INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

CONSEJOS GENERALES DE SEGURIDAD

Julio 2007

SIEMPRE:

1. **Manténgase informado** sobre las novedades y alertas de seguridad.
2. **Mantenga actualizado su equipo,** tanto el Sistema Operativo como cualquier aplicación que tenga instalada.
3. **Haga copias de seguridad** con cierta frecuencia, para evitar la pérdida de datos importante.
4. **Utilice software legal** que le suelen ofrecer garantía y soporte.
5. **Utilice contraseñas fuertes** en todos los servicios, para dificultar la suplantación de su usuario (evite nombres, fechas, datos conocidos o deducibles, etc.).
6. **Utilice herramientas de seguridad** que le ayudan a proteger / reparar su equipo frente a las amenazas de la Red.
7. **Cree diferentes usuarios**, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas

Correo electrónico:

1. **No abra ficheros adjuntos sospechosos** procedentes de desconocidos o que no haya solicitado.
2. **Utilice un filtro anti-spam** para evitar la recepción de correo basura.
3. **Analice los anexos con un antivirus** antes de ejecutarlos en su sistema.
4. **Desactive la vista previa de su cliente de correo** para evitar código malicioso incluido en el cuerpo de los mensajes.
5. **No facilite su cuenta de correo** a desconocidos ni la publique *'alegramente'*.
6. **No responda a mensajes falsos,** ni a cadenas de correos para evitar que su dirección se difunda.
7. **Borre el historial de destinatarios** cuando reenvíe mensajes a múltiples direcciones

Navegación:

1. **No descargue/ejecute ficheros desde sitios sospechosos** porque pueden contener código potencialmente malicioso.

2. **Analice con un antivirus todo lo que descarga** antes de ejecutarlo en su equipo.

3. **Mantenga actualizado su navegador** para que este protegido frente a vulnerabilidades con parche conocido.

4. **Configure el nivel de seguridad de su navegador** según sus preferencias.

5. **Instale un cortafuegos** que impida accesos no deseados a / desde Internet.

6. **Descargue los programas desde los sitios oficiales** para evitar suplantaciones maliciosas.

7. **Utilice *anti-dialers* si navega con RTB o RDSI** para evitar conectarse a Internet a través de números de tarificación adicional, que incrementarían su factura.

8. **Puede utilizar mata-emergentes** para eliminar las molestas ventanas emergentes (*pop-up*) que aparecen durante la navegación, o configurar su navegador para evitar estas ventanas.

9. **Utilice un usuario sin permisos de Administrador** para navegar por Internet, así impide la instalación de programas y cambios en los valores del sistema.

10. **Borre las cookies, los ficheros temporales y el historial cuando utilice equipos ajenos** (públicos o de otras personas) para no dejar rastro de su navegación.

Banca en línea / Comercio electrónico:

1. **Observe que la dirección comienza por http<u>S</u>** que indica que se trata de una conexión segura.

2. **Observe que aparece un *candado*** ( ) en la parte inferior derecha de su navegador.

3. **Asegúrese de la validez de los certificados** (pulsando en el *candado*), que coinciden con la entidad solicitada y sean vigentes y válidos.

4. **Tenga en cuenta que su banco NUNCA le pedirá información confidencial** por correo electrónico ni por teléfono.

5. **Evite el uso de equipos públicos** (cibercafés, estaciones o aeropuertos, etc) para realizar transacciones comerciales.

6. **Desactive la opción 'autocompletar'** si accede desde un equipo distinto al habitual o comparte su equipo con otras personas.

7. **Cierre su sesión cuando acabe,** para evitar que alguien pueda acceder a sus últimos movimientos, cambiar sus claves, hacer transferencias, etc.

8. **Instale alguna herramienta de antifraude** para evitar acceder a páginas fraudulentas.

Chat / Mensajería instantánea:

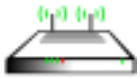
1. **Evite invitaciones a visitar sitios web** que le resulten sospechosas o que procedan de desconocidos.

2. **Rechace ficheros adjuntos** que no haya solicitado o que le parezcan sospechosos.

3. **Tenga precaución al conversar o agregar contactos** desconocidos.

4. **No facilite datos confidenciales** (contraseñas, nombres de usuario, datos bancarios, etc.) a través de estos canales.

5. **Rechace los usuarios 'no deseados',** de los que no quiera recibir mensajes.



Wi-fi:

1. **Fije un número máximo de equipos** que se puedan conectar al punto de acceso.
2. **Apague el punto de acceso** cuando no vaya a utilizarlo.
3. **Desactive la difusión de su SSID** (nombre de su red wifi) para evitar que equipos externos identifiquen automáticamente los datos de su red inalámbrica.
4. **Active el filtrado por dirección MAC** para que sólo los dispositivos permitidos tengan acceso a la red.
5. **Cambie la contraseña por defecto** ya que muchos fabricantes utilizan la misma clave para todos sus equipos.
6. **Utilice encriptación** WPA (o WEP si su sistema no permite la primera), para impedir que el tráfico de red sea fácilmente legible. Se recomienda WPA ya que WEP es inseguro.
7. **Desactive la asignación dinámica de IP (DHCP)** a nuevos dispositivos que se quieran conectar a la red, haciéndose necesaria la asignación manual de las IPs.

Equipos portátiles:

1. **No deje el portátil desatendido en lugares públicos** para evitar que sea sustraído.
2. **Utilice un candado físico** para anclar el portátil cuando vaya a ausentarse temporalmente.
3. **Cifre el contenido** del portátil para evitar el acceso a los datos si el equipo es robado.
4. **Elimine datos innecesarios** que puedan estar almacenados en el portátil.

Dispositivos móviles:

1. **Desactive el bluetooth o infrarrojos** mientras no los vaya a utilizar.
2. **Configure el dispositivo en modo oculto**, para que no pueda ser descubierto por atacantes.
3. **No acepte conexiones de dispositivos que no conozca** para evitar transferencias de contenidos no deseados.
4. **Instale un antivirus y manténgalo actualizado** para protegerse frente al código malicioso.
5. **Ignore / borre SMS o MMS de origen desconocido** que inducen a descargas o accesos a sitios potencialmente peligrosos.
6. **Active el acceso mediante PIN** (al bluetooth y al móvil) para que sólo quién conozca este código pueda acceder a las funcionalidades del dispositivo.
7. **Bloquee la tarjeta SIM en caso de pérdida** para evitar que terceros carguen gastos a su cuenta.
8. **No descargue software de sitios poco fiables o sospechosos** para impedir la entrada por esta vía de códigos potencialmente maliciosos.
9. **Lea los acuerdos de usuario del Sw que instala** por si se advierte de la instalación de componentes no deseados (software espía).

Juegos en línea:

1. **Evite compartir usuario / contraseña** tanto dentro como fuera de la plataforma del juego.
2. **Actualice el software del juego** para evitar fallos de seguridad conocidos.
3. **No adquiera créditos en páginas de subastas en línea** sin que estén certificados por los creadores del juego.
4. **Vigile los movimientos de su cuenta/tarjeta bancaria** si la tiene asociada al juego, para detectar movimientos ilícitos.
5. **Controle su tiempo de juego** ya que esta actividad pueden ser muy adictivo

Internet y los menores:

1. **Eduque al menor** sobre los posibles peligros que puede encontrar en la Red.
2. **Acompañe al menor en la navegación** cuando sea posible, sin invadir su intimidad.
3. **Advierta al menor de los problemas de facilitar información personal** (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.
4. **Desaconséjele participar en charlas radicales** (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.
5. **Infórmele de que no todo lo que sale en Internet tiene que ser cierto,** ya que pueden ser llevados a engaño con facilidad.
6. **Preste atención a sus 'ciber-amistades'** en la misma media que lo hace con sus amistades en la vida real.
7. **Pídale que le informe** de cualquier conducta o contacto que le resulte incómodo o sospechoso.
8. **Vigile el tiempo de conexión** del menor a Internet para evitar que desatienda otras actividades.
9. **Utilice herramientas de control parental** que le ayudan en el filtrado de los contenidos accesibles por los menores.
10. **Cree una cuenta de usuario limitado** para el acceso del menor al sistema.

Redes P2P:

1. **Analice todos los archivos** que se descargue a través de las redes de intercambio de ficheros.
2. **No comparta software ilegal** ya que incurriría en un delito.
3. **Ejecute el cliente P2P en una sesión de usuario con permisos limitados** para aislarlo de otros componentes críticos del sistema.
4. **Modifique el nombre de las carpetas de descarga** ya que muchos códigos maliciosos buscan rutas fijas para replicarse.
5. **Preste atención a la extensión de los ficheros que descarga**, podrían indicar amenazas (por ejemplo, una imagen nunca tendrá extensión .exe).