



Algunos consejos sobre seguridad Informática

En el año 1988, la Association for Computing Machinery (ACM) declaró al 30 de Noviembre como el “Día Internacional de la Seguridad Informática” y en su conmemoración, el INPI se ha sumado a la iniciativa promovida por Secretaría de Gabinete, con el objetivo de **concientizar respecto de las amenazas que atentan contra la seguridad de la información.**

Consejos para la Oficina

Utilice contraseñas siempre y cámbielas periódicamente, estas deben tener por lo menos 7 caracteres y han de incluir símbolos números y letras, esto hará que sea más difícil de descifrar, por métodos como la fuerza bruta. También podemos tomar la previsión de no guardar las contraseñas en nuestro navegador que puede ser muy cómodo a la hora de acceder a las cuentas de correo, por ejemplo, pero que pueden ser usados por algún virus para auto enviarse usando nuestro mail.

Consejos para el Hogar

Revisemos el Windows y Office update para estar al día con las actualizaciones sobre fallos de seguridad. Podemos configurar nuestras actualizaciones de seguridad para que sean automáticas.

Instalemos algún Firewall (filtro de paquetes y aplicaciones de internet) personal como ZoneAlarm este en este caso ofrece versiones gratuitas.

Instale un bloqueador de Spyware gratuito. Como Spybot Search & Destroy. Manténgalo actualizado por lo menos una vez a la semana.

Si usamos Outlook o Outlook Express, use las versiones actuales o busque actualizaciones en Office Update. Verifiquemos que nuestro antivirus este configurado para revisar el correo saliente y entrante.

Instale antivirus hay versiones gratuitas del software , manténgalo actualizado o configúrelo de manera que se actualice automáticamente tanto el programa como la base de datos de virus. Podemos usar algunos servicios de escaneo gratuitos en línea

Algunas Definiciones

(programa maligno). Cualquier programa creado con intenciones de molestar, dañar o sacar provecho en las computadoras infectadas.

Programas Espias

En informática, pequeño software que, al igual que un virus biológico, infecta a una computadora y se propaga en ella con diversos propósitos como daño, robo de información, molestia, etc. y por lo general intenta pasar desapercibido por el usuario el mayor tiempo posible. Los virus se incluyen dentro de los malwares (programas malignos).

El contagio por un virus suele producirlo el mismo usuario al ejecutar un programa que está infectado y toma los servicios básicos del sistema operativo para lograr sus objetivos. Suele quedar residente en memoria.

Malware: worm en inglés. En informática, tipo de virus que se autoréplica, residiendo en memoria.

Existen dos variantes de gusanos. Los que comienzan a consumir los recursos de la computadora por su incontrolada replicación de sí mismos, afectando el rendimiento o produciendo bloqueos del sistema.

Y la otra variante más actual en donde los gusanos suelen usar la red conectada a la computadora infectada para autoreplicarse enviando copias de sí mismo a otros nodos. A diferencia de los virus, no necesitan adjuntarse a programas existentes para funcionar.

Existen distintos tipos de gusanos:

Gusanos de emails, gusanos de IRC, gusanos de mensajeros instantáneos, gusanos de redes de intercambio de archivos, gusanos de internet en general. El objetivo de los gusanos puede ser desde la simple replicación, o hacer propagandas, colapsar una red, etc.

Phishing es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. El objetivo más común, suele ser la obtención de dinero del usuario que cae en la trampa. Por lo general, el engaño se basa en la ignorancia del usuario al ingresar a un sitio que presume legal o auténtico.

El spamming es el abuso de cualquier tipo de sistema de mensajes electrónicos y, por extensión, cualquier forma de abuso en otros medios como spam en mensajería instantánea, en foros, en blogs, en buscadores, en mensajes en teléfonos móviles, etc.