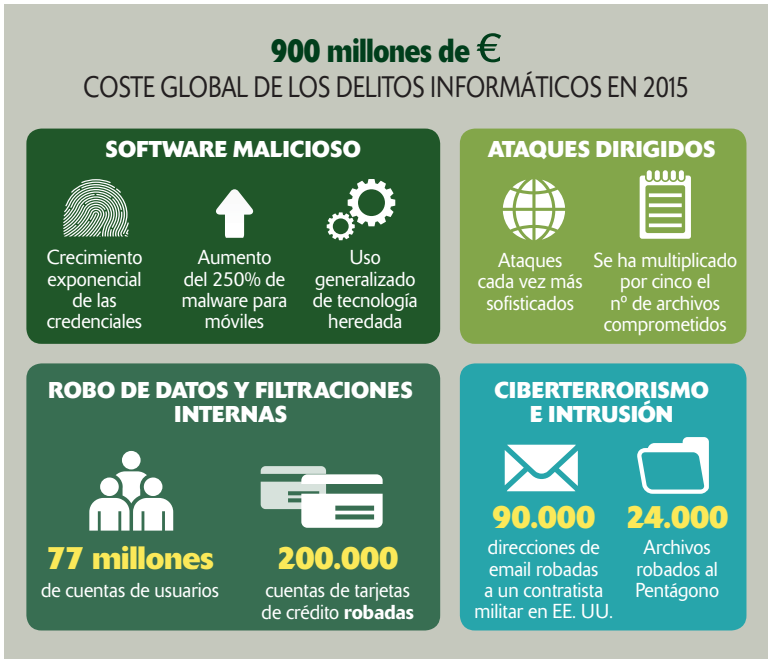
NUEVOS DESAFÍOS TIC

UNE-ISO/IEC 27002

La guía en la era de la ciberseguridad

PricewaterhouseCoopers estima que los delitos informáticos de 2015 suponen un coste de 900 millones de euros. Por ello la ciberdelincuencia es hoy uno de los principales retos de dimensión global. Para hacerle frente es fundamental desplegar sólidas herramientas de ciberseguridad. La Norma UNE-ISO/IEC 27002, recientemente incorporada al catálogo de normas técnicas de AENOR, es una eficaz guía para determinar controles de seguridad.

Coste global de los delitos informáticos para las organizaciones



Fuente: *Global State of Information Survey 2015 - PwC*

Paloma García
Dirección de Normalización
AENOR

Si bien no hay una definición común para conceptos como ciberseguridad, ciberespacio, ciberdelincuencia, ciberespionaje o ciberataques, éstos están presentes en el día a día de la actividad empresarial. De hecho, se tienen en cuenta en todo análisis de riesgos y en el diseño de cualquier estrategia de negocio.

La ciberseguridad es la primera línea de defensa contra la ciberdelincuencia, y por ello las políticas europeas y nacionales de seguridad contemplan la ciberseguridad como una línea de actuación con entidad propia que hay que desplegar y dotar de las medidas de apoyo necesarias para alcanzar objetivos concretos.

La Agenda Europea de Seguridad, publicada en abril, establece para los próximos cinco años tres prioridades esenciales para la seguridad europea; una de ellas es la ciberdelincuencia que contempla como una de las mayores amenazas para el desarrollo del mercado único digital. Esto se corresponde con el hecho de que los usuarios de Internet de la Unión Europea siguen estando muy preocupados por los ciberataques. El 85% de las organizaciones considera que el riesgo de ser víctimas de estos ataques va en aumento (según el Eurobarómetro sobre ciberseguridad publicado en febrero de 2015). En el marco europeo se está finalizando el desarrollo de la futura Directiva de la seguridad de las redes y la información, conocida como Directiva NIS, cuya implantación en los Estados miembro contribuirá a avanzar en este marco de protección.

En el escenario nacional, bajo el marco de la Estrategia de Seguridad Nacional (2103) se publica la Estrategia de Ciberseguridad Nacional, que explícitamente recoge en su línea de acción 5 *Seguridad y resiliencia de las TIC en el sector privado* la necesidad de impulsar el desarrollo de estándares en ciberseguridad a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción.

Confianza digital

Avanzar en la construcción de un clima de confianza que contribuya al desarrollo de la economía y la sociedad digital, con la ciberseguridad como herramienta que lo posibilite, es uno de los objetivos del Plan de Confianza Digital, enmarcado dentro de la Agenda Digital para España.

La Ley de Seguridad Nacional (Ley 36/2015), aprobada en septiembre de 2015, en su artículo 10, señala la ciberseguridad como uno de los ámbitos de especial interés de la seguridad nacional.

El Dictamen del Comité Económico y Social de 16 de diciembre de 2014, en su punto 1.6 indica que "Las empresas y las organizaciones han de incrementar el nivel de concienciación acerca de la responsabilidad en materia de ciberseguridad a nivel directivo. Es preciso comunicar explícitamente a los directores de todas las organizaciones las responsabilidades empresariales potenciales derivadas de la adopción de unas políticas y medidas inadecuadas en materia de ciberseguridad", y de hecho en algunos entornos esta recomendación se ha pasado a considerar dentro de la Responsabilidad Social Corporativa.

Muchas son las soluciones tecnológicas en el mercado que ayudan a conseguir los objetivos actuales de ciberseguridad de las organizaciones. Pero para garantizar una adecuada protección, el consenso es unánime sobre el hecho de que la seguridad que se puede lograr a través de medios técnicos es limitada y debe ser apoyada por la gestión y los procedimientos apropiados. La ciberseguridad es una cuestión que se debe abordar desde un nivel directivo. Es de esta manera como la seguridad de la información continúa posicionándose como factor clave entre los diferentes aspectos que hay que gestionar en una organización. El término "información" hace referencia a todos aquellos datos que desde algún punto de vista se considera necesario "controlar", ya sea por obligación legislativa -aspectos de privacidad y protección de datos personales-, datos esenciales para la actividad y estrategia de la organización, o bien aquellos de interés para terceros.

Estructura de dominios de seguridad de la nueva versión UNE-ISO/IEC 27002

NUEVOS DESAFÍOS TIC

UNE-ISO/IEC 27002

El modelo de gestión que contribuye a este ordenamiento es el internacionalmente reconocido como SGSI (Sistema de Gestión de la Seguridad de la Información) recogido en la Norma UNE- ISO/IEC 27001 *Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos*, cuya versión revisada se publicó por AENOR en octubre del año 2014.

Para ayudar a la implantación de un SGSI, se ha elaborado la Norma UNE-ISO/IEC 27002 *Tecnología de la Información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información*, incorporada al catálogo de AENOR el pasado mes de julio y revisada también desde su anterior versión de 2009. Esta norma está diseñada para que las organizaciones la utilicen como documento guía a la hora de seleccionar controles dentro del proceso de implantación de un SGSI, tanto desde un enfoque general como teniendo en cuenta entornos de riesgos específicos para la seguridad de la información. Es aplicable para organizaciones de cualquier tipo, tamaño y sector que manejan información y datos.

En un mundo interconectado, la información y sus procesos, los sistemas, las redes y el personal implicados en su operación, manejo y protección son activos que, al igual que otros, resultan valiosos para el negocio de una organización y, en consecuencia, requieren protección contra diversos peligros. Una adecuada gestión de la seguridad de la información reduce los riesgos protegiendo a las organizaciones frente a amenazas y vulnerabilidades, y en consecuencia reduce el impacto en sus activos.

La seguridad de la información se logra mediante la implantación de un conjunto adecuado de controles, lo que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de *software* y *hardware*. Estos controles se deben establecer,

La UNE-ISO/IEC 27002 incluye 14 dominios de seguridad, con 35 objetivos de control y 114 controles que hay que implantar

implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización. La identificación de los controles que deberían implantarse requiere una planificación cuidadosa y de detalle, junto al apoyo de todo el personal de la entidad, así como de partes externas a la misma (accionistas, proveedores, etc.).

UNE-ISO/IEC 27002

La nueva versión de la UNE-ISO/IEC 27002 mantiene la estructura de la norma en capítulos que asemejan diferentes dominios de la seguridad que hay que tener en cuenta, cada

uno de los cuales presenta una serie de objetivos de seguridad a los que asigna una serie de controles y acompaña de una guía de implantación con información detallada para cada control, junto con información adicional para algunos controles.

La nueva versión consta de 14 dominios de seguridad (capítulos 5 al 18) que contienen un total de 35 objetivos de control, que reflejan qué es lo que se quiere conseguir, y 114 controles que hay que implantar. Se ha pasado de 11 a 14 dominios de seguridad. De éstos, cuatro son de carácter técnico, uno físico y nueve de gestión, cuando la anterior versión tenía tres, uno y siete, respectivamente. El aumento en los capítulos de seguridad se debe a que aparecen dos nuevos capítulos, uno dedicado a la criptografía y otro a las relaciones con proveedores, y el antiguo capítulo de gestión de comunicaciones y operaciones, en la nueva versión se divide en dos capítulos separados.

Se reducen tanto los objetivos de control, 35 frente a los 39 de la anterior versión, como la cantidad de controles de 133 a 114: 11 nuevos controles; 27 controles eliminados; 8 controles de la versión de 2005 se han consolidado en 4 y 1 control se ha dividido en 2.

La actual versión de la Norma UNE-ISO/IEC 27002 es una herramienta eficaz para ayudar a todo tipo de organizaciones a avanzar en la implantación de una cultura de seguridad de la información, que complemente el resto de actuaciones encaminadas a reforzar la ciberseguridad, uno de los motores más importantes para el desarrollo de la economía y la sociedad digital. ◗

CURSOS Y PUBLICACIONES DE AENOR RELACIONADAS

- **Fundamentos de la Gestión de la Seguridad de la Información según ISO 27002**
- **Pack Sistemas de Gestión de Seguridad de la Información (SGSI)**

OPINIÓN

Félix Barrio
Gerente
Instituto Nacional de Ciberseguridad (INCIBE)
Coordinador
AEN/CTN 71/SC 27/ GT 1

Norma innovadora

La publicación de la Norma UNE-ISO/IEC 27002 responde, sin duda, a las expectativas del sector por cuanto introduce una serie de innovaciones que venían siendo demandadas por muchos profesionales y expertos en ciberseguridad. En primer lugar, no sólo se trata de una traducción al castellano de la ISO 27002:2013, sino que intenta mejorar la definición de conceptos críticos en el campo de las medidas de gestión de seguridad que, en su versión inglesa, no resulta sencillo trasladar. Y es que, la precisión entre lo que es simplemente recomendable o necesario a la hora de implantar un sistema de gestión de seguridad de la información resulta esencial. La creciente necesidad de mejorar la capacidad de respuesta de una organización ante las cada vez más numerosas formas de amenazas y riesgos para la seguridad de la información ha supuesto una profunda renovación de esta nueva versión. Es por tanto, una norma innovadora ante los crecientes retos para la ciberseguridad.

En segundo lugar, la nueva serie de normas ISO 2700X supone una acertada puesta al día, lo que es especialmente visible en ámbitos tecnológicos en constante renovación como, por ejemplo, el uso de dispositivos móviles y la adopción de medidas reguladoras y de prevención y respuesta relacionadas con ellos. Además, se han clarificado otros aspectos relativos a la organización, como la formación, concienciación o asignación de roles y responsabilidades al personal o a terceros. En resumen, esta norma constituye un documento de cabecera indispensable para el profesional de la ciberseguridad. Imprescindible.