INTRODUCCION A LA SEGURIDAD INFORMATICA

La seguridad informática es el área que trata de la protección completa de un sistema informático, como la protección del hardware, el software y los datos, en este OVI aprenderá los objetivos de la seguridad informática, los estándares, las normas de redes, los protocolos concebidos para minimizar y combatir los riesgos.

Hoy en día, las empresas tienen su sistema informático conectado a Internet para que le ayude en su proceso productivo y si se producen fallos de seguridad, las consecuencias pueden ser desastrosas para estas, bien por la pérdida de información o por el mal funcionamiento de los equipos.

Con unas **buenas políticas de seguridad, tanto físicas como lógicas**, conseguiremos que nuestros sistemas sean menos vulnerables a las distintas amenazas, pues nadie puede asegurar que un sistema sea cien por cien seguro, incluso hasta la seguridad de la NASA y del Pentágono han sido violadas por hackers en algún momento. Hay una lucha permanente entre los técnicos protectores de los sistemas informáticos y las personas que buscan rendimientos económicos fáciles, o simplemente su minuto de gloria al superar el reto de asomarse al otro lado de la barrera de protección.

Necesidad de un enfoque global

Frecuentemente, la seguridad de los sistemas de información es objeto de metáforas. A menudo, se la compara con una cadena, afirmándose que el nivel de seguridad de un menudo, se la compara con una cadena afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma manera forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas abiertas.

Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad a nivel global y que debe constar de los siguientes elementos:

- **Concienciar a los usuarios acerca de los problemas de seguridad**
- **Seguridad lógica**: es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.
- **Seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc.**
- **Seguridad física**, o la seguridad de infraestructuras materiales: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc.

Cómo implementar una política de seguridad

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una **política de seguridad** que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias.
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Es más, dado que el/la administrador/a es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concientización. Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente
- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

Las causas de inseguridad

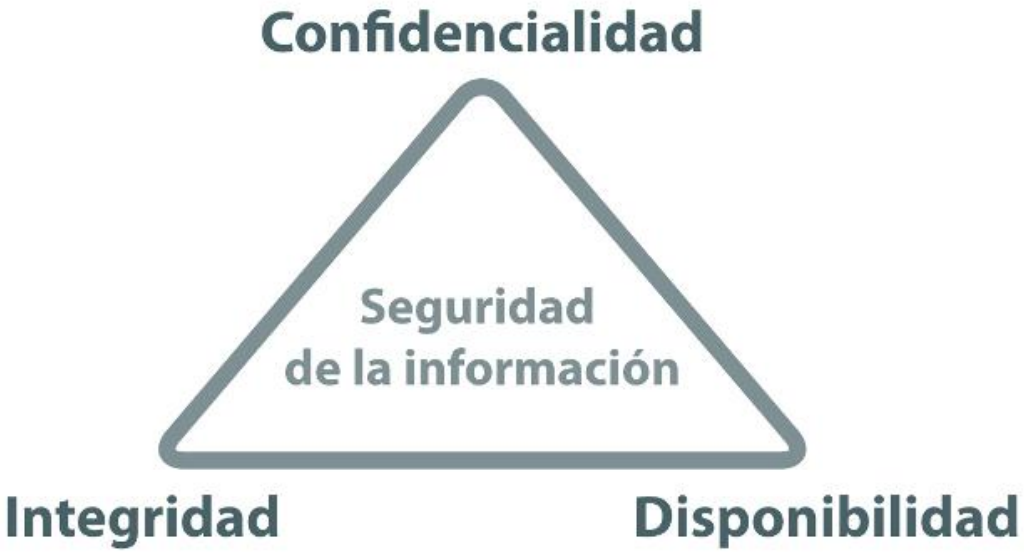
Generalmente, la inseguridad se puede dividir en dos categorías:

- **Un estado de inseguridad activo**; es decir, la falta de conocimiento del usuario sobre las funciones del sistema, algunas de las cuales pueden resultar perjudiciales para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita)
- **Un estado de inseguridad pasivo**; es decir, la falta de conocimiento de las medidas de seguridad disponibles (por ejemplo, cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan)

Objetivos de la seguridad informática

En seguridad se habla de niveles de seguridad ya que la seguridad absoluta no existe, siempre existirá el riesgo de que nuestro sistema informático sea atacado con éxito. Por lo tanto, lo que pretenderemos será aplicar políticas de seguridad que hagan que los sistemas sean lo más fiable posible, entendiendo por fiabilidad la probabilidad de que un sistema informático se comporte tal y como se espera de él.

Según el estándar ISO27002, la seguridad de la información se caracteriza por prevenir las actividades que atentan contra la: confidencialidad, integridad y disponibilidad.



La **confidencialidad** es la capacidad de garantizar que la información, almacenada en el sistema informático o transmitido por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos fueran sustraídos (por ejemplo, robo de un portátil de la empresa), estos no podrán ser interpretados.

La **disponibilidad** es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles en todo momento para los usuarios autorizados. Esto será muy importante, por ejemplo, para las empresas que dan servicios online.

La **integridad** es la capacidad de garantizar que los datos no serán alterados sin autorización. Por ejemplo, en una transmisión de información por red (transacción bancaria, compra online, etc.), los datos enviados en el origen, deberán ser los mismo que los recibidos en el destino.

Cada entorno de trabajo priorizará más unos objetivos u otros. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad. En cambio, en un servidor de archivos en red, se priorizará la disponibilidad frente a la confidencialidad. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo

REFERENCIAS BIBLIOGRAFICAS

- http://fpg.hol.es/Seguridad-Informatica-I/index.html
- http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica