de 2011. Proporciona una **guía sobre la gestión de incidentes de seguridad en la información**.

ISO/IEC 27036:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía en cuatro partes de **seguridad en las relaciones con proveedores**:

- 27036-1, visión general y conceptos
- 27036-2, requisitos comunes
- 27036-3, seguridad en la cadena de suministro TIC
- 27036-4, seguridad en outsourcing (externalización de servicios).

ISO/IEC 27037:

Publicada el 15 de Octubre de 2012. Es una **guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales** potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

ISO/IEC 27038:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en una **guía de especificación para seguridad en la redacción digital**.

ISO/IEC 27039:

En fase de desarrollo, con publicación prevista en 2013. Consistirá en una **guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS)**.

ISO/IEC 27040:

En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una **guía para la seguridad en medios de almacenamiento**.

ISO/IEC 27041:

En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una **guía para la garantizar la idoneidad y adecuación de los métodos de investigación**.

ISO/IEC 27042:

En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una **guía con directrices para el análisis e interpretación de las evidencias digitales**.

ISO/IEC 27043:

En fase de desarrollo, con publicación prevista no antes de 2014. **Desarrollará principios y procesos de investigación**.

ISO/IEC 27044:

En fase de desarrollo, con publicación prevista no antes de 2014. **Gestión de eventos y de la seguridad de la información** - Security Information and Event Management (SIEM).

ISO/IEC 27799:

Publicada el 12 de Junio de 2008. Es una norma que proporciona directrices para **apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002**, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.