(Management - Normas ISO)

Seguridad de los activos de información

Comienza el día. Despertamos escuchando la radio con los datos del tiempo, la situación de los transportes públicos y un resumen de las principales noticias. **Información**. Durante el viaje al trabajo, leemos el informe del proyecto, y comparamos el cuadro de situación, con las fechas y los desarrollos finalizados. **Información**.

Llegamos a la oficina; nuestra tarjeta de acceso no funciona correctamente, no reconoce el código de barras, volvemos a intentar y entramos. **Información**. Nos dirigimos a nuestro escritorio, ingresamos usuario y contraseña, accedemos a nuestra computadora. **Información**. Abrimos nuestros programas de desarrollo, la última versión de los códigos fuentes, los documentos de análisis y diseño, los informes de requerimientos, accedemos a la base de datos en cuestión y nos disponemos a trabajar. **Información**. Teléfono..., el nuevo integrante del equipo nos solicita soporte sobre el componente de encriptación que estaba publicado en la librería de nuestra base de conocimiento de desarrollo. **Información**.

El asesor externo en protocolos de comunicación nos visita a fin de acordar un mejor esquema que brinde mayor eficiencia al programa que estamos desarrollando. **Información**. En las últimas horas, coordinamos con el resto del equipo la integración de los diferentes desarrollos para armar la versión final, a fin de instalarla en el ambiente de prueba, para ser testeada con los casos de prueba elaborados por los usuarios calificados. **Información**. El resultado de estas pruebas determinará que entreguemos a nuestros clientes el producto final en forma anticipada a nuestros competidores. Entendemos que ellos están retrasados en su desarrollo debido al incidente eléctrico que afectó a toda la zona. Nosotros pudimos sobrellevar esta eventualidad gracias a nuestro sitio alternativo de contingencia en las afueras de la ciudad. **Información. Información. Y más información**.

¿Qué es un activo de información?

Si nos tomamos unos minutos para analizar la situación anterior, comprenderemos que, en cada una de las actividades que desarrollamos a diario, estamos en contacto con información que nos permite mejorar el conocimiento y aprender, reducir nuestra incertidumbre al darnos la posibilidad de decidir la mejor acción entre varias, o proporcionar una serie de reglas con fines de control o evaluación.

La información se convierte en un activo, tan importante como los activos económicos y humanos que posee la organización, y, por consiguiente, debe ser protegida de un modo adecuado. Ninguna persona estaría de acuerdo en perder dinero porque tiene un agujero en el bolsillo. Ningún líder de proyecto estaría conforme en perder uno de los talentos de su equipo, particularmente, en medio de un proyecto. Ningún programador estaría motivado para comenzar su día laboral al enterarse de que la última versión del código fuente finalizado ayer se ha perdido a causa de que el servidor que lo almacenaba quedó fuera de funcionamiento y la última copia de seguridad disponible es de un mes atrás.

¿Qué es la seguridad de la información?

La **seguridad de la información** protege los activos de información con respecto a una gran cantidad de amenazas, y asegura a la organización que la frecuencia y el impacto de los riesgos sean mínimos, considerando que la rentabilidad y la relación costo/beneficio sean los más eficientes. Las organizaciones, para funcionar, dependen de sus sistemas aplicativos, bases de datos, redes de comunicaciones, procesos internos y personas. Muchos de estos aplicativos no fueron diseñados y desarrollados para que sean seguros, debido a que el esquema de seguridad aplicado a ellos era obsoleto o desconocido. La planificación del desarrollo de un aplicativo nos permite reducir lo desconocido. En el marco de la seguridad, debemos realizar la planificación paralela, que considere los diferentes controles para la protección de los activos de información.

La **seguridad de la información** es un proceso que evoluciona con toda la organización. Si bien está coordinada y centralizada por el personal especializado

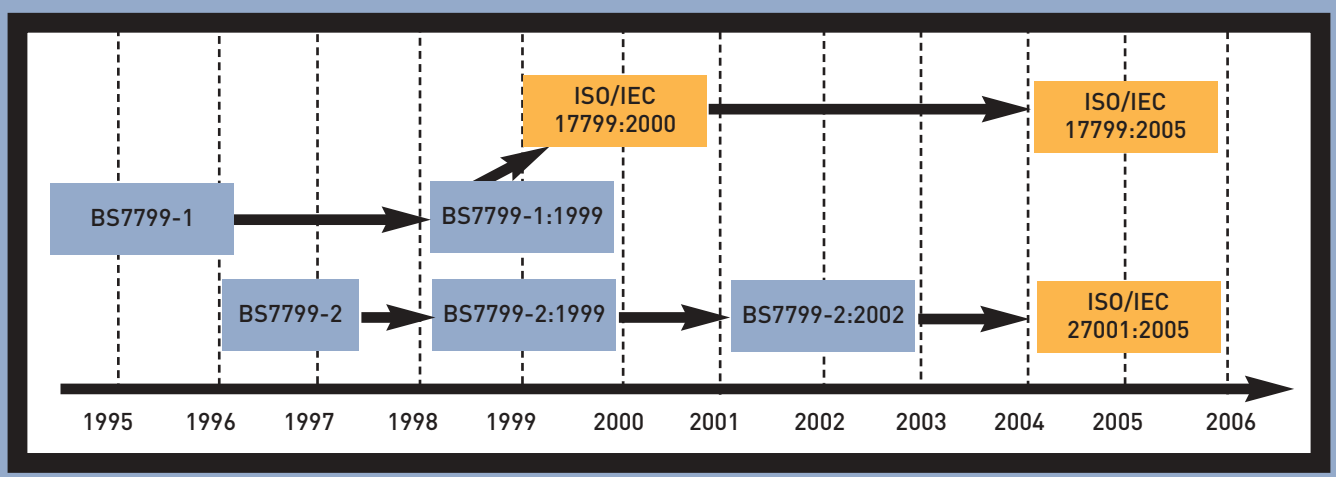
LOS TRES PILARES DEL VALOR DE LA INFORMACIÓN

¿Cuál es el valor de los activos de información para nuestra organización, para nuestro equipo de trabajo y para nosotros mismos? A fin de determinarlo, debemos conocer los tres pilares que clasifican la importancia y la prioridad de estos activos:

- → **CONFIDENCIALIDAD**: Sólo podrán acceder a la información (usarla, leerla o escucharla) las personas que estén autorizadas.
- → **INTEGRIDAD**: La información con la que se trabaja debe ser completa y precisa, poniendo énfasis en la exactitud, tanto en su contenido como en los procesos involucrados en su procesamiento. Este pilar determina la manera en que es controlada la persona antes de acceder a la información.
- → **DISPONIBILIDAD**: La información estará disponible siempre que cualquier persona autorizada necesite hacer uso de ella, clasificando este pilar de acuerdo con la velocidad de recuperación necesaria para que la información esté disponible.

Las actividades de las organizaciones existen por la información utilizada. Analicemos las normas y las buenas prácticas aplicadas a su protección, gestión y uso, que determinarán su éxito.

OSCAR ANDRÉS SCHMITZ
Ingeniero en Sistemas de Información.
oscar_schmitz@yahoo.com.ar



Estándares de la seguridad de la información: BS 7799, ISO 17799 y ISO 27001.

(IRM, *Information Risk Management*), involucra el compromiso de todas las personas de la empresa; incluso, en muchos casos es extensivo a sus clientes y proveedores, es decir que es un proyecto multidisciplinario aplicado a la cadena de valor completa. Aunque existen medios tecnológicos o técnicos que permiten mejorar la seguridad, actualmente no son suficientes por sí solos: debemos complementarlos con un detallado análisis e identificación de los puntos de riesgo, una cuidadosa planificación de los controles por realizar, una gestión de seguridad que involucre a todos y una adecuada implementación de procedimientos de acuerdo con lo relevado.

¿Para qué utilizar un estándar o buena práctica internacional?

A esta altura del artículo, deberíamos preguntarnos: "¿Somos **concientes** del esquema de seguridad que estamos aplicando a nuestros activos de información? ¿Somos **competentes** al realizarlo?". Estas preguntas tienen como objetivo cuestionarnos qué posición ocupamos frente a la seguridad de la información. ¿Seremos **ciegos** al respecto?, es decir que no sólo no sabemos, sino que ni siquiera sabemos que no sabemos. ¿Seremos **ignorantes**?, esto es que sabemos que no sabemos. En este caso, somos concientes de que no sabemos y debemos aprender, pasando de ser incompetentes a competentes, y permitiéndonos ser **aprendices** de los conceptos de la seguridad de la información. Puede ser que algunos no quieran ser aprendices, y tomen la posición de la persona **cretina**, quien sabe que no sabe, pero finge saber..., esta posición no es recomendable, debido a que no nos permite crecer como profesionales.

Es inevitable que para ser aprendices de estos conceptos, y tener el grado de competencia que requiere la organización, debamos compararnos. Podemos compararnos con otros profesionales, con otros equipos de trabajo o con otras organizaciones, pero siempre existirá una duda sustancial con respecto a si la otra parte está realizando en forma correcta y efectiva la aplicación de la seguridad. Por eso existen **estándares o**

VENTAJAS DE BUENAS PRÁCTICAS

- → Anula los efectos negativos de "reinventar la rueda".
- → Reduce la dependencia con los expertos tecnológicos internos o externos.
- → Mejora el potencial del personal que tiene menos experiencia en el equipo de trabajo.
- → Mejora y facilita la colaboración con otros equipos de trabajo externos a la organización.
- → Reduce los riesgos en términos de su frecuencia e impacto.
- → Disminuye la cantidad de errores.
- → Mejora la calidad de la información utilizada.
- → Mejora la calidad de los procesos de trabajo.
- → Mejora las habilidades para gestionar y monitorear las actividades del equipo de trabajo.
- → Reduce los costos operativos basándose en la estandarización incremental de los procesos.
- → Mejora la confianza entre integrantes del equipo, organización, socios, clientes y proveedores.
- → Crea respeto ante las entidades reguladoras o controladoras externas.
- → Protege a la organización y le provee de un valor diferencial.

Pirámide donde se muestran las etapas pertenecientes a los puntos estratégico, táctico y operativo.

buenas prácticas internacionales, que son utilizados como recomendaciones dentro de un esquema referencial por seguir, que nos permiten clarificar nuestro estado de conciencia y nos proveen del conocimiento para aprender a ser más competentes al respecto. Las buenas prácticas se relacionan, simplemente, con **"la mejor manera de realizar las cosas"**.

En los últimos años, el uso de la TIC ha definido un valor diferencial en las organizaciones. El conjunto de aplicaciones, bases de datos, redes de comunicaciones y equipamiento utilizado determinan un aspecto crítico en el éxito de las actividades comerciales. La TIC determina una ventaja competitiva que permite mejorar la productividad y la calidad de la información circulante en la organización. Pero también su aplicación implica riesgos, que debieran ser conocidos y controlados dentro de un esquema que conviva con las actividades normales de la organización. Las buenas prácticas determinan el esquema conceptual sobre el cual debemos desarrollar las actividades relacionadas con la TIC.

Los **estándares o buenas prácticas internacionales** determinan el camino que debemos seguir para alcanzar un objetivo puntual, pero **no nos aseguran el éxito**. Pueden ser comparados con un mapa o con una hoja de ruta, que nos presenta un esquema con base conceptual y teórica tendiente a servir de guía en las actividades que desarrollamos para alcanzar el objetivo propuesto. El mapa no nos anticipa lo que realmente puede presentarse en el territorio que vamos a recorrer, porque **él mismo no es el territorio**. Con el fin de acortar la brecha entre el mapa y el territorio (entre lo teórico y la realidad), es fundamental obtener de los recursos involucrados **compromiso, responsabilidad y aplicación del sentido común**. Además de estos factores, la persona que lidere este proceso deberá apoyarse, principalmente, en su experiencia práctica dentro del esquema que presente la normativa en cuestión.

La **efectividad y la excelencia** estarán condicionadas por cómo personalicemos las buenas prácticas de la organización, de qué manera las implementemos y, posteriormente, cómo las mantengamos actualizadas. La efectividad y la excelencia serán resultados de la capacidad que posea el líder de este proceso para combinar los recursos humanos de la organización, del presupuesto económico, y de la secuencia de objetivos intermedios y finales, frente a las recomendaciones que impartan las buenas prácticas acerca de cómo hacer bien las cosas.

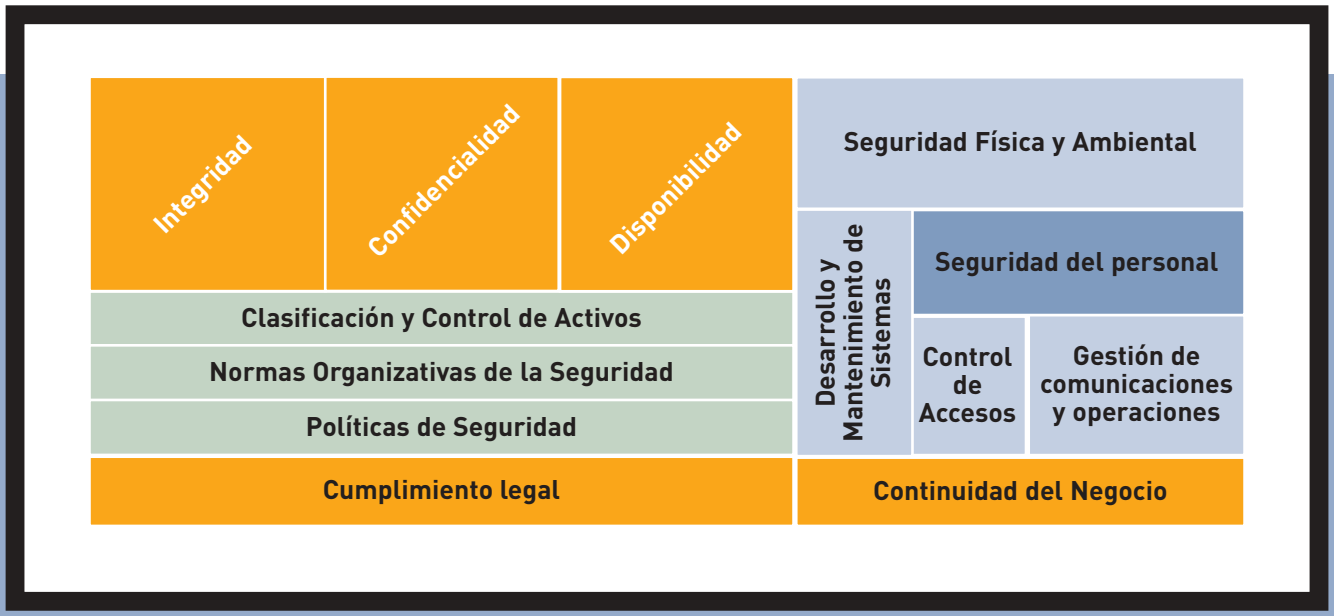
Estándares aplicados a la seguridad de la información

En el año 1995, el Instituto Británico de Normas Técnicas (BSI) publicó las primeras normativas relacionadas con varios aspectos de la gestión de la seguridad informática. Connotaciones de gran importancia se sucedieron en los años subsiguientes, tales como la problemática del año 2000 (Y2K), la unificación de la moneda europea y el impacto económico en Europa frente a la consolidación del euro. La primera edición del estándar, **BS 7799**, no brindó los resultados esperados, y se transformó en una normativa poco flexible y difícil de aplicar a conceptos básicos de la seguridad informática, que, por aquel entonces, no resultaba una necesidad importante y prioritaria. En este período, los problemas de las funcionalidades de Internet, el uso de correo electrónico y los delitos informáticos, entre otros, no resultaban graves o no eran considerados como tales; recién se estaba conformando la base para lo que significarían, años después, en el concepto de riesgo e impacto.

En 1999, se desarrolló la segunda versión de la BS 7799, que se dividió en dos partes, totalmente mejoradas. La **BS 7799-1:1999** (Parte 1) estaba asociada a la tecnología de la información y a los códigos de prácticas para la gestión de la seguridad de la información, y contenía el estándar con sus recomendaciones. Por su parte, la

DOMINIOS DE CONTROL

1. Políticas de Seguridad
2. Normas Organizativas de la Seguridad
3. Clasificación y Control de Activos
4. Cumplimiento Legal
5. Control de Accesos
6. Seguridad del Personal
7. Seguridad Física y Ambiental
8. Desarrollo y Mantenimiento de Sistemas
9. Continuidad del Negocio
10. Gestión de Comunicaciones y Operaciones



Protección de los activos de información basados en ISO/IEC 17799.

BS 7799-2:1999 (Parte 2) se asociaba a los sistemas de gestión de la seguridad de la información y a las especificaciones sobre guías de uso de la primera parte, y ponía el énfasis en la implementación de las recomendaciones y en su certificación.

Durante esta transición, la Organización Internacional de Estándares (ISO) y la Comisión Electrónica Internacional (IEC) conformaron un comité técnico con el fin de analizar, en forma paralela, la normativa técnica BS 7799. En el año 2000, la ISO/IEC adoptó y publicó la primera parte bajo el nombre de **ISO/IEC 17799:2000**. El desarrollo efectuado por la ISO/IEC en esta normativa recibió la aceptación que no habían tenido sus predecesores, y fue reconocida y adoptada a nivel internacional. En junio de 2005, la **ISO/IEC 17799:2005** fue actualizada, particularmente, en aspectos de análisis de riesgos, alineación de las políticas de seguridad con los requerimientos del negocio, monitoreos y control de accesos, administración de incidentes y, por último, entrenamiento y toma de conciencia de los usuarios finales con respecto a los temas de seguridad.

La segunda parte de la BS 7799 fue revisada en 2002, y fue adoptada por la ISO en 2005, lo cual dio origen al estándar **ISO/IEC 27001:2005**, que referencia a la certificación de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 17799

ISO/IEC 17799 es un estándar internacional publicado por la Organización Internacional de Estándares y la Comisión Internacional Electrotécnica, con el fin de proveer de un esquema estándar y de un conjunto de recomendaciones que sirvan como guía a los responsables de la iniciación, implementación, mantenimiento y mejora de la gestión de la seguridad de la información. Es la normativa técnica de seguridad de la información más reconocida a nivel internacional. Su objetivo principal es **proteger adecuadamente los activos de información** de una organización. Esta normativa fue desarrollada en forma flexible, y es neutral a la tecnología (programas o equipamiento) por utilizar; de esta manera, los conceptos que en ella se explicitan son fácilmente adaptables a los cambios tecnológicos que se producen en el mercado informático y a las diferentes plataformas que existen dentro de una misma organización.

Supongamos que debemos transportar algunos activos valiosos de información de nuestro interés. Éstos son valorizados, como ya indicamos, según los pilares de integridad, confidencialidad y disponibilidad. Por ejemplo: el paquete de programas desarrollado para entregar a nuestro cliente, el conjunto de documentación de análisis y diseño de la propuesta de desarrollo que se realizará si éste es aprobado, el conjunto de componentes y servicios de seguridad que son utilizados como base para cualquier desarrollo de aplicativos, o la lista de mis contactos de futuros clientes y los precios acordados a los cuales les venderé el software desarrollado. Todos éstos son activos de información valiosos que significarán un paso clave en las tareas que estamos realizando. En nuestro ejemplo, serán transportados en un camión adecuado a nuestras necesidades costo/ beneficio en materia de la seguridad.

Siguiendo con nuestro ejemplo, un camión puede estar conformado bajo las características que uno considere apropiadas; por ejemplo, las especificaciones del tipo de ruedas, motor, vidrios, carrocería, equipos electrónicos y eléctricos, cabina, comodidades del conductor y acompañantes, entre otros. Cada uno de estos componentes es definido por una persona que toma bajo su responsabilidad la conducción de estos activos de información, que son valiosos para nosotros. Asimismo, debemos aclarar que el camión sólo podrá funcionar si todas las partes que lo conforman se encuentran en completa armonía e integración. La rueda por sí sola no es el camión, pero el camión necesita de la rueda para cumplir la función de camión. Si alguna de las partes no está presente, o si alguna de ellas no funciona correctamente, el camión no podrá cumplir con la función para la cual se lo necesita.

Aplicando los conceptos básicos de la ISO/IEC 17799, el camión de nuestro ejemplo es transformado en un Sistema de Gestión de la Seguridad de la Información (SGSI), conformado por cada una de las partes que, en este caso, se denominan **dominio de control**. Éstos están unidos integralmente y deben ser analizados en forma conjunta, consolidando los puntos de estudios de tecnología, procesos y personas.

Estructuralmente, la ISO/IEC 17799 se encuentra dividida en **10 dominios de control**, que cubren todas las necesidades de seguridad de la información en los diferentes niveles: estratégico, táctico y operativo. Dentro de estos dominios se establecen 36 objetivos de control y 127 controles propiamente dichos, definidos mediante procedimientos, monitoreos, controles y rutinas prácticas que conllevan la mitigación o la reducción del nivel de riesgo que afrontan las organizaciones.