Auditoría de Seguridad de Organizaciones, fortalezas y debilidades de la Norma ISO 17799

Lic. Javier F. Diaz [jdiaz@info.unlp.edu.ar]
CC. Viviana Harari [vharari@info.unlp.edu.ar]
Lic. Paula Venosa [pvenosa@info.unlp.edu.ar]
LINTI -Laboratorio de Investigación de Nuevas Tecnologías Informáticas -Facultad de Informática - Universidad Nacional de La Plata.
TEL(0221)422-3528

Resumen

La información puede existir en diversas formas y constituye un elemento valioso para toda organización. Las amenazas a las cuales está expuesta dicha información son cada vez más sofisticadas y aumentan día a día.

A fin de lograr una mayor protección de la información surge la necesidad de definir pautas para resguardarla. La norma ISO[1] 17799 nace en respuesta a dicha necesidad.

Esta norma es un estándar para manejo de la seguridad de la información reconocido internacionalmente. Es un modelo que actualmente es aplicado en todo tipo de organizaciones y aplicaciones. En el año 2002 se homologó en Argentina como IRAM[2] 17799.

Este artículo presenta sus fortalezas y debilidades partiendo de un análisis detallado de la misma.

Introducción

La Norma ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar. No importa el tamaño de la empresa u organización o si se aplica a toda o a sectores de la misma, lo importante es el "grado de dependencia informática" que tenga.

Es una normativa internacional que compila guías para implantar las mejores prácticas en la seguridad de la información.

Su precursora fue la norma británica BS7799[3] publicada en febrero de 1995.

La norma fue ampliamente reconocida luego de haber sido publicada por la ISO en diciembre del 2000. En el año 2002 se homologa en Argentina como IRAM 17799, sin existir aún reglamentación alguna.

Organización de la norma

Este estándar detallado de la seguridad se organiza en diez secciones importantes:

1. Administración de la continuidad del negocio
2. Control de acceso
3. Desarrollo y mantenimiento del sistema
4. Seguridad física y ambiental
5. Cumplimiento
6. Seguridad del personal
7. Organización de la seguridad
8. Gestión de comunicaciones y operaciones
9. Clasificación y control del activo
10. Política de la seguridad

Descripción de la norma

La norma define a la "**información**" como un "recurso", que, como el resto de los importantes activos comerciales, tiene "valor para una organización" y por consiguiente debe ser debidamente protegida.

---

[1] ISO: International Organization for Standarization [http://www.iso.ch/]
[2] IRAM: Instituto Argentino de Normalización [http://www.iram.com.ar]
[3] http://www.bsi-global.com/

Considera que la "**seguridad de la información**", protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

Considera, también, que la información puede existir de muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes o expuesta en una conversación, y que en cualquiera de estos medios pueden existir puntos, donde puedan presentarse amenazas. Por lo tanto, sea cual fuera la forma en que se adquiera la información, o los medios por los cuales se distribuya o almacene, siempre deberá ser protegida en forma adecuada.

La seguridad de la información, deberá preservar básicamente, las características de confidencialidad[4], integridad[5] y disponibilidad[6].

La norma considera que para lograr dicha seguridad, se deben implementar un conjunto adecuado de controles, que abarquen políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Se deben establecer estos controles para garantizar que se logren los objetivos específicos de la seguridad de la organización.

La norma justifica la "**necesidad de la seguridad de la información**", debido a que la confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial de la organización.

Además considera que, las organizaciones y sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados. Además, hoy en día, la dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. También, la tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. La norma establece, que debe existir un gran compromiso de todo el personal de la empresa, para poder mantener una buena seguridad del sistema de información. Pone el acento en que se debe contar con el apoyo de la alta gerencia y con que, el personal específico de seguridad debe ser idóneo y de gran capacidad y si no se cuenta con eso, la organización debe pensar en el asesoramiento experto de organizaciones externas. También plantea que, se debe capacitar al personal no destinado a la seguridad, para que sepa cómo debe comportarse para poder mantener la seguridad de la organización y que se puede requerir la participación de proveedores, clientes y accionistas.

La norma considera que, si los controles de seguridad de la información se incorporan en la etapa de especificación de requerimientos y diseño, resultarían considerablemente más económicos y eficaces.

---

[4] La confidencialidad garantiza que la información sea accesible sólo por aquellas personas autorizadas.

[5] La integridad garantiza la exactitud y totalidad de la información y los métodos de procesamiento.

[6] La disponibilidad garantiza que los usuarios autorizados tengan siempre acceso a la información y a los recursos relacionados con ella.

Con respecto a "**cómo establecer los requerimientos de seguridad**", la norma considera que es esencial que una organización identifique sus requerimientos de seguridad. Los tres recursos principales que plantea para lograrlo son:

a. Evaluar los riesgos que enfrenta la organización. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.
b. Los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.
c. El conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

Para "**evaluar los riesgos en materia de seguridad**", la norma establece que el análisis de los riesgos realizado a toda la organización, o sólo a partes de la misma, debe ser de tipo "cualitativo" y no "cuantitativo" y que la evaluación de los mismos es una consideración sistemática de los siguientes puntos:

a. Impacto potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos;
b. Probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos. Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse a cabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

El análisis de los riesgos debe ser dinámico y cíclico. Debe efectuarse periódicamente sin importar si hubo o no modificaciones tecnológicas u operativas. Con los sucesivos análisis de riesgo realizados, se evalúan los problemas que ocurrieron debido a la falta de medidas tomadas, para luego implementar contramedidas. Esto hace posible que el análisis de riesgo se vaya ajustando progresivamente a la realidad de la organización y forme parte del mantenimiento del sistema de seguridad informático.

Por lo tanto es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de reflejar los cambios en los requerimientos y prioridades de la empresa, considerar nuevas amenazas y vulnerabilidades (lo cual debe hacerse permanentemente y debe estar a cargo de personal especializado) y corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones deben llevarse a cabo con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la gerencia está dispuesta a aceptar. Frecuentemente, las evaluaciones de riesgos se realizan primero en un nivel alto, a fin de priorizar recursos en áreas de alto riesgo, y posteriormente en un nivel más detallado, con el objeto de abordar riesgos específicos.

Con respecto a la "**selección de controles**", la norma establece que una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable (lo cual no implica que siempre debe llegarse a un nivel cero). Establece además que, la selección de los controles pueden hacerse utilizando como base esta norma u otros estándares, o bien pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda.

Existen diversos modos de administrar riesgos y la norma plantea ejemplos de estrategias generales, por ende puede suceder que los controles planteados no sean aplicables a todo tipo de organizaciones[7].

Los controles deben seleccionarse teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad. También deben tenerse en cuenta los factores no monetarios, como el daño en la reputación. Muchas veces puede suceder que un determinado control no sea aplicado, ya que el costo de hacerlo supera el costo que el riesgo implica. La norma establece que es importante documentar correctamente cuáles son los controles que no son aplicados, justificando la causa de la no aplicación de los mismos. Como la norma plantea análisis cíclicos, en una nueva etapa puede llegar a ocurrir que el control no aplicado deba ser aplicado, ya sea en forma completa o parcial.

Algunos controles expuestos en esta norma, pueden considerarse como principios rectores que proporcionan un buen "**punto de partida para la implementación de la seguridad de la información**". Están basados en requisitos legales fundamentales, o bien se consideran como práctica recomendada de uso frecuente concerniente a la seguridad de la información.

Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden: la protección de datos y confidencialidad de la información personal, la protección de registros y documentos de la organización y los derechos de propiedad intelectual.

Para la norma, estos controles son hipótesis mínimas, lo cual indica que siempre deben "aplicarse". Los detalles de estos controles se plantean en el punto 12 de la misma.

Los controles, considerados por la norma como práctica recomendada de uso frecuente en la implementación de la seguridad de la información, comprenden:

a. documentación de la política de seguridad de la información (detallado en el punto 3.1.1);
b. asignación de responsabilidades en materia de seguridad de la información (detallado en el punto 4.1 .3);
c. instrucción y entrenamiento en materia de seguridad de la información (detallado en el punto 6.2.1);
d. comunicación de incidentes relativos a la seguridad (detallado en el punto 6.3.1);
e. administración de la continuidad de la empresa (detallado en el punto 11.1).

Estos controles son aplicables a la mayoría de las organizaciones y en la mayoría de los ambientes, pero se debe tener en cuenta que si bien, todos los controles mencionados son importantes, la relevancia de cada uno de ellos debe ser determinada teniendo en cuenta los riesgos específicos que afronta la organización. Por ello, si bien el enfoque delineado precedentemente se considera un buen punto de partida, éste no pretende reemplazar la selección de controles que se realiza sobre la base de una evaluación de riesgos.

La experiencia ha demostrado que los siguientes factores, a menudo resultan críticos para la implementación exitosa de la seguridad de la información, dentro de una organización:

a. política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa;
b. una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional;
c. apoyo y compromiso manifiestos por parte de la gerencia;
d. un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos;
e. comunicación eficaz de los temas de seguridad a todos los gerentes y empleados;
f. distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas;
g. instrucción y entrenamiento adecuados;
h. un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

[7] Por ejemplo el punto 8.1.4 describe cómo pueden separarse las tareas para evitar fraudes y errores. Sin embargo esto no sería una buena opción para aplicar en las organizaciones más pequeñas, en las cuales resultaría necesario llevar a cabo otros métodos para lograr el mismo objetivo de control.

Este código de práctica puede ser considerado como un punto de partida para el desarrollo de lineamientos específicos, aplicables a cada organización. No todos los lineamientos y controles de este código de práctica resultarán aplicables. Más aún, es probable que deban agregarse controles que no están incluidos en este documento.

Ventajas de su uso:

Hoy día las empresas y organizaciones tienen un gran nivel de **dependencia informática** y esto implica que sean más **vulnerables a las amenazas de seguridad**. Además los sistemas de las empresas u organizaciones dialogan con otros sistemas. Por lo tanto, en lo relacionado con los parámetros de seguridad utilizados, es muy importante basarse en un estándar para poder ajustarse y ser compatibles con los otros sistemas.

Utilizar un estándar homologado, provocará que haya pocas posibilidades de tener que cambiar aspectos del manejo de seguridad informática cuando se establecen acuerdos con otras partes.

Con respecto al tema de auditorias, también presenta ventajas, ya que existirá una tendencia a su uso, a pesar que no exista una ley que lo imponga.

Una empresa que está certificada con la norma ISO 17799 puede ganar frente a los competidores no certificados, ya que un cliente potencial, para el cual la seguridad es un aspecto de suma importancia, optará por la empresa que cumpla con las características inherentes al cumplimiento de la norma.

Algunas desventajas encontradas:

La norma 17799 no tiene una forma de valoración de las soluciones técnicas. Si bien rescata la política de toma de conciencia, revisión y testeo, no posee una forma de valoración absoluta respecto de lo efectivo que es la seguridad (como podría ser usar productos certificados por algún organismo).

Respecto de cuestiones de valoración de riesgo y perfiles de usuarios la norma ISO 15404[8] es mucho más completa y permite aplicarse a productos concretos y no sólo a organizaciones.

La evaluación de seguridad de sistemas integrados y los problemas que surgen de seguridad de manejo de sistemas integrados/interoperables, así como los problemas derivados de utilizar un identidad de red genérica no tienen un marco preciso de evaluación (o justipreciación de riesgo) por esta norma.

Conclusiones:

Esta norma es débil en relación a la tecnología, describe los aspectos a tener en cuenta para garantizar la seguridad de una organización pero no describe cómo testear que lo que ella sugiere sea implementado.

La naturaleza de la norma es filosófica, su cumplimiento implica que la organización es conciente de los controles de seguridad que deben establecerse, pero no asegura necesariamente la implementación de estos controles.

Por lo anteriormente expuesto, creemos que es posible enriquecer la norma con otras propuestas (como la norma ISO 15404 y estándares para integración de la W3C y otros organismos) para poder tener una forma más precisa de auditar seguridad teniendo en cuenta en mayor detalle los aspectos de tecnología informática y de comunicaciones.

Referencias:

http://www.ins.com/
http://www.iram.com.ar/
"Prepare su Empresa de acuerdo a la Norma ISO-IRAM 17799 de Seguridad Informática" del Prof. Gustavo Aldegani

[8] La norma ISO 15408 es una norma que contiene criterios de evaluación de la seguridad de tecnologías de la información (Information technology – Security techniques -- Evaluation criteria for IT security): http://www.commoncriteria.org/