Nota Informativa

Con motivo de la celebración del Día de Internet

La Agencia Española de Protección de Datos publica una nueva Guía de Recomendaciones a Usuarios de Internet

● La AEPD es miembro del Comité de Impulso del Día de Internet

● En la Guía se analizan los principales riesgos que aparecen actualmente en la Red y se enumeran algunas recomendaciones para tratar de prevenir sus efectos

● Las normas en materia de Telecomunicaciones y Servicios de la Sociedad de la Información atribuyen a la Agencia la tutela de los derechos y garantías de usuarios en el ámbito de las comunicaciones electrónicas

(**Madrid, 16 de mayo de 2006).** Mañana **miércoles 17 de mayo** se celebra **en España la II edición del Día de Internet, una iniciativa que tiene como** objetivo **difundir y promover el uso de Internet** en toda la Sociedad y conseguir que Internet sea cada vez más accesible para las personas que tienen alguna discapacidad.

Para la **Agencia Española de Protección de Datos (**AEPD), que forma parte **del Comité de Impulso** de dicha celebración, las nuevas tecnologías de las telecomunicaciones **son elemento imprescindible en desarrollo de la sociedad actual**, y por ello resulta prioritario crear un **entorno de confianza** para el empleo de Internet y generar en el ciudadano una **cultura para la protección de sus datos en el entorno digital de la Sociedad de la Información**, de la que dependerá que cada persona pueda hacer un uso seguro de Internet.

Con este objetivo, y sumándose a las iniciativas puestas en marcha con motivo del Día de Internet a nivel mundial, la **Agencia Española de Protección de Datos ha elaborado una nueva Guía de Recomendaciones a Usuarios de Internet.** La publicación, cuyo contenido íntegro estará disponible a partir mañana en la página Web de la Agencia (www.agpd.es), está **estructurada en 11 apartados** en los que se **analizan los principales riesgos que aparecen actualmente en la Red y se enumeran algunas recomendaciones para tratar de prevenir sus efectos**. De ellas podemos destacar:

- **Navegación por Internet.**

● Es conveniente la utilización y actualización periódica de "software antivirus" y de seguridad específicos, así como configurar el software del navegador con las opciones de seguridad más restrictivas.
● El intercambio y la entrega de datos de carácter personal deberá efectuarse en los sitios web que dispongan de protocolos seguros y de política de privacidad.
● El equipo debe protegerse mediante contraseña, impidiendo con ello los inicios de sesión y accesos no autorizados.

● Debe asegurarse la confianza o acreditación de los sitios web antes de proceder a la descarga de archivos.

-Correo electrónico

● Usar de forma cuidadosa su dirección de correo electrónico.
● Mantener actualizados su sistema operativo, programa de correo y antivirus.
● No proporcione su dirección de correo electrónico si no está seguro de las intenciones de aquel que se la requiere y evite difundir cuando no sea necesario las direcciones de correo electrónico de otras personas de las que disponga.
● No reenviar mensajes sin haber comprobado de forma previa que no representan un riesgo potencial para sus destinatarios. No siga los mensajes en cadena.
● Solicitar información y seguir las limitaciones de uso de las cuentas de correo que utilice en el marco de sus relaciones laborales o profesionales.

-Virus, gusanos y ataques de Ingeniería Social.

● Sea cuidadoso con los programas que instala.
● Añada programas "cortafuegos" y de detección y eliminación de "software espía".
● No proporcione información sobre sus identificadores de usuario y mucho menos sobre sus claves de acceso.
● Adopte sistemas adicionales de seguridad en el acceso a sus cuentas de servicio.

-Comercio y Banca electrónica.

● Antes de aportar ningún tipo de datos personales debemos aseguramos que se ha establecido una conexión segura con el portal.
● El mejor procedimiento para identificar nuestra identidad es utilizar certificados digitales. El DNI electrónico cumple con todos los requisitos de seguridad para autenticar nuestra identidad en Internet.
● Desconfiar de los correos electrónicos que informan de cambios políticas de seguridad y solicitan datos personales y claves de acceso.
● No dejar desatendido el ordenador mientras está conectado.
● Es conveniente mantener el anonimato en los formularios de petición de datos de sitios web excepto cuando sea imprescindible el aportar datos personales para obtener un servicio.

-Servicios de mensajería instantánea y chats.
● El "Nick" no debe proporcionar información personal.
● No facilitar datos que puedan afectar a nuestra intimidad, nombres de pantalla, direcciones de correo electrónico, etc a interlocutores no conocidos.
● No abrir ficheros ni ejecutar programas adjuntos a un mensaje no solicitado o procedentes de remitentes desconocidos.

-Uso de Internet por menores.

● Los menores deben acceder al equipo a través de cuentas de usuario limitadas o restringidas.
● Los menores deben ser informados acerca de los peligros en el uso de Internet, advirtiéndoles de que no compartan o faciliten información desconocidos, que no abran los

ficheros adjuntos en los mensajes de correo electrónico y que eviten la descarga de archivos o programas.
● Los menores deben acceder a Internet a través de entornos personalizados, pudiendo utilizarse para la navegación software de filtrado de páginas de contenido no adecuado y que permita la elaboración de informes de actividad de sitios visitados.
● Deberá utilizarse software que permita el bloqueo de las ventanas emergentes.
● Los menores deberán utilizar las salas de Chat que dispongan de moderador o supervisor.
● Los menores deberán ser informados adecuadamente cuando se recaben datos sobre su persona

-Los servicios de llamadas a través de Internet utilizando el protocolo IP, también conocida como telefonía IP o VoIP.

● Actualmente la VoIP no sustituye al teléfono tradicional ni a la telefonía móvil tradicional, ya que no están asegurados ni el secreto de las comunicaciones ni los servicios básicos.
● Vigile los ficheros e imágenes transmitidos durante las conversaciones.

-Las Redes entre iguales de intercambio de ficheros, también conocidas como Peer to Peer

● Es conveniente la instalación de un "cortafuegos" que proteja el acceso no deseado al propio ordenador.
● Es preferible no descargar programas ejecutables o ficheros que sean susceptibles de contener "software malicioso".
● No instale el "software servidor", a no ser que esté absolutamente seguro de lo que hace.

Garantía de los derechos de los usuarios por parte de la AEPD

La AEPD es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos. **Las normas en materia de Telecomunicaciones y Servicios de la Sociedad de la Información atribuyen a la Agencia** la tutela de los derechos y garantías de usuarios en el ámbito de las comunicaciones electrónicas. Entre ellas, la defensa de la privacidad de los usuarios de Internet frente al Spam**.**