LA SEGURIDAD DE LOS ACTIVOS DIGITALES EN LA EMPRESA ACTUAL

Silvia Renteria,
Lic. en Informática
Xavier Uriarte,
Ingeniero Industrial
Cristina Martinez,
Lic. en Informática
Tatiana Bartolomé,
Ingeniera Informática
Artzai Picón,
Ingeniero Industrial
Robotiker-Tecnalia

Seguridad es la característica de un sistema por la cual se puede decir que el sistema está libre de peligro, daño o riesgo. En el ámbito informático sería la característica que lo hace infalible frente a la destrucción, interceptación o modificaciones no deseadas. Aunque la seguridad nunca podrá ser garantizada al 100% es necesario definir unas estrategias que permitan garantizar la seguridad del sistema hasta unos límites adecuados con un costo asumible.

¿Qué proteger?

Los tres elementos principales que se deben proteger son: el *hardware*, el *software* y los datos. Por *hardware* se entiende los elementos físicos, como son, el procesador, los discos duros, los cableados, …etc. Por *software* se entiende el conjunto de programas que hacen funcionar el hardware, entre estos , se pueden destacar tanto el sistema operativo como las aplicaciones. Y, por último, por datos se refiere a toda la información que maneja tanto el *hardware* como el *software*, por ejemplo, los datos que se encuentran en una base de datos o los paquetes de datos o tramas que viajan por la red.

¿Qué es la seguridad de 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. La seguridad de la información protege a ésta de un amplio elenco de amenazas para asegurar la continuidad del negocio, minimizar los daños a la Organización y maximizar el entorno de las inversiones y las oportunidades de negocio.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en filmes o hablada en conversación.

La seguridad de la información se caracteriza aquí como la preservación de:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a ella.
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la Organización.

¿Por qué es necesaria la seguridad de información?

La información y los procesos que la apoyan, sistemas y redes son activos de la Organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, tesorería, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada y debería apoyarse en una gestión y procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la Organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organi-

zaciones externas también puede ser necesaria.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de requisitos y en la fase de diseño.

¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad, para ello existen tres fuentes principales:

• La primera fuente procede de la **valoración de riesgos** de la Organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

• La segunda es el **conjunto de requisitos legales, estatutarios y regulatorios** que debería satisfacer la Organización, sus socios comerciales, los contratistas y los proveedores de servicios.

• La tercera está formada por los **principios, objetivos y requisitos** que forman parte del tratamiento de la información que la Organización ha desarrollado para apoyar sus operaciones.

¿De qué es necesario protegerse?

Existen diferentes factores de los que es aconsejable protegerse. A continuación se nombran algunos.

• Personas

- La mayoría de las amenazas en definitiva provienen de las personas. Estas pueden ser: personal de una empresa, ex empleados, *hackers, crackers,* etc.

• Amenazas lógicas

- Entre éstas podemos destacar entre *software* incorrecto como *bugs* y *exploits*, puertas traseras, virus, herramientas de seguridad, etc.

• Problemas físicos, podemos encontrarnos problemas de varios tipos:

- Sobrecargas eléctricas e interrupciones de alimentación: se pueden solucionar utilizando redundancia en elementos como las fuentes de alimentación, utilizando sistemas de alimentación ininterrumpida (SAI).

- Temperaturas extremas, humedad, polvo, etc: se pueden llegar a solucionar estos problemas en salas con equipos críticos como servidores colocando climatizadores, deshumidificadores, etc.

- Accesos físicos no autorizados, robo de *hardware*: uso de contraseñas,…etc.

- Fallos en elementos físicos: soluciones de redundancia como RAID's por ejemplo.

- Fallos en CPU.

- Fallos de memorias

- Destrucción física de datos y borrados accidentales de información: este problema se puede llegar a solucionar siguiente una política de seguridad como el de realizar copias de seguridad frecuentemente.

- Catástrofes: humo, incendios, terremotos, etc.

Las medidas organizativas como fundamento de la seguridad digital

En la actualidad son muchas las empresas que han implantado medidas técnicas para proteger la seguridad de sus sistemas. Sin embargo, no han realizado un análisis detallado de sus requerimientos de seguridad ni han explicitado cuáles son sus objetivos o cómo llevarlos a cabo.

Es necesario por tanto dar un especial énfasis a las medidas organizativas que definan la estrategia de la empresa en materia de seguridad digital. Estas medidas deben definir de forma primordial los siguientes elementos:

Plan de seguridad

Todo plan de seguridad debe cubrir todos los aspectos relacionados con la misma: cómo deben operar los usuarios, normas de uso, normas de seguridad, *passwords*, etc. Idealmente se deberían prevenir todas las eventualidades, pero en la realidad no siempre es posible.

Otra regla a cumplir es que toda política debe adecuarse a las necesidades y recursos que dispone una empresa. Se trata por tanto de valorar los costes en que podemos incurrir en caso de una catástrofe y contrastarlos con el coste de las medidas de seguridad.

Los elementos a definir en el documento de plan de seguridad de una empresa son los siguientes:

• Arquitectura de los sistemas existentes: sistemas de red, servidores, comunicaciones, etc.

¿CÓMO PROTEGERSE? FACTORES RELEVANTES EN LA SEGURIDAD DIGITAL

Seguridad digital	
Factores estructurales	Instalaciones: control de acceso, riesgo de desastre (inundación, incendio) Suministro eléctrico a los sistemas informáticos
Factores tecnológicos	Arquitectura de la red, sistemas de comunicaciones Servidores y servicios: equipos, configuración, servicios soportados Herramientas y sistemas de seguridad Contratos de mantenimiento y soporte con terceras empresas
Factores humanos	Recursos humanos: funciones, coordinación, formación
Factores organizativos	Procedimientos para la gestión y control de la seguridad

• Acceso físico a los diferentes equipos.
• Definición de los perfiles existentes.
• Parcelación de los bloques de información según su contenido, alcance y visibilidad de la misma.
• Parcelación de los servicios y aplicaciones existentes.
• Política de acceso de los diferentes perfiles a los recursos identificados (información y servicios/aplicaciones). Altas y bajas de recursos humanos. Privacidad de los datos interna y externamente.
• Política de encriptación de datos, tanto en información actual como en información de *back-up*.
• Política de securización de servidores.
• Política de copias de seguridad.
• Política de contraseñas, firmas electrónicas, etc.
• Política de aplicaciones corporativas instaladas en los equipos del usuario final.
• Política de actualización de antivirus.
• Política de utilización del correo electrónico.
• Política de navegación en Internet.
• Aplicación de la LOPD a los datos sensibles de la empresa.

Plan de contingencia

Como complemento al plan de seguridad es necesario contar con un plan de contingencia ante fallos tanto de los sistemas como de las personas encargadas de los mismos.

Para cada uno de los sistemas identificados como críticos en la auditoria de seguridad es necesario elaborar una lista de acciones a llevar a cabo en caso de cualquier fallo que les pueda afectar.

Dicha lista debe ser clara y concisa, orientada a que pueda realizarla alguien con poca o ninguna experiencia en el sistema en base a unas instrucciones detalladas y secuenciales que faciliten la recuperación del recurso o sistema afectado aunque sea en un modo de funcionamiento a bajo rendimiento o con prestaciones mínimas. Sería aconsejable disponer de dos niveles de actuación, uno que permita una operatividad restringida en un corto espacio de tiempo y otro que permita posteriormente la vuelta a la normalidad.

OTROS ELEMENTOS A TENER EN CUENTA. LA LEGISLACIÓN ACTUAL

Dentro de la seguridad digital es de especial importancia la referida a los datos y procesos sujetos a legislación específica en nuestro país. En concreto, las dos principales leyes de obligado cumplimiento en este aspecto son las siguientes:

LOPD

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) es de obligado cumplimiento e impone diversas obligaciones a todas las empresas y profesionales posean bases de datos con datos de carácter personal.

Las principales obligaciones son tres:

1. Notificar ante la Agencia de Protección de Datos todos los ficheros que contengan datos de carácter personal (personal, clientes, proveedores, asociados, etc).
2. Adecuar la actividad de la empresa a las obligaciones establecidas para recabar, tratar y comunicar datos de carácter personal.
3. Elaborar el Documento de Seguridad obligatorio (Real Decreto 994/1999).

LSSICE

La Ley tiene como principal objetivo la trasposición de la Directiva 200/31/CE (la Directiva del Comercio electrónico). Sin embargo, se ha aprovechado para regular muchos otros factores que afectan a la llamada "Sociedad de la Información", en particular aspectos tan distintos como obligaciones de Servicio Universal, o la legalidad o ilegalidad de los actos que cualquier particular puede realizar, o no realizar, en la red.

Lo que la Directiva 2000/31/CE denomina "Sociedad de la información" viene determinado por la expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información.

La gestion de la seguridad

La información es un activo y, como otros activos del negocio, tiene valor para la empresa y debe ser protegido de manera adecuada.

Un sistema de gestión de la seguridad de la información (SGSI) comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

Proporciona mecanismos de salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y los planes estratégicos de la Organización. Existen diferentes normas y estándares que ofrecen recomendaciones para realizar la gestión de la seguridad de la información y que pueden ser utilizadas por los responsables de iniciar, implantar o mantener la seguridad de una organización. Estos estándares proporcionan una base común para el desarrollo de normas de seguridad dentro de las organizaciones, así como para proporcionar confianza en las relaciones entre organizaciones.

Los principales estándares para la gestión de la seguridad de la información son los siguientes:

• **UNE-ISO/IEC 17799:2002:** *"Código de buenas prácticas para la gestión de la seguridad de la información"*

Se trata de un conjunto de recomendaciones para iniciar, implantar y mantener un SGSI, condicionadas por la legislación específica de cada país y equivale a la norma británica BS 7799:Parte 1.

Comprende un total de 127 controles de seguridad agrupados en los siguientes apartados:

- Política de seguridad.
- Aspectos organizativos.
- Clasificación de activos.
- Seguridad del personal.
- Seguridad física y del entorno.
- Comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Continuidad del negocio.
- Conformidad.

• **UNE 71502:2004:** *"Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)"*

A diferencia de la anterior, ésta es una norma certificable y equivale a la británica BS 7799:Parte 2. Esta norma especifica los requisitos para establecer, implantar, documentar y evaluar un SGSI de acuerdo con la UNE-ISO/IEC 17799, dentro del contexto de los riesgos identificados por la Organización.

Conclusiones

En toda empresa u organización la seguridad debe entenderse de forma global y se deben tomar todas las medidas necesarias para evitar cualquier tipo de perjuicio, si ésta no es la adecuada.

Hasta no hace mucho tiempo, las empresas eran unos espacios "cerrados" para la gente que no trabajaba en las mismas, pero con la explosión que supuso Internet y el desarrollo de nuevas formas de comunicación y nuevas aplicaciones, el sentimiento general, y la realidad, es que ahora esas mismas empresas son mucho más accesibles y por lo tanto más vulnerables que antes.

Continuamente están apareciendo nuevos delitos informáticos, ya sean: substracción de dinero, bienes de servicio, *software, hardware,* informes... Pero no hay que pensar que los ataques provienen siempre del exterior de la empresa. También pueden aparecer en el interior de la misma, ya sea conscientemente o inconscientemente, incluso por descuido o desconocimiento.

Es necesario tener claramente definido cuál es la información importante que se tiene en la empresa y tomar un conjunto de acciones y medidas destinadas a proteger esa información así como en asegurar el cumplimiento de la ley vigente.

Es conveniente tener siempre presentes estos puntos o acciones a realizar: definir las necesidades y requerimientos de cada sistema, establecer políticas, definir normas y procedimientos de actuación, elegir las herramientas más adecuadas para cada caso, implantar la solución que se crea como la más idónea y realizar auditorias y verificaciones de la seguridad en los sistemas de la empresa. ■