Instituto Tecnológico Superior de Tacámbaro

Ingeniería en sistemas computacionales

Verificación Y Validación

Trabajo:

4.3 Políticas de seguridad

A L U M N A:

Nuñez Mendoza Anallely

P r o f e s o r a:

Nadia Ibeth Gutiérrez Hernández

A 01 de junio de 2017

Introducción

Sin importar si están conectadas por cable o de manera inalámbrica, las redes de computadoras cada vez se tornan más esenciales para las actividades diarias.

Convirtiéndose en una herramienta importante para que personas no autorizadas puedan acceder y realicen daños.

Para que exista un orden en las redes de computadoras están las políticas las cuales deciden quien tiene acceso y quien no, cuales son las privilegios que se tienen y además se deben de cumplir ciertos criterios a la hora de crear redes.

4.3 Políticas de seguridad.

La seguridad de red, generalmente, se basa en la limitación o el bloqueo de operaciones de sistemas remotos.

SEGURIDAD FÍSICA

Son aquellos mecanismos --generalmente de prevención y detección-- destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

A continuación mencionaremos algunos de los problemas de seguridad física con los que nos podemos enfrentar y las medidas que podemos tomar para evitarlos o al menos minimizar su impacto.

Problemas de seguridad física

Protección del hardware

El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

- Acceso físico
- Desastres naturales
- Alteraciones del entorno

SEGURIDAD PERIMETRAL

ELEMENTOS DE SEGURIDAD PERIMETRAL

SEGURIDAD LÓGICA

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

- CONTROLES DE ACCESO:

  Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

- **ROLES**

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc.

- **CONTROL DE ACCESO INTERNO**

Los controles de acceso interno determinan lo que un usuario (o grupo de usuarios puede o no hacer con los recursos del sistema.

- **CONTROL DE ACCESO EXTERNO**

Los controles de acceso externo son una protección contra la interacción de nuestro sistema con los sistemas, servicios y gente externa a la organización.

Conclusión

Existen algunas políticas de seguridad que se deben cumplir para que haya un buen funcionamiento de las redes y así estar lo mejor que se pueda.

El gran crecimiento que se tiene de las redes de computadoras ha sido mucho y por ello es que la seguridad también ha crecido a la par, día a día se trata de buscar la mejor forma para estar protegidos, pero al mismo tiempo, en cuanto sale algún software o hardware, algunas personas, mejor conocidas como piratas informáticos, encuentran esos puntos débiles, que usando su ingenio, crean programas para destapar esas debilidades que existen en ellas.

A pesar de todo esto, también hay herramientas de seguridad como los firewalls, los sistemas de protección como el kerberos, y la criptografia, que se van actualizando y tapan esos huecos que podían tener en sus versiones o generaciones anteriores, pero en si hay muchísimas herramientas de las cuales se pueden conseguir y usar.