# Una caja de herramientas de seguridad protege a las organizaciones de los ciberataques

*María Lazarte*
*2015-12-17*

Los ciberataques son uno de los principales riesgos a los que se puede enfrentar una organización. Por ello, contar con normas y sistemas para mantener protegida la información nunca ha sido tan importante como en el mundo digital actual. Esta es la razón por la que la serie ISO/IEC 27000 sobre técnicas de seguridad para la tecnología de la información se ha actualizado con el fin de proporcionar valor añadido y confianza a las organizaciones.

En una encuesta global realizada por ISACA en 129 países, solo el 38% de los encuestados consideró que estaban preparados para un ciberataque, a pesar de que el 83% creía que es una de las tres principales amenazas a las que las organizaciones se enfrentan hoy en día. Con tanta información personal y confidencial gestionada de forma electrónica, habría mucho que perder si ésta se viera comprometida.

El profesor Edward Humphreys, coordinador del grupo de trabajo responsable de los sistemas de gestión de seguridad de la información (SGSI) de ISO, subraya: "Para garantizar la seguridad en el panorama digital actual, todas las organizaciones, sea cual sea su tamaño, deben establecer un marco de trabajo de gestión como punto de partida para hacer frente a los riesgos cibernéticos. La norma ISO/IEC 27001 se diseñó para ayudar a las organizaciones a hacerlo. La norma es el 'lenguaje común' del mundo cuando se trata de evaluar, tratar y gestionar los riesgos relacionados con la información".

A continuación, se presentan las últimas revisiones y adiciones de la serie ISO/IEC 27000 —todas publicadas en 2015—, que forman parte de la "caja de herramientas de riesgos cibernéticos" ISO/IEC 27001, para ayudar a mantener estos riesgos bajo control.

## Protección de la información en la nube (ISO/IEC 27017)

Se acaba de publicar un nuevo código de prácticas para los controles de seguridad de la información de los servicios en la nube, la norma ISO/IEC 27017. La nube es una de las innovaciones más utilizadas en el frenético mundo actual del comercio y los negocios. A medida que el servicio gana adeptos, los usuarios están exigiendo garantías de que los datos almacenados y procesados en la nube están seguros. Por su propia naturaleza, el mercado de los servicios en la nube es global, con proveedores repartidos por amplias zonas geográficas, y los datos se transfieren de forma rutinaria a través de fronteras nacionales. Por ello, contar con unas directrices internacionales es esencial.

Según Satoru Yamasaki, uno de los revisores que trabajaron en la norma, "ISO/IEC 27017 ayudará a los proveedores de servicios a llegar a un entendimiento común con sus clientes con respecto a los controles de seguridad adecuados y la forma de implementarlos. Esta norma internacional para los controles de seguridad en la nube facilitará el desarrollo y la expansión de unos sistemas de computación en la nube seguros".

Las nuevas directrices son el resultado de una iniciativa conjunta de los principales desarrolladores del mundo de las normas internacionales —IEC, ISO y ITU— para garantizar la máxima difusión.

## Soluciones integradas para servicios (ISO/IEC 27013)

Cada vez hay más organizaciones que están optando por combinar un sistema de gestión de la seguridad de la información (ISO/IEC 27001) con un sistema de gestión de servicios (ISO/IEC 20000-1). Un sistema integrado implica que una organización puede gestionar de manera eficiente la calidad de sus servicios, procesar los comentarios de los clientes y resolver problemas garantizando a la vez la seguridad de la información.

ISO/IEC 27013 ofrece una estrategia sistemática para facilitar la integración de un sistema de gestión de la seguridad de la información con un sistema de gestión de servicios, lo que se traduce en menores costos de implementación y evita la duplicación de esfuerzos, ya que solo se necesita una auditoría, en lugar de dos, para obtener la certificación.

## Comunicaciones intersectoriales e interorganizacionales (ISO/IEC 27010)

Cuando una organización comparte información con otra, ¿cómo pueden ambas tener la certeza de que sus datos estarán seguros? ISO/IEC 27010 es una adición sectorial a la caja de herramientas de ISO/IEC 27000, que ofrece directrices para la iniciación, la implementación, el mantenimiento y la mejora de la seguridad de la información en las comunicaciones interorganizacionales e intersectoriales. Incluye principios generales sobre la manera de cumplir con estos requisitos utilizando la mensajería establecida y otros métodos técnicos. Se espera que la norma fomente el crecimiento de las comunidades globales de intercambio de información.

Como el Dr. Mike Nash, uno de los revisores de la norma ISO/IEC 27010, señala, "la norma ISO/IEC 27010 básicamente personaliza y aplica las normas ISO/IEC 27001 e ISO/IEC 27002 a la comunicación entre organizaciones. Contar con esta norma proporciona a una organización la tranquilidad de que la información que ha compartido con otra no será revelada por accidente". Esta norma es particularmente relevante para la protección de la infraestructura nacional crítica, en la que el intercambio seguro de información confidencial es esencial. Su uso está también extendido entre los equipos de respuesta a incidentes de seguridad.

## Detectar y prevenir ciberataques (ISO/IEC 27039)

¿Cómo pueden las organizaciones detectar y prevenir las intrusiones cibernéticas en sus redes, sistemas y aplicaciones? Las prácticas recomendadas muestran que tienen que ser capaces de saber cuándo y cómo se produce una intrusión en su red, sistema o aplicación. También deben estar preparadas para identificar la vulnerabilidad que se ha aprovechado y los controles que se deben implementar para prevenir intrusiones similares en el futuro. Una forma de hacerlo es usar un sistema de detección y prevención de intrusiones (SDPI).

ISO/IEC 27039 proporciona directrices para preparar e implementar un SDPI y cubre aspectos tan cruciales como la selección, la implementación y el uso. La norma resulta especialmente útil en el mercado actual, donde hay muchos productos y servicios de SDPI de código abierto y comercialmente disponibles basados en diferentes tecnologías y estrategias. La norma ISO/IEC 27039 guía a las organizaciones en todo el proceso.

## Auditoría y certificación (ISO/IEC 27006)

Cada vez más organizaciones están recurriendo a las auditorías de certificación de terceros para demostrar que cuentan con un sistema sólido de gestión de la seguridad de la información (SGSI) que se ajusta a los requisitos de la norma ISO/IEC 27001. La norma ISO/IEC 27006 establece los requisitos que los organismos de certificación y registro deben cumplir para ser acreditados y poder ofrecer servicios de certificación con la norma ISO/IEC 27001.

"ISO/IEC 27006 es una acreditación de referencia para los organismos de certificación que ofrecen servicios relacionados con la norma ISO/IEC 27001", explicó el profesor Humphreys, que añadió: "Esto es importante porque la acreditación de organismos de certificación proporciona confianza adicional en el proceso de auditoría y credibilidad en el certificado que otorgan".

*Fuente: Página web de ISO*
*Traducción al español: Secretaría Ejecutiva de COPANT*