USAL
UNIVERSIDAD
DEL SALVADOR

MAESTRÍA EN AUDITORIA DE SISTEMAS

TRABAJO DE TESIS SOBRE:

La Gobernabilidad de la Seguridad de la Información en el proceso de Gobierno Corporativo

TUTOR A CARGO: Enzo Taibi

ALUMNO: Gerardo Oscar Cosachov

Abril 2006

INDICE

I. Introducción

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El hombre buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otras personas, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban con mucho cuidado en locales de difícil acceso, a cuya forma y contenido sólo tenían acceso quienes estuviesen autorizados o listos para interpretarla.

En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, y en muchos casos, llegando a tener un valor superior.

La década del 90 puede ser caracterizada como la década de la tecnología informática. Los avances en los campos de la computación y las telecomunicaciones tuvieron un fuerte impacto en las costumbres sociales y en la economía mundial, provocando cambios revolucionarios, similares a los vividos durante la Revolución Industrial. En especial debe destacarse el crecimiento de Internet como medio de comunicación entre consumidores, negocios y gobiernos.

En la actualidad las empresas y organizaciones gubernamentales dependen en gran medida para su funcionamiento, de la tecnología informática.

Al mismo tiempo que se generalizaba el uso de la tecnología informática y de Internet, también aparecieron nuevos riesgos derivados de vulnerabilidades propias de las tecnologías y sistemas implantados. Como la seguridad completa es prácticamente imposible, lo que debe procurarse es reducir los riesgos a un nivel aceptable para cada organización

Hasta hace poco, la tecnología informática era vista como un "mecanismo de soporte" dentro de las organizaciones; sin embargo actualmente es considerada un proceso integrado al negocio, debiendo la Dirección asegurarse que las estrategias, el planeamiento, las operaciones, la protección de las inversiones y el ambiente de control y seguridad en el

que se desarrollan los procesos relacionados con la TI estén en concordancia con los lineamientos generales de toda la organización.

Debido al valor reconocido de la información como "activo crítico" de una organización, deben implementarse diversas medidas para protegerla y mantenerla segura. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información, incrementó la dificultad de proteger la información de accesos no autorizados. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. El éxito de un programa de seguridad no depende por lo tanto sólo de las habilidades técnicas de quienes manejan a diario la TI, sino que para lograr su objetivo requiere de la decisión e involucramiento de la Alta Gerencia, y de todos los empleados de la organización.

La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

Los objetos reales o tangiles (joyas, pinturas, dinero, etc) están protegidos por técnicas que los encierran detrás de rejas o dentro de cajas fuertes, bajo la mira de cámaras o guardias de seguridad. Pero ¿y la información que se encuentra dentro de servidores de archivos, qué transita por las redes de comunicación ó que es leída en una pantalla de computadora? ¿cómo hacer para protegerla, ya que no es posible usar las mismas técnicas de protección de objetos reales?

Cuando hablamos de "información", nos referimos a tres elementos:

- la información propiamente dicha
- los equipos que la soportan: software (sistemas aplicativos y sistemas operativos), hardware (infraestructura tecnológica) y organización (estructura departamental y funcional, distribución de funciones, ambiente físico)
- las personas que los utilizan, o se los usuarios finales.

La seguridad de la información se puede definir como la preservación de las siguientes características básicas:

a) confidencialidad, es decir garantizar que la información sea accesible sólo por aquellas personas autorizadas a tener acceso a ella.
b) Integridad, a efectos de salvaguardar la exactitud y totalidad de la información

c) Disponibilidad, de modo de garantizar que los usuarios autorizados tengan acceso a la información toda vez que lo requieran.

II. ¿Quiénes son los responsables de la seguridad?

"*La seguridad está relacionada con la cultura y los valores. Los altos directivos deben tomarse la seguridad como una cuestión de política empresarial y no como una cuestión de tecnología. Requiere capacidad de mando, no tecnológica. Si sus empleados piensan en la línea correcta, identificarán y resolverán los problemas de seguridad. Si ven la seguridad como una molestia y un impedimento, burlarán los mecanismos de seguridad y minarán su eficacia"* (William Malik, vicepresidente y director del área de investigación de Gartner Group, 28/12/2000, libro "Seguridad Digital", página 41)

La seguridad está más relacionada con la cultura y los valores que con firewalls y otros sistemas de detección de intrusiones. Lo manifestado por William Malik, sugiere que los procesos y la tecnología se han de adaptar tanto a los requisitos específicos de la empresa como a la cultura corporativa. Igual que el sistema de alarma de los vehículos, los procesos y la tecnología de seguridad no funcionarán si alguien olvida activarlos. Y si funcionan, no serán efectivos si se hace caso omiso de la advertencia.

Según William Malik *"en el caso de la seguridad, los mayores réditos se obtienen fomentando la conciencia, es decir, valores, cultura y comportamientos adecuados. La historia está repleta de ejemplos en los que una buena administración supera las limitaciones de la tecnología. Sin embargo, no tenemos ejemplos en los que una buena tecnología supere las limitaciones de una administración ineficiente"*.(libro "Seguridad Digital, página 42)

Las personas son la parte más importante de la seguridad, pero también la parte más vulnerable. Para convertir su mayor vulnerabilidad en su mejor activo no necesita despedir a nadie; lo que necesita es hacer que las personas entren a formar parte de la solución.

La seguridad de la información es un desafío para la gobernabilidad de las organizaciones; para que sea efectiva es necesario el involucramiento de la Alta Dirección. Así como el Gobierno Corporativo consiste en un conjunto de políticas y procedimientos a través de las cuales las organizaciones son gerenciadas, la gobernabilidad de la seguridad de la información es un subconjunto de esas políticas y procedimientos. El gerenciamiento de los riesgos, el "reporting" y la responsabilidad por su gestión, son aspectos centrales de estas políticas y procedimientos de control interno.

La seguridad de la información es responsabilidad de todas las personas que conforman una organización. Esta responsabilidad debe comenzar en la Alta Dirección, manifestando un claro compromiso, a través de la asignación de los recursos necesarios para cumplir con este objetivo. Asimismo las políticas relacionadas con la seguridad de la información deben ser comunicadas a toda la organización y también a los clientes y proveedores. (Organización extendida)

Cuando mencionamos la responsabilidad de todos los miembros de una organización nos referimos a: Board directivo, Alta dirección, gerentes, empleados y usuarios. Cada uno en su nivel puede aportar a la gobernabilidad de la seguridad informática.

El Board Directivo debería: a) entender la criticidad de la información y de la seguridad informática para la organización. b) asignar los recursos necesarios para el desarrollo de un programa de seguridad que esté en línea con la estrategia general de la compañía. c) aprobar el desarrollo e implementación de un programa de seguridad de la información d) solicitar reportes periódicos para conocer el grado de avance en la implantación del mencionado programa.

La Alta Dirección debería: a) designar a una persona responsable del programa de seguridad (Information Security Officer), quien será el encargado de desarrollar e implementarlo. b) informar al Board respecto de las vulnerabilidades significativas halladas, de los planes de remediación a desarrollar para mitigarlas, y del riesgo residual (riesgo que está dispuesto a asumir la organización).

El nivel gerencial de la organización debería: a) supervisar el desarrollo e implementación de políticas, procedimientos, estándares y guías sobre seguridad informática, tomando como base algunos de los estándares aceptados a nivel mundial, como por ejemplo la norma ISO / IEC 17799 b) controlar que el desarrollo del programa de seguridad se encuentre alineado con la estrategia general de la organización c) desarrollar evaluaciones de riesgo, determinando el impacto que puede causar la explotación de una vulnerabilidad en los sistemas de información.(uso no autorizado, revelación, falta de continuidad de procesamiento, destrucción de información) d) desarrollar planes de remediación de las vulnerabilidades detectadas e) efectuar testeos periódicos de los controles implementados

para mitigar los riesgos, a efectos de asegurar que se encuentran correctamente implantados y funcionan en forma adecuada. f) verificar que la organización tenga personal suficientemente entrenado para el desarrollo e implementación de los planes de seguridad. g) controlar que todos los empleados, proveedores y clientes, son conscientes de sus responsabilidades en el cumplimiento del programa de seguridad.

Empleados y usuarios: a) tomar conciencia e implantar en su ámbito de responsabilidad las políticas, normas y prácticas recomendadas para proteger la seguridad de la información b) reportar las vulnerabilidades ó incidentes que tuvieran lugar en sus lugares de trabajo.

Del mismo modo que una buena campaña de marketing, la campaña de seguridad ha de ser bien presentada, acompañada de programas de formación y materiales bien diseñados. Debe estar integrada en los procedimientos estándares de recursos humanos y formar parte de la orientación y del contenido de los cursos de formación que se impartan. Si tuviéramos que elegir entre un equipo bien instruido y bien formado que utilice tecnología mediocre o un equipo que disponga de las tecnologías más recientes, pero que carezca de una formación y de un conjunto de directrices adecuados, elegiríamos la primera opción.

III. En búsqueda de una cultura de seguridad

En 1992 la OECD (Organización para la Cooperación y el Desarrollo Económico), publicó la denominada "guía para la seguridad de los sistemas de información", cuyos principales propósitos son:

a) promover una cultura de seguridad entre todos los "participantes" (gobiernos, empresas, organizaciones no comerciales e individuos, que desarrollan, poseen, proveen, administran servicios informáticos y usan los sistemas de información y las redes) como un medio para proteger los sistemas de información y las redes.
b) Concientizar acerca de los riesgos a los que están sometidos los sistemas de información, y haciendo referencia a las políticas, normas, procedimientos y medidas disponibles para mitigar estos riesgos; asimismo destacando la necesidad de la adopción de las mismas y su implementación.
c) Establecer un marco de referencia para ayudar a los "participantes" a entender los aspectos de la seguridad de la información y respetar valores éticos y en el desarrollo e implementación de políticas, normas, procedimientos y medidas de seguridad.
d) Promover la cooperación y el intercambio de información entre todos los "participantes", en la implementación de las medidas de seguridad.
e) Promover la consideración de la seguridad como un objetivo importante entre todos "participantes" involucrados en el desarrollo e implementación de estándares de seguridad.

En esta guía la OECD estableció nueve principios que no deben ser considerados en forma aislada, sino como un cuerpo normativo:

1) Conciencia: los "participantes" deben ser conscientes de la necesidad de proveer seguridad a los sistemas de información y redes, y conocer que es lo que pueden realizar para mejorar la seguridad.

   Conciencia de los riesgos y conocimiento de las medidas de seguridad que se pueden implementar, es la primera línea de defensa. Los sistemas de información y las redes pueden ser afectados tanto por riesgos internos como externos. Los "participantes" deben comprender que las fallas de seguridad pueden afectar significativamente los sistemas y redes que administran. Los "participantes" deben

ser conscientes del daño que pueden ocasionar a otros, como consecuencia de la interdependencia (fruto de la alta conectividad a las redes) entre los diferentes "actores". Asimismo los "participantes" deben conocer las actualizaciones disponibles para los sistemas operativos y redes que soportan sus sistemas de información, y las medidas que pueden implementar para mejorar la seguridad.

2) Responsabilidad: todos los "participantes" son responsables por la seguridad de los sistemas de información y las redes.
   Cada miembro de una organización tendrá un grado de responsabilidad acorde con la función que desempeñe. Cada participante debería revisar periódicamente sus propias políticas, normas, procedimientos y medidas de seguridad, y evaluar si las mismas son las apropiadas para la defensa de sus sistemas y redes.
   Aquellos que desarrollan, diseñan y proveen productos y servicios deben publicar y distribuir información apropiada, incluyendo actualizaciones en forma oportuna, de manera que los usuarios sean capaces de entender las nuevas funcionalidades ofrecidas para proteger sus sistemas de información.

3) Respuesta: los "participantes" deben actuar en forma oportuna y cooperativa para prevenir, detectar y responder a incidentes de seguridad. Deben compartir información acerca de amenazas y vulnerabilidades, e implementar procedimientos para que en forma rápida se puedan neutralizar los incidentes de seguridad.

4) Ética: los "participantes" deben respetar los legítimos intereses de los otros "participantes", es decir que cada organización / individuo debe reconocer que su acción o inacción puede perjudicar a un tercero. Los "participantes" deben procurar el desarrollo y adopción de conductas que promuevan el respeto de los legítimos intereses de las otras partes.

5) Democracia: la seguridad de los sistemas de información y redes debe ser compatible con los valores escenciales de una sociedad democrática, es decir que deben respetarse principios tales como la libertad para expresas ideas, intercambiar información, protección de información privada y transparencia.

6) Evaluación de riesgos: los "participantes" deben realizar evaluaciones de riesgos. Estas evaluaciones permiten identificar amenazas y vulnerabilidades y deben ser lo suficientemente amplias como para tener en cuenta factores internos y externos, como la tecnología, los recursos humanos y servicios prestados por terceros. La evaluación de riesgos permitirá determinar el nivel de riesgo aceptable para cada organización, como así también ayudar en la selección de medidas de control para mitigar los riesgos a los que están expuestos los sistemas de información.

7) Incorporar la "seguridad" en el diseño e implementación de sistemas: los "participantes" deben incorporar la seguridad como un elemento esencial en el momento del diseño de los sistemas de información y las redes. Las medidas de seguridad deben incluir aspectos técnicos y no técnicos y deben estar en relación con el valor de los activos informáticos que han de protegerse.

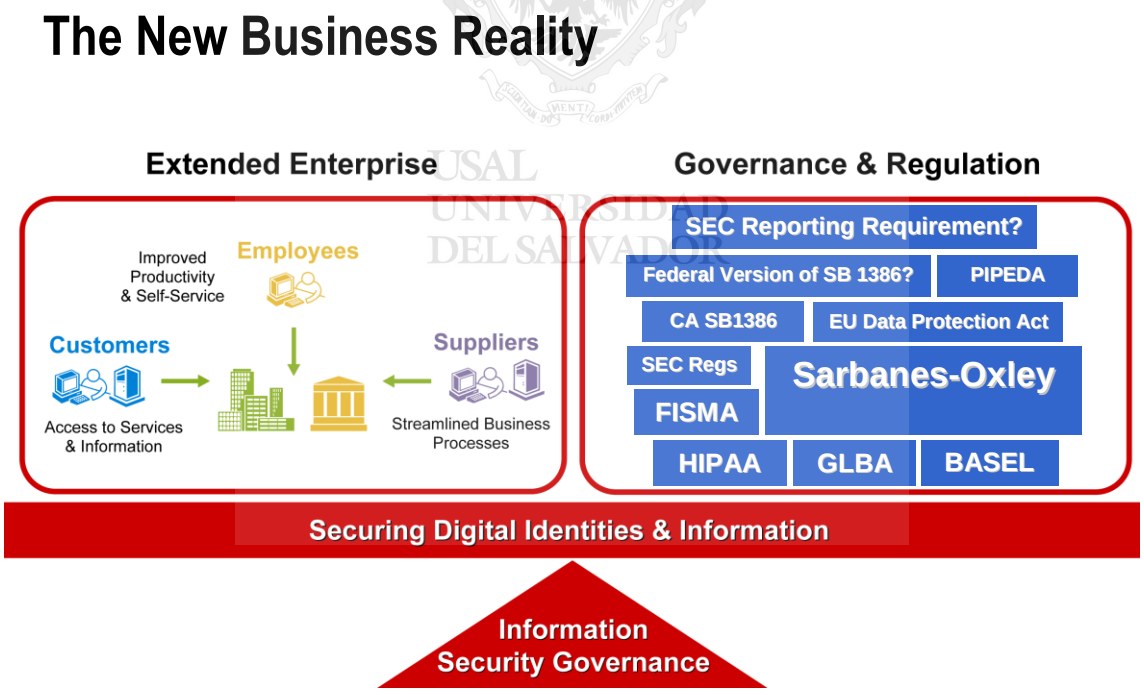
8) Gerenciamiento de la seguridad: la administración y gerenciamiento de la seguridad debe estar basada en una evaluación de riesgos que considere todas las actividades y actores de la organización. Deben preverse controles preventivos frente a nuevas amenazas, detección y respuesta a incidentes de seguridad, medidas para la recuperación de los sistemas, periódicas revisiones independientes y auditorías. Las políticas, normas, procedimientos y estándares a ser aplicados, deben ser coordinados e implantados en forma integral, para crear un ambiente de control "coherente" y "robusto".

9) Reevaluación: los "participantes" deben revisar y reevaluar periódicamente la seguridad de los sistemas de información y las redes, y efectuar las modificaciones que correspondan a las políticas, normas, procedimientos y estándares; esto se debe a que continuamente aparecen nuevas amenazas y vulnerabilidades.

IV. La seguridad en la "Organización Extendida" y regulaciones gubernamentales

Para mantener y aumentar sus ventajas competitivas, cada vez más las organizaciones proveen a sus proveedores, clientes, usuarios externos a la organización y empleados mayor acceso a la información, a través de la implantación de nuevos sistemas de información y el acceso a sus web-sites.

Pero existe una preocupación: tanto los individuos como las organizaciones desean que las transacciones se realicen en un ambiente "seguro": los individuos desde el punto de vista que se preserve la confidencialidad de las transacciones que realizan por internet, y no ser víctimas de fraudes, y las organizaciones que desean brindar a sus clientes un servicio que permita la reducción de costos y el crecimiento de sus ventas y utilidades, al mismo tiempo temen por las amenazas que existen en el mundo de la tecnología.
Un entorno de seguridad adecuado debe tener en cuenta tanto la red de la compañía como la de otras asociadas a ella. Esto nos lleva al concepto de la organización extendida.



Siempre que se unen dos sistemas, se adquieren una serie de controles predefinidos. Estos controles heredados podrían no ser adecuados para el entorno operativo actual. De acuerdo con Milholland, de EDS, "*nos dimos cuenta en Boeing, cuando adquiríamos nuevas*