Un acercamiento a las mejores prácticas de seguridad de información internacionalmente reconocidas en el estándar ISO 17799:2005

Cómo pueden las organizaciones asegurar y cumplir las regulaciones para preservar la confidencialidad, integridad y disponibilidad de su información

Jaime Yory
Gerente General
Director de Operaciones Internacionales de MVA
Bogotá, Colombia
Septiembre 7 de 2006

Mayorista de Valor Agregado

www.mvaonline.com

Agenda

- Algunos conceptos básicos y terminología
- La Seguridad
- La seguridad de la información
- ¿Qué es la norma ISO 17799?
- Estructura de la norma
- Dominios & Objetivos de control
- Ventajas
- Conclusiones
- Recomendaciones
- Agenda de Presentaciones

Algunos Conceptos Básicos (1)

La Información

"La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada." ISO/IEC 17799

Algunos Conceptos Básicos (2)

Vulnerabilidad

- Vulnerabilidad: Una debilidad (o agujero) en la seguridad de la organización
  - Puntos y control de acceso (lógicos y físicos)
  - Falta de Mantenimiento
  - Personal sin conocimiento
  - Desactualización de los sistemas críticos
  - Una vulnerabilidad, por sí misma, no produce daños. Es un condicionante para que una amenaza afecte un activo

Algunos Conceptos Básicos (3)

Amenaza

- Declaración intencionada de hacer un daño (Virus, acceso no autorizado, robo)

  Eventos naturales que pueden desencadenar daños materiales o pérdidas inmateriales en sus activos. Las amenazas se pueden materializar y transformarse en agresiones

Riesgo

- Potencial explotación de una vulnerabilidad de un activo de información por una amenaza.

  Se valora como una función del Impacto, Amenaza, Vulnerabilidad y de la probabilidad de un ataque exitoso

Ataque

- Acción intencional e injustificada (desde el punto de vista del atacado). Intento por romper la seguridad de un sistema o de un componente del sistema.

Algunos Conceptos Básicos (4)

Atacante

- Alguien que deliberadamente intenta hacer que un sistema de seguridad falle, encontrando y explotando una vulnerabilidad

  Externos & Internos

  Internos: Difíciles de detener porque la organización esta forzada a confiar en ellos. Conocen cómo trabaja el sistema y cuáles son sus debilidades.

  "Quizás el error mas común de seguridad es gastar considerables recursos combatiendo a los atacantes externos ignorando las amenazas internas"

  "Hay que conocer los atacantes: Motivaciones, objetivos, expertise, acceso, recursos, aversión al riesgo"

Safety & Security

- Prevención en contra de actos no intencionales Vs intencionales por parte de terceros

La Seguridad

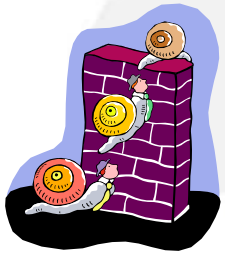
- Es difícil de medir, la mayor parte del tiempo oímos de ella cuando solo cuando falla
- La medición de los resultados es clave para justificar la inversión ante la alta gerencia
- La Seguridad es una sensación y una realidad. Sentirse seguro no es realmente estar protegido.
- El concepto de seguridad es altamente subjetivo, por tanto cada uno determina su nivel de riesgo y lo que está dispuesto a dar por las medidas que tome.
- No hay un nivel correcto de seguridad, existe un juicio personal sobre el nivel de riesgo aceptable y lo que constituye una amenaza.

Seguridad de la Información (1)

- El objetivo de la **seguridad de la información** es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Seguridad de la Información (2)

- La seguridad de la información se define como la preservación de:
  - **Confidencialidad**. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso
  - **Integridad**. Garantía de la exactitud y totalidad de la información y de los métodos de procesamiento.
  - **Disponibilidad**. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a los recursos relacionados.
- Todo esto, según el nivel requerido para los objetivos de negocio de la empresa.



Seguridad de la Información (3)

Objetivos

- Asegurar la continuidad de la empresa.
- Mantener la competitividad, la rentabilidad, los recursos generales, el cumplimiento de las leyes y la imagen comercial.
- Minimizar el riesgo.
- Maximizar las oportunidades del negocio.

Seguridad de la Información (4)

Por qué es necesaria

- Gran variedad de Riesgos y Amenazas: Fraudes, espionaje, sabotaje, vandalismo, incendio, inundación, Hacking, virus, denegación de servicio, etc.
- Provenientes de múltiples fuentes.
- Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información interconectados.
- La mayoría de los sistemas de información no han sido diseñados para ser seguros.

Seguridad de la Información (5)

Qué sucede si falla?

- Pérdidas o falsos datos financieros
- Pérdida de negocios, clientes y cuota de mercado
- Responsabilidad legal – denuncias, litigios, multas, etc.
- Daño a la imagen de la empresa
- Interrupción de las operaciones
- Mayores costos de operación
- Costo de recuperación para volver a la situación inicial

Evaluación y Análisis de Riesgos

Análisis de riesgos - Es una consideración sistemática:

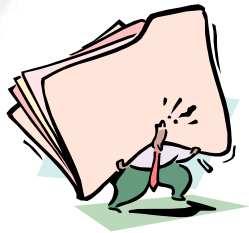
- Se estima el impacto potencial de una falla de seguridad en los negocios y sus posibles consecuencias de pérdida de la confidencialidad, integridad o disponibilidad
- Se evalúa la probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas, vulnerabilidades y controles implementados.
- Establecimiento de PRIORIDADES y ACCIONES

Selección e Implementación de Controles

- Deben tenerse en cuenta en función del costo Vs la reducción de los riesgos a un nivel aceptable y de las pérdidas que podrían producirse
- Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden:
  - Protección de datos y confidencialidad de la información personal.
  - Protección de registros y documentos de la organización
  - Derechos de propiedad intelectual

Selección e Implementación de Controles

- Los controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información comprenden:
  - Documentación de la política de seguridad de la información
  - Asignación de responsabilidades en materia de seguridad de la información
  - Instrucción y entrenamiento en materia de seguridad de la información
  - Comunicación de incidentes relativos a la seguridad
  - Administración de la continuidad de la empresa



¿Qué es la norma ISO 17799?

- ISO 17799 es una norma internacional que ofrece **recomendaciones** para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

  Existen multitud de **estándares** aplicables a diferentes niveles pero ISO 17799 como estándar internacional, es el más extendido y aceptado.

Objetivo de la norma ISO 17799

- El **objetivo** de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

Sistema de Gestión de la Seguridad de la Información (SGSI)

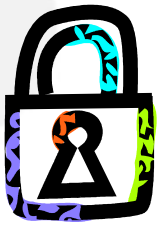
- La norma ISO 17799 recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un **Sistema de Gestión de la Seguridad de la Información** (SGSI)

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
  - Redactada de forma flexible e independiente de cualquier solución de seguridad concreta
  - Proporciona buenas prácticas neutrales con respecto a tecnologías o fabricantes específicos.
  - Aplicable a todo tipo de organizaciones, con independencia de su tamaño u orientación de negocios.

Gestión de la Seguridad de Información

La norma ISO 17799:2005 establece **once dominios de control** que cubren por completo la Gestión de la Seguridad de la Información:

1. **Política de seguridad**: Dirigir y dar soporte a la Gestión de la seguridad de la información -directrices y recomendaciones-
2. **Aspectos organizativos de la seguridad**: Gestión dentro de la Organización (recursos, activos, tercerización, etc.)
3. **Clasificación y control de activos**: Inventario y nivel de protección de los activos.
4. **Seguridad ligada al personal**: Reducir riesgos de errores humanos, robos, fraudes o mal uso de los recursos



Gestión de la Seguridad de Información

Dominios de control (Continuación)

5. **Seguridad física y del entorno**: Evitar accesos no autorizados, violación, daños o perturbaciones a las instalaciones y a los datos
6. **Gestión de comunicaciones y operaciones**: Asegurar la operación correcta y segura de los recursos de tratamiento de información
7. **Control de accesos**: Evitar accesos no autorizados a los sistemas de información (de usuarios, computadores, redes, etc)
8. **Desarrollo y mantenimiento de sistemas**: Asegurar que la seguridad está incorporada dentro de los sistemas de información. Evitar pérdidas, modificaciones, mal uso.

Gestión de la Seguridad de Información

Dominios de control (Continuación)

9. **Gestión de incidentes**: Gestionar los incidentes que afectan la seguridad de la información
10. **Gestión de continuidad del negocio**: Reaccionar a la interrupción de las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres.
11. **Conformidad con la legislación**: Evitar el incumplimiento de leyes, regulaciones, obligaciones y de otros requerimientos de Seguridad.

Gestión de la Seguridad de Información

De estos once dominios se derivan los

- **Objetivos de control,** resultados que se esperan alcanzar mediante la implementación de controles y
- **Los controles,** que son las prácticas, procedimientos y/o mecanismos que reducen el nivel de riesgo.

Ventajas de la adopción de la norma ISO 17799

- Aumento de la **seguridad efectiva** de los sistemas de información.
- Correcta **planificación** y gestión de la seguridad.
- Garantías de **continuidad del negocio**.
- **Mejora continua** a través del proceso de auditoría interna.
- Incremento de los niveles de **confianza** de los clientes y *socios de negocios*.
- Aumento del **valor comercial** y mejora de la **imagen** de la organización.

Orientación de la norma ISO 17799?

- La norma ISO 17799 **no** es una norma tecnológica.
- La seguridad de la información es un asunto que compete a la alta gerencia no al área tecnológica, por lo cual es un asunto empresarial.
- La gente toma decisiones de seguridad basados en los riesgos percibidos no en los riesgos reales, por lo cual el análisis de riesgos es fundamental para los negocios

Conclusiones

- ISO 17799 es una norma internacional que ofrece r**ecomendaciones** para realizar la gestión de la seguridad de la información
- La norma se estructura en **once dominios de control** que cubren por completo todos los aspectos relativos a la seguridad de la información.
- Implantar ISO 17799 puede requerir de un trabajo de **consultoría** que adapte los requerimientos de la norma a las necesidades de cada organización.

Conclusiones

- La adopción de ISO 17799 presenta múltiples **ventajas** para la organización, entre ellas el primer paso para una certificación ISO 27001, pero ni la adopción de ISO 17799, ni la certificación garantizan la inmunidad de la organización frente a problemas de seguridad.
- Hay que hacer análisis periódicos de los Riesgos y monitorear continuamente la situación
- La seguridad no es un tema de un día ni un tema exclusivo del departamento de TI
- Hay que prepararse para entender la norma y avanzar en el seguimiento de las recomendaciones establecidas.

Bibliografía

- Beyond Fear, Bruce Schneier – Copernicus Books
- Nueve claves para el éxito, Una visión general de la implementación de la norma NTC-ISO/IEC 27001, Alan Calder
- Esquema de la Norma IRAM-ISO IEC 17799, INSTITUTO ARGENTINO DE NORMALIZACIÓN

Programación del evento - Salón Oxford

1. Cómo crear una estrategia efectiva de navegación, filtrado y control de contenido
2. Establecimiento de políticas corporativas, control antispam y educación de los usuarios con el uso del correo electrónico
3. Cómo prevenir y combatir la nueva generación de amenazas: malware, spyware, adware, keyloggers, phishing, spoofing, IM, games, P2P

Programación del evento Victoria 2

1. Cómo detectar, prevenir y responder a los ataques, intrusiones y otras fallas de los Sistemas a través de dispositivos de administración unificada de amenazas (UTM's)
2. Alta disponibilidad, clustering, replicación de datos y Planes de continuidad de negocios (BCP)
3. Protección contra hackers - Monitoreo y vigilancia no invasiva de vulnerabilidades

Programación del evento – Victoria 3

1. Monitoreo y control de Servidores, Firewalls, routers, Switches, PBX´s y otros elementos activos de red. Consolas centrales de administración.
2. Cómo establecer y controlar las políticas de uso de los dispositivos personales. La Seguridad en los puntos finales de la red.
3. Autenticación & Encripción - más allá de los passwords, para hacer boot, discos duros y dispositivos móviles