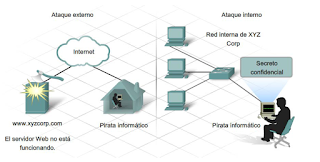
### Mecanismos de seguridad física y lógica: Control de acceso, respaldos, autenticación y elementos de protección perimetral

La seguridad física cubre todo lo referido a los equipos informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red. La seguridad lógica se refiere a las distintas aplicaciones que se ejecutan en cada uno de estos equipos.

Sin embargo, no todos los ataques internos son intencionales. En algunos casos la amenaza interna puede provenir de un empleado confiable que capta un virus o una amenaza de seguridad mientras se encuentra fuera de la compañía y, sin saberlo, lo lleva a la red interna.



La mayor parte de las compañías invierte recursos considerables para defenderse contra los ataques externos; sin embargo, la mayor parte de las amenazas son de origen interno. De acuerdo con el FBI, el acceso interno y la mala utilización de los sistemas de computación representan aproximadamente el 70% de los incidentes de violación de seguridad notificados.

No se pueden eliminar o evitar completamente los riesgos de seguridad. Sin embargo, tanto la administración como la evaluación efectiva de riesgos pueden minimizar significativamente los riesgos de seguridad existentes. Para minimizar los riesgos es importante comprender que no existe un único producto que pueda asegurar una organización. La verdadera seguridad de redes proviene de una combinación de productos y servicios junto con una política de seguridad exhaustiva y un compromiso de respetar esa política.

Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información. Puede ser tan simple como una política de uso aceptable o contener muchas páginas y detallar cada aspecto de conectividad de los usuarios, así como los procedimientos de uso de redes. La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Mientras que la mayoría de los usuarios domésticos no tiene una política de seguridad formal por escrito, a medida que una red crece en tamaño y en alcance, la importancia de una política de seguridad definida para todos los usuarios aumenta drásticamente. Algunos de los puntos que deben incluirse en una política de seguridad son: políticas de identificación y autenticación, políticas de contraseñas, políticas de uso aceptable, políticas de acceso remoto y procedimientos para el manejo de incidentes.

Cuando se desarrolla una política de seguridad es necesario que todos los usuarios de la red la cumplan y la sigan para que sea efectiva.

* Ø Políticas de identificación y autentificación
* Ø Políticas de contraseña
* Ø Políticas de usos aceptables
* Ø Políticas de acceso remoto
* Ø Procedimiento de mantenimiento de red
* Ø Procedimientos de administración de incidentes

La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Los procedimientos de seguridad implementan políticas de seguridad. Los procedimientos definen la configuración, el inicio de sesión, la auditoría y los procesos de mantenimiento de los hosts y dispositivos de red. Incluyen la utilización tanto de medidas preventivas para reducir el riesgo como de medidas activas acerca de la forma de manejar las amenazas de seguridad conocidas. Los procedimientos de seguridad abarcan desde tareas simples y poco costosas, como el mantenimiento de las versiones actualizadas de software, hasta implementaciones complejas de firewalls y sistemas de detección de intrusiones.

### Seguridad física, protección desde el interior



La mayoría de los expertos coinciden en que toda seguridad comienza con la seguridad física. El control del acceso físico a los equipos y a los puntos de conexión de red es posiblemente el aspecto más determinante de toda la seguridad. Cualquier tipo de acceso físico a un sitio interno deja expuesto el sitio a grandes riesgos. Si el acceso físico es posible, normalmente se pueden obtener archivos protegidos, contraseñas, certificados y todo tipo de datos. Por suerte, existen armarios seguros y dispositivos de control de acceso de muchas clases que pueden ayudar a combatir este problema. Para obtener más información sobre la seguridad física de los centros de datos y salas de red, consulte el Documento técnico de APC nº82, “Physical Security in Mission Critical Facilities” (“Seguridad física en instalaciones de misión crítica”).

### Entre los mecanismos de seguridad lógica tenemos:



El Control de Acceso a la Red, también conocido por las siglas NAC (Network Access Control ) / 802.1x tiene como objetivo asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información, etc.

El fenómeno BYOD (Bring Your Own Device) en el que los empleados utilizan sus propios dispositivos (tabletas, portátiles, smartphones) para acceder a los recursos corporativos está acelerando la adopción de las tecnologías NAC para autenticar al dispositivo y al usuario.

Existen una serie de fases como:

* Detección: es el hecho de detectar el intento de conexión física o inalámbrica a los recursos de red reconociendo si el mismo es un dispositivo autorizado o no.
* Cumplimiento: es la verificación de que el dispositivo cumple con los requisitos de seguridad establecidos como por ejemplo dispositivo autorizado, ubicación, usuario, antivirus actualizado.  
  Cuando un dispositivo no cumple los requerimientos se puede rechazar la conexión o bien mandarlo a un portal cautivo “Cuarentena”.
* Remediación: es la modificación lógica de dichos requisitos en el dispositivo que intenta conectarse a la red corporativa.
* Aceptación: es la entrada del dispositivo a los recursos de red en función del perfil del usuario y los permisos correspondientes a su perfil que residen en un servicio de directorio.
* Persistencia: es la vigilancia durante toda la conexión para evitar la vulneración de las políticas asignadas.

### Autentificación



Por autentificación entenderemos cualquier método que nos permita comprobar de manera segura alguna característica sobre un objeto. Dicha característica puede ser su origen, su integridad, su identidad, etc. Consideraremos tres grandes tipos dentro de los métodos de autentificación:

Ø Autentificación de mensaje. Queremos garantizar la procedencia de un mensaje conocido, de forma que podamos asegurarnos de que no es una falsificación. Este mecanismo se conoce habitualmente como firma digital.

Ø Autentificación de usuario mediante contraseña. En este caso se trata de garantizar la presencia de un usuario legal en el sistema. El usuario deberá poseer una contraseña secreta que le permita identificarse.

Ø Autentificación de dispositivo. Se trata de garantizar la presencia de un dispositivo válido.Este dispositivo puede estar solo o tratarse de una llave electrónica que sustituye a la contraseña para identificar a un usuario.

### Elementos de la seguridad perimetral



La seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Entre estos sistemas cabe destacar los radares tácticos, videosensores, vallas sensorizadas, cables sensores, barreras de microondas e infrarrojos, concertinas, etc.

Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de soportación (autosoportados, soportados, enterrados, detección visual, etc.).

También cabe destacar la clasificación dependiendo del medio de detección. En esta se clasificarían en:



- Sistemas Perimetrales Abiertos: Los que dependen de las condiciones ambientales para detectar. Como ejemplo de estos son la video vigilancia, las barreras infrarrojas, las barreras de microondas. Esta característica provoca falsas alarmas o falta de sensibilidad en condiciones ambientales adversas.



- Sistemas Perimetrales Cerrados: Los que no dependen del medio ambiente y controlan exclusivamente el parámetro de control. Como ejemplo de estos son los antiguos cables microfónicos, la fibra óptica y los piezo-sensores. Este tipo de sensores suelen ser de un coste mas elevado.

Ejemplos de cometidos de la seguridad perimetral:

Ø Rechazar conexiones a servicios comprometidos

Ø Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico) o entre ciertos nodos.

Ø Proporcionar un único punto de interconexión con el exterior

Ø Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet

Ø Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet

Ø Auditar el tráfico entre el exterior y el interior

Ø Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos...