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

COMISIÓN DE PROTECCIÓN DE DATOS PERSONALES

Decálogo de
PRIVACIDAD EN REDES SOCIALES
y protección
de datos personales

1. USA CONTRASEÑAS FUERTES Y ÚNICAS :

- Crea contraseñas complejas con una combinación de letras, números y símbolos.
- Utiliza una contraseña diferente para cada cuenta importante.
- Considera el uso de un gestor de contraseñas para almacenar y utilizar tus contraseñas de forma segura (NordPass, RoboForm, 1Password, KEEPER, DASHLANE, Bitdefender PM, Sticky Password).

2. HABILITA LA AUTENTICACIÓN DE DOS FACTORES (2FA*) :

- Activa 2FA en todas las cuentas que lo ofrezcan.
- Utiliza aplicaciones de autentificación en lugar de SMS cuando sea posible, ya que son más seguras (andOTP, Twilio Authy, Autenticador de Google, Step Two).

3. REVISA Y CONFIGURA LA PRIVACIDAD DE TUS REDES SOCIALES :

- Ajusta la configuración de privacidad para limitar quién puede ver y acceder a tu información.
- Revisa periódicamente tus configuraciones para asegurarte de que sigues protegido.
- Asegúrate de que los sitios web que visitas utilizan httpS, lo cual indica que son seguros.

4. CUIDA LO QUE COMPARTES EN LÍNEA :

- Evita publicar información personal, como direcciones, números de teléfono y datos financieros.
- Piensa antes de compartir ubicaciones en tiempo real.

5. UTILIZA CONEXIONES SEGURAS :

- Conéctate a internet a través de redes Wi-Fi seguras.
- Evita el uso de redes públicas para transacciones sensibles.

6. MANTÉN TUS PROGRAMAS INFORMÁTICOS ACTUALIZADOS :

- Instala actualizaciones de programas, aplicaciones y parches de seguridad en todos tus dispositivos.

- Configura las actualizaciones automáticas siempre que sea posible.

7. INSTALA Y ACTUALIZA PROGRAMAS INFORMÁTICOS DE SEGURIDAD:

- Utiliza programas antivirus y antimalware reconocidos (Avast free, AVG Internet security, Bitdefender, Karpersky, McAfee).
- Realiza escaneos regulares para detectar y eliminar amenazas potenciales.

8. CONFIGURA LA PRIVACIDAD DE TUS DISPOSITIVOS MÓVILES :

- Revoca permisos innecesarios para aplicaciones que soliciten acceso a tu cámara, micrófono y ubicación.
- Descarga aplicaciones solo desde fuentes confiables como la App Store o Google Play.

9. DESCONFÍA DE LOS CORREOS ELECTRÓNICOS Y ENLACES SOSPECHOSOS :

- No abras correos electrónicos ni enlaces de remitentes desconocidos o sospechosos.
- Verifica la autenticidad de los enlaces antes de hacer clic en ellos, especialmente en correos electrónicos que parezcan legítimos pero inesperados.

10. REALIZA COPIAS DE SEGURIDAD DE TUS DATOS :

- Haz copias de seguridad regulares de tus datos personales e información importante, en un dispositivo externo o en un servicio de almacenamiento en la nube seguro.
- Asegúrate de que tus copias de seguridad estén cifradas para mayor protección.

**La autenticación en dos fases (2FA) es un método de seguridad de administración de identidad y acceso que requiere dos formas de identificación para acceder a los recursos y los datos. Obtenido en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-two-factor-authentication-2fa*