POLÍTICAS DE SEGURIDAD INFORMÁTICA

Ciro Antonio Dussan Clavijo

SISTEMAS

Resumen

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. La creación de políticas de seguridad es una labor fundamental que involucra las personas, los procesos y los recursos de la compañía. Este articulo presenta los puntos clave a tener en cuenta para diseñar una política de seguridad basándose en la norma ISO 17799.

Abstract

The globalizatión of the economy has demanded that the companies implement technological platforms that support the new form to make businesses. The use of Internet for this aim, entails to that projects of computer science security are developed that guarantee integrity, availability and accessibility of the information. The creation of security policies is a fundamental work that it involves the people, the processes and the resources of the company. This I articulate presents/displays the key points to consider to design a security policy being based on norm ISO 17799.

Palabras clave

Seguridad Informática, Políticas de Seguridad, Norma ISO 17799, transacciones electrónicas

Fecha de recepción: 20 - 04 - 2006 Fecha de aceptación: 02- 06 - 2006

Introducción

El mundo digital se ha integrado en toda la sociedad de una forma vertiginosa, en nuestro diario vivir son más las personas que se apoyan en Internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre ip, descargar música o el libro favorito, hacer publicidad, etc. Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas. Las "transacciones" electrónicas nos permiten ahorrar tiempo y recursos, pagar los servicios públicos, transferir de una cuenta bancaria a otra, participar en una subasta para comprar un vehículo, pagar un boleto de avión etc. En todos estos ejemplos hay algo en común, el dinero, y cuando hablamos de tan escaso pero tan apreciado bien las empresas deben garantizar la implementación de políticas de seguridad informática[1].

Los que trabajan en el mundo empresarial, deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información en el complejo mundo de los negocios. Cada vez encontramos más gerentes interesados en entender las reglas del negocio, entre ellas las referentes a las políticas de seguridad informática. El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación y afectar los ciclos del negocio.

Las empresas han implementado un modelo de acceso a la información más abierto y a la vez más distribuido, lo cual redunda en beneficios tales como:

- **Mayor productividad por empleado: Los empleados agilizan su trabajo, toman mejores decisiones y responden con rapidez a las cambiantes demandas del mercado en el que se mueven, al tener un acceso seguro a la información que necesitan desde cualquier lugar y en cualquier momento.**

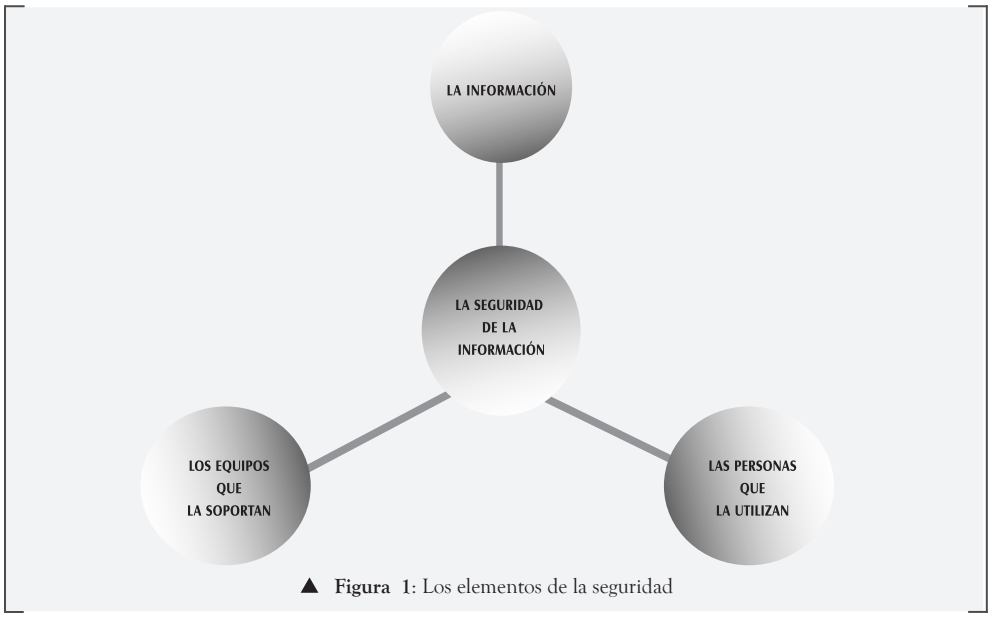
- **Reducción de costos: Reduce los costos e incrementa la efectividad a través de las herramientas de colaboración y de la conectividad de red**
- **Integración de los procesos de negocios: Incrementa las ventas al permitir una relación más estrecha con los clientes y los socios de negocios, a través de comunicaciones seguras y procesos colaborativos.**

Para aprovechar estos beneficios, las empresas necesitan tener una infraestructura de informática segura, que minimice los riesgos asociados con la seguridad y los costos de administración y operaciones.

El secreto del éxito, tanto individual como de un negocio, de una empresa estatal, etc. , depende cada vez más de la habilidad para poder comunicarse con cualquiera, en tiempo real y con los niveles de seguridad necesarios. La aparición de la conectividad generalizada a través de Internet, así como de dispositivos cada vez más potentes y omnipresentes, ha causado una revolución en el terreno de las comunicaciones y la informática.

Con los beneficios que nos brindan las nuevas posibilidades de conectividad, emergen también una serie de nuevos riesgos. Muchas empresas son amenazadas en sus activos, y más aún cuando el activo más importante es la información. El deterioro de ésta puede representa millones de dólares en pérdidas en el mundo de los negocios. Las vulnerabilidades[2] en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso, hackers y crakers que penetran los sistemas de seguridad. Los elementos que la seguridad (ver Fig. 1) de la información busca proteger son:

- **La información**
- **Los equipos que la soportan**
- **Las personas que la utilizan**



▲ **Figura 1**: Los elementos de la seguridad

El primero de los tres principios de la seguridad de la información que aplicamos es la integridad, la cual nos permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra.

El principio de la confidencialidad de la información tiene como propósito el asegurar que sólo la persona correcta acceda a la información que queremos distribuir.

Una vez que nos aseguramos que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que debemos garantizar es que llegue en el momento oportuno, y precisamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad. Para que una información se pueda utilizar, deberá estar disponible.

Es importante, además, que todos los empleados de la compañía tomen conciencia sobre el manejo de la información de forma segura, ya que de nada sirve cualquier sistema de seguridad, por complejo y completo que este sea, si los empleados, por ejemplo, facilitan su usuario y contraseña a personas ajenas a la empresa y con esto dejan abierta la puerta a posibles ataques o filtraciones de información crítica al exterior de la compañía.

Es importante tener claro cuáles son los tipos de amenazas más comunes a las cuales están expuestas las empresas hoy en día. La Tabla 1 hace un resumen en este sentido.

El análisis y evaluación de riesgos permite a las compañías tener una visión más clara sobre sus vulnerabilidades y de los esfuerzos que deben hacer para mejorar.

En el mundo de las certificaciones de calidad y en el cumplimiento de estándares internacionales que permitan acceder a nuevos mercados o se brinden nuevos valores agregados que marquen una diferenciación o ventaja competitiva, las políticas definen la forma de hacer las cosas, el mejoramiento de los procesos. Reconocer las limitaciones y restricciones de la tecnología es un buen paso para entender la importancia de las políticas. En este sentido podemos definir la política como un instrumento gerencial que traza una dirección predeterminada describiendo la manera de manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los colaboradores de la empresa la orientación que necesitan para tomar decisiones presentes y futuras.

Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.

Tipos de Amenazas	Ejemplos
Suplantación	• Falsificar mensajes de correo electrónico • Reproducir paquetes de autenticación
Alteración	• Alterar datos durante la transmisión • Cambiar datos en archivos
Repudio	• Eliminar un archivo esencial y denegar este hecho • Adquirir un producto y negar posteriormente que se ha adquirido
Divulgación de información	• Exponer la información en mensajes de error • Exponer el código de los sitios Web
Denegación de servicio	• Inundar una red con paquetes de sincronización • Inundar una red con paquetes ICMP falsificados
Elevación de privilegios	• Explotar la saturación de un búfer para obtener privilegios en el sistema • Obtener privilegios de administrador de forma ilegítima

▲ **Tabla 1**: Amenazas al sistema de informática de la empresas

Aunque las políticas de seguridad informática varían de una organización a otra, un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes van dirigidas las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales especificas sobre el tratamiento de las políticas. Estas son obligatorias y pueden considerarse a una ley propia dentro de la organización.

Una política de seguridad son un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico.

Áreas de normalización de las políticas de seguridad

- **Tecnológica: Se refiere a los esfuerzos que se deben realizar para el buen funcionamiento de la plataforma de hardware, software y telecomunicaciones. Servidores, estaciones de trabajo, sistemas operativos, bases de datos, acceso a Internet etc. Algunas personas relacionan directamente los problemas de seguridad con el área tecnológica pero es importante hacer relevancia que se parte de la ética profesional y la buena conducta de los usuarios.**

- **Humana: En definitiva todos se convierten en usuarios los proveedores, clientes, empleados etc. y para ellos se enfocan los recursos y esfuerzos. Este aspecto va muy ligado a la cultura organizacional y cómo se integran en sus actividades diarias aspectos como la ética, la responsabilidad, capacitación y mejoramiento continuo.**

Elaboración de la política

Para elaborar una política de seguridad de la información es importante tomar en cuenta las exigencias básicas y las etapas necesarias para su producción.

1. **Exigencias de la Política: La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado en seguridad de los profesionales involucrados con su aplicación y comprometimiento. Es importante considerar que para la elaboración de una política de seguridad institucional se debe:**

   a. **Integrar el comité de seguridad responsable de definir la política (equipo multidisciplinario)**
   b. **Elaborar el documento final (preocupaciones de la administración, atribución de las responsabilidades de las personas involucradas, legislación y cláusulas contractuales, prevención contra amenazas, educación y formación en seguridad de la información.)**
   c. **Hacer oficial la política una vez que se tenga definida (aprobación por parte de la administración, mecanismos de comunicación efectiva a socios, empleados, proveedores y clientes de la empresa).**

2. **Etapas de producción de la política: Elaborar una política es un proceso que exige tiempo e información. Es necesario saber cómo se estructura la organización y cómo son dirigidos en la actualidad sus procesos.**

Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.

A partir de este reconocimiento, se evalúa el nivel de seguridad existente para poder después detectar los puntos a analizar para que esté en conformidad con los estándares de seguridad.

El trabajo de producción se compone por distintas etapas, entre otras:

a. Objetivos y ámbito (presentación del tema de la norma en relación con sus propósitos y contenidos)

b. Entrevista (identificar junto con los usuarios las preocupaciones que ellos tienen con los activos, los procesos de negocio)

c. Investigación y análisis de documentos (se identifican y analizan los documentos existentes en la organización)

d. Reunión de política (se discuten los temas y se redactan las políticas)

e. Glosario de la política (aclaración de dudas conceptuales alrededor de la política)

f. Responsabilidades y penalidades (identificar a los responsables por la gestión de la seguridad y cumplimiento de tareas)

Documentos de una política de seguridad

Un modelo propuesto según la norma ISO 17799 la cual recomienda la aplicación de estándares encaminados a la seguridad informática plantea tres grandes secciones:

• Las directrices son un conjunto de reglas generales de nivel estratégico donde se expresan los valores de la seguridad de la organización. Es propuesta por el líder empresarial de la

organización y tiene como su base la misión y visión para abarcar toda la filosofía de la seguridad de la información[3].

• Las normas son un conjunto de reglas generales y específicas de la seguridad de la información que deben ser usadas por todos los segmentos involucrados en todos los procesos de negocio de la institución, y que deben ser elaboradas por activo, área, tecnología, proceso de negocio, público a que se destina, etc. Las normas de seguridad para usuarios son dirigidas para el uso de ambientes informatizados, basadas en aspectos genéricos como el cuidado con las claves de acceso, manejo de equipos o estaciones de trabajo, inclusión y exclusión de usuarios, administración de sistemas operativos, etc.

• Los procedimientos e instrucciones de trabajo son un conjunto de orientaciones para realizar las actividades operativas, que representa las relaciones interpersonales e ínter departamentales y sus respectivas etapas de trabajo para su implementación y mantenimiento de la seguridad de la información.

Acompañamiento de la política

Una política de seguridad para que sea efectiva , necesita contar con elementos indispensables que apoyen este proceso: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas[4].

Las organizaciones pueden definir unos ámbitos básicos o esenciales en donde empezar a implementar políticas de seguridad; entre los más comunes encontramos:

• Seguridad física: acceso físico, estructura del edificio, centro de datos[5].

• Seguridad de la red corporativa: configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.

• Seguridad de usuarios: composición de claves, seguridad en estaciones de trabajo, formación y creación de conciencia.

• Seguridad de datos: criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.

• Auditoria de seguridad: análisis de riesgo, revisiones periódicas, visitas técnicas, monitoreo y auditoria.

• Aspectos legales: prácticas personales, contratos y acuerdos comerciales, leyes y reglamentación gubernamental.

Conclusión

Las políticas deben ser claras, concisas, contextualizadas a una realidad, enfocadas a las forma de hacer negocios de la empresa. Según las cifras presentadas en estudios relacionados con seguridad informática en las empresas más de un 60% de las compañías no cuenta con programas establecidos de seguridad informática. En un momento en donde Colombia firma un tratado de libre comercio (TLC) con los Estados Unidos, la industria nacional debe hacer un gran esfuerzo en fortalecer su plataforma tecnológica e invertir en programas de seguridad. Es responsabilidad de los gerentes de las empresas liderar estos proyectos que permitan entrar a una economía soportada en un mundo digital.

CITAS

1. Políticas de Seguridad Informática, Charles Cresson Wood, CISA – CISSP, capítulo 1 pág. 8, Las políticas de seguridad informática representan un tipo especial de reglas de negocios documentadas. Hace 25 años no existía tal necesidad de políticas, pero el cambio ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscapersonas y los computadores. Los que trabajan en el ambiente empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información generada en el complejo mundo de los negocios.

2. Estándares de Seguridad, ISACA, COBIT Normatividad General, Pag. 5. Hoy en día, las vulnerabilidades son explotadas a una velocidad mucho mayor por aquellas personas cuya intención es dañar los activos de las empresas. Dicha velocidad implica que debemos estar más alertas que nunca, no sólo actuando en consecuencia, sino también previniendo posibles riesgos y problemas de seguridad.

3. ISO27001:2005 "Information Security Management- Specifications for an ISM" , Chapter 3, page 58. El establecimiento de una política de seguridad, integra un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandardizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico. A partir de sus principios, es posible hacer de la seguridad de la información un esfuerzo común, en tanto que todos puedan contar con un arsenal informativo documentado y normalizado, dedicado a la estandardización del método de operación de cada uno de los individuos involucrados en la gestión de la seguridad de la información.

4. Véase, Sistemas de Información Gerencial, Segunda Edición, pag. 45, El entrenamiento de personas debe ser constante, de tal manera que se actualice toda la empresa con relación a los conceptos y normas de seguridad, además de sedimentar la conciencia de seguridad, para tornarla como un esfuerzo común entre todos los involucrados.

5. Vease Norma ANSI TIA/EIA (Instituto Nacional Americano de Normalización), ISO 17799 version 2000, Capítulo 1, Dominós de Seguridad. Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizacionesinternaci onales de estándares. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la OrganizaciónInternacional para laNormalización.

BIBLIOGRAFÍA

BS7799:1 "Information Security Management- Part 1: Code of practice for informationsecurity management"

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION Estándares de Seguridad, ISACA, IEC/ISO.http://www.isaca..org

http://www.crt.org

ISO27001:2005 " Information Security Management- Specifications for an ISM"

ISO/IEC 17799:2005 "Information Technology- Code of Practice for Information Security Management"

ISO/IEC TR 13335 "Information Technology - Guidelines for the management of IT security" (GMITS), VERSION 2002. Part 1: Concepts and models for IT security. Part 2: Managing and planning IT security. Part 3: Techniques for the management of IT security (en revisión!) Part 4: Selection of safeguards Part 5: Management guidance on network security

MICROSOFT TEHCNET ACADEMY SECURITY http://www.microsoft.com/technet/seguridad

WOOD,Charles Cresson. Políticas de Seguridad Informática, CISA – CISSP, 2004. Segunda Edición. http://www.netiq.com
IEEE, Norma ISO 17799 versión 2000.

Ciro Antonio Dussán Clavijo
Administrador informático. Especialista en sistemas gerenciales de ingeniería, especialista en auditoria de sistemas academia de seguridad de Microsoft. Director ejecutivo de Funib. Gerente de proyectos de CD Com Ltda., ingeniero de soporte Ministerio de Educación Nacional. Ingeniero de Planeación Nacional. Docente universitario (Facultad de Ingeniería de Sistemas Unilibre Cali). Consultor de TI y seguridad informática Grupo de investigaciones Sinergia COL 001785