

## SEGURIDAD DE SISTEMAS INFORMÁTICOS

La seguridad en sistemas de información es un tema en constante crecimiento y difusión. La necesidad de asegurarnos que no seamos espiados, que nuestra información no sea robada ni eliminada, e incluso que nuestra empresa no vea interrumpida su normal operación a causa de no implementar controles adecuados, es un tema que llega para quedarse.

La palabra seguridad, en informática, es tan amplia como pueda imaginarse. Abarca desde temas tan obvios como el cuidado por robos de máquinas y equipamiento, hasta temas mucho menos obvios como el resguardar la base de datos de los mismos empleados de una empresa que deben hacer accesos a ella, pero muy controlado.

Los riesgos que tratan de batallarse a través de la implementación de una seguridad adecuada son incluso un punto clave para la competitividad, porque la información contenida en la organización tiene valores a veces no pensados con la importancia necesaria. Veamos:

- **Importancia estratégica de la Información:** aquella información que es clave, la que provee una ventaja sobre los competidores. Ejemplos son: Secretos de negocio (¿qué pasaría si se roba la fórmula secreta de la Coca-Cola?); Lista de precios al consumidor; Campañas de marketing, Costos de los productos y servicios adquiridos de proveedores, o información de contacto de esos proveedores.
- **Confiabilidad de Información para la toma de decisiones:** abarca desde información financiera hasta de operaciones. Ejemplos de esto son: Información de sistemas para diagnósticos médicos a pacientes (no hablemos sólo de grandes y complejos sistemas, hablemos también de un simple fichero de historias clínicas. Recuerde que esta información debe ser resguardada); Información para procesar órdenes y para planificar los procesos de producción (pensemos en una fábrica que por alguna razón pierde la información de las últimas órdenes necesarias para programar su próxima producción)
- **Confidencialidad de los datos:** hay muchos motivos por los que ciertas informaciones deben resguardarse por ser confidenciales. A veces, los motivos son éticos, otras veces son incluso legales. Ejemplos son: Información de seguridad nacional; Información de propuestas presentadas en un llamado a licitación; Información sobre procesos judiciales.
- **Expectativa de terceros:** Nuestros clientes, proveedores, accionistas y hasta el público general, espera que nosotros hagamos un uso apropiado de la información por ellos facilitadas. Ejemplos son: Información personal y de tarjetas de clientes y/o proveedores; tarjetas de créditos o cuentas bancarias; software adquirido por licencia (¿esperan las grandes empresas desarrolladoras de programas y sistemas operativos que no hagamos copias ilegales?)

Es muy importante puntualizar que el rol que cumplen los gerentes o administradores en la toma de decisiones respecto de la estructura de seguridad adoptada y las políticas consecuentes están bajo su responsabilidad. Una empresa puede tener los medios para implementar una seguridad adecuada, pero antes debe establecerse un marco, un programa, y una estructura y políticas completamente relacionadas con la de la organización.

### CUÁLES SON LOS RIESGOS

Los riesgos son muchos pero pueden enmarcarse diciendo que: la integridad, confidencialidad y disponibilidad de los datos están en riesgo debido a:

- **Errores humanos, accidentes u omisiones:** comprobado por grandes empresas de auditoría, este es el riesgo que de forma directa tiene las mayores consecuencias e implican las mayores pérdidas todos los años. Estos errores son causados por datos entrados incorrectamente o errores de programación de los programas. (¿sabía que se dijo que el error que causó la explosión del Challenger allá por el año 1986 fue de un "data-entry"?, data-entry es la persona encargada de ingresar los datos)

al sistema.)

- Empleados y ex empleados: la gran parte de los delitos perpetrados a sistemas informáticos suelen ser realizados por ex empleados o empleados con accesos mal autorizados.
- Entes externos a la organización: ¿le suena la palabra “hackers”? La publicidad adversa que puede traer el haberse descubierto un bache de seguridad aprovechado por un hacker puede traer consecuencias muy costosas en términos monetarios y no monetarios.
- Daños en el ambiente: el fuego es una de las catástrofes más significativas y más controlables. Estos fuegos pueden ocurrir en el mismo lugar donde están las computadoras, pero usualmente se originan en áreas adyacentes y se extienden hacia esa área. El fuego, humo y agua pueden dañar severamente los sistemas informáticos y hasta dejarlos inutilizables.
- Cortes de energía eléctrica o transmisión de electricidad “sucias”: los equipos informáticos necesitan energía “limpia”. Las subas y bajas de tensión pueden tener consecuencias graves y los cortes de energía pueden causar pérdidas de datos y de capacidades operacionales si no se implementan los sistemas de prevención adecuados.
- Desastres naturales y otras amenazas físicas: terremotos, tornados, inundaciones y otros incidentes similares tienen poca probabilidad de suceso, pero consecuencias muy graves y demandan una planificación de seguridad.
- Interrupciones por movimientos civiles: protestas, guerras civiles, huelgas y actos de terrorismo deben estar entre los riesgos bajo control.
- Introducción de código dañino: virus, gusanos, y demás códigos que son considerados malignos pueden ser introducidos al sistema informático por medios muy diversos. Pueden causar hasta una completa inoperabilidad durante el tiempo necesario para identificar, aislar y remover ese código. Ese tipo de código puede ser introducido por programas legítimos e información autenticada. ¿Podría clasificarse al S-P-A-M como un uso de un medio de comunicación legítimo, para fines legítimos o ilegítimos, pero con consecuencias desastrosas, como la posible introducción de código maligno, identificación de información confidencial y accesos no deseados a sistemas informáticos organizacionales?

Estos riesgos deben encontrar frente de batalla del lado de los controles implementados en los sistemas informáticos. Los controles se dividen en dos grandes grupos: Controles Físicos y Controles Lógicos. Los primeros restringen el acceso físico a áreas informáticas y equipos y los segundos restringen el acceso lógico, o acceso a través de una interfase.

## LOS CONTROLES FÍSICOS

Los controles físicos son la más básica y común forma de implementar control sobre los sistemas de información. Las áreas sensibles que demandan controles físicos no son sólo aquellas donde se encuentran los equipamientos para la operación diaria de la organización sino aquellas áreas utilizadas para almacenar sistemas de soporte y de resguardo de información de backup. Incluye discos y cintas (y por qué no, carpetas) con información.

Los controles físicos deben resguardar la información ante: accesos físicos, peligros ambientales y peligros de fuego y agua.

Empecemos entonces a conocer cuáles son los controles y los medios posibles de control:

### Controles:

- Acceso físico: controles y monitoreos sobre accesos no sólo en áreas donde se encuentran los equipos informáticos sino en otras tales como áreas donde se encuentran los cableados. Además, controles sobre cableados telefónicos, eléctricos, de red, y de control de calefacción.

- Peligros ambientales: se refiere no sólo al ambiente físico que rodea al negocio sino también al ambiente del negocio mismo. Los peligros ambientales son los riesgos por causas naturales y hechos por el hombre. Incluye el derrame de productos químicos, disturbios civiles u alborotos.

- Protección ante fuego y el agua: el fuego y el agua, junto a los daños producidos como consecuencia de procedimientos de extinción del primero (por el humo y los productos químicos utilizados) son dos de las causas más comunes de daños en equipamientos informáticos. El fuego puede nacer en áreas adyacentes e incluso edificios contiguos y las aguas pueden deberse a sistemas de aire acondicionado, sistemas de cañerías cercanas en los pisos o las paredes.

Es tarea de un auditor informático el establecer los riesgos físicos presentes en un área y establecer los controles de seguridad adecuados. Por supuesto, esto siempre va acompañado de ciertos objetivos de seguridad, para establecer el marco, las políticas y los programas correspondientes.

### Medios de control físico:

Los humanos al reconocer a una persona con la vista hacemos dos tareas casi conjunta e instantáneamente: identificación y autenticación. Para las computadoras, estas tareas son independientes y mucho más complicadas de realizar.

La identificación consiste en preguntar a una persona quién es, y muy distinto, el autenticar a una persona es corroborar que esa persona es quien dice ser.

Los métodos de autenticación suelen ser divididos en tres grandes categorías, en función de lo que utilizan para la verificación de identidad:

- Algo que la persona sabe
- Algo que la persona posee
- Una característica física de la persona o un acto involuntario del mismo. Esta última categoría se conoce con el nombre de autenticación biométrica.

Veamos de qué se trata:

- Algo que la persona sabe. Ejemplos de esto son las claves de acceso, una clave de seguridad para la apertura de puertas, un PIN en cajeros automáticos. Este es el sistema más ampliamente usado debido al bajo costo de implementación y uso, pero es también el más vulnerable. Basta con no mantener secreta una clave para que el sistema sea violado.

- Algo que la persona posee. Ejemplos de esto son las tarjetas magnéticas e inteligentes y las llaves de acceso. Una tarjeta inteligente (o *smartcard*) es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la adulteración, que ofrece funciones para un almacenamiento seguro de información y también para el procesamiento de la misma. En la práctica, las tarjetas inteligentes poseen un chip empotrado en la propia tarjeta que puede implementar un sistema de ficheros cifrado y funciones criptográficas, y además puede detectar activamente intentos no válidos de acceso a la información almacenada. Las tarjetas de accesos a cajeros, solamente incorporan una banda magnética donde va almacenada cierta información del propietario de la tarjeta.

Las ventajas de utilizar tarjetas inteligentes como medio para autenticar usuarios son muchas frente a las desventajas; se trata de un modelo ampliamente aceptado entre los usuarios, rápido, y que incorpora *hardware* de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Además, su uso es factible tanto para controles de acceso físico como para controles de acceso lógico. Como principal inconveniente de las *smartcards* podemos citar el coste adicional que supone para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas; aparte, que un usuario pierda su tarjeta es bastante fácil, y durante el tiempo que no disponga de ella o no puede acceder al sistema.

En nuestra próxima edición de Estr@tegia Magazine seguiremos con el tema de la seguridad de los sistemas informáticos y desarrollaremos los métodos más utilizados para la autenticación biométrica.