SEGURIDAD DE LA INFORMACIÓN
Autor: Ing. Héctor Méndez Olivares

¿Que es la seguridad de la información?

Podemos afirmar que la “Seguridad” es una NECESIDAD BÁSICA ya que se encuentra implícita en la prevención de la vida y las posesiones, haciéndola tan antigua como estas.

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura Sumeria (3000 AC) o el Hammurabi (2000 AC). La Biblia, Homero, Ciceron, Tzun Tzu y Cesar representan obras en donde aparecen ciertos rasgos de la seguridad en un entorno de guerra y el gobierno.

La seguridad desde la aparición de la vida misma, es un tema intrínseco a la existencia misma, en forma tal que cualquier organismo, para evitar amenazas, reacciona con métodos defensivo a su alcance: LUCHANDO o HUYENDO, para evitar cualquier daño. Posteriormente la lucha por la vida evolucionó en conceptos como ALERTAR, EVITAR, DETECTAR, ALARMAR y REACCIONAR.

Conforme las sociedades se hacen más complejas, la seguridad ha evolucionado con ellas, conformando FAMILIAS o CLANES que de una manera organizada podían prevenir y contrarrestar cualquier ataque de otras familias o clanes, así como transmitir las experiencias de generación en generación (ESTO ES INFORMACIÓN VALIOSA QUE DEBE PRESERVARSE).

El siguiente paso en la evolución de la seguridad fue la especialización, dando como resultado la SEGURIDAD PERIMETRAL (EJERCITO), concebida para proteger contra amenazas externas. Así cómo la SEGURIDAD INTERNA (EJERCITO O POLICÍA), encargados de proteger el ORDEN INTERNO contra amenazas (revueltas, espías o terroristas) a la estabilidad de los clanes, feudos o

reinos. Intensificando el desarrollo de “tácticas” y “estrategias”, tanto para conocer los movimientos de los contrarios, como para defenderse de estos, creando incluso, ciudades amuralladas que evitaran el “ACCESO” a extraños o enemigos.

Hoy día, la seguridad puede verse desde dos perspectivas muy definidas, la LEGISLATIVA y la TECNOLÓGICA. De la primera se hacen cargo los políticos, quienes tienen por función decidir sobre su importancia, los delitos en que se puede incurrir con su respectivo castigo, teniendo grandes logros en materia de prevención de crímenes, terrorismo y riesgo, más que en el concepto mismo de seguridad.

En cuanto a la TECNOLÓGICA, la seguridad está en manos de los “tecnólogos” y en ocasiones en manos de la dirección de las organizaciones, debiendo tomar en cuenta el grado de concientización de cada uno de nosotros respecto a la importancia de la información.

Es en este proceso donde se aprecia que no se ha agregado nada nuevo al concepto que los ya conocidos desde la antigüedad, convirtiendo a los actuales en sólo perfeccionamientos de aquellos que iniciaron con murallas, puertas, fosos, cerradoras, trampas, vigilancias, etc., las cuáles por ende han desarrollado nuevas técnicas para franquearlas.

LA SEGURIDAD ES HOY DÍA UNA PROFESIÓN COMPLEJA CON FUNCIONES ESPECIALIZADAS.

Los problemas nunca se resuelven, al igual que la “energía” no desaparecen, **“se transforman”**, por lo que la solución a los problemas será necesariamente su TRANSFORMACIÓN en problemas diferentes, tal vez mas pequeños o aceptables. Un claro ejemplo de esto es la necesidad de comunicarnos a través de una red compleja, donde la implementación de un sistema informático puede solucionar el problema de velocidad de procesamiento, pero puede crear

problemas como el del personal remplazado por la tecnología, que descontentos pueden generar un problema de SEGURIDAD INTERNA.

Si analizamos el problema a fondo, podemos distinguir tres figuras principales:

Un PROTECTOR que es normalmente el poseedor del “valor” o quién lo tiene a su cargo. El COMPETIDOR-AGRESOR que se podría identificar como aquel que desea poseer o dañar el “bien”. Y el VALOR, en sí mismo.

Aclarando que el PROTECTOR no necesariamente es el poseedor del “valor” , así como el AGRESOR no sólo requiere poseer el bien o valor, sino que probablemente busque desvirtuar o dañar a estos. De igual manera podemos identificar el “VALOR” como un tangible o intangible, como el honor, la intimidad, el conocimiento, la información, etc.

La seguridad es un problema de antagonismo y competencia. Si no existe un competidor-amenaza el problema no es de seguridad.

Pero, ¿qué valor o bien es el que debemos proteger?.....

El ámbito de la seguridad no puede circunscribirse sólo a los accesos, a los equipos o a la recepción de una organización, por lo que debe iniciar por SU RAZON DE SER, su negocio o función, como tal.

Podríamos igualar en importancia un archivo interceptado por un HACKER a un FAX o una base de datos de clientes y proveedores, archivos contables, etc., retenidos o destruidos por un empleado molesto o peor aún, la EXTRACCIÓN de nuestra base de datos para VENDERLAS a alguna empresa o gobierno extranjero. A final de cuentas el efecto es el mismo. PERDIDA DE INFORMACIÓN, sólo que el primero requirió del uso de la tecnología para poder obtenerlo, mientras que en los siguientes casos, el esfuerzo fue mínimo y el costo para la institución u organización, probablemente muy alto.

Aquí comienza la distinción entre “Seguridad de la Información” y “Seguridad Informática”, donde la segunda es parte indispensable de la primera y ambas se complementan a través de POLÍTICAS Y PROCEDIMIENTOS.

Pero, ¿de dónde surgen estas políticas y procedimientos?, y ¿quién debe hacerse cargo de implementarlas, administrarlas y actualizarlas?

Existen instituciones internacionales que se dedican a elaborar estándares que sirven de base para la regulación del comportamiento seguro tanto en las instituciones como en las organizaciones y empresas. De hecho para poder ser NORMA, tiene que ser dictada por una AUTORIDAD, que sea CONFIABLE y RECONOCIDA. Tal es el caso de ISO, BS, COBIT, ITIL, etc.

En México existe un sin numero de instituciones gubernamentales, las cuales han tratado de cubrir sus requerimientos de seguridad, siguiendo múltiples y variados métodos, usando diferentes metodologías y sistemas, de acuerdo a lo que el mercado les ofrece y no acorde a la operación y fin de cada una de estas instituciones.

Esto es debido a que el término Seguridad, se entiende como el vigilante que “guarda” los accesos a las instalaciones (Seguridad Física) o como los sistemas, dispositivos o aplicaciones informáticas, usados como “defensa” contra virus o intrusos, protegiendo nuestros “bienes informáticos” (Seguridad Lógica).

Sin embargo existen aún huecos muy importantes sobre la “INFORMACIÓN” como tal, la cuál es el BIEN MAS PRECIADO. Cómo ejemplo podemos mencionar al “Padrón Electoral” que fue vendido a empresas de mercadotecnia extranjeras (según lo comentado en noticieros) o el hecho de que muchas empresas nos envíen correos electrónicos o nos llamen por teléfono para ofrecernos una nueva tarjeta de crédito sin que hubiésemos hecho solicitud alguna, así como la

posibilidad de que un empleado molesto con acceso a la información, la dañe, altere o desaparezca.

En ocasiones la falta de capacitación en el manejo de los sistemas de cómputo, puede hacer que un usuario inexperto, “permita” la entrada a “extraños” a las redes institucionales, a través de programas de P2P , Chat en línea o troyanos cargados por visitar sitios “atractivos” en la Web.

El problema viene cuando sin el conocimiento y sin la normatividad se comienza a “prohibir”, por ejemplo, la navegación en internet. Probablemente algunos empleados argumenten que lo necesitan para trabajar, cuando realmente los requerimientos de uso de este tipo de tecnología les tome para cuestiones de trabajo sólo un 45% por ciento del tiempo total de acceso. (Datos promedio de mediciones realizadas en servicios de Valoración en Instituciones y organizaciones en los últimos 2 años, en México).

Otro detalle muy importante es el hecho de que se confunda a menudo el término de Seguridad de la Información, con el de Seguridad Informática, por lo que la mayoría de las veces se le “encarga” a la Dirección, Gerencia o Departamento de Informática el que se haga cargo de la SEGURIDAD DE LA INFORMACIÓN.

La pregunta sería si esta área altamente especializada, tiene además la capacidad de crear NORMAS y hacer que el resto de los empleados, proveedores y clientes las CUMPLAN.

La respuesta es NO y además en la mayoría de las veces se les tacha (cuando aplican restricciones) de “VILLANOS”, además que no cubren áreas como información impresa, “Seguridad Física”, SANCIONES, ó cambios en estructura o procesos.

En México existen muy buenos esfuerzos por establecer NORMAS y PROCEDIMIENTOS para salvaguardar la INFORMACIÓN del público en general,

sin embargo aún son muy limitadas en su contenido, alcance e interpretación, por lo que es necesario establecer e implementar una normativa, acorde con los estándares internacionales, que sea la base para el establecimiento e implementación de normativas más particulares que estén de acuerdo a los objetivos, y razón de ser de cada institución.

Con ello organizaciones, empresas y público en general podrían tener una línea de guia para establecer los puntos básicos de SEGURIDAD DE LA INFORMACIÓN que les permita conservarla, administrarla y hasta incluso intercambiarla de una manera segura.

Cuando hablamos de Normas de SEGURIDAD, también debemos asociar el término de PENALIZACIÓN, ya que toda VIOLACIÓN de la normatividad, deberá tener una CONSECUENCIA que permita que un potencial infractor lo piense más de dos veces, antes de cometer un error.

Para poder lograr esto, es importante tomar en cuenta algunos aspectos básicos que deben considerarse en un esquema de seguridad basado en normas.

Política de seguridad

Las políticas de Seguridad permiten dirigir y determinar acciones de apoyo, compromiso y dirección, a fin de lograr metas de seguridad de la información, debiendo incluir:

Documentación de la Política de Seguridad de la Información: Es un juego de implementaciones independientes, con información conceptual que determina las metas de seguridad de la organización. Este documento, junto con una jerarquía de normas, pautas, y procedimientos, ayuda en la implementación, fortaleciendo los estatutos de la política.

Propiedad y Revisión: Debe existir un compromiso de continuidad de la documentación de la política de Seguridad de la Información, estableciendo responsables (Comité de Seguridad) y agendas de revisión.

.

Seguridad orgánica

Las directivas de la Seguridad Orgánica, requieren de la creación de una guía que permita la creación, sustento y administración de la infraestructura de seguridad incluyendo:

Foro de Seguridad de la Información: proporciona un comité **multi-disciplinario** enfocado a discutir y diseminar la información sobre seguridad que se emite, a lo largo de la organización.

Funcionario de Seguridad del Sistema de Información: actúa como un punto central de contacto para los problemas de seguridad de información, dirección, y decisiones.

Responsabilidades de Seguridad de información: se asignan responsabilidades de seguridad de información individuales inequívocamente y se detallan dentro de las descripciones del trabajo.

Procesos de autorización: asegura que las consideraciones de seguridad se evalúen y las aprobaciones se obtengan para un nuevo y modificado sistema de procesamiento de la información.

Especialista en Información: mantiene relaciones con especialistas independientes, accesando a la experiencia no disponible en la organización.

Cooperación orgánica: mantiene la relación entre compañeros, información compartida y las autoridades que reglamentan en forma local.

Revisión independiente: mecanismos para permitir revisiones independientes, sobre la efectividad de la seguridad.

Acceso a terceros: mecanismos para regular la interacción con terceros dentro de la organización basados en los requisitos del negocio.

Outsourcing: los contratos de outsourcing de la organización deben tener requisitos de seguridad claros.

Clasificación de recursos y Controles

La Clasificación de recursos y controles determina la capacidad de la infraestructura de seguridad para proteger los recursos de la organización, incluyendo:

Responsabilidad e inventario- Estableciendo los mecanismos para mantener un inventario exacto de recursos, estableciendo la propiedad y responsiva de todos los recursos.

Clasificación- Establece los mecanismos para clasificar recursos de acuerdo al impacto en el negocio u operación de la organización.

Identificación- Identiificando los recursos acorde a las normas que los cubren.

Manipulación – Manejo de estándares; Incluyendo su introducción, Transferencia, Remoción, y disposiciones de todos los recursos; Basados en la clasificación de recursos.

Seguridad del personal

Las directivas de control de la Seguridad del Personal de una organización, debe poseer la habilidad de reducir los riesgos inherentes dentro de las interacciones humanas, incluyendo:

Protección del Personal - Políticas dentro de la estructura legal y cultural que determinan la calificación y conveniencia de aquel personal con acceso a los

recursos de la organización. Esta estructura puede basarse en las descripciones del trabajo y/o clasificación de los recursos.

Responsabilidades de seguridad - El personal debe ser claramente informado sobre sus responsabilidades de seguridad de la información, incluyendo los códigos de conducta y acuerdos de confidencialidad.

Los términos y condiciones de empleo - El personal debe ser informado claramente sobre sus responsabilidades de seguridad de información como una condición de empleo.

Entrenamiento - El conocimiento de seguridad de la información obligatorio dirigido a todos los empleados, incluyendo nuevas contrataciones y empleados establecidos.

Recursos - Un proceso formal para tratar con las violaciones a las políticas de seguridad de la información.

Seguridad física y Medioambiental

Directivas de control de riesgos sobre la seguridad Física y Medioambiental inherentes a las premisas de la organización, incluyendo:

Localidad - Deben analizarse premisas orgánicas respecto a los riesgos medioambientales.

Perímetro de seguridad físico - Las premisas del perímetro de seguridad física, deben definirse claramente. Las premisas dadas pueden tener zonas múltiples basadas en nivel de la clasificación u otros requisitos de la organización.

Control de acceso - las brechas en el perímetro de seguridad físico deben tener los controles de acceso/salida apropiados, correspondientes con su nivel de clasificación.

Equipo - los equipos deben mencionarse dentro de las premisas para asegurar la integridad y la disponibilidad, tanto física como medioambiental.

Traslado de recursos - los mecanismos para rastrear la entrada y salida de recursos a través del perímetro de seguridad.

General - las políticas y normas, como la utilización equipo, el almacenamiento seguro, y el principio de "escritorio limpio", deben existir para gobernar la seguridad operacional dentro del área de trabajo.

Administración de Comunicaciones y Operaciones

Las directivas de control de la administración de Comunicaciones y Operaciones de una organización, es la habilidad para asegurar el correcto y seguro funcionamiento de los recursos, incluyendo:

Procedimientos operacionales - el juego comprensivo de procedimientos, en apoyo de normas de la organización y las políticas.

Control de cambios - el proceso para manejar y controlar los cambios en la configuración, incluyendo los combios en el Sistema de Administración de la Seguridad de la Información.

Administración de incidentes - es el mecanismo para asegurar la respuesta oportuna y eficaz ante cualquier incidente de seguridad.

Segregación de responsabilidades - la segregación y rotación de responsabilidades, minimizan la posibilidad de colusión y la exposición sin control.

Capacidad de Planeación - es el mecanismo para supervisar y proyectar la capacidad de la organización, para asegurar la disponibilidad de los recursos, ininterrumpidamente.

Aceptación del sistema - es la metodología para evaluar los cambios en el sistema para asegurar la confidencialidad, integridad y disponibilidad continuas.

Código malicioso - son los controles para disminuir el riesgo de introducción de código malicioso en los sistemas.

Lineamientos Internos - son las políticas, normas, pautas y procedimientos para dirigir las actividades y quehaceres rutinarios como respaldos programados y logging.

Administración de la red - son los controles para gobernar la operación segura de la infraestructura de redes.

Manejo de los Medios - son los controles que determinan el manejo seguro y la disposición de medios de almacenamiento de la información y la documentación.

Intercambio de información - son los controles para gobernar el intercambio de información, incluyendo los contratos con el usuario final, contratos del usuario y mecanismos de transporte de la información.

Control de acceso

Las directivas de Control de acceso constituyen la habilidad de una organización para controlar el acceso a los recursos, basándose en los requisitos de seguridad del negocio, y que incluyen:

Requisitos del Negocio - Son las políticas que controlan el acceso a los recursos de la organización, basándose en requisitos del negocio y lo que se "necesita saber".

Administración de usuarios - Son los mecanismos para:

- Registrar y deshabilitar usuarios
- Control y revisión de accesos y privilegios
- Administración de Passwords

Responsabilidades del usuario - informando a los usuarios de sus responsabilidades en el control de acceso, incluyendo el uso de contraseñas y acciones sobre el equipo desatendido.

Control de acceso a la red - Es la política sobre el uso de los servicios de la red, incluyendo los mecanismos (cuando sea apropiado) para*:*

- Autenticar Nodos
- Autenticar a los usuarios externos
- Definición de Rutas
- Control de dispositivos de Seguridad de la Red
- Mantenimiento de segmentación de la Red
- Control de las conexiones de Red
- Mantenimiento de los servicios de seguridad de la Red

Control de acceso al Host –Establecen los mecanismos (cuándo es apropiado) para:

- Identificar automáticamente las terminales
- Asegurar el acceso (log-on)
- Autenticar a los usuarios
- Administrar Passwords
- Asegurar las utilidades del Sistema
- Proporcionar la capacidad de coacción del usuario, como "bopton de pánico"
- Habilitar terminales, usuarios o conexiones interrumpidas

Control de acceso a la aplicación - Limita el acceso a aplicaciones basadas en tipo de usuario o niveles de autorización de la aplicación.

Monitoreo de Acceso - son los mecanismos para supervisar el acceso al sistema, así como su uso, para descubrir actividades no autorizadas.

Informática móvil - establece las políticas y normas para protejer los recursos informáticos portátiles, como laptops y proyectores, garantizando el acceso seguro y estableciendo las responsabilidades del usuario.

Desarrollo de Sistemas y Mantenimiento

Las directivas de control en el desarrollo de sistemas y el mantenimiento representan la habilidad de una organización para asegurar el uso de controles de seguridad apropiados, incluyendo:

Requerimientos de Sistemas de Seguridad - Incorporando consideraciones de seguridad de la información, dentro de las especificaciones de cualquier sistema a desarrollarse o adquirirse.

Requisitos de seguridad de aplicación–las corporaciones información seguridad consideraciones en la especificación de cualquier desarrollo de la aplicación o procuración.

Criptografía – Políticas, Normas y procedimientos que determinan el uso y mantenimiento de controles criptográficos.

Sistemas de Integrdad – mecanismos para controlar el acceso, verificar la integridad de los datos y programas operativos, incluyendo procesos de seguimiento, evaluación y la incorporación de facilidades de actualización y "parches".

Seguridad en Desarrollos – Integra Control de Cambios y revisiones técnicas en los preocesos de Desarrollo.

Administración de la Continuidad del Negocio (BCM)

Las directivas del control de Administración de la Continuidad del Negocio (BCM), de una organización, es la habilidad de contrarestar las interrupciones en la operación normal, e incluye:

Planeación de Continuidad del Negocio (BCP) – es la estrategia de continuidad del negocio, con base en un Análisis e Impacto o RIESGO.

Pruebas de Continuidad del Negocio (BCT) – Son las pruebas y la documentación de la estratégia de continuidad del negocio. En esta parte los procedimientos son probados y corregidos ciclicamente.

Mantenimiento de la Continuidad del Negocio (BCM) - Identifica cuán apropiada es la estrategia del Plan de Continuidad del Negocio así cómo su revaloración y mantenimiento.

Cumplimiento

El control del Cumplimiento proporciona a la organizacion, la habilidad de continuidad para cumplir con la regulaciión, estatutos, contratos y requerimientos de seguridad, incluyendo:

Requerimientos Legales – creación de consciencia sobre:

- Legislación de relevancia
- Derechos de propiedad intelectual
- Registros de Salvaguarda de la Organización
- Privacidad de la Información
- Prevención del mal-uso de la información
- Regulación sobre criptografía
- Recoleccion de Evidencia

Requerimientos Técnicos – mecanismos usados para verificar la ejecución e las políticas de seguridad y su implementación.

Auditoría – Auditoriá de los controles a efecto de maximizar su efectividad, minimizando las interrupciones y protegiendo las herramientas de auditoría.

Si consideramos lo anterior como sólo “aspectos básicos”, podemos ver que la seguridad es algo más que instalar dispositivos, aplicaciones comerciales o íncluso la “moda tecnológica” y tiene mucho más que ver, con la organización, método y diciplina.

Requiere de una guía general que permita particularizar pero al mísmo tiempo cumplir con la NORMATIVIDAD asumiendo responsabilidades sobre los incumplimientos de esta, creando una normatividad que sea ejemplo en las instituciones gubernamentales y que “invite” a la iniciativa privada a continuarla y ser parte de ella. Contando con una pauta y una institución a la que se pueda recurrir para dar parte de eventos y buscar respuesta a incidentes de manera más eficaz.

Ing. Héctor Méndez Olivares
Especialista en Seguridad de la Información
Septiembre de 2003.