

Manual de **SEGURIDAD DIGITAL** para organizaciones de la sociedad civil



Manual de **SEGURIDAD DIGITAL** para organizaciones de la sociedad civil



Contenido

Presentación página 5

- 1.** Conceptos básicos
de seguridad digital página 6
- 2.** Protección
de dispositivos página 8
- 3.** Gestión de contraseñas
y verificación en dos pasos página 11
- 4.** Navegación segura
en internet página 14
- 5.** Seguridad en
redes sociales página 18
- 6.** Respuesta
a incidentes página 22
- 7.** Ciberseguridad en actividades
y eventos página 25
- 8.** Uso de mensajería
instantánea página 29
- 9.** Respaldo y almacenamiento
de información página 33
- 10.** Seguridad avanzada
para activistas página 36

Conclusión página 41

Presentación

En un mundo cada vez más digitalizado, las organizaciones de la sociedad civil (OSC) dependen en gran medida de las tecnologías de la información para llevar a cabo sus actividades. Sin embargo, esta creciente dependencia expone a las OSC a una serie de riesgos cibernéticos que pueden comprometer su misión, reputación y la seguridad de sus colaboradores. Este manual tiene como objetivo proporcionar a las OSC las herramientas y conocimientos necesarios para proteger sus datos, sistemas y comunicaciones, y así garantizar su trabajo en pro de una sociedad mejor, con más democracia y libertad.

Esperamos que este Manual sirva de apoyo al trabajo que realizan y los invitamos a compartirlo.

Cedice Libertad

1.

Conceptos básicos de seguridad digital

¿Qué es la seguridad digital y por qué importa?

La seguridad digital es el conjunto de prácticas, herramientas y medidas diseñadas para proteger la información, dispositivos y comunicaciones frente a amenazas en línea. Para miembros de organizaciones de la sociedad civil, la seguridad digital no solo protege datos personales, sino también la integridad de sus organizaciones y la seguridad de sus equipos de trabajo.

En países donde la censura, la vigilancia y los bloqueos en internet son frecuentes, garantizar la seguridad digital es fundamental para:

- Proteger la privacidad individual y colectiva.
- Evitar ataques como hackeos, espionaje o robo de información.
- Asegurar la continuidad del trabajo de la organización ante intentos de intimidación.

Principios fundamentales de la seguridad digital

Toda estrategia de seguridad digital debe basarse en los siguientes principios:

- 1. Confidencialidad:** Asegura que la información sea accesible solo para quienes están autorizados.
Ejemplo: Usar cifrado para proteger documentos sensibles de una ONG.
- 2. Integridad:** Garantiza que la información no sea alterada sin autorización.
Ejemplo: Proteger archivos importantes contra modificaciones por *malware* o atacantes.

3. Disponibilidad: Asegura que la información y los sistemas estén accesibles cuando se necesitan.

Ejemplo: Tener copias de respaldo de datos críticos en caso de un ataque o falla técnica.

Amenazas comunes

El contexto presenta desafíos únicos que afectan la seguridad digital del trabajo que desarrollan las organizaciones de la sociedad civil.

1. Bloqueos de internet: Restricciones de acceso a páginas web y servicios en línea.

Solución: Uso de VPN para sortear bloqueos.

2. Vigilancia digital: Monitoreo de comunicaciones privadas y redes sociales.

Solución: Uso de mensajería cifrada y configuración de privacidad en redes.

3. Hackeos y ataques a cuentas: Suplantación de identidad o accesos no autorizados a cuentas.

Solución: Uso de contraseñas fuertes y verificación en dos pasos.

4. Phishing: Intentos de engaño para obtener información confidencial mediante correos o mensajes falsos.

Solución: Reconocer correos sospechosos y evitar hacer clic en enlaces no confiables.

5. Robo o confiscación de dispositivos: Pérdida física de equipos que contienen información sensible.

Solución: Cifrado de dispositivos y respaldo de datos.

2.

Protección de dispositivos

Los dispositivos electrónicos (teléfonos, computadoras y tabletas) son herramientas fundamentales para activistas y miembros de las organizaciones, pero también representan un gran riesgo si no están debidamente protegidos. A continuación, se describen medidas clave para asegurar estos equipos.

2.1 Configuración segura de dispositivos

Establece un PIN o contraseña segura para acceder al dispositivo

1. En Android:

- Ve a «Configuración».
- Selecciona «Seguridad» o «Pantalla de bloqueo y seguridad».
- Toca «Tipo de bloqueo de pantalla».
- Elige «PIN» o «Contraseña» e introduce un código seguro (al menos 6 caracteres).
- Confirma el código para habilitar el bloqueo.

2. En iOS:

- Ve a «Configuración».
- Selecciona «Face ID y código» o «Touch ID y código» (según el modelo).
- Toca «Activar código».
- Introduce un código numérico seguro y confírmalo.

Habilita el bloqueo automático:

1. En Android:

- Ve a «Configuración».
- Selecciona «Pantalla» o «Pantalla de bloqueo».
- Busca la opción «Suspensión» o «Bloqueo automático» y configura el tiempo (recomendado: 1-2 minutos).

2. En iOS:

- Ve a «Configuración».
- Selecciona «Pantalla y brillo».
- Toca «Bloqueo automático» y elige un tiempo breve (recomendado: 1-2 minutos).

Desactiva las opciones de desbloqueo inseguras:

Evita el desbloqueo con huellas digitales o reconocimiento facial si existe el riesgo de que alguien pueda obligarte a usar estas opciones. Prioriza el uso de PIN o contraseña.

2.2 Actualizaciones del sistema operativo y aplicaciones

Mantener el sistema operativo y las aplicaciones actualizadas es una de las formas más sencillas de prevenir vulnerabilidades:

- Activa las actualizaciones automáticas para asegurarte de tener siempre la última versión.
- Actualiza regularmente tus navegadores, aplicaciones de mensajería y programas de seguridad.

2.3 Antivirus y su importancia en teléfonos móviles

Los teléfonos móviles, al igual que las computadoras, pueden ser víctimas de virus y otros tipos de *malware*, especialmente si descargas aplicaciones fuera de las tiendas oficiales o haces clic en enlaces sospechosos.

Recomendaciones:

- Descarga un antivirus confiable desde la tienda oficial de tu sistema operativo (por ejemplo, Avast Mobile Security, Bitdefender o Norton Mobile Security).
- Configura el antivirus para realizar análisis automáticos y detectar amenazas de forma oportuna.
- Evita instalar aplicaciones de origen desconocido.

2.4 Copias de seguridad regulares

Asegúrate de realizar respaldos periódicos de tus datos en caso de pérdida o confiscación de dispositivos:

- **Métodos seguros:**

- Almacenamiento en la nube (por ejemplo, Google Drive, OneDrive o Tresorit).
- Discos duros externos protegidos con contraseña.

- **Frecuencia recomendada:**

- Realiza copias semanales si manejas información crítica.

2.5 Protección frente al robo o confiscación

1. Habilita funciones de rastreo:

- **En Android:** Ve a «Configuración > Google > Seguridad > Encontrar mi dispositivo» y actívalo.
- **En iOS:** Ve a «Configuración > Tu nombre > Buscar > Buscar mi iPhone» y actívalo.

2. Activa el borrado remoto:

- Configura tu dispositivo para que puedas borrar los datos de forma remota si es robado.

3. Respalda información sensible:

- No guardes documentos críticos únicamente en tu dispositivo. Utiliza servicios en la nube o unidades externas cifradas.

2.6 Buenas prácticas con dispositivos físicos

- No prestes tu dispositivo a personas desconocidas o de poca confianza.
- Evita dejar tu equipo desatendido en lugares públicos.
- Usa fundas o accesorios que hagan tu dispositivo menos llamativo para evitar robos.

3.

Gestión de contraseñas y verificación en dos pasos

Las contraseñas y la verificación en dos pasos (2FA) son la primera línea de defensa contra accesos no autorizados a tus cuentas y dispositivos. A continuación, te mostramos cómo gestionar contraseñas de forma segura e implementar la 2FA para proteger tu información.

3.1 Creación de contraseñas seguras

Una contraseña segura debe ser:

- Larga: Al menos 12 caracteres.
- Compleja: Incluir letras mayúsculas, minúsculas, números y símbolos.
- Única: Nunca reutilices la misma contraseña para múltiples cuentas.

Buenas prácticas al crear contraseñas con reglas mnemotécnicas:

1. Escoge el nombre de una canción o frase que recuerdes fácilmente.
Ejemplo: «lavacamariposa»
2. Cambia algunas letras por caracteres especiales o números siguiendo un patrón constante. Ejemplo: «L@v@c@m@r!p0s@».
3. Agrega un prefijo o sufijo específico para cada cuenta. Por ejemplo:
 - Para Facebook: «fb.L@v@c@m@r!p0s@».
 - Para Twitter (X): «tw.L@v@c@m@r!p0s@».
 - Para Instagram: «ig.L@v@c@m@r!p0s@».

De esta manera, tendrás contraseñas únicas, seguras y fáciles de recordar.

3.2 Uso de gestores de contraseñas

Un gestor de contraseñas es una herramienta que almacena y genera contraseñas seguras de manera automática. Estas son algunas opciones confiables:

- **Bitwarden:** Gratuito, de código abierto y permite hasta 4 dispositivos en la versión gratuita.
- **LastPass:** Permite sincronización entre dispositivos, pero la versión gratuita solo admite una sesión por dispositivo.
- **1Password:** Excelente para usuarios de iOS y cuenta con integraciones avanzadas para equipos.

Recomendaciones clave:

- Asegúrate de recordar siempre la contraseña maestra del gestor. Esta debe ser larga, única y altamente segura.
- Nunca compartas la contraseña del gestor con nadie.

3.3 Verificación en dos pasos (2FA)

La verificación en dos pasos añade una capa extra de seguridad al requerir dos elementos para acceder a tus cuentas:

1. Algo que sabes (tu contraseña).
2. Algo que tienes (un código enviado a tu teléfono o generado por una *app*).

Cómo activar la 2FA en servicios esenciales:

1. Gmail:

- Ve a «Configuración de cuenta» en tu perfil de Google.
- Selecciona «Seguridad» y luego «Verificación en dos pasos».
- Sigue las instrucciones para habilitarla usando una aplicación autenticadora.

2. Facebook:

- Ve a «Configuración > Seguridad e inicio de sesión».
- Haz clic en «Usar autenticación en dos pasos».
- Configura la 2FA con *app* autenticadora o llave de seguridad.

3. Twitter (X):

- Ve a «Configuración > Seguridad y acceso a la cuenta».
- Selecciona «Autenticación en dos factores».
- Actívala usando un método disponible (*app* autenticadora).

4. Instagram:

- Ve a «Configuración > Seguridad > Autenticación en dos pasos».
- Elige una aplicación autenticadora.

5. TikTok:

- Ve a «Configuración y privacidad > Seguridad > Verificación en dos pasos».
- Selecciona el método deseado: *app* autenticadora.

6. WordPress:

- Instala un *plugin* como «Two Factor» o «Google Authenticator».
- Configura el *plugin* según las instrucciones y vincula con una aplicación autenticadora.

Aplicaciones autenticadoras recomendadas:

1. **Authy:** Fácil de usar, permite sincronizar tus códigos en múltiples dispositivos y realizar copias de seguridad cifradas.
2. **Google Authenticator:** Ligera y compatible con la mayoría de servicios.

No recomendamos la utilización de sms (mensajes de texto) como forma de verificación en dos pasos

3.4 Manejo de preguntas de seguridad

Las preguntas de seguridad suelen ser un punto débil.

Refuerza este aspecto:

1. Crea respuestas falsas pero memorables (por ejemplo, para «¿Cuál es tu comida favorita?» responde «EstrellaVerde»).
2. Usa un gestor de contraseñas para almacenar estas respuestas.
3. Si es posible, evita preguntas de seguridad y prioriza la 2FA.

4.

Navegación segura en internet

El acceso a internet es esencial para activistas y miembros de ONG, pero también puede convertirse en un punto vulnerable si no se toman las precauciones adecuadas. A continuación, te explicamos cómo proteger tu privacidad y seguridad mientras navegas.

4.1 Uso de navegadores seguros

El navegador que utilizas puede marcar la diferencia en tu seguridad en internet. Algunos navegadores populares ofrecen mejores opciones de privacidad y protección que otros:

Navegadores recomendados:

1. Firefox:

- Configurable para mejorar la privacidad.
- Permite instalar extensiones como uBlock Origin (bloqueador de anuncios) y HTTPS Everywhere (fuerza conexiones seguras).

2. Brave:

- Bloquea rastreadores y anuncios de forma predeterminada.
- Incluye opción para navegar en Tor desde el navegador.

3. Tor Browser:

- Diseñado para el anonimato.
- Redirige tu tráfico a través de la red Tor, ocultando tu dirección IP.
- Recomendado para situaciones de alto riesgo donde la privacidad es fundamental.

Hacer Google Chrome más seguro:

Aunque no es el navegador más privado, puedes mejorar su seguridad:

- Instala extensiones como uBlock Origin, Privacy Badger y HTTPS Everywhere.

- Activa la sincronización solo en dispositivos confiables.
- Desactiva el rastreo en «Configuración > Privacidad y seguridad > Enviar solicitud de no rastrear».
- Usa el modo «Invitado» para evitar guardar historial en dispositivos compartidos.

4.2 Uso de VPN

Una VPN (Red Privada Virtual) es una herramienta que cifra tu conexión a internet y oculta tu dirección IP, ayudándote a:

- Acceder a contenido bloqueado o censurado.
- Proteger tu información cuando utilizas redes Wi-Fi públicas.

VPN recomendadas:

- **ProtonVPN:** Seguro, confiable y con versión gratuita.
- **RiseupVPN:** Diseñado específicamente para activistas.
- **Lantern:** Ideal para sortear bloqueos.
- **Psiphon:** Fácil de usar en contextos de censura.
- **Tunnel Bear:** Opciones gratuitas y fáciles de configurar.

Precaución:

Evita VPN no recomendadas por la comunidad de Derechos Humanos y Derechos Digitales, especialmente aquellas asociadas a empresas en China, Rusia o Irán, ya que podrían comprometer tu privacidad.

4.3 Navegación en modo incógnito

El modo incógnito evita que tu navegador guarde tu historial y *cookies* de navegación. Sin embargo, **no protege tu privacidad ante tu proveedor de internet o sitios web.**

Cuándo usarlo:

- Al acceder a servicios en dispositivos compartidos.
- Para evitar que se guarden *cookies* o historiales de sesión.

Nota: Usa el modo incógnito junto con una VPN para mejorar tu privacidad.

4.4 Bloqueo de rastreadores y anuncios

Muchos sitios web utilizan rastreadores para recopilar información sobre tus hábitos de navegación. Puedes protegerte con herramientas adicionales:

Extensiones recomendadas:

- **uBlock Origin:** Bloquea anuncios y rastreadores.
- **Privacy Badger:** Detecta y bloquea rastreadores invasivos.
- **HTTPS Everywhere:** Fuerza conexiones seguras (HTTPS) siempre que sea posible.

4.5 Precaución al hacer clic en enlaces

Al hacer clic en enlaces desconocidos, podrías exponerte a ataques de *phishing* o sitios web maliciosos. Sigue estas recomendaciones:

- **Verifica la URL:** Asegúrate de que provenga de una fuente confiable.
- **Evita acortar enlaces sospechosos:** Usa herramientas como VirusTotal para analizar enlaces antes de abrirlos.
- **Desconfía de correos o mensajes urgentes:** Los atacantes suelen usar técnicas de ingeniería social para presionarte a hacer clic.

4.6 Descargas seguras

Evita descargar *software* o archivos de sitios no oficiales. Podrían contener *malware* o virus:

- Descarga aplicaciones exclusivamente desde las tiendas oficiales (Google Play Store, App Store).
- Verifica las firmas digitales de los archivos descargados cuando sea posible.

4.7 ¿Quién puede ver mi navegación en internet?

Cuando navegas por internet, diferentes actores pueden observar y registrar tu actividad dependiendo de cómo esté configurada tu conexión:

Actores involucrados:

1. Proveedor de servicios de internet (ISP):

- Puede ver qué sitios visitas y cuándo lo haces.
- Puede registrar tus actividades si no usas herramientas como VPN.

2. Sitios web:

- Los sitios que visitas pueden recopilar información sobre tu dispositivo, ubicación aproximada y actividad dentro de su página.
- Usan *cookies* para rastrear tu comportamiento en línea.

3. Redes Wi-Fi públicas:

- Si no está cifrada, cualquier persona conectada a la misma red podría interceptar tu tráfico.

4. Gobiernos y entidades de vigilancia:

- En contextos represivos, pueden monitorear la actividad de usuarios en internet para controlar o censurar información.

5.

Seguridad en redes sociales

Las redes sociales son herramientas esenciales para la comunicación y organización de activistas y ONG, pero también representan un riesgo si no se gestionan de manera segura. A continuación, te explicamos cómo proteger tus perfiles y publicaciones en plataformas como Facebook, Instagram, X (antes Twitter) y TikTok.

5.1 Configuración de privacidad en redes sociales

Cada red social ofrece configuraciones de privacidad que te permiten limitar quién puede ver tu información y publicaciones. Sin embargo, la decisión de mantener un perfil público o privado depende de cada activista. Si deseas construir una marca personal o llegar a una mayor audiencia, podrías optar por mantener tu perfil público, asumiendo el riesgo. Si no consideras esto necesario, es recomendable configurar la privacidad de tus redes sociales para mayor seguridad.

Facebook:

1. Ve a «Configuración y privacidad > Configuración > Privacidad».
2. Ajusta:
 - Quién puede ver tus publicaciones futuras: Solo amigos o configuraciones personalizadas.
 - Quién puede enviarte solicitudes de amistad: Amigos de amigos.
 - Revisión de publicaciones: Activa la opción para aprobar publicaciones en las que te etiqueten antes de que aparezcan en tu perfil.

Instagram:

1. Ve a «Configuración > Privacidad».
2. Configura:
 - Cuenta privada: Solo tus seguidores aprobados podrán ver tus publicaciones.

- Etiquetas: Activa la aprobación manual de fotos o videos donde te etiqueten.
- Mensajes: Restringe los mensajes directos de personas que no sigues.

X (Twitter):

1. Ve a «Configuración y privacidad > Privacidad y seguridad».
2. Ajusta:
 - Protege tus posts: Solo los seguidores aprobados podrán ver tus publicaciones.
 - Opciones de etiquetado: Restringe quién puede etiquetarte en fotos.
 - Mensajes directos: Desactiva la recepción de mensajes de personas que no sigues.

TikTok:

1. Ve a «Configuración y privacidad > Privacidad».
2. Configura:
 - Cuenta privada: Solo las personas que apruebes podrán seguirte y ver tus videos.
 - Sincronización de contactos: Desactívala para evitar que personas conocidas encuentren tu perfil.
 - Comentarios y mensajes: Limita estas funciones a seguidores aprobados.

5.2 Publicación segura de contenido sensible

Si necesitas compartir información sensible o denunciar una situación, sigue estas recomendaciones:

1. Evita publicar en tiempo real:

- Retrasa las publicaciones para evitar que alguien pueda localizarte en el momento.

2. Omisiones intencionales:

- Elimina detalles que puedan identificar tu ubicación exacta, como nombres de calles o lugares reconocibles.

3. Usa metadatos seguros:

- Borra metadatos de fotos o videos antes de publicarlos utilizando herramientas como ExifTool o aplicaciones similares.

4. Usa cuentas secundarias:

- Crea cuentas separadas para contenido sensible y mantén tu cuenta principal para interacciones personales.

5.3 Protección contra hackeos de cuentas

Los hackeos son una amenaza constante para las cuentas en redes sociales. Asegúrate de protegerlas con estas medidas:

1. Activa la verificación en dos pasos (2FA):

- Habilítala en todas tus cuentas utilizando una aplicación autenticadora como Authy o Google Authenticator.

2. Revisa los dispositivos conectados:

- En Facebook, Instagram y X (Twitter), puedes ver y cerrar sesión en dispositivos conectados desde «Configuración > Seguridad».

3. Cambia contraseñas regularmente:

- Usa contraseñas largas, únicas y generadas por un gestor de contraseñas.

4. Desconfía de enlaces sospechosos:

- Evita hacer clic en enlaces enviados por mensajes directos o correos que no reconozcas.

5.4 Gestión de cuentas de ONG y activismo

Si gestionas cuentas de una organización, sigue estas prácticas para evitar riesgos:

1. Usa cuentas compartidas seguras:

- Si es viable, utiliza herramientas como Hootsuite o Buffer para publicar sin compartir contraseñas directas. Si no es posible, asegúrate de que las contraseñas sean largas y seguras, y cambia las credenciales regularmente.

2. Limita el acceso:

- Da acceso solo a personal autorizado y revísalo periódicamente.

3. Realiza auditorías de seguridad:

- Verifica regularmente la configuración de privacidad y seguridad de las cuentas.

6.

Respuesta a incidentes

A pesar de tomar medidas de seguridad, pueden ocurrir incidentes que comprometan dispositivos, cuentas o datos. Tener un plan de acción claro es esencial para minimizar el impacto. A continuación, se describen los pasos a seguir ante los incidentes más comunes:

6.1 Qué hacer si un dispositivo es robado o confiscado

Pasos inmediatos:

1. Bloquea el dispositivo de forma remota:

- **Android:** Ve a Encuentra mi dispositivo e inicia sesión con tu cuenta de Google. Bloquea el dispositivo y borra los datos si es necesario.
- **iPhone:** Ve a iCloud > «Buscar mi iPhone». Marca el dispositivo como perdido o elimina los datos remotamente.

2. Cambia las contraseñas de las cuentas vinculadas:

- Prioriza cuentas críticas como correo electrónico, redes sociales y servicios bancarios.
- Activa la verificación en dos pasos si no lo has hecho previamente.

3. Notifica a tu equipo:

- Informa a tus compañeros sobre el incidente para que tomen precauciones adicionales.

4. Denuncia el robo si es seguro hacerlo:

- Presenta la denuncia ante las autoridades locales y guarda una copia del reporte.

6.2 Cómo manejar accesos no autorizados a cuentas

Indicadores de que tu cuenta ha sido comprometida:

- Cambios en tu información personal (correo, contraseña, etc.).

- Actividad que no reconoces, como publicaciones o mensajes enviados sin tu consentimiento.
- Alertas de inicio de sesión desde dispositivos desconocidos.

Pasos inmediatos:

1. Cambia tu contraseña:

- Usa una contraseña única y segura, generada por un gestor de contraseñas.

2. Revisa los dispositivos conectados:

- Cierra sesión en todos los dispositivos que no reconozcas.
Por ejemplo:
 - **Facebook:** Ve a «Configuración > Seguridad e inicio de sesión > Dónde has iniciado sesión».
 - **Google:** Ve a «Tu cuenta > Seguridad > Tus dispositivos».

3. Habilita la verificación en dos pasos:

- Añade una capa de seguridad adicional a tus cuentas para evitar futuros accesos no autorizados.

4. Contacta al soporte de la plataforma:

- Si no puedes recuperar el acceso, solicita asistencia para restablecer tu cuenta.

6.3 Respaldo y recuperación de información

Importancia de los respaldos:

Tener copias de seguridad actualizadas permite recuperar información crítica en caso de incidentes como robo, daño o eliminación accidental de datos.

Buenas prácticas para el respaldo:

1. Haz copias regulares:

- **Frecuencia recomendada:** Semanal para datos críticos.

2. Usa múltiples ubicaciones de almacenamiento:

- **Local:** Discos duros externos cifrados.
- **Nube:** Servicios confiables como Google Drive, Tresorit o Proton Drive.

3. Verifica la integridad de los respaldos:

- Asegúrate de que los archivos se hayan copiado correctamente y sean accesibles.

Pasos para la recuperación:

1. Identifica el respaldo más reciente.
2. Restaura los datos en un dispositivo seguro.
3. Cambia contraseñas y refuerza las medidas de seguridad antes de usar los datos restaurados.

7.

Ciberseguridad en actividades y eventos

Las actividades y eventos como talleres y movilizaciones representan momentos clave para la participación, pero también son escenarios donde la seguridad digital puede verse comprometida. Estas recomendaciones te ayudarán a minimizar riesgos durante estos momentos.

7.1 Seguridad digital en talleres y capacitaciones

Antes del taller:

1. Evalúa los riesgos del entorno:

- Identifica posibles amenazas como infiltración, vigilancia o sabotaje.

2. Prepara dispositivos seguros:

- Usa dispositivos configurados para minimizar vulnerabilidades (por ejemplo, sin información sensible almacenada).
- Actualiza el sistema operativo y las aplicaciones.

3. Proporciona lineamientos de seguridad a los participantes:

- Comparte recomendaciones básicas como evitar redes Wi-Fi públicas y no compartir enlaces o archivos sin verificar.

Cómo seleccionar a los participantes del taller:

1. Establece criterios claros de participación:

- Define qué tipo de personas o perfiles son relevantes para el objetivo del taller.
- Prioriza participantes con referencias confiables o que pertenezcan a redes o grupos conocidos.

2. Solicita información previa:

- Pide datos como nombres completos, organización a la que pertenecen y su experiencia previa en el tema.

3. Verifica antecedentes:

- Realiza búsquedas en redes sociales para confirmar su identidad y actividad.
- Contacta a terceros que puedan validar la información del participante.

4. Establece recomendaciones de ubicación:

- Si el taller es presencial, organiza el evento en un lugar discreto y seguro.
- Considera la posibilidad de dividir los grupos si hay dudas sobre la seguridad de todos los asistentes.

Durante el taller:

1. Establece reglas de privacidad:

- Prohíbe grabaciones o fotos sin el consentimiento de todos los participantes.

2. Usa herramientas seguras para la comunicación:

- Plataformas como Signal o Jitsi Meet son ideales para la comunicación en tiempo real.

3. Monitorea el entorno digital:

- Identifica cualquier actividad inusual en las redes Wi-Fi o dispositivos.

7.2 Seguridad en protestas y movilizaciones

Antes de la protesta:

1. Configura tu teléfono para mayor seguridad:

- Activa el bloqueo por PIN o contraseña.
- Desactiva la sincronización automática de datos sensibles (correo, fotos, etc.).
- Lleva un dispositivo secundario si es posible, dejando tu teléfono principal en casa.

2. Minimiza la información personal:

- Elimina datos innecesarios y desactiva las notificaciones de aplicaciones sensibles.

3. Informa a alguien de confianza:

- Comunica tu ubicación y horario estimado de regreso.

Durante la protesta:

1. Usa aplicaciones seguras:

- Utiliza Signal o Briar para la comunicación.

2. Desactiva conexiones innecesarias:

- Mantén desactivado el Bluetooth y Wi-Fi para evitar rastreos.

3. Protege tus archivos:

- Usa aplicaciones como Haven para registrar cualquier intento de manipulación de tu dispositivo.

Uso de Haven:

Haven es una aplicación diseñada para convertir tu dispositivo móvil en un sistema de monitoreo de seguridad. Es especialmente útil para detectar manipulaciones o accesos no autorizados a tu dispositivo durante protestas o actividades.

1. Cómo funciona:

- Utiliza los sensores del teléfono (micrófono, cámara, acelerómetro) para registrar actividad sospechosa.
- Envía alertas y registros a un dispositivo secundario o a tu correo electrónico.

2. Pasos para configurarlo:

- Descarga Haven desde la tienda oficial de aplicaciones o su página de GitHub.
- Configura las alertas y selecciona los eventos que deseas monitorear (sonido, movimiento, etc.).
- Vincula un número de contacto o correo para recibir las notificaciones.

3. Recomendaciones de uso:

- Instálalo en un dispositivo secundario que puedas dejar en un lugar fijo.
- Úsalo para monitorear entradas, habitaciones o mochilas durante actividades.

Después de la protesta:

1. Revisa tu dispositivo:

- Verifica si hay aplicaciones nuevas o cambios inesperados en la configuración.

2. Limpia datos sensibles:

- Borra chats y archivos que ya no sean necesarios.

7.3 Uso seguro de Wi-Fi público

Evita redes no confiables:

- Si es indispensable usarlas, conecta siempre una VPN confiable como ProtonVPN o RiseupVPN.

Desactiva el uso compartido:

- Asegúrate de desactivar la opción de compartir archivos o impresoras en redes públicas.

Verifica la autenticidad de la red:

- Confirma el nombre exacto de la red antes de conectarte para evitar ataques de tipo «man-in-the-middle».

7.4 Monitoreo y prevención de vigilancia digital

1. Usa herramientas para detectar vigilancia:

- Aplicaciones como «GlassWire» o «NetGuard» pueden ayudarte a identificar actividad sospechosa en tu red.

2. Reduce tu huella digital:

- Publica en redes sociales solo información esencial y evita detalles sobre tu ubicación en tiempo real.

3. Cifra tus comunicaciones:

- Usa aplicaciones de mensajería que ofrezcan cifrado de extremo a extremo.

8.

Uso de mensajería instantánea

La mensajería instantánea es una de las herramientas de comunicación más utilizadas por activistas y ONG, pero su seguridad varía dependiendo de la aplicación utilizada. En esta sección, analizamos los riesgos y recomendaciones para el uso de SMS, WeChat, Telegram, WhatsApp, Signal y Wire.

8.1 SMS (Mensajes de texto)

Los mensajes de texto tradicionales (SMS) carecen de cifrado y pueden ser interceptados fácilmente por actores malintencionados o proveedores de servicios.

Riesgos:

- Sin cifrado: Cualquier mensaje enviado por SMS puede ser leído por terceros.
- Suplantación de identidad: Los SMS pueden falsificarse con técnicas como el *spoofing*.

Recomendaciones:

- Evita enviar información sensible por SMS.
- Usa SMS solo como última opción en ausencia de aplicaciones más seguras.

8.2 WeChat

WeChat es una aplicación popular en algunos países, pero presenta serias preocupaciones de seguridad y privacidad debido a su vinculación con el gobierno chino.

Riesgos:

- Monitoreo gubernamental: Los mensajes pueden ser escaneados y almacenados.
- Falta de transparencia: No ofrece garantías claras sobre el cifrado de extremo a extremo.

Recomendaciones:

- Evita usar WeChat para comunicaciones sensibles.
- Si necesitas usarlo, limita la información compartida y utiliza otros medios para discusiones confidenciales.

8.3 Telegram

Telegram es una aplicación popular que ofrece algunas funciones de seguridad, pero no utiliza cifrado de extremo a extremo de manera predeterminada en los chats regulares.

Riesgos:

- Los chats por defecto no están cifrados de extremo a extremo.
- La información puede almacenarse en los servidores de Telegram.

Recomendaciones:

- Usa «chats secretos» para habilitar el cifrado de extremo a extremo.
- Activa la autodestrucción de mensajes en los chats secretos para mayor seguridad.
- No compartas información altamente sensible en Telegram.

8.4 WhatsApp

WhatsApp ofrece cifrado de extremo a extremo de manera predeterminada, lo que lo hace más seguro que muchas otras aplicaciones. Sin embargo, es importante tener en cuenta que pertenece a Meta (Facebook).

Riesgos:

- Los metadatos (qué, cuándo, con quién) no están cifrados.
- Al enviar fotos en calidad HD, los metadatos no se eliminan.
- La seguridad de las copias de seguridad en la nube depende del cifrado habilitado por el usuario.

Recomendaciones:

- 1. Activa la verificación en dos pasos:** Protege tu cuenta con una capa adicional de seguridad.
- 2. Desactiva las copias de seguridad en la nube o habilita su cifrado:** Esto evitará que las copias sean vulnerables a accesos externos.

3. Revisa la configuración de privacidad:

- Ajusta quién puede ver tu foto de perfil, estado y última conexión.
- Limita esta información a «Mis contactos» o «Mis contactos excepto...» si lo consideras necesario.

4. Configura los estados:

- Define manualmente quién puede ver tus estados para evitar compartir información con personas innecesarias.

5. Activa los mensajes temporales:

- Configura tus chats para que los mensajes desaparezcan automáticamente después de un período definido.

6. Utiliza chats restringidos:

- Limita el acceso a conversaciones sensibles y evita que otros puedan hacer capturas de pantalla si es posible.

7. Verifica los códigos de seguridad de tus contactos:

- Asegúrate de que estás comunicándote con la persona correcta.

8.5 Signal

Signal es ampliamente considerado como una de las aplicaciones de mensajería más seguras debido a su cifrado de extremo a extremo y su compromiso con la privacidad.

Ventajas:

- Cifrado de extremo a extremo para todos los mensajes y llamadas.
- Sin almacenamiento de metadatos.
- Opciones avanzadas de seguridad, como mensajes que desaparecen.

Recomendaciones:

- Utiliza Signal como tu principal herramienta de comunicación para temas sensibles.
- Habilita mensajes que desaparecen para proteger información a corto plazo.
- Cambia el ícono de la aplicación en la configuración para que no sea reconocible como Signal en caso de revisiones de dispositivos.

8.6 Wire

Wire es otra aplicación segura que ofrece cifrado de extremo a extremo y está diseñada para uso personal y profesional.

Ventajas:

- Cifrado de extremo a extremo para mensajes y videollamadas.
- Compatible con dispositivos múltiples sin comprometer la seguridad.
- Transparencia: Es de código abierto y cumple con las normativas europeas de privacidad.

Recomendaciones:

- Usa Wire como una alternativa a Signal para comunicaciones confidenciales.
- Revisa periódicamente las sesiones activas y cierra las innecesarias.

9.

Respaldo y almacenamiento de información

Los datos son uno de los recursos más valiosos para activistas y organizaciones. Protegerlos mediante respaldos y almacenamiento seguro garantiza su disponibilidad y evita el acceso no autorizado. En esta sección abordaremos cómo implementar sistemas de respaldo, herramientas de cifrado y estrategias para eliminar datos de manera segura.

9.1 Sistemas de respaldo seguros

Tipos de respaldo:

1. Local:

- Almacenamiento en dispositivos físicos como discos duros externos o memorias USB.
- Ventajas: Control total sobre los datos.
- Riesgos: Pérdida o daño físico.

2. En la nube:

- Servicios como Google Drive, Tresorit o Proton Drive.
- Ventajas: Acceso desde cualquier lugar y copia de seguridad redundante.
- Riesgos: Dependencia de terceros.

Buenas prácticas para respaldos:

1. Realiza respaldos regulares (al menos semanalmente para datos críticos).
2. Mantén múltiples copias en diferentes ubicaciones (regla 3-2-1):
 - 3 copias de los datos.
 - 2 formatos diferentes (local y nube).
 - 1 copia fuera del lugar principal.
3. Usa discos duros cifrados para respaldos locales.
4. Verifica periódicamente la integridad de los respaldos.

9.2 Herramientas de cifrado para documentos y archivos

El cifrado es esencial para proteger datos sensibles, asegurando que solo personas autorizadas puedan acceder a ellos.

Herramientas recomendadas:

1. Veracrypt:

- *Software* gratuito para crear volúmenes cifrados en discos locales o externos.
- Ofrece opciones de cifrado avanzado (AES, Serpent, Twofish).

2. BitLocker (Windows):

- Integrado en algunas versiones de Windows.
- Permite cifrar discos completos o unidades externas.

3. FileVault (Mac):

- Cifra todo el disco duro de manera nativa.

4. Cryptomator:

- Diseñado para cifrar archivos almacenados en la nube.

Recomendaciones:

1. Usa contraseñas largas y complejas para proteger tus volúmenes cifrados.
2. Evita guardar contraseñas en lugares inseguros; utiliza un gestor de contraseñas.
3. Cifra los archivos antes de subirlos a servicios en la nube.

9.3 Cómo eliminar datos de forma segura

Eliminar un archivo de manera convencional no lo borra realmente; los datos pueden ser recuperados con herramientas especializadas. Para garantizar su eliminación total, es necesario usar métodos seguros.

Herramientas para eliminar datos:

1. Eraser (Windows):

- Sobrescribe varias veces los archivos eliminados para hacerlos irrecuperables.

2. BleachBit (Windows, Linux):

- Borra archivos y limpia espacio libre del disco.

3. Secure Empty Trash (Mac):

- Borra archivos eliminados del basurero de forma segura.

4. DBAN (Darik's Boot and Nuke):

- Herramienta para limpiar discos duros completos.

Recomendaciones:

1. Elimina los archivos con herramientas seguras antes de desechar dispositivos.
2. Si el dispositivo contiene información altamente sensible, considera la destrucción física del disco duro.

10.

Seguridad avanzada para activistas

La seguridad avanzada es crucial para activistas que enfrentan mayores riesgos debido a su trabajo en contextos represivos. Esta sección detalla herramientas y prácticas avanzadas para proteger documentos, anonimizar actividades y utilizar sistemas operativos seguros.

10.1 Análisis de metadatos en documentos e imágenes

Los metadatos pueden revelar información sensible, como ubicaciones, nombres de usuarios y fechas. Antes de compartir documentos o fotos, es importante eliminarlos.

Herramientas para eliminar metadatos:

1. ExifTool (Windows, Mac, Linux):

- Una herramienta poderosa para analizar y eliminar metadatos de fotos y documentos.

2. MAT (Metadata Anonymization Toolkit) (Linux):

- Diseñado para eliminar metadatos de diferentes tipos de archivos.

3. Verifica en tu sistema operativo:

- En Windows: Haz clic derecho en el archivo, selecciona «Propiedades > Detalles > Quitar propiedades e información personal».
- En Mac: Usa la vista previa para eliminar metadatos básicos.

Recomendaciones:

1. Revisa y elimina metadatos antes de compartir documentos o imágenes sensibles.
2. Si es posible, utiliza herramientas especializadas como ExifTool para garantizar la eliminación completa.

10.2 Uso de sistemas operativos seguros

Los sistemas operativos seguros ayudan a proteger tu privacidad y anonimato al realizar actividades sensibles. Aquí te damos recomendaciones para Tails, Linux, Windows y Mac.

Recomendaciones para Tails:

1. Usa Tails desde un USB:

- Inicia tu computadora desde un USB con Tails para evitar dejar rastros en el dispositivo.

2. Aprovecha las herramientas integradas:

- Usa Tor Browser para anonimizar tu navegación.
- Protege tus archivos con herramientas de cifrado como VeraCrypt.

3. Mantén el USB seguro:

- Usa una contraseña fuerte para proteger el acceso al USB que contiene Tails.

Recomendaciones para Linux:

1. Elige una distribución segura:

- Usa distribuciones como Ubuntu, Debian o Qubes OS para mayor privacidad.

2. Mantén el sistema actualizado:

- Instala regularmente parches de seguridad.

3. Usa cifrado de disco completo:

- Configura el cifrado al instalar Linux para proteger tus datos en caso de pérdida o robo.

4. Instala herramientas de privacidad:

- Usa *firewalls* como UFW (Uncomplicated Firewall) para proteger tu red.

Recomendaciones para Windows:

1. Mantén el sistema operativo actualizado:

- Activa las actualizaciones automáticas para recibir parches de seguridad.

2. Activa BitLocker:

- Cifra tu disco duro para proteger tus datos en caso de pérdida o robo.

3. Usa una cuenta estándar:

- Evita usar cuentas con privilegios de administrador para reducir el riesgo de instalación de *malware*.

4. Habilita un antivirus confiable:

- Usa Windows Defender o una alternativa confiable y mantenlo actualizado.

5. Configura un *firewall*:

- Asegúrate de que el Firewall de Windows esté activado y configurado correctamente.

6. Desactiva el acceso remoto:

- Desactiva «Escritorio remoto» si no lo necesitas para evitar accesos no autorizados.

Recomendaciones para Mac:

1. Mantén el sistema operativo actualizado:

- Instala las actualizaciones de seguridad tan pronto como estén disponibles.

2. Activa FileVault:

- Cifra tu disco duro para proteger los datos almacenados.

3. Usa una cuenta estándar:

- Configura una cuenta de usuario sin privilegios administrativos para tareas cotidianas.

4. Configura el *firewall*:

- Ve a «Preferencias del sistema > Seguridad y privacidad > Firewall» y actívalo.

5. Desactiva la opción de «Compartir»:

- Desactiva servicios de compartición como AirDrop, Bluetooth y uso compartido de archivos si no los necesitas.

6. Utiliza herramientas de privacidad integradas:

- Configura «Transparencia, Consentimiento y Control» (TCC) para restringir el acceso de aplicaciones a tus datos.

10.3 Anonimato en internet: Tor y otras herramientas

El anonimato en línea protege tu identidad y evita la vigilancia al navegar en internet.

Herramientas recomendadas:

1. Tor Browser:

- Navegador diseñado para proteger el anonimato al redirigir tu tráfico a través de la red Tor.
- Recomendado para acceder a sitios bloqueados o censurados.

2. VPN confiables:

- Utiliza servicios como ProtonVPN o RiseupVPN para cifrar tu tráfico y ocultar tu dirección IP.

3. Brave con Tor:

- Ofrece una opción integrada para navegar a través de la red Tor.

4. DuckDuckGo:

- Motor de búsqueda que no rastrea tu actividad.

Recomendaciones:

1. Usa Tor Browser para actividades donde necesites proteger tu identidad.
2. Combina Tor con una VPN confiable para mayor seguridad.
3. Evita iniciar sesión en cuentas personales mientras usas herramientas de anonimato.

Conclusión

La seguridad digital no es un destino, sino un proceso continuo. Recuerda que somos tan fuertes como nuestro eslabón más débil, y la protección de tu información depende de integrar estas recomendaciones en tus prácticas y procesos diarios. Cada paso que tomes para fortalecer tu seguridad, desde eliminar metadatos hasta usar sistemas operativos seguros, contribuye a reducir los riesgos y proteger frente a amenazas.

Adoptar una mentalidad proactiva y revisar regularmente tus medidas de seguridad te permitirá mantener el control sobre tus datos y proteger tanto tu privacidad como la de tus compañeros y comunidades. ¡Haz de la seguridad digital una prioridad constante!

Manual de SEGURIDAD DIGITAL para organizaciones de la sociedad civil

Elaborado para el Centro de Divulgación del Conocimiento Económico «Cedice Libertad» por **Luis Serrano**, coordinador de la ONG RedesAyuda. Especialista en seguridad digital y derechos humanos con más de diez años de experiencia capacitando en las áreas de derechos humanos, tecnología y digitalización. @redesayuda

Coordinación editorial

Rocío Gujjarro

Corrección

Alberto Márquez

Diseño

ABV Taller de Diseño

Carolina Arnal

© Centro de Divulgación
del Conocimiento Económico
«CEDICE Libertad»

HECHO EL DEPÓSITO DE LEY
Deposito Legal: DC2025000199
ISBN: 978-980-434-067-3
Caracas, Venezuela
Febrero 2025

Centro de Divulgación del Conocimiento Económico «Cedice Libertad»

Av. Andrés Eloy Blanco (Este 2)
Edificio Cámara de Comercio de
Caracas. Nivel Auditorio, Los
Caobos, Caracas, Venezuela.
Teléfono: +58 (212) 571.3357
Correo electrónico:
cedice@cedice.org.ve
www.cedice.org.ve
X: @cedice
RIF: J-00203592-7



El Centro de Divulgación el Conocimiento Económico, A.C. Cedice Libertad, tiene como objetivo principal la búsqueda de una sociedad libre, responsable y humana. Las interpretaciones, ideas o conclusiones contenidas en las publicaciones de Cedice Libertad deben atribuirse a sus autores y no al instituto, a sus directivos, al comité académico o a las instituciones que apoyan sus proyectos o programas. Cedice Libertad considera que la discusión de las ideas contenidas en sus publicaciones pueden contribuir a la formación de una sociedad basada en la libertad y la responsabilidad. Esta publicación puede ser reproducida parcial o totalmente, siempre que se mencione el origen y el autor, y sea comunicado a Cedice Libertad.



ATLAS
NETWORK

