Universidad Tecnológica de Tula - Tepeji

Noticias Tecnológicas

Seguridad Informática

Contenido:

La seguridad informática se enfoca a la protección de la infraestructura computacional, la información y todo lo relacionado con la misma.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas o leyes para minimizar los posibles daños. Protegiendo así la información, el software, las bases de datos, los archivos y todo lo que se considere importante para una empresa u organización.

Objetivos de la seguridad informática:

1.- Proteger la infraestructura computacional.

Cuidar que los equipos funcionen adecuadamente y prever en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

2.- Proteger la información.

La seguridad debe ser aplicada según los criterios establecidos por los administradores o supervisores. Evitar el acceso de usuarios no permitidos.

Otra función es asegurar el acceso oportuno a la información, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdidas por accidentes, atentados o desastres.

Se recomienda establecer normas que minimicen los riesgos de perdida de información y daños en infraestructura, *ocasionados por los propios usuarios*. Estas normas incluyen: horarios, restricciones, denegaciones, perfiles de usuario, contraseñas, planes de emergencia y todo lo necesario que permita un buen nivel de seguridad y funcionamiento.

Seguridad Informática

Tipos de amenazas:

Existen circunstancias **"no informáticas"** que pueden afectar la información, los cuales son imprevisibles o inevitables:

. Programas maliciosos: programas destinados a perjudicar o a hacer uso ilícito de los recursos del sistema, como lo son los virus.

. Siniestros: robos, incendios, inundaciones, terremotos, etc.

. Intrusos: personas que consigue acceder a los datos o programas sin permisos (cracker).

.Los usuarios: una mala manipulación de los equipos o mala intención de los usuarios también derivan la pérdida información. Así como la falta de conocimiento, imprudencias, descuidos, irresponsabilidad, etc.

"Lo que no está permitido, debe estar prohibido".

Análisis de riesgos.

Lo más importante para una organización es su información, por lo tanto deben de existir técnicas que la resguarden.

Por ejemplo:

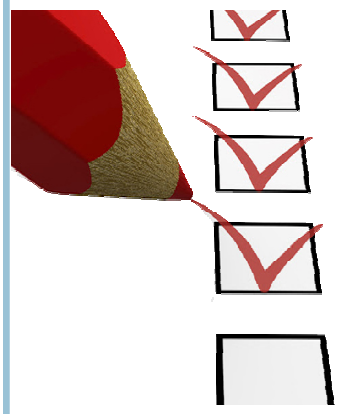
1. Restringir el acceso a los usuarios con claves y permisos.

2. Asegurar que los usuarios no modifiquen información que no les corresponda.

3. Asegurar que se utilicen los datos, archivos y programas correctos.

4. Asegurar que existan sistemas de emergencia alternativos como lo son sistemas automáticos de respaldos, planta de luz, nobreak, etc.

6. Actualizar constantemente las contraseñas de acceso a los sistemas.



Reglas básicas de seguridad informática.

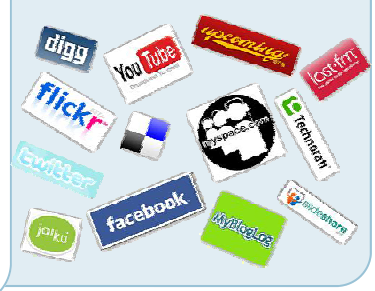
· **Sistema Operativo:** De forma periódica actualizar el Sistema Operativo y sus aplicaciones. Estas actualizaciones solucionan desde pequeños defectos hasta graves problemas de seguridad. Es sencillo hacerlo dirigiéndose a la página web del fabricante, se recomienda activar las actualizaciones automáticas para poder recibir los parches de seguridad de forma automática. Borrar archivos temporales.

Seguridad Informática

- **Antivirus:** Se recomienda instalar solo un Antivirus así como un Anti-Spam en su ordenador, actualizarlo semanalmente, y analizar las unidades locales y externas periódicamente.
- **Copias de seguridad:** Hágalas con regularidad, ya sea en CD-ROM o DVD. Una copia de seguridad reciente le permitirá recuperarse del ataque.
- **Software:** Limite el número de aplicaciones en su computadora y desinstalar el software innecesario, ya que consume recursos de espacio y memoria.
- **Navegación en Internet:** Se recomienda: no acceder a sitios dudosos, evitar los enlaces sospechosos, evitar el ingreso de información personal y financiera en formularios, asegúrese de que la barra de direcciones muestra la dirección exacta, no utilizar tarjeta de débito para sus compras on-line, aceptar sólo contactos conocidos, utilizar contraseñas fuertes, no ejecutar archivos .exe o sospechosos, no abrir enlaces engañosos de premios y/o regalos, configure su navegador para que se borren las cookies y archivos temporales .

- **Contraseñas:** Nunca teclee una contraseña importante, como la de su cuenta bancaria, en formularios de una página web. Cree contraseñas fuertes usando: Letras en minúsculas (de la **a** a la **z**), Letras en mayúsculas (de la **A** a la **Z**), Números (del **0** al **9**) y Caracteres especiales (por ej. !, $, #, o %).
- **Correo electrónico:** Borre el correo basura (spam), sin leerlo. No abra mensajes con ficheros adjuntos y bórrelos de inmediato. Usar contraseñas seguras y cambiarlas periódicamente. Evitar las cadenas.
- **Firewall:** Utilice software de cortafuegos personal. Si puede, oculte su dirección IP.

- **Redes Sociales:** Restringir la información personal en tu perfil, usar nick o apodo para no usar tu nombre verdadero, seleccionar la información que es privada y las fotos a mostrar, valora las solicitudes de amistad que vas aceptar, denunciar cualquier tipo de acoso.
- **Red LAN:** No compartir carpetas con acceso total solo con permisos de usuario, ocultar las carpetas compartidas.
- **Generales:** Antes de manipular los componentes internos de una computadora (memoria Ram), debe descargar la estática tocando algo metálico, usar regulador de voltaje, realizar mantenimiento interno y externo por la acumulación de polvo, revisar la temperatura de los componentes del equipo, desfragmentar periódicamente los disco duros, es responsabilidad del usuario final la instalación de software y hardware y sus consecuencias para efectos de garantía, apague su ordenador cuando no lo esté utilizando, sobre todo si dispone de una conexión permanente a Internet.



Universidad Tecnológica de Tula - Tepeji

Avenida Universidad Tecnológica No. 1000
Col. El 61, El Carmen
Tula de Allende, Hgo.
C.P. 42830
Tel: 01-773-732-91-00
Ext. 122 y 123
Fax: 01-773-732-12-14

e-mail institucional: uttt@uttt.edu.mx
e-mail de soporte: soporte@uttt.edu.mx

www.uttt.edu.mx

De la Cultura y la Ciencia, Crearemos El Futuro.