Diputació de València | Protecció de Dades i Seguretat de la Informació

Boletín Protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 39| Septiembre 2023

RECOMENDACIONES DE SEGURIDAD EN INTERNET

ÍNDICE

RECOMENDACIONES DE SEGURIDAD EN INTERNET

INTRODUCCIÓN.....2
RECOMENDACIONES DE SEGURIDAD EN INTERNET 3
NOTICIAS 11

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

Internet y los servicios que a través de ella se prestan se han convertido en un elemento imprescindible para nuestras vidas.

Además, la explosión de la conectividad mediante el uso masivo de dispositivos móviles inteligentes, especialmente, los *smartphones*, y redes de datos móviles cada vez más rápidas, hace que todos estos servicios se puedan consumir en cualquier lugar y a cualquier hora del día o de la noche, por lo que podemos hablar de "personas conectadas" más que de dispositivos y ordenadores conectados.

Los servicios más usados en la red se prestan gracias a la cantidad de información y datos personales que los usuarios aportamos, tanto a las empresas que ofrecen los servicios como a otros usuarios, por lo que debemos ser conscientes de los riesgos que esto puede suponer para nuestra seguridad y privacidad.

El objetivo de este boletín es promover el uso seguro y responsable de Internet, explicando los riesgos a los que estamos expuestos y proporcionando las pautas necesarias para sacar partido a los servicios sin comprometer nuestra seguridad y privacidad. De este modo, nos servirá también de concienciación para el uso de Internet en nuestro centro de trabajo, los cuales, cada vez son más objetivo de la ciberdelincuencia.

RECOMENDACIONES DE SEGURIDAD EN INTERNET

1. ALMACENAMIENTO DE INFORMACION PRIVADA EN DISPOSITIVOS

Uno de los principales motivos para proteger nuestros dispositivos móviles es salvaguardar nuestra información personal y la de aquellas personas con las que nos comunicamos: contactos, fotografías, vídeos, correos electrónicos, etc.,

CONSEJOS Y RECOMENDACIONES

El riesgo de pérdida o robo siempre va a existir, por tanto, ten en cuenta las siguientes recomendaciones:

- Utiliza un método de bloqueo de la pantalla (código numérico o patrón) y cifra la información para que, si esta situación se produce, dificultes el acceso a la persona que acabe con el dispositivo en sus manos.
- Haz uso de herramientas de seguridad que te ayudarán a localizar el dispositivo, bloquearlo e incluso eliminar la información almacenada en él.
- Realiza copias de seguridad en otro soporte para que, pase lo que pase, no pierdas la información almacenada en el móvil o tableta.

En el dispositivo, sólo dispón de aplicaciones seguras:

- Descargas únicamente a través de las tiendas de aplicaciones (apps) oficiales.
- Revisa previamente la valoración y los comentarios que los usuarios han hecho sobre una determinada app. Cuando se comporta mal o de manera sospechosa, los propios usuarios se encargan de reflejarlo en los comentarios.
- Instala una herramienta antivirus para que detecte posibles apps maliciosas que intenten colarse en tu dispositivo.

En el caso de las redes wifi-públicas a las que nos conectamos, es recomendable que:

- No intercambies información privada o confidencial.
- No te conectes al servicio de banca on-line.
- No realices compras

2. ¿POR QUÉ SON TAN IMPORTANTES LAS CONTRASEÑAS?

Es muy común utilizar la misma contraseña para acceder a distintos servicios, si en algún momento tu contraseña se viera comprometida, el riesgo para tu información personal sería mucho mayor, ya que no sólo podrían acceder a uno de tus servicios sino a todos aquellos en los que utilizases la misma clave para acceder.

Debemos usar contraseñas fuertes y protegerlas. Las contraseñas son las llaves que dan acceso a tus servicios y por ende a tu información personal, por lo que si alguien las consigue podría comprometer tu privacidad.

CONSEJOS Y RECOMENDACIONES

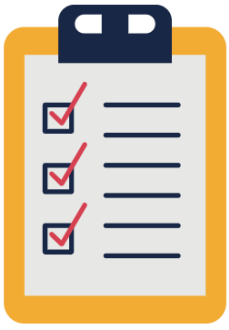
Elige contraseñas fuertes o robustas de al menos 8 caracteres y compuesta por:

- Mayúsculas (A, B, C…)
- Minúsculas (a, b, c…)
- Números (1, 2, 3…)
- Y caracteres especiales ($, &, #...)
- No utilices contraseñas fáciles de adivinar como: “12345678”, “qwerty”, ”aaaaa”, nombres de familiares, matrículas de vehículos, etc.
- No compartas tus contraseñas. Si lo haces, dejará de ser secreta y estarás dando acceso a otras personas a tu privacidad.
- No uses la misma contraseña en varios servicios.

Cuando manejas muchas contraseñas y no eres capaz de recordarlas todas, utiliza un gestor de contraseñas. Es un programa que te permite almacenar de forma segura tus claves de acceso a los diferentes servicios.
Solo necesitas recordar la clave de acceso al gestor de contraseñas, conocida como clave maestra, para consultar el resto de tus contraseñas.

A pesar de lo fuerte o robusta que sea tu contraseña, con el paso del tiempo puede verse comprometida; cambia tus contraseñas periódicamente.

3. ¿SON SUFICIENTES LAS CONTRASEÑAS?



La seguridad de un servicio protegido únicamente por una contraseña depende exclusivamente de la misma, esto implica un riesgo de seguridad ya que, si alguien la obtuviera bajo alguna circunstancia, no solo tendría acceso a tu cuenta de usuario, sino que también podría realizar actividades fraudulentas en tu nombre o curiosear tu información personal.

CONSEJOS Y RECOMENDACIONES

- Una forma de proteger una cuenta de usuario es haciendo uso de sistemas de verificación en dos pasos que consisten en añadir una capa de seguridad extra al proceso de registro/login de un determinado servicio online, es decir, para acceder a él, además de un nombre de usuario y una contraseña, será necesario que facilites un código que sólo tú conoces y que generalmente se obtiene a través del dispositivo móvil.

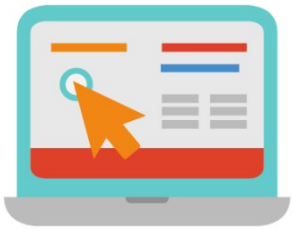
- Así, se dificulta el acceso a terceras personas a tus servicios online, ya que, aunque consigan por algún método tu contraseña, necesitarán también introducir un código que sólo podrán conocer si disponen físicamente de tu teléfono móvil.

- Dependiendo del servicio, podrás usar un método u otro, actualmente el más habitual es el envío de un código a través de un mensaje SMS a un número de teléfono previamente configurado. Una vez recibido dicho código, hay que introducirlo como un segundo paso adicional antes de lograr acceder al servicio.

- Si tienes identificados dispositivos de confianza no tendrás que meter el código cada vez que quieras acceder a un determinado servicio. Marcándolo como tal, solo puntualmente tendrás que introducirlo, haciendo que la doble verificación resulte una tarea más ágil.

- Algunos servicios aun no disponen de opciones de verificación en dos pasos. Si te encuentras en esta situación, asegúrate de usar contraseñas robustas y gestiona éstas adecuadamente para evitar problemas de seguridad y privacidad.

4. FIABILIDAD EN LAS PAGINAS WEBS



El desconocimiento de ciertos aspectos de seguridad provoca que cometas errores, puedas ser víctima de algún fraude o simplemente no hagas nada por miedo. Pero, a continuación, se aportan una serie de consejos y recomendaciones.

CONSEJOS Y RECOMENDACIONES

Lo primero que se debe hacer es asegurar que tu dispositivo está preparado para realizar los distintos trámites, para ello:

- Instala un antivirus y mantenlo actualizado para que detecte las últimas amenazas que circulan por la red.

- Tu equipo y sus programas, como el navegador, también tienen que estar actualizados y correctamente configurados.

- Crea una cuenta de usuario por cada persona que vaya a utilizar el dispositivo.

- La conexión es importante, siempre que vayas a realizar trámites online evita hacerlo desde redes wifi-públicas. Conéctate mejor con el 3G/4G del móvil o desde tu wifi de casa y no te olvides de comprobar si tu red wifi está correctamente configurada para evitar que desconocidos se conecten a ella.

- Cuando visites un sitio, comprueba que realmente es al que querías acceder. Fíjate en la URL, ésta empezará por https y mostrará un candado en la barra de direcciones. Cuando hagas clic sobre dicho candado, la URL también deberá estar bien escrita.

- Cuando termines, no te olvides de cerrar la sesión. Pulsa sobre la opción de cerrar sesión al finalizar. Si no lo haces, tú sesión quedará abierta y tus datos personales y/o bancarios estarán visibles para las personas que utilicen el mismo dispositivo para conectarse a Internet.

<u>Otras recomendaciones útiles en diferentes ámbitos:</u>

Gestiones con tu banca online o la administración pública

- Mantén en secreto tus contraseñas de acceso. No las guardes escritas ni las compartas con nadie.

- No respondas nunca a correos que te soliciten tus datos personales y/o bancarios.

- Ante cualquier duda, contacta directamente con el banco o el servicio público para solucionar el problema.

Compras online

- Comprueba si el precio mostrado es el final o si hay que sumarle otros impuestos o cargos adicionales.

- Averigua las formas de pago permitidas.

- Consulta las opiniones que otros usuarios tienen sobre la página web o el vendedor mediante búsquedas en la red.

- Revisa las condiciones de envío e identifica la política de devoluciones

5. ¿CÓMO PUEDO USAR EL NAVEGADOR PARA QUE NO ALMACENE TODOS LOS PASOS QUE DOY POR INTERNET?

Cuando navegas por Internet, por defecto toda la actividad que has realizado con el navegador se almacena directamente en la memoria de tu ordenador o dispositivo, no desaparece. De tal forma que, es posible saber todos los pasos que diste en un momento dado por Internet. Para evitar esto, y especialmente si haces uso de dispositivos públicos o compartidos con otras personas, los navegadores incorporan la opción “navegación privada”

Debes saber qué información manejan los navegadores sobre ti y qué opciones incorporan para que puedas gestionarla adecuadamente, es importante para poder evitar riesgos como:

- Que toda tu actividad en Internet esté expuesta a cualquier persona que tenga acceso al navegador.
- Dar pistas acerca de tu comportamiento y preferencias en la Red.
- Que tu sesión en un sitio web quede abierta en el navegador y suplanten tu identidad.

La navegación privada evita que otras personas sepan las páginas que has visitado, los productos que has adquirido, la publicidad que te ha interesado, etc.

CONSEJOS Y RECOMENDACIONES

Independiente del navegador que utilices, es necesario que adoptes una serie de medidas para minimizar los riesgos a los que te expones cuando lo usas para navegar por Internet. Por tanto:

- Mantén el navegador actualizado a la última versión.
- Elige complementos y plugins de confianza, descárgalos solo de sitios conocidos y con buena reputación como son las páginas oficiales de los navegadores.
- Instala un verificador de páginas web, normalmente proporcionado por los principales antivirus.
- Revisa las opciones de configuración del navegador y habilita aquellas que consideres más interesantes para proteger tu privacidad y mantenerte más seguro.
- Borra el historial de navegación cuando no lo necesites.
- Elimina las cookies, esos pequeños ficheros que guardan información de los sitios que visitas.

- Utiliza un gestor de contraseñas para almacenar y custodiar tus claves de acceso y evitar así utilizar tus navegadores como gestores de contraseñas.

- Cierra siempre la sesión cuando salgas de una página en la que te hayas autenticado con usuario y contraseña. Con esta acción evitas que si una persona utiliza tu ordenador o tu dispositivo móvil pueda acceder a tu información personal usando la sesión que has dejado abierta

6. ¿QUIÉN PUEDE VER LO QUE PUBLICO EN UNA RED SOCIAL?

CONSEJOS Y RECOMENDACIONES

Cuando te registres, algunas redes sociales te solicitarán muchos datos sobre ti: domicilio, lugar de trabajo, colegio, gustos, aficiones, familiares, etc., que no son obligatorios. Valora qué información personal quieres proporcionar.

Hay cierto tipo de información que no deberías publicar en tus perfiles para que no comprometa tu privacidad ni sea utilizada:

- Datos personales
- Contraseñas
- Datos bancarios
- Teléfono móvil
- Planes para las vacaciones
- Comportamientos inapropiados
- Ideologías
- Datos médicos o relativos a tu salud

Además, con el paso de los años, lo que publicas en Internet se convierte en tu reputación digital.

Revisa las opciones de configuración de cada red social para tener controlados los principales aspectos de privacidad y seguridad:

- Conocer quién tiene acceso a tus publicaciones
- Saber quién te puede etiquetar

- Si tu perfil está visible a los buscadores de Internet
- Conocer la geolocalización de las publicaciones, etc.

7. RIESGOS EN SERVICIOS DE MENSAJERIA INSTANTÁNEA

Conocer las estrategias de engaño que utilizan los ciberdelincuentes te puede ayudar a evitar caer en sus trampas, suelen sutilizar algunos de estos métodos:

- Mensajes de contactos desconocidos
- Enlaces a páginas web que no conoces a donde te redirigen, mucho menos si se trata de un enlace acortado.
- Bulos y mensajes en cadena. No los reenvíes.
- Contrasta la información y asegúrate que es veraz. Pon especial atención si el mensaje en aquellos casos en que pueda sonar alarmista, (si no haces lo que te piden pasara algo) o se solicita información privada (datos personales, bancarios, de domicilio...) o contiene premios y cupones o sorteos, los cuales antes tiene que rellenar una encuesta y/o realizar la descarga de alguna aplicación:

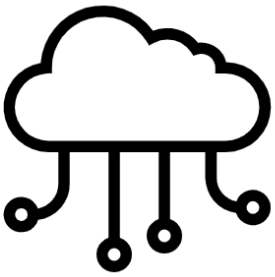
CONSEJOS Y RECOMENDACIONES

- Foto de perfil: Busca una que no sea muy comprometida.
- Bloqueo de usuarios: Decide con quién quieres mantener comunicación y con quién no.
- Información de estado: No utilices tu estado para facilitar información privada sobre ti.
- Asegúrate de que el intercambio de mensajes esté cifrado, así, aunque alguien los intercepte, no podrá comprenderlos.
- Haz uso de la opción de chat privado y/o secreto y evita que personas ajenas a la conversación puedan espiarla.
- Realiza copias de seguridad sino quieres perder los mensajes de chat.

Las apps de mensajería instantánea en smartphones no suelen pedir usuario y contraseña cada vez que las utilizamos. Esto significa que, en caso de pérdida o robo, la persona que se haga con el dispositivo podría enviar mensajes a todos los contactos de la víctima haciéndose pasar por ella.

8. QUE HAY QUE TENER EN CUENTA EN SERVICIOS CLOUD

Los servicios de almacenamiento en la nube te permiten acceder a tus ficheros desde cualquier lugar y dispositivo, incluyendo smartphone o tablet, crear carpetas para organizar la información y compartir archivos si lo necesitas. Incluso tienes la opción de seleccionar una carpeta de tu dispositivo que se sincronice automáticamente con el servicio en la nube, generando de este modo una copia de seguridad online de la información. Sin embargo, estas ventajas se pueden convertir en inconvenientes si no tomas las medidas de seguridad y privacidad adecuadas.



CONSEJOS Y RECOMENDACIONES

Elige las opciones y los servicios de almacenamiento que mejor se adapten a tus necesidades, lee sus términos y condiciones de uso antes de aceptarlos y sigue estos consejos:

- Asegúrate que el acceso al servicio en la nube sea bajo HTTPS.
- Configura correctamente las opciones de privacidad y seguridad que proporciona el servicio.
- Para mayor seguridad, cifra tus datos más confidenciales antes de subirlos al servicio de la nube.
- Utiliza una contraseña robusta de acceso y no la compartas.
- Haz copias de seguridad en soportes alternativos.
- Si compartes ficheros, asegúrate que el destinatario es realmente quien deseas.

"En la mensajería instantánea; Contrasta la información y asegúrate que es veraz. Pon especial atención si el mensaje en aquellos casos en que pueda sonar alarmista, (si no haces lo que te piden pasara algo) o se solicita información privada (datos personales, bancarios, de domicilio...) o contiene premios y cupones o sorteos, los cuales antes tiene que rellenar una encuesta y/o realizar la descarga de alguna aplicación:".

MATERIAL COMPLEMENTARIO

- Articulo técnico sobre "Medidas para minimizar el seguimiento en internet" (AEPD). Puedes consultar el artículo en este enlace.
- Articulo Tecnico sobre "Acceso de aplicaciones a la pantalla en dispositivos Android" (AEPD). Puedes consultar el artículo en este enlace.
- Articulo Tecnico sobre "Introducción a las tecnologías 5G y sus riesgos para la privacidad" (IAEPD). Puedes consultar el artículo en este enlace.
- Infografía sobre "10 Consejos para comprar en internet de forma segura" (AEPD). Puedes consultar la infografía en este enlace.
- Infografía "Compra segura en Internet" (AEPD). Puedes consultar el artículo en este enlace.
- Infografía "Recomendaciones para el uso seguro del internet de las cosas " (AEPD). Puedes consultar la infografia este enlace.

NOTICIAS

- **La APDCAT emite una Recomendación en relación con la contratación de la figura del Delegado de Protección de Datos.** La Autoridad Catalana de Protección de Datos (APDCAT) ha publicado la Recomendación 2/2023, para advertir a las entidades de su ámbito de actuación que hay que tener en cuenta la relevancia de funciones a desarrollar a la hora de fijar los precios del contrato de los servicios de delegado de protección de datos personales (DPD). Esto después de constatar licitaciones en las que se ha tenido en cuenta exclusivamente el factor precio e, incluso, se ha establecido un valor estimado del contrato notoriamente bajo en relación con la actividad a desarrollar. Consulta la Recomendación en este enlace.

- **La AEPD sanciona a la Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias (CEUCD) por vulnerar los artículos 13, 6.1 y 32 del RGPD en el uso de la plataforma educativa Google Suite.** El IES dio de alta en la plataforma al hijo menor de edad del reclamante durante el curso 20/21 sin su autorización y con anterioridad a su implantación por la CEUCD, la cual tuvo lugar en el curso 21/22 en el marco del Convenio firmado por la Consejería con GOOGLE. Además, no se acredita que se haya facilitado toda la información prevista en el artículo 13 RGPD. Consulta la Resolución en este enlace.

- **La AEPD sanciona al Ayuntamiento de Santiago de Compostela por la forma en la que remitió una notificación en la que se exponían los datos de un conductor en una denuncia por exceso de velocidad.** El reclamante recibió una carta sin sobre que fue recogida por un familiar. Consulta la Resolución en este enlace.