Introducción a la seguridad informática

Álvaro González Sotillo

19 de enero de 2019

Índice

1. Presentación del tema

En este tema hablaremos de los conceptos básicos de la Seguridad Informática.

No son conceptos nuevos ni creados a propósito para ésta disciplina.

La mayor parte de ésta terminología ha sido adoptada de terminología ya existente en el ámbito empresarial, referida a la seguridad en un concepto amplio.

La Seguridad Informática se encarga de los aspectos relacionados con la seguridad de los equipos informáticos, pero también de todo lo que le rodea de manera más o menos directa: personas, datos, software, instalaciones...

2. Sistemas de información y sistemas informáticos.

2.1. Sistema de información:

Un sistema de información es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para

conseguir sus objetivos.

Esos elementos son:

- Recursos, como ordenadores, componentes, periféricos, conexiones, aplicaciones, sistemas operativos, y otros recursos no necesariamente informáticos, desde un teléfono a una grapadora.
- Equipo humano
- Información: datos organizados que tienen un significado. Pueden estar en un soporte informático o no.
- Actividades: muy importante... toda organización realiza varias actividades en su negocio. (Ej.: una pequeña tienda tiene varias actividades: vender productos a los clientes, hacer pedidos a los proveedores, controlar la cantidad de productos almacenados, gestionar los gastos, ingresos, impuestos, etc...)

2.2. Sistema informático:

Un Sistema informático está formado por un conjunto de elementos físicos (hardware, conexiones, cables...) lógicos (Software de aplicación, de base, protocolos) y también podemos considerar con frecuencia al componente humano.

Un sistema informático **da soporte a las actividades de los sistemas de información**. Las empresas diseñan sus actividades conforme a la información que manejan... Nunca pensando en el sistema informático que les va a dar soporte. Lo importante para ellas, lógicamente, es que esas actividades se desarrollen de manera ordenada, eficaz y eficiente. Los sistemas informáticos, cuando están bien diseñados y utilizados, contribuyen en esos aspectos. (INFORMÁTICA=Tratamiento autoMÁTICO de la INFORmación).

No necesariamente todas las actividades de la empresa requieren de sistemas informáticos.

3. Seguridad

La seguridad es la disciplina que se ocupa de diseñar las **normas, procedimientos, métodos y técnicas** destinados a conseguir un sistema de información seguro y confiable.

Todos los elementos que participan en un sistema de información pueden verse afectados por factores de diversa índole que pueden poner en peligro su estabilidad y normal funcionamiento.

Con respecto a la Seguridad Informática, debemos tener en cuenta, que de todos esos elementos, debemos poner especial atención en la **información,** pues es el elemento más sensible de la empresa, y la que tiene un valor *incalculable*... pero siempre por detrás, por supuesto, de la seguridad de las personas.

Reflexiona sobre ésto: ¿Tendría sentido anteponer la seguridad de la información o de cualquier otro elemento a la seguridad de las personas?

Nuestro trabajo se centrará en la seguridad de los sistemas informáticos, pero siempre teniendo en mente que la protección va encaminada hacia las **actividades** de una empresa... a intentar que no se vean vulneradas o afectadas por ninguna circunstancia, y por supuesto, tampoco la información que manejan. Es decir, a que los *sistemas de información* continúen su ritmo con la máxima normalidad posible. Para ello actuamos sobre los sistemas informáticos que les dan soporte.

Nuestra disciplina se encarga poco de la seguridad de las personas, por eso no tendrá especial relevancia. Eso no significa que sea, sin duda, el aspecto clave de la seguridad... simplemente, que ésta disciplina se enfoca principalmente hacia la seguridad de los sistemas de información.

Para afrontar la seguridad de un sistema, deberemos conocer los elementos del sistema, los peligros que pueden acechar y las medidas que deberían adoptarse para lograr esa seguridad. No obstante, lo estudiaremos desde un punto de vista formal, utilizando terminología estándar del sector de la seguridad.

Reflexiona sobre ésto: ¿Se puede lograr la seguridad total? Es decir... estar totalmente protegido contra cualquier cosa.

Hay un dicho en el sector de la seguridad:

La cadena siempre se rompe por el eslabón más débil

A menudo se dice también que ese eslabón suele implicar al factor humano.
Reflexiona sobre ésto:¿Crees que en efecto, el factor humano es el eslabón más débil?

4. Propiedades de un sistema de información seguro.

¿Qué le pedimos a un sistema de información seguro? ¿Que no se cuelgue? ¿Que no nos borre cosas? ¿Que no lo puedan hackear?.... Si... por supuesto. Estas cosas y muchas otras más. Formalmente hablando, hay tres *propiedades* básicas que un sistema de información debe mantener al máximo que sea posible. Prácticamente todo lo que le pidamos a un sistema de información que consideremos seguro cae dentro de mantener estas tres propiedades altas:

4.1. INTEGRIDAD:

Garantizar la autenticidad y precisión de la información, sin importar el momento en que se solicita.

Dicho de otra forma, que los datos no son alterados ni destruidos de modo no autorizado, ni accidentalmente. Si los datos se pierden, se borran, se modifican, se corrompen, o se añaden datos nuevos fraudulentos o erróneos consideramos que se ha perdido la integridad de un sistema de información. Esto puede ocurrir con datos que están almacenados ("quietos", en un fichero, o base de datos, o manejados por una aplicación...) o con datos que se está en un sistema de comunicaciones (se están "moviendo"... y llegan a su destino en un estado diferente al que fueron emitidos.

4.2. CONFIDENCIALIDAD:

Garantizar que los datos almacenados estén únicamente al alcance de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada.

Es decir, no sólo que se pueda acceder a información si se está autorizado, sino que se además, debe hacerse dentro de la actividad correspondiente.

Si un sistema de información permite que un dato cualquiera llegue a ser visto por alguien que no está autorizado supone una pérdida de la confidencialidad. El concepto va todavía más lejos... Si el dato llega a una persona que sí es un destinatario legítimo de la información, pero llega por un mecanismo no autorizado, o un momento no autorizado, o utilizando algún procedimiento no autorizado, también consideramos que se ha producido una pérdida de la confidencialidad.

4.3. DISPONIBILIDAD:

El grado en que un dato está en el lugar, momento y forma en que es requerido por un usuario autorizado.

Dicho de otro modo, que la información que se solicite esté disponible en un periodo de tiempo razonable"desde que se solicita por un usuario autorizado.

La pérdida de la disponibilidad sólo implica en sí misma que en un momento dado, una información que se solicita no es devuelta por un sistema. Esto no implica que la información haya perdido la integridad... sólo que no se puede proporcionar en ese momento.

4.4. Otras propiedades de seguridad.

Además de las tres propiedades fundamentales de un sistema de información seguro (la disponibilidad, confidencialidad e integridad), y de la cualidad de no-repudio, a menudo se utilizan otras propiedades de seguridad en algunos sistemas, según sean útiles o no:

- **No repudio**: La capacidad de determinar quién creó, modificó o accedió a cierta información, de forma que ni el emisor/creador pueda negar su participación, ni el receptor pueda negar que tuvo dicha información disponible. Esta característica de la seguridad cobra importancia a la hora de realizar transacciones seguras en un sistema informático, con aplicaciones variadas. Por ejemplo, en la administración electrónica, es vital que el ciudadano pueda probar que ha tramitado en plazo sus obligaciones tributarias, y que el estado no pueda alegar que no recibió la documentación.

- **Autenticación**: Más allá de la confidencialidad, las medidas o servicios de autenticación intentan garantizar la identidad de las personas o entidades que intentan acceder a la información. Se puede exigir la autenticación en el origen de los datos, en el destino o en ambas. Está ligada a la **confidencialidad**, ya que el sistema informático necesita saber quién accede al sistema para garantizar esta última. Se necesita para el **no-repudio**.

- **Control de acceso**: Son las medidas o servicios que no sólo permiten o impiden el acceso de personas o entidades a la información, sino que además, suelen registrar constancia del hecho del acceso o el intento de acceso. Relacionado con la **confidencialidad** y el **no-repudio**.

5. Medidas de seguridad. Clasificaciones.

Para proteger la información, es necesario establecer una serie de medidas. Las medidas de seguridad pueden clasificarse de varias maneras. Nosotros vamos a mencionar dos:

5.1. SEGURIDAD ACTIVA / SEGURIDAD PASIVA:

Atendiendo al carácter que tenga, hablamos de medidas de seguridad

- **Activas**: aquellas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. Podemos decir que tienen un carácter **preventivo**. Intentan *impedir* que ocurra un incidente. Por ejemplo, en un coche, el ABS es una medida de seguridad activa, ya que es un mecanismo electrónico que ayuda al conductor a frenar el coche... intenta evitar, prevenir un incidente.

- **Pasivas**: aquellas cuyo objetivo es minimizar la repercusión de un incidente de seguridad una vez producido. Podemos decir que tienen un carácter **correctivo**. No intentan evitar un incidente, sino reducir sus posibles efectos adversos. Por ejemplo, en un coche, un cinturón de seguridad es una medida de seguridad pasiva: no intenta evitar un accidente, sino que, de producirse, los daños para el ocupante del vehículo sean menores.

Una determinada medida de seguridad casi siempre cae en uno de los dos grupos. Es poco frecuente encontrar medidas de seguridad que simultáneamente puedan considerarse activas y pasivas... no obstante, como haberlas, haylas. Por ejemplo, cualquiera de los antivirus modernos, por un lado intenta *impedir* la entrada de virus y malwares, y por otro lado, si entran y el antivirus los detecta intentará minimizar su impacto.

5.2. SEGURIDAD FÍSICA / SEGURIDAD LÓGICA

Referido ya al ámbito exclusivo de la seguridad informática, podemos hablar de

- **Seguridad lógica**: cuando la medida va destinada a la protección de la información o del software.
- **Seguridad física**: cuando la medida va destinada a la protección del hardware.

Quizá estés pensando en el hecho de que el hardware, a veces es soporte del software y los datos... Por ejemplo... Si protejo un ordenador servidor con un SAI (el ordenador es hardware), pero el servidor en su interior contiene datos... entonces ¿el SAI es una medida de seguridad física o lógica? Es física... protege de manera directa al hardware... y los datos del servidor también, pero de manera indirecta.

En general, el hardware en sí no es un recurso demasiado valioso. Hay medidas de seguridad física dirigidas a él porque prácticamente siempre es el soporte de los datos.

6. Referencias

- Adaptado de Víctor J. Fernández
- Versión en PDF