PRIVACIDAD, INTEGRIDAD E IDENTIFICACIÓN

Seguridad de la información - Seguridad Web

Existen muchas definiciones del término seguridad. Simplificando, y en general, podemos definir la seguridad como: "Característica que indica que un sistema está libre de todo peligro, daño o riesgo."

Cuando hablamos de seguridad de la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca 'por el camino'. Si es más fácil acceder a ella también es más fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.

Existen también diferentes definiciones del término Seguridad Informática. De ellas nos quedamos con la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado desde octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).
“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.”

Como vemos el término seguridad de la información es más amplio ya que engloba otros aspectos relacionados con la seguridad más allá de los puramente tecnológicos.

Seguridad de la Información: modelo PDCA

Bases de la Seguridad Web

Fiabilidad

Existe una frase que se ha hecho famosa dentro del mundo de la seguridad. Eugene Spafford, profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que “el

único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él".

Hablar de seguridad informática en términos absolutos es imposible y por ese motivo se habla mas bien de fiabilidad del sistema, que, en realidad es una relajación del primer término.

Definimos la Fiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él.

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- Confidencialidad: acceso a la información solo mediante autorización y de forma controlada.
- Integridad: modificación de la información solo mediante autorización.
- Disponibilidad: la información del sistema debe permanecer accesible mediante autorización.

Existe otra propiedad de los sistemas que es la Confiabilidad, entendida como nivel de calidad del servicio que se ofrece. Pero esta propiedad, que hace referencia a la disponibilidad, estaría al mismo nivel que la seguridad. En nuestro caso mantenemos la Disponibilidad como un aspecto de la seguridad.

Confidencialidad

En general el término 'confidencial' hace referencia a "Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas."
En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el del ejército de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Por otra parte, determinadas empresas a menudo desarrollan diseños que deben proteger de sus competidores. La sostenibilidad de la empresa, así como su posicionamiento en el mercado pueden depender de forma directa de la implementación de estos diseños y, por ese motivo, deben protegerlos mediante mecanismos de control de acceso que aseguren la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de encriptación utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

Integridad

En general, el término 'integridad' hace referencia a una cualidad de 'íntegro' e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable.".

En términos de seguridad de la información, la integridad hace referencia a la la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

La integridad hace referencia a:

- la integridad de los datos (el volumen de la información)
- la integridad del origen (la fuente de los datos, llamada autenticación)

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

Disponibilidad

En general, el término 'disponibilidad' hace referencia a una cualidad de 'disponible' y dicho de una cosa "Que se puede disponer libremente de ella o que está lista para usarse o utilizarse."

En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados”. Es decir, un sistema es disponible si permite no estar disponible.

Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.

Como resumen de las bases de la seguridad informática que hemos comentado, podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la

confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

Dependiendo del entorno de trabajo y sus necesidades se puede dar prioridad a un aspecto de la seguridad o a otro. En ambientes militares suele ser siempre prioritaria la confidencialidad de la información frente a la disponibilidad. Aunque alguien pueda acceder a ella o incluso pueda eliminarla no podrá conocer su contenido y reponer dicha información será tan sencillo como recuperar una copia de seguridad (si las cosas se están haciendo bien).

En ambientes bancarios es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.

Mecanismos básicos de seguridad

Autenticación

Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras.

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)
4.

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

La técnica más usual (aunque no siempre bien) es la autenticación utilizando contraseñas. Este método será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

Además, la contraseña debe ser confidencial. No puede ser conocida por nadie más que el usuario. Muchas veces sucede que los usuarios se prestan las contraseñas o las anotan en un papel pegado en el escritorio y que puede ser leído por cualquier otro usuario, comprometiendo a la empresa y al propio dueño, ya que la acción/es que se hagan con esa contraseña es/son responsabilidad del dueño.

Para que la contraseña sea difícil de adivinar debe tener un conjunto de caracteres amplio y variado (con minúsculas, mayúsculas y números). El problema es que los usuarios difícilmente recuerdan contraseñas tan elaboradas y utilizan (utilizamos) palabras previsibles (el nombre, el apellido, el nombre de usuario, el grupo musical preferido,...), que facilitan la tarea a quién quiere entrar en el sistema sin autorización.

Autorización

Definimos la Autorización como el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

El mecanismo o el grado de autorización puede variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.

En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.

Por otra parte, solo se debe dar autorización a acceder a un recurso a aquellos usuarios que lo necesiten para hacer su trabajo, y si no se le negará. Aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen.

Administración

Definimos la Administración como la que establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.

Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.

La administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos.

Normalmente todos los sistemas operativos que se precian disponen de módulos específicos de administración de seguridad. Y también existe software externo y específico que se puede utilizar en cada situación.

Auditoría y registro

Definimos la Auditoría como la continua vigilancia de los servicios en producción y para ello se recaba información y se analiza.

Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

Definimos el Registro como el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo.

Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada.

Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

Mantenimiento de la integridad

Definimos el Mantenimiento de la integridad de la información como el conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada.

Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos está: uso de antivirus, encriptación y funciones 'hash'.

Identificación - Escritura Web

Redactar para la web

Leer en pantalla:

– factores externos
– internet

Escribir para la web

Al redactar para la web es importante **ajustar al máximo los contenidos** considerando:

– a **quién** van dirigidos (usuarios)
– con qué **finalidad** (misión de la web)
– características de la **lectura en pantalla**

Para ello conviene tener nociones de cómo redactar los contenidos en el entorno web, distintas en relación al medio impreso.

Leer en pantalla- Factores externos

Postura corporal:

– la **espalda es más propensa a sufrir** con períodos largos frente al ordenador pues la posición corporal que adoptamos para leer una pantalla de ordenador es generalmente menos relajante que la que adoptamos para leer un libro

– la **distancia entre los ojos y el texto en pantalla suele ser mayor** que cuando leemos un libro por lo que nuestro campo visual aumenta y podemos abarcar más elementos con la vista provocando **más distracciones**.

Contexto:

– la **percepción del tiempo y la atención varían** con la lectura digital pues se produce en un entorno multiárea e hipertextual:

– los usuarios:

se conectan por **espacios cortos de tiempo**

tienen **menos paciencia**

buscan la **inmediatez**

– internet:

cada página **compite** con miles de páginas similares

algunas conexiones se pagan por tiempo de conexión: **menos tiempo igual a más barato**

Leer en pantalla – Internet

Barrido visual:

- El 80 % de las personas **escanean el texto** porque: leemos entre un 25% y 30% **más lento** en internet
- nuestra vista **se cansa más rápido**
- queremos **saber enseguida** si estamos en el sitio correcto

Factor F de lectura:

los usuarios al leer una página web efectúan un movimiento similar a la letra F, suelen prestar más atención al inicio del texto y van dispersando su atención a medida que avanzan.

Impaciencia:

sólo se lee el 20% del contenido de las páginas

un usuario está una media de 5 segundos en una página

porque quiere encontrar de la forma más rápida lo que tiene en mente; cualquier información que no coincida con ese objetivo pasará a ser invisible.

Atención selectiva:

Palabras clave:

cuando se lee en pantalla, se buscan las palabras clave y se ignora el resto

Ceguera del *Banner*:

los mensajes con formato de *banner* (publicidad) se ignoran, pues los estímulos cuando se repiten dejan de serlo

Escribir para la web

Estructura del texto:

Es importante comenzar por la conclusión y luego desarrollar el tema.

El título y la primera frase han de describir el contenido del resto del texto, los dos primeros párrafos deben mostrar la información más importante pues tienen más probabilidades de ser leídos con más detención.

Cada párrafo debería expresar una idea.

Estilo:

Utilizar las palabras que el usuario conoce ya que facilita la identificación de la información reduciendo los tiempos de la tarea.

Ser concretos y directos:

Evitar:

voz pasiva

frases largas

subordinadas

perífrasis verbales

palabras ambiguas

Mejor:

verbos en infinitivo

palabras con significado claro

empatizar con lector

Utilizar palabras clave en títulos y subtítulos o marcar en negrita las del texto:

mejora el escaneado del texto,

el usuario capta más rápido la temática

aumenta el impacto del mensaje

los textos ganan visibilidad

Conviene escoger las palabras clave correctas, las que usen nuestros usuarios.

Los textos compactos no permiten escanear la información. Para romper la uniformidad del texto recurrir a los listados, enlaces, sangrados, dos puntos, alienación, ancho de línea, colores, negrita, etc.

Cuidar el formato de letra y contraste: evitar tipografía con serifa; evitar utilizar una fuente inferior a 10 puntos; utilizar suficiente contraste entre color de fondo y letra para poder leer sin forzar la vista.