Datuak Babesteko
Euskal Bulegoa

Agencia Vasca de
Protección de Datos

"Privacidad y seguridad en Internet y en la web social" (AVPD. Diario de noticias de Gipuzkoa, "Internet Eskola" 25 oct. 2009)

Las Tecnologías de la Información y la Comunicación, y particularmente la Web social, basada en comunidades de usuarios que se comunican a través de las redes sociales, blogs, wikis, etc., además de ser espacios para expresar nuestras opiniones y, por tanto, un espacio de libertad, pueden constituir un riesgo para la privacidad de las personas. Y esto porque las redes sociales constituyen una gran acumulación de información personal y, además, son básicamente redes de desconocidos, debido a que permiten ampliar progresivamente el número de contactos de cada usuario ya que establecen, por defecto, la accesibilidad para los amigos de tus amigos. Estos riesgos pueden tomar la forma de una excesiva intrusión en la vida privada (difusión de grabaciones o publicidad no consentidas) o de daños a la intimidad y a la reputación, a través de comentarios, invención de historias, creación de perfiles falsos, suplantación de personalidad, etiquetado de fotos, etc., y, cada vez con mayor frecuencia, a través del cyberbullying o acoso a través de las tecnologías de la información. Si un usuario desea que un comentario o una fotografía sean retiradas de la red social, debe solicitarlo a los responsables de la misma, ejerciendo así el derecho de cancelación. En caso de que considere que sus derechos han sido vulnerados puede denunciar los hechos en la Agencia de Protección de Datos. Sin embargo, es un error creer que se puede mantener un control de los datos y opiniones personales que se incorporan en Internet, ya que es muy difícil cancelarlos o eliminarlos totalmente. Por estas razones, la Agencia Vasca de Protección de Datos (AVPD) considera necesario concienciar a las personas acerca de la importancia del respeto a la vida privada, y por ello ha puesto a disposición de la ciudadanía algunos recursos educativos. En concreto, ha editado un video titulado ***Las Luces funcionan*** (AVPD, 2008) y ha desarrollado un **campaña educativa** dirigida a la población escolar. A pesar de los riesgos a la vida privada y a la dignidad, nadie va a renunciar a Internet. En consecuencia, se trata de minimizar los riesgos adoptando medidas preventivas. A continuación se resumen algunas **recomendaciones** a partir de diversas publicaciones de la Agencia Española de Protección de Datos, del Instituto Nacional de Tecnologías de la Comunicación y de la consultora S21sec:

La responsabilidad de los internautas como editores de contenidos. Lo adecuado es limitar la información que cada persona hace pública acerca de una misma, evitando datos, imágenes o videos comprometedores que puedan afectar la vida personal o profesional presente o futura. Asimismo, no publicar información de otras personas -por ejemplo, fotos- sin su autorización. Tener especial cuidado con la información sobre lugares, planes o viajes, pues puede facilitar un robo en el domicilio.

Uso del correo electrónico sin difundir direcciones electrónicas de otras personas. Para ello, utilice el campo "con copia oculta (CCO)".

Uso de seudónimos o nicks para crear una identidad digital. Así únicamente será conocido por su círculo de contactos.

Leer la política de privacidad antes de registrarse como usuario y configurar el grado de privacidad del perfil de usuario de la red social.

Aceptar como contacto en su lista de amigos de una red social sólo a personas conocidas.

No indicar en una red social datos personales que faciliten su búsqueda (dónde vive, trabaja o estudia, lugares que frecuenta, etc.).

Especiales medidas para proteger a los menores de edad. Instalar un bloqueador de contenidos y asegurarse de que el menor sólo accede a las páginas recomendadas para su edad. Si es menor de catorce años, se necesita el consentimiento de los padres o tutores para registrarse en una red social. Explicar a los menores los riesgos y las medidas de seguridad, asegurándose de que no utilicen su nombre completo ni información personal.

Utilizar contraseñas difíciles de adivinar. Un mínimo de ocho caracteres alfanuméricos con mayúsculas y minúsculas.

Seguridad en el Comercio y Banca Electrónicas. Es necesario asegurarse de que se ha establecido una conexión segura con el portal. Se ha de desconfiar de los correos electrónicos, supuestamente del banco, que informan de cambios en las políticas de seguridad y solicitan datos personales y claves de acceso.

Borrar con regularidad los cookies y el historial de los buscadores de información como google, yahoo, etc. Así evitará que le envíen publicidad personalizada.

Instalar software antivirus y programas cortafuegos. Éstos últimos le protegen del acceso no deseado al ordenador.