

Manual para la protección de la

identidad personal

en plataformas digitales



Introducción

La identidad personal es un activo que debe ser protegido en todos los canales digitales. Este manual contiene recomendaciones prácticas y visuales para ayudarte a minimizar riesgos y prevenir fraudes o suplantaciones en distintos entornos digitales.

1 Redes sociales (Facebook, Instagram, TikTok, X (Twitter), etc.)



★ Recomendaciones

Responsabilidad del usuario

- Evita publicar datos sensibles que puedan poner en riesgo tu seguridad (tales como su domicilio, teléfono, ubicación en tiempo real, colegio de los niños o su logo, lugar de trabajo, entre otros).
- Cuidado con los retos, juegos o test que piden información personal o que requieran acceder a tus fotos y contactos.
- No guardes tus contraseñas de acceso en los navegadores.
- Verifica los perfiles antes de aceptar solicitudes de amistad o seguimiento.

⚙ Configuraciones en redes sociales

- Configura la privacidad de tus publicaciones: permite que solo amigos o seguidores aprobados puedan visualizar tus publicaciones.
- Desactiva la ubicación automática de fotos.
- Activa la autenticación de doble factor.



Correo electrónico (Gmail, Hotmail, etc.)



Recomendaciones

Responsabilidad del usuario y configuraciones en el correo electrónico

- Verifica la dirección del remitente minuciosamente al recibir un correo.
- Si recibes un correo y te solicitan ejecutar alguna acción (hacer clic o entregar sus datos personales), repórtalo y llama inmediatamente al Banco.
- No compartas códigos de accesos, pin, contraseña o tokens.
- Evita hacer clic en enlaces sospechosos.
- No descargues documentos de correos sospechosos o dudosa procedencia.
- Utiliza contraseñas únicas y fuertes; cámbialas de manera periódica.
- Activa la autenticación de doble factor.
- Evita guardar tus contraseñas de acceso en los navegadores.



Redes sociales profesionales (LinkedIn, etc.)



Recomendaciones

Responsabilidad del usuario y configuraciones en redes sociales profesionales

- Activa la autenticación de doble factor.
- Verifica los perfiles antes de aceptar solicitudes de amistad o seguimiento.
- Comparte solo información laboral relevante.
- Revisa quién puede ver su información de contacto.
- Evita aceptar conexiones sin contexto profesional.
- Configura la privacidad de tus publicaciones: permite que solo amigos o seguidores aprobados puedan visualizar tus publicaciones.



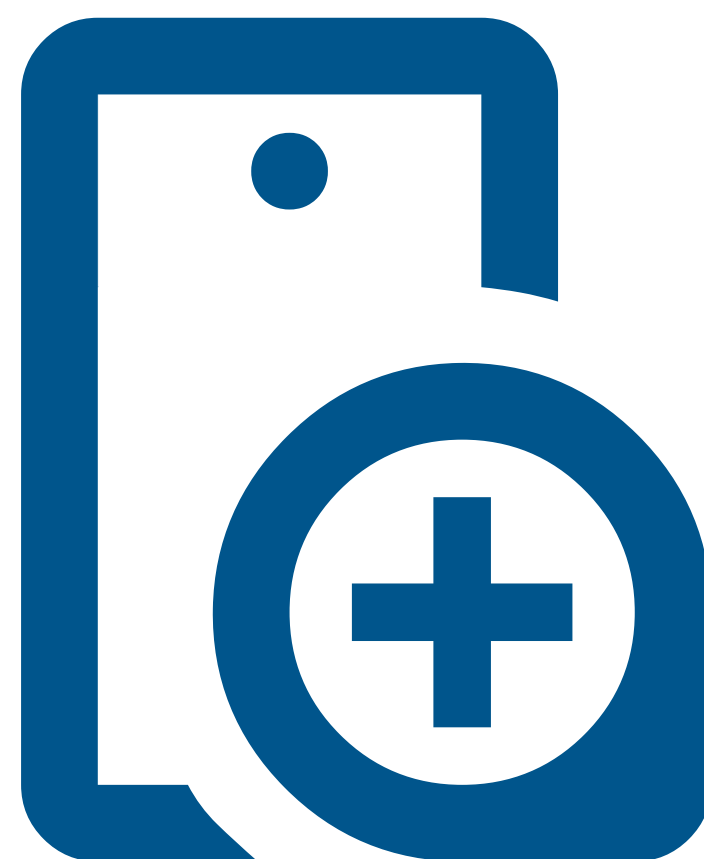
Mensajerías instantáneas (WhatsApp, Telegram, etc.)



Recomendaciones

- Activa la autenticación de doble factor y de extremo a extremo.
- Bloquea contactos desconocidos.
- No compartas códigos de verificación.
- Verifica si alguien está usando tu cuenta en otro dispositivo.

Dispositivos móviles



Teléfono celular



Recomendaciones

- Activa biometría para acceder y bloquear tu dispositivo.
- Use aplicaciones de identificación y bloqueo de llamadas.
- No instales aplicaciones fuera de tiendas oficiales.
- Configura permisos de Apps adecuadamente y revísalos periódicamente. Elimina los que no sean necesarios de acuerdo con la naturaleza y función de cada una.
- Considera adquirir un antivirus para tus dispositivos.



Computadora personal



Recomendaciones

- Utiliza antivirus actualizados y firewall personal.
- No repitas contraseñas.
- Mantén el sistema operativo y navegador actualizados.
- Realiza copias de seguridad regularmente.
- Opta por redes wifi seguras y evita las públicas sin VPN.
- No dejes tus dispositivos visibles en vehículos o escritorios públicos.
- Usa bloqueo por contraseña, PIN o biometría (huella, reconocimiento facial).



Consejos generales

Si recibes algún mensaje a través de SMS, redes sociales, mensajería instantánea o una llamada:

- Sospecha si transmiten sentidos de urgencias, amenazas u ofrecen regalos inesperados.
- Consulta fuentes oficiales ante dudas.
- Educa a familiares y colegas.
- Revisa la configuración de privacidad de tus cuentas de cada tres a seis meses.
- No compartas información sin verificar su veracidad.



Súper consejo

Recuerda que el Banco nunca te llamará o escribirá para pedirte, ni por correo electrónico, redes sociales, SMS o llamadas, tu información financiera o personal. Ante las dudas, no respondas. Cuelga y dirígete a la sucursal más cercana o llama directamente a nuestro Centro de Contacto al 809-960-2121.