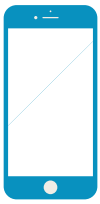
LIFELINE
FOR EMBATTLED CIVIL SOCIETY ORGANIZATIONS

LISTA DE VERIFICACIÓN DE MEDIDAS PRÁCTICAS DE SEGURIDAD PARA LAS ORGANIZACIONES DE LA SOCIEDAD CIVIL

La siguiente información es un extracto de las Herramientas Lifeline para las OSC que trabajan en espacios restringidos (www.csolifeline.org/advocacy-toolkit). Proporciona una breve descripción de cómo las organizaciones de la sociedad civil pueden reflexionar sobre la seguridad digital en el marco de la participación en las campañas de incidencia política.

Asunto	Recomendaciones	Consejo/Recurso

Seguridad del dispositivo 	• Proteja su dispositivo con una contraseña
	• Actualice su sistema operativo cuando se le solicite
	• Ejecute el antivirus
	• Haga una copia de seguridad de sus dispositivos con regularidad
	• Borre información sensible con asiduidad (podría utilizar un software de borrado seguro para limpiar el dispositivo, si procede)
	• No conecte dispositivos a puertos USB públicos o memorias USB desconocidas a su dispositivo
	• No utilice redes WiFi públicas que no sean fiables
	• No deje los dispositivos desatendidos en espacios públicos, hoteles, conferencias
		• Utilice un software de gestión de contraseñas para almacenar sus contraseñas: **Keepass**, **LastPass**, **Dashlane**
		• Algunos antivirus gratis como **Avira**, **AVG**, **Avast**, vienen integrados en el Windows Defender
		• Borre sus datos de forma segura: **Bleachbit**
		• Para la copia de seguridad en la nube:
		  • Almacenamiento en la nube con cifrado end to end: **Tresorit**
		  • Cifrado del lado del cliente **Client-side encryption https://cryptomator.org/** para sus archivos en la nube

Cifrado de archivos y discos 	• Habilite el cifrado del disco completo en su dispositivo • Use **Bitlocker** para Windows, **Filevault** para Mac, o un programa gratuito de código abierto de cifrado de discos – **VeraCrypt** • La mayoría de los teléfonos inteligentes vienen con el cifrado activado, compruebe la configuración para confirmarlo • Si procede, asegúrese de encriptar las unidades flash para proteger los datos	• Con el cifrado ACTIVADO, tanto el dispositivo como la contraseña serán necesarios para descifrar los datos encriptados. • Un recurso útil: "Manteniendo sus datos seguros" **https://ssd.eff.org/en/module/keeping-your-data-safe**
Seguridad en el email y las redes sociales 	• Use contraseñas seguras: **https://xkcd.com/936/** • No use la misma contraseña para más de un servicio • Si es posible, implemente la autenticación de dos factores • Tenga mucho cuidado al abrir enlaces o archivos adjuntos	• La autenticación de dos factores (2FA) refuerza la seguridad de acceso al sistema al requerir un método adicional de autenticación • Lista de sitios web e información sobre si soportan o no la autenticación de dos factores: **https://twofactorauth.org/**

El Fondo Lifeline de asistencia a organizaciones de la sociedad civil en Riesgo brinda asistencia financiera de emergencia a organizaciones de la sociedad civil (OSC) que se encuentran bajo amenazas o ataques así como subvenciones de respuesta rápida para campañas de incidencia política y resiliencia para dar apoyo a las OCS que luchan contra las restricciones al espacio cívico. Para más información, visite **https://www.csolifeline.org** o contacte **info@CSOLifeline.org**. Encuéntranos en Twitter **@CSOLifeline**.

Asunto	Recomendaciones	Consejo/Recurso
Servicios de correo electrónico basados en la web con cifrado end to end 	En el correo electrónico con cifrado end to end solo el remitente y el destinatario pueden leer los mensajes intercambiados y los datos compartidos entre ellos.	Algunas opciones gratuitas de servicios basados en la web: • **Protonmail** • **Tutanota** • **Hushmail**
Comunicación por correo electrónico cifrado 	Si le preocupa la privacidad de internet y la seguridad de su comunicación, uno de los sistemas comunes de cifrado es el PGP. Se basa en la criptografía de clave pública y con este cifrado puede estar seguro de que sus datos están a salvo y de que solo los destinatarios a los que iba dirigido el correo podrán leer el contenido de su comunicación.	• Guía explicativa de Pretty Good Privacy (cifrado PGP) en: **https://guides.accessnow.org/tag_pgp.html** • **Mailvelope** (plugin del navegador) • Lista de aplicaciones de correo electrónico que **soportan OpenPGP standard: https://www.openpgp.org/software/**
Aplicaciones de mensajería cifrada: 	• Tenga en cuenta qué aplicaciones son las más seguras para su país o región: **https://securityinabox.org/en/guide/secure-communication/**: datos del usuario y privacidad, metadatos, noticias recientes sobre seguridad. (La app Signal se encuentra entre las aplicaciones que tienen los más altos estándares de seguirdad a fecha de octubre 2019) • Revise la configuración de privacidad y seguridad de cada aplicación. • Aunque utilice las aplicaciones más seguras, existe la posibilidad de que alguien pueda acceder a sus conversaciones sensibles o archivos personales al estar almacenados en algún lugar de su dispositivo, por lo que es fundamental que cree un proceso para revisar el contenido de la aplicación y eliminar los mensajes sensibles con regularidad (por ejemplo, utilice la función de eliminar mensajes si es posible)	• Haga que su móvil sea seguro **https://securityinabox.org/en/guide/smartphones/** • Piense en lo que necesita para que su aplicación de mensajería sea seguro **https://www.eff.org/deeplinks/2018/03/thinking-about-what-you-need-secure-messenger** • Signal, la aplicación de mensajería segura **https://freedom.press/training/locking-down-signal/** • Consejos de seguridad del whatsapp (tiene algunos problemas de seguridad) **https://www.whatsapp.com/safety** • Cómo hacer sus aplicaciones de mensajería seguras **https://guides.accessnow.org/IM_Tips.html**
Navegación segura: 	• Actualiza su versión del navegador con regularidad. • Comprueba la autenticidad del sitio web (en el enlace, el icono HTTPS debe aparecer al principio). • Haga que su navegación sea más segura: **https://www.eff.org/https-everywhere** • Utilice una VPN para proteger su información de navegación de personas ajenas (concretamente si usa una Wi-Fi pública o compartida).	Una VPN es un túnel encriptado entre dos dispositivos que le permite acceder a cada sitio web y servicio en línea de forma privada y segura. • Guía de comparación de VPN **https://thatoneprivacysite.net/** • Ejecute su propia VPN **https://getoutline.org/en/home**