

Conceptos Básicos de Seguridad Informática

- **Es imposible eliminar el riesgo**

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia, conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente independiente de las medidas que tomemos, por lo que debemos hablar de **niveles de seguridad**, la seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener **altos niveles de seguridad** en los sistemas informáticos.

- **Lo importante es proteger la información**

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la **confidencialidad**, la **integridad** y **disponibilidad** de la información.

- **Confidencialidad**

La confidencialidad o privacidad es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas" la interceptación o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

- **Integridad**

La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

- **Disponibilidad**

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

- **Otros problemas comunes**

Otros problemas importantes de seguridad son la **autenticación**, es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser; la **no repudiación**, o sea que alguien niegue haber enviado una determinada información (que

efectivamente envió) y los **controles de acceso**, esto es quien tiene autorización y quien no para acceder a una pieza de información determinada.

Finalmente se tiene el problema de la **verificación de la propiedad de la información**, es decir que una vez que se ha detectado un fraude determinar la procedencia de la información dolosa.

- **Desastres naturales y no intencionales**

No todos los riesgos que amenazan la información son de origen doloso. Es por ello que las medidas de seguridad no deben limitarse a la mera protección contra ataques e intrusiones de terceros, pues dentro de la misma organización y por parte de individuos de confianza existen riesgos contra la disponibilidad de la información ya sea por **negligencia, descuido, ignorancia** o cualquier otro tipo de mala práctica no dolosa la información puede ser alterada, sustituida o permanentemente borrada. Además están siempre presentes los riesgos de pérdida o alteración por virus o **situaciones fortuitas de fuerza mayor**, tales como incendios, inundaciones o catástrofes naturales.

- **Las técnicas de respaldo y los sistemas redundantes**

Los sistemas de respaldo (backup) y los sistemas redundantes son dos técnicas para proteger los datos contra pérdida por borrado accidental o desastres fortuitos, ambos sistemas son complementarios en cuanto a la seguridad que ofrecen ya que tanto los respaldos como la redundancia por si solos tienen problemas.

- **Redundancia: los sistemas RAID**

Un RAID (matriz redundante de discos económicos) es un conjunto de unidades de disco que aparecen lógicamente como si fueran uno solo. Así los datos, distribuidos en bandas, se dividen entre dos o más unidades. Esta técnica incrementa el rendimiento y proporciona una redundancia que protege contra el fallo de uno de los discos de la formación. Existen varios niveles RAID a partir del nivel 0, en el que los datos se dispersan en varias unidades pero no hay redundancia (más eficiencia, menos cero seguridad), luego el nivel 1 o **mirroring** (espejo) en el cual los datos se escriben duplicados en distintas unidades, este método no incrementa el rendimiento pero si la seguridad y es, de hecho uno de los más utilizados. Los demás niveles RAID son una combinación de los conceptos anteriores y buscan aumentar la seguridad y el rendimiento simultáneamente.

Existen sistemas operativos, que ofrecen administración RAID incorporada, como por ejemplo Windows NT que ofrece los niveles 0, 1 y 5. Como es obvio si se implementa el nivel 1 (discos espejo, donde todo lo que se escribe en un disco es duplicado automáticamente) , **la duplicación debe ser en un disco físico diferente.**

- **Tolerancia a fallos**

La tolerancia a fallos es la capacidad de un sistema a responder a un suceso inesperado, como puede ser una falla en el suministro eléctrico o una falla de hardware de forma que no se pierdan datos. Es importante notar que la redundancia **no protege** contra el borrado accidental, la operación negligente, etc. ya que cualquier operación (aún las erróneas) es automáticamente duplicada en todas las unidades. Así, la redundancia, junto con los sistemas de alimentación ininterrumpida (UPS y grupos electrógenos) proporciona seguridad solamente en caso de cortes de suministro o fallas de hardware.

- **Respallos (backup)**

Los respaldos consisten en copias efectuadas manual y periódicamente de la información que se desea proteger ¿cuál es el objeto de respaldar manualmente si tenemos un sistema redundante?, la ventaja de los respaldos es que por efectuarse según ciertos períodos la información respaldada no es exactamente igual a la actual. Esto permite cierta protección contra los errores humanos, borrado accidental o uso negligente ya que si nos damos cuenta a tiempo (esto es, **antes de que se respalde el error**) podremos recuperar los datos con cierto desfase de tiempo y solo será necesario actualizar ese desfase.

Hay multitud de técnicas de respaldo, las más recomendables son las que dejan dos desfases (diarios y semanales por ejemplo) ya que proporcionan cierta seguridad de que si se respaldó el error en el primer período aún nos queda un segundo para recuperar.

- **Virus y Troyanos**

Finalmente tenemos las amenazas de los virus y programas troyanos. Los mecanismos conocidos hasta el momento para la propagación de virus son los **archivos ejecutables** (con extensión .exe, .com o .bat) y los componentes de Microsoft Office que aceptan macros con el lenguaje Visual Basic para Aplicaciones (principalmente **Word y Excel con macros**). Los troyanos se propagan a través de archivos ejecutables. Así la única forma conocida en que un virus puede instalarse en un equipo es:

1. Ejecutando un programa infectado, ya sea directamente desde un diskette, bajado desde Internet o abierto desde un attach recibido por correo electrónico.
2. Abriendo un documento del Office 97 (o superior) teniendo deshabilitada o haciendo caso omiso a la alerta contra macrovirus habilitada por defecto en Office.

Es decir que las precauciones elementales contra la adquisición de un virus son:

1. No usar programas grabados en diskette (particularmente juegos o utilidades de procedencia desconocida).
2. No usar programas bajados de sitios poco confiables de Internet.
3. No abrir attach de correo electrónico cuyo contenido o remitente se desconozcan o no sean de confianza.

Universidad Nacional Abierta y a Distancia – UNAD - Vicerrectoría Académica y de Investigación - VIACI
Escuela: Ciencias Básicas Tecnología e Ingeniería Programa: Ingeniería de Sistemas

Licencia Creative Commons



Bibliografía

Página con conceptos básicos

<http://www.bradanovic.cl/pcasual/ayuda3.html>

PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

Costas Santos, Jesús. Seguridad informática. Madrid, ES: RA-MA Editorial, 2014.

<http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=16&docID=11038505&tm=1493089988568>

Conceptos básicos en materia de seguridad

Escrivá Gascó, Gema, Romero Serrano, Rosa María, and Ramada, David Jorge. Seguridad informática.

<http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=9&docID=10820963&tm=1493090650896>