(Management - Normas ISO)

Seguridad de la información con la ISO/IEC 17799

La ISO/IEC 17799 nos permite cubrir las necesidades de seguridad de los activos de información dentro del alcance de diez dominios de control, los cuales serán puntualmente desarrollados a continuación.

Análisis de la ISO/IEC 17799 orientado al desarrollo de software

Los dominios de control organizan el estándar internacional para cubrir todos los puntos que los responsables de la gestión de la seguridad deben tener en cuenta. Particularmente, algunos de estos dominios tienen más relación con las políticas estratégicas y los compromisos de la máxima autoridad responsable de la organización; otros ponen foco en actividades tácticas o de supervisión y control; en tanto que un último conjunto se aplica a rutinas operativas prácticas, presentes en el accionar cotidiano.

En esta sección desarrollaremos la ISO/IEC 17799 en cada uno de los objetivos de estos dominios, mencionando lo indicado en la normativa, y complementando con comentarios y ejemplos relacionados con nuestra experiencia. Dado que los lectores se relacionan, principalmente, con los desafíos que presentan el **desarrollo, la programación y el mantenimiento de software**, ahondaremos, entonces, en aquellos dominios u objetivos que, directamente, se refieran a este tema, y sólo mencionaremos aquellos que, indirectamente, estén asociados a ellos. Las siguientes secciones están identificadas según esta asociación: directa o indirectamente.

Políticas de seguridad

Este primer dominio tiene como objetivo impartir directrices sobre la administración y el soporte a la seguridad de la información. En tal sentido, estas políticas establecen la prioridad y la importancia que posee el concepto de la seguridad en toda la cadena de valor de nuestra organización o equipo de trabajo. Son aplicadas como base para la toma de decisiones y determinan el accionar dentro de la organización, establecen cómo será el producto final que nuestros clientes tendrán en tal concepto, y cuáles serán los requisitos mínimos con que los proveedores o servicios tercerizados deberán contar para participar en nuestras actividades en relación a la calidad de la seguridad establecida. Este dominio, en la práctica, constituye un conjunto de documentos que contienen políticas, principios y normas de seguridad que reflejan las actividades en términos de seguridad dentro de la organización.

Es fundamental el compromiso y el soporte de la máxima autoridad responsable de la organización, para que el espíritu de estas políticas sea parte de la práctica habitual en las actividades de los equipos de trabajo, a fin de obtener efectividad en la aplicación de estas medidas.

Normas organizativas de la seguridad

Infraestructura de la seguridad de la información

Tiene como objetivo gestionar la seguridad de la información dentro de la organización, considerando tanto a los responsables conductores y a personas referentes, como a los procesos de comunicaciones y de concienciación de la seguridad de la información. La infraestructura requiere de una persona que desarrolle actividades multidisciplinarias, dado que su objetivo es involucrarse en cada una de las actividades de los equipos de trabajo y trasladar, con prácticas concretas, la protección de los activos propios de cada una de las funciones de estas áreas. En nuestra actividad de desarrollo de aplicaciones, una de las funciones que se necesita definir es el rol de IRM o responsable de la seguridad de la información. Dependiendo del tamaño del equipo de trabajo, esta tarea podrá recaer en

	INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD
Menor Seguridad	Pública	Nominal	Recuperable
⋮	Restringido	Estándar	Manual
⋮	Confidencial	Individual	Automático
Mayor Seguridad	Secreta	Doble Intervención	Inmediata

Clasificación de los activos de información

La información en torno al desarrollo de software tiene características especiales, y su seguridad debe estudiarse en forma particular.

OSCAR ANDRÉS SCHMITZ
Chief Information Officer
de ING Bank
Oscar_schmitz@yahoo.com.ar

una sola persona o en un equipo, con la consecuente división de tareas. Sus responsabilidades serán las siguientes: definir las políticas, los procedimientos y las guías de seguridad; coordinar las implementaciones desde la perspectiva de seguridad y aplicar las buenas prácticas internacionales; identificar y analizar puntos de riesgo en los procesos y en las aplicaciones; proponer soluciones basadas en la mitigación o en la reducción del riesgo; estudiar vulnerabilidades de los sistemas aplicativos y de los programas de base utilizados; analizar las tendencias frente a los incidentes reportados y actuar en referencia. Estas actividades podrán ser complementadas, necesariamente, con expertos frente a los avances del mercado tecnológico, o en lo que a metodología y buenas prácticas se refiere.

Otros roles importantes que debemos destacar dentro del equipo de trabajo son: responsables en los monitoreos de seguridad, administración de la seguridad (cuentas de usuarios, recursos informáticos y bases de datos), administración de sistemas, operadores del centros de cómputos, responsables de las bibliotecas o versiones de aplicativos y, propiamente, el equipo de desarrollo.

Seguridad del acceso de un tercero

Su objetivo es mantener la seguridad del mecanismo de procesamiento de información y de los activos de información de la empresa a los que acceden terceros. Tengamos presentes dos ejemplos, el del camión y el de la casa propia. ¿A quién dejarían entrar en su camión durante el transporte de los activos? En nuestras casas, ¿quiénes tendrían permitido el ingreso? Ahora bien, no sólo debemos definir quién puede hacer qué cosa, sino esto último: ¿cuáles son las cosas a las que tendría acceso? La persona que ingrese en nuestra casa, ¿podrá acceder y utilizar todos los elementos de todos los cuartos? El que acceda a la cabina del camión, ¿tendrá permitido conducirlo, manipular los mecanismos de la carga o disponer de los controles de la consola? En particular, debemos considerar ejemplos sobre servicios técnicos de programación o de sistemas de bases de datos, cuyo personal externo, muchas veces, debe acceder desde nuestras computadoras o, directamente, desde el centro de cómputos a la información que consolida nuestras actividades. ¿Qué controles aplicamos en estos casos?

Tenemos que identificar todos los aspectos vinculantes a aquellas personas ajenas al equipo de trabajo, quienes tienen que acceder a las instalaciones de nuestra organización y a nuestros activos de información. Sobre estas terceras partes, debemos aplicar los conceptos de seguridad sobre integridad, confidencialidad y disponibilidad, aun con mayor rigurosidad que sobre las personas de la propia organización. La identificación y la evaluación del riesgo, frente a los activos de información a los que podrían acceder, son los puntos prioritarios que debemos tener en cuenta. Otros temas por considerar en este aspecto son los tipos de accesos físicos o lógicos, el para qué tendrá acceso, si el acceso será in-situ o virtual, cómo definiremos el contrato con la tercera parte en relación a la confidencialidad de la información a la que tenga acceso, y la responsabilidad de sus actividades dentro de nuestras instalaciones, si los terceros tendrán o no posibilidad de copiar y de utilizar la información propia fuera de la organización.

Contratación externa

El objetivo, en este caso, es mantener la seguridad de la información cuando la responsabilidad de su procesamiento se encuentra a cargo de otra organización contratada. Supongamos que tenemos que transportar (proteger) más activos de información de lo que nuestro camión tiene capacidad. Una de las opciones permitidas sería contratar un camión a un tercero, con o sin conductor. ¿Qué características deberían cumplir cualquiera de estos camiones de terceras partes? Naturalmente, la respuesta sería: las mismas o mejores que las empleadas en nuestros camiones.

En nuestras actividades de desarrollo, la contratación externa es una de las prácticas más comunes, dado que, principalmente, buscamos alcanzar un grado de especialización alto en lo que estamos desarrollando, en particular, en el diseño y en la programación. En términos comerciales, este concepto resulta indiscutible, pero, en términos de seguridad de la información, deben tomarse los recaudos pertinentes; es decir, aplicar a las organizaciones contratantes las mismas políticas de seguridad que nosotros empleamos en la nuestra.

Veamos dos ejemplos muy comunes en la actualidad. El primero es la contratación de terceros para el desarrollo de módulos que no conforman el núcleo del sistema que estamos programando. En este caso, gran parte de los componentes de programación y parte de la documentación técnica deben ser suministrados a estos terceros, con el objetivo de que desarrollen los requerimientos pedidos. El segundo ejemplo es el almacenamiento de información propia en servidores de terceros, o *hosting*. En este caso, es más notorio y explícito el traslado de los activos de información fuera de nuestra organización.

Sobre estas contrataciones, mencionaremos algunos puntos para tener en cuenta: revisión de las políticas de seguridad de las otras organizaciones, acuerdos de confidencialidad entre ambas partes, contratos sobre responsabilidades, funciones, nivel de acceso y uso de la

TIPIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Los activos de información están presentes en la organización de diversas formas conocidas por todos nosotros:

- → Directorios, archivos o bases de datos
- → Aplicaciones o programas aplicativos
- → Sistemas o redes de comunicaciones
- → Componentes de hardware
- → Correos electrónicos
- → Medios removibles (discos, cintas, discos ópticos, videos, pen drives, etc.)
- → Soportes físicos escritos o impresos

información, mecanismos de control de la integridad y confidencialidad de los activos de información, disponibilidad del servicio, tipo de servicio, horarios y fechas acordadas, niveles de seguridad y posibilidad de auditorías periódicas.

Clasificación y control de los activos

Responsabilidad sobre los activos de información

Su objetivo es mantener la protección adecuada de los activos de la organización. Complementando los roles indicados en las secciones anteriores, dentro de la organización debemos definir roles acordes a los activos de información que se necesiten proteger. Éstos pueden ser: dueños de los activos, custodios y usuarios calificados propios de cada grupo de información, que tendrán asignados responsabilidades y controles por efectuar sobre dichos activos.

> Un módulo de seguridad alineado a normativas internacionales brinda una ventaja competitiva y un valor agregado al producto final.

Para controlar los activos, deberíamos tener un inventario en el que se indique el activo de información en cuestión, tipo, dueño, custodia y su clasificación (tema que desarrollaremos más adelante).

Clasificación de los activos de información

Debemos asegurar que los activos de información se reciban en un nivel de protección adecuado. Una vez inventariados los activos, éstos deberán ser clasificados, a fin de actuar y aplicar la seguridad correspondiente. Dentro del equipo de trabajo, una buena práctica es ordenar todos los componentes de programación clasificados y relacionarlos con los otros. Particularmente, existen algunos programas que son más importantes que otros, en relación al conocimiento específico de las personas involucradas y a la importancia que tienen en el proyecto de desarrollo. Asimismo, las bases de datos contendrán tablas con información más importante que otras. Las tablas de clientes y de transacciones tienen más prioridad e importancia, mientras que las tablas referenciales, las clásicas código-descripción, tienen menos importancia. La documentación no deja de ser un activo y, por lo tanto, requiere de su clasificación. Entendemos que los presupuestos con horas por recurso y costos, el plan estratégico de colocar un programa nuevo en el mercado o la lista de actividades diarias tienen diferente peso sobre el hecho de clasificarlos de más a menos importantes.

La información posee diferentes grados de sensibilidad y niveles de importancia. Algunos activos pueden requerir un nivel de protección adicional o una administración particular. El esquema de clasificación que utilicemos debe definir, claramente, los distintos niveles de estratificación de los activos, con la posibilidad de identificarlos y de relacionarlos con los esquemas de seguridad más adecuados y, en caso de que fuera necesario, con medidas complementarias acerca de su uso y control.

Cumplimiento legal

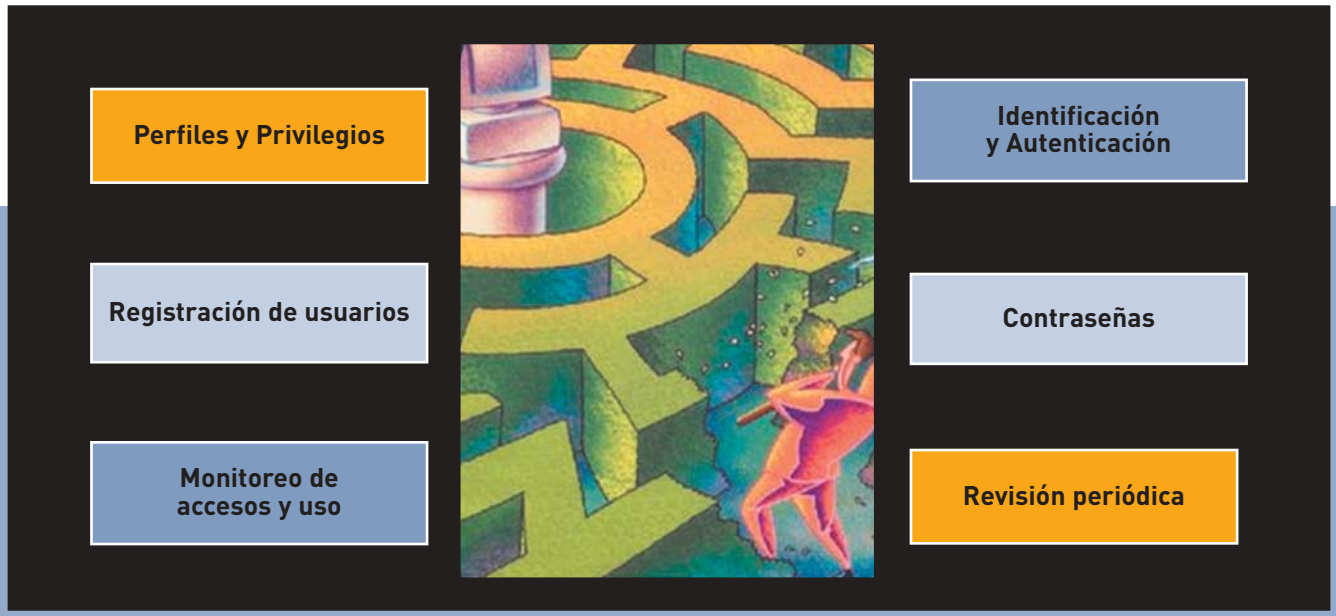
El punto que cabe resaltar sobre este concepto es evitar la violación de cualquier tema legal, contractual u obligaciones entre partes en relación a los compromisos y responsabilidades de la organización. Uno de los aspectos más importantes se relaciona con la **propiedad intelectual** de los programas desarrollados por el equipo de trabajo. Los programas y, con ello, los elementos que los integran (objetos, componentes, estructuras de base de datos, librerías, etc.) conforman el principal activo de información de los equipos de desarrollo y mantenimiento de sistemas. De acuerdo con los compromisos contractuales y los convenios impartidos por las **licencias** sobre los programas comercializados, debemos considerar los aspectos referidos al alcance de uso de nuestros desarrollos. Esto incluye: copias de la seguridad permitida, limitaciones de uso máximo según los usuarios finales y/o usuarios concurrentes y/o máquinas y/o servidores, transferencia y uso de los programas por terceros, y copia de la información referida a los manuales de usuario, documentación funcional y técnica.

Control de accesos

Administración del acceso del usuario

El pilar de la integridad de la información es el más destacado en este punto, basado en la esencia de impedir el acceso a las personas sin la autorización correspondiente. La administración de los accesos de los usuarios puede analizarse de acuerdo con las características de las funciones que agrupan:

- **Registración de usuarios**: Deben existir procedimientos que nos permitan registrar, formalmente, las autorizaciones de los accesos de los usuarios. Los formularios de acceso, junto con toda la información particular, es uno de los reportes que, naturalmente, es pedido en las aplicaciones.
- **Perfiles y privilegios**: Los tipos de acceso a un activo difieren de una persona a otra. La habilitación para acceder no implica pleno acceso al activo en cuestión, sino que, por el contrario, cada persona tendrá definidos algunos privilegios de actividades y/o acciones que puede realizar. Cuando estos privilegios o acciones permitidas se agrupan para ser asignadas a más de una persona, se las integra en lo que llamamos **perfiles**. La funcionalidad de asignación individual de privilegios, el armado y la asignación de perfiles, y los reportes de vinculación entre acciones y usuarios son puntos para tener en cuenta en cualquier desarrollo de aplicaciones desde la perspectiva de seguridad de la información.
- **Identificación y autenticación**: ¿Quiénes somos? ¿Cómo nos identificamos dentro? ¿Cómo nos reconocen? Los controles de accesos deberían de poder contestar, en forma sistémica, estas preguntas. La identificación del usuario de manera unívoca tiene el fin de realizar los controles y los monitoreos pertinentes. El proceso de autenticación permite corroborar que la persona que



Principales consideraciones en un control de acceso.

dice que es, verdaderamente sea. Este proceso puede estar acompañado por un método de encriptación o de tecnología aplicada en tarjetas inteligentes.

- **Contraseñas:** La gestión de contraseñas en cualquier contexto de aplicación es un tema muy extenso, por lo cual sólo mencionaremos los puntos que deben ser considerados en un aplicativo o programa. Las características funcionales que podemos resaltar son: configuración de longitudes de contraseñas, determinación y validación, cantidad de intentos fallidos, cantidad de contraseñas históricas no repetitivas, período de vencimiento y cambio de contraseñas, y funciones de encriptación utilizadas.
- **Monitoreo de accesos y uso:** Este punto consolida dos conjuntos de actividades: la registración en las bases de datos y la explotación de esta información a través de reportes puntuales requeridos por las áreas de seguridad de la información o de auditoría. La registración se basa en desarrollar las funciones de almacenamiento y en la incorporación de éstas en el programa, en cada uno de los eventos que necesitemos capturar del usuario. Ejemplos válidos son: ingreso y egreso del sistema, cambio de la contraseña, acceso a la ventana de administración de usuarios, y bloqueo de usuario debido a que se superó la cantidad de accesos fallidos o exitosos. A cada una de las actividades importantes del sistema le corresponde una registración, con la información necesaria, en una o varias tablas de la base de datos. La información ahí consolidada nos brinda un conjunto de datos homogéneos que pueden ser explotados y resultan de gran soporte para analizar las actividades desarrolladas por los usuarios dentro de los sistemas.
- **Revisión periódica:** La revisión periódica de las actividades registradas en los sistemas, frente a los privilegios y a los perfiles que tiene asignado cada uno de los usuarios, nos permite evaluar, periódicamente, la veracidad y la necesidad de mantener los accesos actuales. Para hacerlo, debemos desarrollar un conjunto de reportes dentro del aplicativo, que permitan efectuar este proceso de manera eficiente.

Control de acceso a las aplicaciones

El acceso a las aplicaciones es un caso particular del control de accesos, ya que no sólo nos focalizamos en el acceso en sí, sino también en la información que contienen los sistemas.

Cuando planificamos el desarrollo de un sistema, esquemáticamente, lo dividimos en módulos o grupos funcionales. Un grupo de módulos está relacionado directamente con el núcleo principal del negocio en cuestión, mientras que muchos otros son módulos comunes a todos los sistemas. Ejemplo de estos últimos son: administración de tablas de relleno (tablas clásicas de código y descripción), funciones de ayuda del sistema y, sobre lo que estamos investigando, el módulo completo de seguridad, un módulo de seguridad perfectamente alineado con las normativas de la ISO/IEC 17799 y con la flexibilidad necesaria para estar tranquilos en el desarrollo de cada uno de nuestros proyectos informáticos. Generalmente, dejamos el módulo de seguridad para la última fase del proyecto, cuando los recursos y los tiempos se volvieron escasos, lo cual origina un desarrollo pobre, con recortes de funcionalidad, y un producto fuera de lo que, necesariamente, requiere nuestro cliente responsable de la seguridad de la información. Un módulo de seguridad alineado con las normativas y los estándares internacionales nos brinda una ventaja competitiva y un valor agregado, para cualquier otro producto que proyectemos, considerando reducción de costos, sobre la inversión de dinero y tiempos de realizarlo una única vez.

Anteriormente nos preguntamos: ¿A quién dejarían entrar en su camión durante el transporte de los activos? ¿Cuáles son los privilegios a los que tendría acceso? El que acceda a la cabina del camión, ¿tendrá permitido conducirlo, manipular los mecanismos de la carga o disponer de los controles de la consola? Éstas son preguntas simples, que, por lo general, no se tienen en cuenta durante el desarrollo de un proyecto.

Los dominios estudiados hasta ahora componen la cúpula de la pirámide de los dominios de control: estratégico y táctico. Las actividades operativas se presentan con una frecuencia mayor y, por eso, en la próxima entrega comenzaremos a desarrollarlas.

Oscar Andrés Schmitz es Ingeniero en Sistemas de Información (UTN, 1997) y Master en Business Administration (MBA), CEMA 2005. Es CIO de ING Bank, desde 2001, responsable del área de desarrollo, tecnología, comunicaciones, IRM y procedimientos. Trabajó en la implantación y certificación corporativa de ISO/IEC 17799 en 2004, de acuerdo con el plan corporativo desarrollado por ING Bank a nivel internacional.