¿CÓMO PODEMOS PROTEGER NUESTRAS COMUNICACIONES?

Recomendaciones básicas en seguridad digital

SweFOR Colombia - 20 años

Con esta publicación les compartimos unas recomendaciones básicas para proteger la comunicación digital. Así podemos disminuir los riesgos que pueden afectar la privacidad de nuestras comunicaciones, la pérdida de información u otras amenazas derivadas del uso de las tecnologías de la información y la comunicación en el trabajo de defensa de derechos humanos.

Texto: Área Autoprotección SweFOR Colombia y Anar.Coop
Impresión y diseño:
f.8 imagen f.8imagen@gmail.com
Cris2.8 2.8colombia@gmail.com

Bogotá D.C. octubre 2024

1 Cuida el acceso a los equipos y cuentas, es la puerta de entrada

Bloquea la pantalla de tu celular y de tu computador.
Accede a:

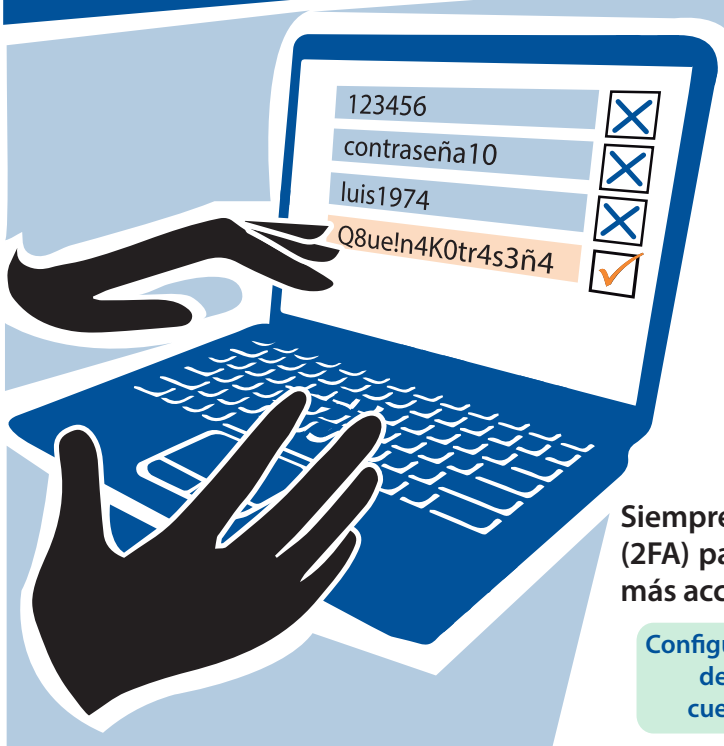
Ajustes o Configuración → Bloqueo y seguridad/ personalización → Bloqueo de pantalla

En tu computador puedes poner una contraseña entrando en la opción de inicio de sesión. Así solo tú podrás entrar en el equipo.

Procura siempre usar contraseñas. En el celular, tanto el PIN como el patrón pueden ser fáciles de descifrar.

Nunca utilices la opción de recordar o autoguardar contraseña cuando accedas a tus cuentas desde un navegador. Especialmente cuando te conectes en equipos que no son tuyos.

Usa buenas contraseñas



Estas deben ser:

- Frases, no palabras, con más de 20 caracteres. ☑
- No deben tener información personal como números de identificación, fechas de cumpleaños o nombres de familiares. ☑
- Una mezcla de números, símbolos, letras minúsculas y mayúsculas. ☑
- Únicas, no utilizadas en más de una cuenta. ☑
- Privadas, solo tú debes conocerlas. ☑

Siempre que sea posible, activa la verificación de dos pasos (2FA) para acceder a tus cuentas. Con esto evitas que alguien más acceda y tome control de tu información. Encuéntrala en :

Configuración de la cuenta → seguridad → verificación en dos pasos/ Autenticación en dos factores.

2 Mantén tu sistema actualizado y borra la información que no necesites

Actualiza tus aplicaciones para reducir el riesgo de sufrir fallas, pérdidas o robos de información.

Cada cosa que haces en el celular queda guardada: las imágenes y videos que tomas, los archivos que descargas, los historiales de navegación, llamadas y redes a las que te has conectado. Revisa y borra regularmente lo que no estás utilizando (archivos, historiales, aplicaciones) para liberar espacio, mejorar el rendimiento y la velocidad de tu celular. De esta manera tendrán también un mayor control de la información que almacenas en tu dispositivo.

Ajustes o Configuración

- → Almacenamiento → Liberar espacio
- → Aplicaciones → Liberar espacio
- → Actualizaciones del sistema

Estas opciones pueden variar dependiendo del modelo de tu celular.

3 Desactiva Datos, Wifi, Bluetooth y Ubicación cuando no los uses

Tu celular tiene varias antenas que permanentemente están enviando y recibiendo señales con tu ubicación física, relacionada con tu actividad en sitios web y aplicaciones de internet.

Es difícil establecer cuánta y qué tipo de información sobre tu comportamiento pasa por estas antenas, o quién exactamente puede conocer esa información, pero puedes apagarlas siempre que no las estés usando para algo específico. Además, al tenerlas apagadas ahorras batería en tu celular.

En Ajustes o Configuración puedes activar o desactivar los Datos móviles, Wifi y Bluetooth, así como los servicios de Ubicación, y puedes activar el Modo Avión. Si necesitas asegurar que no se conozca tu ubicación física, es mejor no llevar el celular contigo.

4 Ojo con los permisos, lee la letra pequeña

Descarga aplicaciones solo desde sitios oficiales y de confianza, y revisa siempre sus "Términos y condiciones" o "Condiciones de servicio" antes de aceptar e instalar. Esto aplica también cuando estés creando cuentas en redes sociales o cualquier otro servicio en línea.

Es importante conocer y ajustar los permisos que le das a todas las aplicaciones instaladas en tu celular. Siempre que sea posible, escoge "permitir solo con la app en uso". Puedes revisar:

Ajustes o Configuración → Aplicaciones → Permisos de aplicaciones

Ten cuidado si vas a quitar permisos en aplicaciones preinstaladas en tu celular, pues esto puede afectar su funcionamiento.

5 Revisa y ajusta las configuraciones de privacidad

Puedes controlar quién puede contactarte (enviarte mensajes, llamarte, agregarte a grupos) y quién puede ver tus datos (nombre, foto, número de teléfono, última conexión, ubicación ,…).

En el computador o el celular, y en todas las aplicaciones que usas, busca la opción :

Ajustes o Configuración → **Privacidad**

Ajustes o Configuración → **cuenta** → **Privacidad**

Recuerda que en aplicaciones de mensajería y redes sociales puedes también bloquear perfiles y contenidos que prefieras no ver. Y también puedes reportarlos directamente a las plataformas si consideras que son ofensivos o violentos.

6 Si es sospechoso o desconocido, mejor no abrir

Con los avances en Inteligencia Artificial, es cada vez más fácil manipular textos, audios, fotos y videos, y esto se utiliza para robar datos, acceder a cuentas e instalar programas maliciosos que se utilizan para monitoreo y vigilancia.

No tienes que reaccionar rápidamente. Siempre que recibas mensajes de alerta, concursos o notificaciones de que ganaste algo, reflexiona qué tan posible es que sea real. No descargues ni abras documentos, no envíes dinero ni des click en enlaces desconocidos, a menos que tengas completa certeza de quién los envía.

7 Comunícate siempre de forma segura

Utiliza aplicaciones cifradas como Signal o Whatsapp para todas tus comunicaciones personales, de manera que la información se quede entre ustedes, no en terceras personas. Las llamadas telefónicas y mensajes SMS no son canales seguros; tanto el proveedor del servicio como entes externos pueden intervenir estas comunicaciones fácilmente.

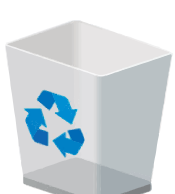
En tu celular, Signal funciona como una caja fuerte, pues no permite que otras aplicaciones accedan a la información que allí se comparte (fotos, textos, audios, datos). Siempre que quieras descargar un contenido recibirás una alerta. Esta es una protección con la que no cuenta Whatsapp.

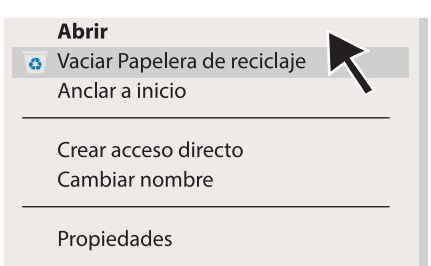
Configura la desaparición automática de mensajes. Esto es útil no solo para proteger información sensible, sino para ir liberando espacio en tu celular.

8 No compartas información sensible en equipos y redes públicas

Si vas a utilizar un equipo que no es tuyo, abre el navegador en modo incógnito o privado, y asegúrate que la dirección de los sitios que visitas empieza con https:// (la s es lo más importante).

Al terminar, cierra cualquier sesión que hayas abierto (de correo o redes sociales). Y si has descargado algún archivo, recuerda borrarlo y vaciar la papelera de reciclaje.





Las redes públicas son inseguras, ten en cuenta:

- Si la red no tiene contraseña, mejor no conectarse.
- Si para conectarte debes poner datos personales (correo electrónico, documento de identidad…) no es necesario que sean datos reales.
- Evita abrir tus cuentas, es decir, escribir tu nombre de usuario y contraseña.

El Movimiento Sueco por la Reconciliación - SweFOR, busca con su trabajo la promoción de una cultura de paz y noviolencia en el mundo, promoviendo el manejo pacífico de los conflictos y el respeto a los derechos humanos y al derecho internacional humanitario, como ejes fundamentales para la construcción de una paz sostenible.

En el programa Servicio de Paz y Acompañamiento Internacional de SweFOR acompañamos a personas defensoras de derechos humanos en Colombia que se encuentran bajo amenaza, brindándoles protección a través de presencia preventiva, acompañamiento político e incidencia, comunicación estratégica y capacitación en autoprotección colectiva y diferenciada.

SweFOR Colombia - 20 años

Los contenidos de esta publicación son responsabilidad exclusiva de SweFOR en el marco del Proyecto Colombia del Programa Servicio de Paz, financiado por la Embajada de Suecia en Colombia.

Con el apoyo de la Embajada de Suecia

Suecia
Sverige

www.swefor.org
Swefor Colombia
SweFORColombia
sweforcolombia