

EL ABC DE LA SEGURIDAD

Amenaza: Individuo, entidad o situación que aprovecha una vulnerabilidad.

Antivirus: Son todos aquellos programas que identifican, detienen y eliminan virus. Asimismo, permiten analizar las unidades de disco y otros elementos de una computadora en busca de virus.

Atacante: Persona interesada en vulnerar la seguridad de un sistema.

Código malicioso: Programa que es instalado intencionalmente en un sistema con un fin no autorizado. Su instalación puede tener como objetivo:

- Extenderse por otras computadoras en una red o por internet.
- Robar información y claves.
- Eliminar archivos e incluso formatear el disco duro.
- Mostrar publicidad invasiva.

Confidencialidad: Propiedad de los datos que asegura que estos sean conocidos únicamente por personas y procesos autorizados.

Cookie: Son archivos de texto que se crean cada vez que se visita una página web. Estos archivos contienen información relacionada con las actividades realizadas en un sitio web.

Contraseña: Clave de acceso necesaria para que una persona ingrese a un servicio, sistema o aplicación. También conocida como password por su traducción al inglés.

Control de acceso: Mecanismos, controles y métodos para limitar el acceso a los recursos a sujetos autorizados.

Dirección IP: Es la dirección con que se identifica un equipo de cómputo conectado a una red (por ejemplo Internet). Consta de 4 números separados por puntos y cada uno es menor de 256. Por ejemplo: 192.200.44.69.

Disponibilidad: Propiedad de los datos, información y sistemas de información que asegura su acceso y uso en tiempo y forma requeridos.

DNS (Sistema de Nombres de Dominio): Método para resolver el nombre de un equipo de cómputo a una dirección IP. Los equipos de cómputo en la red se identifican a través de sus direcciones IP.

Firewall: Es un mecanismo de protección utilizado para establecer un control de acceso entre internet y un equipo de cómputo. Funciona a través de políticas de seguridad y cuando un programa o código malicioso trata de acceder a un equipo de cómputo este mecanismo lo detendrá y evitará su acceso.

Información: Es todo hecho, dato, u opinión o conjunto de ellos que se relacionan en un orden lógico y que identifican, simbolizan o representan una realidad, propósitos, postulados y funcionamiento de una entidad.

Integridad: Propiedad de los datos e información que asegura que estos estén completos y sean exactos.

ISP (Internet Service Provider): Es el proveedor de acceso a Internet. En México los proveedores más conocidos son Telmex, Axtel o Avantel.

EL ABC DE LA SEGURIDAD

Malware: Es un código malicioso que permanece inactivo hasta que es activado por un evento que realiza un usuario, sistema o aplicación.

No repudio: Propiedad automatizada de aceptación y confirmación de quien realiza una transacción.

Actualización de seguridad: Archivos adicionales que sirven para solucionar las posibles carencias, vulnerabilidades o defectos de funcionamiento de un software, sistema o aplicación.

PIN: Es el número secreto que se proporciona al usuario de un servicio a fin de probar su identidad.

Riesgo: Probabilidad de que una amenaza explote una vulnerabilidad.

URL (Uniform Resource Locator): Dirección a través de la cual se accede a las páginas Web en Internet (o a otras computadoras).

Virus: Un virus es una pequeña aplicación o una cadena de código que infecta sistemas o aplicaciones produciendo efectos molestos, nocivos e incluso destructivos e irreparables.