1 Protégete desde tus dispositivos

- **Actualiza constantemente** el sistema operativo y las aplicaciones.
- **Configura un método de autenticación** para acceder a tus dispositivos, como contraseñas o autenticación biométrica.
- Sincroniza tu información o **haz respaldos frecuentes** de tu información en la nube.
- Descarga aplicaciones únicamente de tiendas o sitios oficiales, y **revisa los permisos que otorgas a estas.**
- Cuando no los utilices, **apaga el bluetooth y el wifi.**
- Activa las configuraciones para **localización y borrado remoto del dispositivo.**
- No conectes USB o discos duros que no sean de **total confianza.**
- Utiliza un **antivirus licenciado** y procura mantenerlo actualizado.

2 Asegura tus cuentas digitales

- **Utiliza contraseñas seguras** que sean difíciles de adivinar.
- **Evita usar la misma contraseña para varias cuentas** digitales o servicios en internet.
- **Habilita la autenticación en dos pasos** o doble factor de autenticación. 2FA
- Configura las opciones de **seguridad y privacidad.**
- **Verifica periódicamente** los dispositivos que acceden a tus cuentas.

3 Navega seguro

- Valida que los sitios donde ingresas tu datos **sean seguros** (HTTPS).
- **Evita realizar transacciones o ingresar información personal al estar conectado a redes wifi públicas.** Si es completamente necesario, utiliza un software VPN confiable.
- **Ten cuidado con lo que descargas** en sitios desconocidos.
- Para acceder a sitios financieros, **evita seguir enlaces y escribe directamente la dirección de la entidad en el navegador.**

4 Mejora tus contraseñas

- Crea contraseñas seguras, mínimo de 12 caracteres y que sean **difíciles de adivinar.**
- **Nunca compartas** tus contraseñas.
- **No escribas tus contraseñas** ni las expongas en lugares visibles.
- **Utiliza un gestor de contraseñas** para ayudarte a recordarlas y almacenarlas de manera segura.
- **Cambia tus contraseñas con frecuencia**, máximo cada 90 días .

5 Identifica correos sospechosos

- **Verifica muy bien la dirección de correo del remitente**. Aunque sea de un conocido, sospecha de solicitudes urgentes.
- **Sin dar clic**, ubica el mouse sobre cualquier enlace o vínculo recibido para **verificar el sitio** al cual te redireccionará.
- **Mantente alerta ante errores gramaticales o de ortografía**: pueden ser un indicio de un correo malicioso cuando provienen de supuestas entidades oficiales.
- **Sospecha de correos genéricos** que no estén dirigidos a tu nombre.
- **Evita abrir o descargar** archivos adjuntos de remitentes desconocidos.

Fuente: Centro de Proteccion Digital SURA