

Integridad y Confidencialidad de la Información (*)



La información es el principal patrimonio de cualquier organización, por lo que su protección y seguridad resulta imprescindible, máxime en un momento en el que Internet y las relaciones electrónicas se han establecido como la nueva forma de relacionarse, con las ventajas innegables, pero también con los riesgos que ello conlleva. La criptografía de clave pública (PKI) se convierte así en la forma más efectiva de garantizar la confidencialidad y la integridad de la información y, por lo tanto, su seguridad.

Clara Baonza

Podría definirse la seguridad de la información como la habilidad para proteger la información y los recursos respecto a la confidencialidad y la integridad. En este sentido es preciso garantizar la autenticación, confidencialidad, integridad y disponibilidad. No se puede defender el sistema con un concepto de fortaleza donde levantemos murallas empleando distintos productos. Hoy en día, los sistemas se asemejan más a ciudades con múltiples vías de entrada y salida, más que a fortalezas. Ciudades que, además, deben ser muy ágiles.

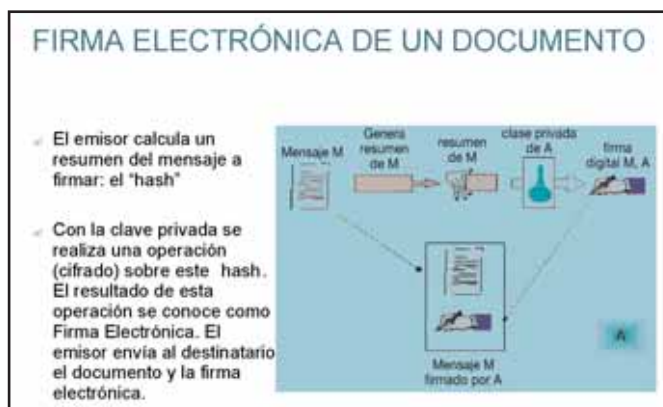
Así pues, las características principales de la seguridad son la **confidencialidad** (necesidad de que esa información únicamente sea conocida por personas autorizadas), **integridad** (hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la huella digital) y **disponibilidad** (capacidad de estar siempre disponible para ser procesada por las personas autorizadas). Si alguna de estas características falla no estamos ante nada seguro.

Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.

Activos, amenazas y vulnerabilidad para la información

Las amenazas causan pérdidas o daños a la información de una organización. Se trata de agentes capaces de explotar los fallos de seguridad (vulnerabilidades), son constantes y pueden ocurrir en cualquier momento. Existen amenazas humanas (maliciosas externas o internas, y no maliciosas) y desastres naturales (incendios, inundaciones, terremotos...).

Las amenazas para un ataque informático son similares a las de un ata-



Fuente: Asimelec



que en un entorno convencional, pero Internet incluye tres nuevas posibilidades, y cada una de ellas por separado son muy difíciles de controlar, pero las tres juntas pueden tener efectos devastadores. La primera, la automatización, aunque los sistemas actuales de auditoría de passwords pueden comprobar más de 200.000 contraseñas por segundo.

En segundo lugar, la posibilidad de actuar a distancia. No es imprescindible estar cerca del objetivo. Además se puede atacar desde un país que no tenga legislación al respecto.

Por último la distribución de las técnicas de ataque. Cuando un hacker descubre una nueva vulnerabilidad, crea un exploit y dos horas después hay miles de hackers que lo único que tienen que hacer para atacar el sistema es ejecutar un programa. Por ello, la velocidad con la que se puede atacar no permite que la seguridad se base en medidas reactivas, para cuando se quiere reaccionar pueden haberse realizado miles de transacciones o haber copiado todo lo que pueda ser de interés.

En cuanto a las vulnerabilidades, son aquellos elementos que, al ser explotados por amenazas, afectan a la confidencialidad, disponibilidad e integridad de la información. Pueden ser de varios tipos:

- ❶ **Físicas:** ambiente en el que se almacena o maneja la información.
- ❷ **Hardware:** defectos de fabricación, desactualización, mantenimiento inadecuado.
- ❸ **Naturales:** condiciones de la naturaleza que pueden provocar riesgo.
- ❹ **Humanas:** daños que las personas pueden causar a la información (hackers, virus, empleados descontentos...).
- ❺ **Software:** aplicaciones que permiten accesos indebidos.
- ❻ **Almacenamiento:** soportes físicos utilizados para almacenar información.
- ❼ **Comunicación:** fallos en la transmisión de la información.

Las acciones que evitan o eliminan las vulnerabilidades son las medidas de seguridad y sus objetivos pueden ser de varios tipos: **preventivas** (evitan los puntos débiles), **perceptivas** (encuentran actos que supongan un riesgo) y **correctivas** (corrección de problemas cuando ocurren). Se basan, además, en el establecimiento de controles técnicos, jurídicos y organizativos. Es decir, en el desarrollo de políticas y planes de seguridad, estableciendo los estándares de seguridad que deberán cumplir todos los usuarios. Así, por ejemplo, nos encontramos con la ISO 17799 que

establece un marco para la gestión de la seguridad de la información; o la LOPD que es de obligado cumplimiento; o sistemas de criptografía que garantizan la confidencialidad e integridad en las comunicaciones de datos.

Criptografía de clave pública (PKI)

El uso de tecnología de clave pública (PKI) es la forma más efectiva de garantizar la confidencialidad y la integridad de la información. Está basada en el uso de un par de claves, una de distribución pública y otra en poder únicamente del propietario. La clave del propietario debe ser guardada de forma segura y se denomina clave privada; mientras que la clave pública se da a conocer a todos aquellos que quieran comunicarse de forma segura con el propietario.

Los dos aspectos esenciales de esta criptografía son la firma electrónica y el cifrado. La primera de ellas es una de las formas de combatir las amenazas a la integridad de la información. La firma electrónica permite comprobar que un mensaje enviado o recibido no ha sido modificado desde su creación. Así, el emisor calcula un resumen del mensaje a firmar o huella digital (función hash). Con la clave privada se realiza una operación (cifrado) sobre este hash. El emisor envía al destinatario el documento y la firma electrónica. El destinatario comprueba usando la clave pública del firmante el contenido del hash y lo compara con otro hash que calcula, verificando que no se ha alterado. Hay que tener en cuenta que una función hash es irreversible, por tanto su comprobación se realizará aplicando de nuevo la misma función hash al mensaje. Además, es casi imposible que dos mensajes diferentes tengan el mismo mensaje resumen, por lo que dos mensajes parecidos producen huellas digitales completamente diferentes (es imposible reconstruir el mensaje original a partir de su hash y también es imposible generar un mensaje con un hash determinado).

Actualmente existen diferentes funciones hash, entre las que destacan MD5 (desarrollada por el profesor Ronald L. Rivest en 1991 en el que el mensaje resumen generado es de 128 bits y su implementación es más rápida), el SHA-1 (Secure Hash Algorithm, una familia de algoritmos desarrollados por la Agencia de Seguridad Americana y publicados por el Instituto Nacional de Estándares y Tecnologías de EEUU, en donde el mensaje resumen generado es de 160 bits, más lento que el MD5 aunque su mayor longitud le confiere una mayor seguridad frente a los ataques de fuerza bruta) y el RIPEMD-160 (desarrollado en Europa y publicado en 1996, en el contexto del proyecto RIPE de la UE y propuesto en segundo lugar por el ETSI junto a SHA-1 como alternativa al uso de MD5).

En cuanto al cifrado de datos (confidencialidad de la información), el autor de los datos genera una clave de cifrado (3DES) a través de un dispositivo seguro. Para comunicar dicha clave al/los destinatarios, se les transmitirá cifrada con su respectiva clave pública. Únicamente el/los legítimos receptores podrán obtener la clave con la que se cifraron los datos.

[*] Comisión de Seguridad y Confianza en TI de Asimelec. Extracto de las ponencias presentadas en el 1º Foro de Seguridad de las TIC en Simo 2005 por parte de las empresas Giesecke&Devrient y Safelayer.

