Sistema Nacional de Transparencia
Acceso a la Información Pública y Protección de Datos Personales

COMISIÓN DE VINCULACIÓN, PROMOCIÓN, DIFUSIÓN Y COMUNICACIÓN SOCIAL

Buenas prácticas para la Protección de Datos Personales y la Privacidad en el uso de Internet y las Redes Sociales".

Comisión de Vinculación, Promoción, Difusión y Comunicación Social del Sistema Nacional de Transparencia.

1. ¿**SABÍAS QUE** tus dispositivos móviles, tabletas, computadoras portátiles y de escritorio, así como todo los demás que tengan conexión a internet, **almacenan mucha información privada**?

   Por lo tanto, **debemos proteger nuestros dispositivos para salvaguardar nuestra información personal** (contactos, fotografías, vídeos, correos electrónicos, etc.) **y la de aquellas personas con las que interactuamos**.

   RECOMENDACIONES:

   - ✓ Utilizar un **código numérico o patrón** como bloqueo de la pantalla de tus dispositivos. Además, **cifra la información** para que se dificulte el acceso a la misma.
   - ✓ Haz uso de **herramientas de seguridad** que te ayudarán a localizar el dispositivo, bloquearlo e incluso eliminar la información almacenada en el mismo.
   - ✓ Realiza **copias de seguridad** en otro dispositivo para que no pierdas la información almacenada en el móvil o tableta.
   - ✓ Descarga **aplicaciones seguras** a través de las tiendas de las apps oficiales. Además de revisar previamente las **valoraciones y comentarios** que los usuarios han realizado sobre la app.
   - ✓ Instala una **herramienta antivirus** para que detecte posibles apps maliciosas que intenten colarse en tus dispositivos.
   - ✓ En caso de conectarte con **redes de wifi públicas**, evita intercambiar información privada o confidencial, no conectarse a la banca en línea y no realices compras.

Robo/extravío de dispositivo

Redes wifi públicas

Apps maliciosas

2. **¿Sabes cómo** configurar tus redes sociales para que únicamente tus amigos vean tu contenido?

   Las redes sociales ponen a nuestro alcance distintos contenidos para que podamos difundirlos y compartirlos con otras personas, por ejemplo, la información de nuestra vida personal, familiar o profesional, sin embargo, dicha información, aunque la borres, **quedará registrada en los servidores de la red social** y, además, **cualquiera que la haya visto podría haber hecho uso de ella, ya sea copiándola o difundiéndola**.

   RECOMENDACIONES:

   - ✓ Cuando te registres en alguna red social, **valora detenidamente que información personal quieres proporcionar**.
   - ✓ **Determinada información no debería publicarse en los perfiles de la red social** para que no comprometa tu privacidad ni sea utilizada en tu contra, como:
     - ◆ Datos personales
     - ◆ Contraseñas
     - ◆ Datos bancarios
     - ◆ Teléfono móvil
     - ◆ Planes para las vacaciones
     - ◆ Comportamientos inapropiados
     - ◆ Insultos, palabras malsonantes
     - ◆ Ideologías
     - ◆ Datos médicos o relativos a tu salud.

   - ✓ Revisa minuciosamente 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.

Privacidad y seguridad en Instagram:
https://www.youtube.com/watch?v=cIAD2vv72TM

Privacidad y seguridad en Facebook:
https://www.youtube.com/watch?v=xItJJCR7DBw

Privacidad y seguridad en Twitter:
https://www.youtube.com/watch?v=NKHGRIfgamU

Privacidad y seguridad en Snapchat:
https://www.youtube.com/watch?v=H8D7BDnDL9E

Privacidad y seguridad en WhatsApp:
https://www.youtube.com/watch?v=RpwRtQN9iv0

Privacidad y seguridad en YouTube:
https://www.youtube.com/watch?v=fgnJokNOqSw

3. ¿**Conoces** por qué debemos usar contraseñas seguras?

Las **contraseñas son la llave que da acceso a tus servicios y en consecuencia a tu información personal**, por lo que, si alguien tiene acceso a ellas, podría comprometer tu privacidad, haciendo cosas como:

- ◆ Publicar en tu nombre en redes sociales
- ◆ Leer y contestar correos electrónicos haciéndose pasar por ti
- ◆ Acceder a tu servicio de banca en línea
- ◆ Comprar en tu nombre si a la cuenta del servicio tienes asociado un medio de pago

RECOMENDACIONES:

- ✓ Debes elegir **contraseñas fuertes o robustas de al menos 8 caracteres** y compuesta por mayúsculas, caracteres especiales, números, etc.
- ✓ **Evita utilizar contraseñas fáciles** de descifrar, como tu nombre, fecha de nacimiento, etc.
- ✓ Recuerda **no compartir tus contraseñas y no utilizar la misma para varios servicios**.
- ✓ Puedes utilizar un **gestor de contraseñas**, que es un programa que te permite almacenar de forma segura tus claves de acceso a los diferentes servicios.
- ✓ Además, **cambia tus contraseñas periódicamente**.

4. ¿**Sabes** cómo puedes eliminar los datos personales que aparecen en los resultados de los buscadores?

En ocasiones pensamos que, un sitio web o buscador es fiable y responde a una determinada finalidad, por lo que no desconfiamos al entregar nuestra información personal sin informarnos bien sobre el tratamiento y uso que se dará a la misma, lo cual es un error, porque **puede provocar la pérdida de control de dicha información**.

Recomendaciones:

- ✓ Puedes **ejercer tus derechos ARCO de acceso, rectificación, cancelación y oposición sobre tus datos**, ante el responsable de tratamiento de los mismos, que es el sitio web o buscador que aparece en el aviso de privacidad.
- ✓ Si has ejercido tus derechos y no has recibido una respuesta o no estás de acuerdo con lo que te han contestado, puedes presentar una reclamación ante el Instituto Nacional de Transparencia y Acceso a la Información Pública y Protección de Datos Personales (INAI).
- ✓ Recuerda que para que un sitio web o buscador sea seguro, como mínimo debe figurar la siguiente información:
    - ◆ Denominación social, domicilio social (dirección postal), información mercantil, etc.
    - ◆ Cómo van a tratar tus datos personales (finalidad) y cómo puedes ejercer tus derechos con relación a tus datos personales.

5. ¿**Conoces** qué debes saber si quieres guardar tu información personal en la nube?

Los **servicios de almacenamiento en la nube te permiten acceder a tus ficheros desde cualquier lugar y dispositivo**, crear carpetas para organizar la información y compartir archivos si lo necesitas, sin embargo, estas ventajas se pueden convertir en inconvenientes si no tomas las **medidas de seguridad y privacidad adecuadas**.

RECOMENDACIONES:

- 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.

FUENTES DE CONSULTA

- Medidas para minimizar el seguimiento en internet. Agencia Española de Protección de Datos (AEPD).
  Disponible en: https://www.aepd.es/es/documento/nota-tecnica-evitar-seguimiento.pdf
- Orientaciones para prestadores de servicios de Cloud Computing. Agencia Española de Protección de Datos (AEPD).
  Disponible en: https://www.aepd.es/es/documento/guia-cloud-prestadores.pdf
- Proyecto de vídeos online "Protege tus datos en Internet" de la Agencia Española de Protección de Datos (AEPD).
  Disponible en: https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/protege-tu-privacidad
- Guía de Privacidad y Seguridad en Internet. Agencia Española de Protección de Datos (AEPD), Instituto Nacional de Ciberseguridad (INCIBE) y Oficina de Seguridad del Internauta (OSI).
  Disponible en: https://www.aepd.es/es/documento/guia-privacidad-y-seguridad-en-internet.pdf