Guía complementaria Módulo 4: Derechos Digitales y Seguridad Digital; Curso Democracia Inclusiva y Derechos en Acción; OTD Chile, enero 2026.

Introducción

La seguridad digital es el conjunto de prácticas y herramientas que ayudan a proteger tu información personal y la de tu organización en internet. Esta guía está pensada para apoyar con herramientas prácticas a les estudiantes del curso Democracia Inclusiva y Derechos en Acción de OTD Chile.

Contraseñas Seguras

Las contraseñas son la primera barrera de protección en internet. Una contraseña débil puede ser adivinada fácilmente.

Características de una contraseña segura:

- Al menos 14 caracteres.
- Combina letras mayúsculas, minúsculas, números y símbolos.
- No usar datos personales (nombres, fechas de nacimiento, etc.).

Ejemplo: `M!cR0s0ft2026#`

Gestores de contraseñas: Los gestores de contraseñas son programas que guardan y protegen todas tus claves en un solo lugar de forma cifrada. Sirven para crear, almacenar y usar contraseñas seguras sin necesidad de recordarlas todas manualmente.

Gestor	Tipo	Ventajas	Limitaciones	Enlace
KeePassXC	Software libre, local	Gratuito, control total	Requiere instalación y aprendizaje	www.keepassxc.org
Bitwarden	Libre, nube/local	Fácil de usar, multiplataforma	Depende de internet si se usa en la nube	www.bitwarden.com
1Password	Comercial	Interfaz amigable	Tiene costo	www.1password.com
LastPass	Comercial, nube	Acceso desde cualquier lugar	Riesgo si el servicio es atacado	www.lastpass.com

Autenticación en dos pasos (2FA)

La autenticación en dos pasos añade una capa extra de seguridad. Además de tu contraseña, necesitas un segundo factor para entrar.

Método	Cómo funciona	Ventajas	Desventajas
SMS/Correo	Código enviado al teléfono/correo	Fácil de usar	Vulnerable a ataques de SIM swapping y phishing.
App de autenticación	Genera códigos en tu teléfono	Más seguro, funciona sin internet	Riesgo si pierdes el teléfono
Llave física	Dispositivo USB/NFC	Máxima seguridad	Tiene costo, riesgo de pérdida
Biometría	Huella, rostro, iris	Rápido y cómodo	Puede ser falsificado, no siempre aceptado

Ejemplos de apps de autenticación:

- Google Authenticator
- Authy
- Microsoft Authenticator

Llaves físicas de seguridad:

- YubiKey
- SoloKey
- Google Titan Security Key

Comunicación Segura

Para proteger tus conversaciones, usa aplicaciones que cifran los mensajes.

Aplicación	Características	Enlace
Signal	Mensajería cifrada de extremo a extremo	www.signal.org
Element (Matrix)	Chats descentralizados con cifrado	www.element.io
Wire	Mensajería y llamadas seguras	www.wire.com

Navegación Segura en Internet

Un navegador seguro protege tu privacidad y evita rastreadores.

Navegador	Enfoque	Ventajas	Limitaciones	Enlace
Brave	Privacidad y bloqueo de anuncios	Bloquea rastreadores	Algunas webs no cargan bien	www.brave.com
Tor Browser	Anonimato extremo	Oculta IP y tráfico	Más lento	www.torproject.org
Firefox (configurado)	Equilibrio	Código abierto, extensiones	Requiere ajustes manuales	www.mozilla.org/firefox
DuckDuckGo Browser	Privacidad	Bloquea rastreadores	Funciones limitadas	duckduckgo.com
Epic Privacy Browser	Privacidad simplificada	Incluye proxy	Pocas extensiones	www.epicbrowser.com

Correos Electrónicos Seguros

Servicio	Características	Enlace
ProtonMail	Correo cifrado, gratuito	www.proton.me
Riseup	Correo para movimientos sociales	www.riseup.net

Copias de Respaldo Seguras

Hacer copias de respaldo cifradas significa guardar tus archivos en un medio de almacenamiento (disco duro, nube, servidor) pero protegidos con un algoritmo de cifrado, de modo que solo puedan abrirse con una clave o contraseña segura. Esto es clave para activistas, organizaciones y cualquier persona que maneje información sensible.

Herramientas recomendadas:

- VeraCrypt
- Cryptomator
- Duplicati
- GnuPG

Cómo hacer copias de respaldo seguras para los archivos de mi organización

1. Elegir el medio de respaldo

Discos externos / USB → fáciles de usar, pero deben guardarse en lugares seguros.

Servidores autogestionados → mayor control, ideales para colectivos.

Nube cifrada → servicios como Proton Drive, Tresorit o Nextcloud con cifrado extremo a extremo.

2. Usar herramientas de cifrado

VeraCrypt → crea contenedores cifrados o cifra discos completos.

Cryptomator → pensado para cifrar carpetas que luego se sincronizan en la nube.

Duplicati → software libre que hace respaldos automáticos y cifrados en múltiples destinos.

GnuPG (GPG) → para cifrar archivos individuales antes de guardarlos o enviarlos.

3. Configurar la clave de cifrado

Usar una contraseña larga y robusta (mínimo 14 caracteres, combinando letras, números y símbolos).

Guardar la clave en un gestor de contraseñas (KeePassXC, Bitwarden).

No reutilizar la misma clave en otros sistemas.

4. Automatizar respaldos

Programar copias periódicas (diarias, semanales).

Mantener al menos dos copias: una local y otra externa (ej. nube o servidor comunitario).

Verificar regularmente que los respaldos se restauran correctamente.

Recomendaciones de buenas prácticas para respaldar archivos

Principio 3-2-1: 3 copias de tus datos, en 2 tipos de medios, 1 fuera de tu ubicación principal.

Separar respaldos sensibles: no mezclar datos personales con información pública.

Documentar protocolos: que tu equipo sepa cómo cifrar, respaldar y restaurar.

Software libre: Usarlo siempre que sea posible, para mayor transparencia y confianza.

Qué es una VPN

Una VPN (Red Privada Virtual) crea un túnel cifrado entre tu dispositivo y un servidor remoto. Sirve para:

- Ocultar tu dirección IP.
- Proteger datos en redes públicas.
- Evitar censura.

Ejemplos de software VPN:

- OpenVPN
- WireGuard
- ProtonVPN

Organizaciones de Apoyo

Existen varias organizaciones que brindan apoyo para activistas que enfrentan ataques o problemas relacionados a su seguridad digital o de sus organizaciones. Ten cerca sus contactos por si llegas a necesitarlos.

Organización	Apoyo	Enlace
Access Now	Ayuda técnica inmediata frente a ataques digitales	www.accessnow.org/help
Front Line Defenders	Protección a defensores de DDHH	www.frontlinedefenders.org
EFF	Defensa legal y técnica de la libertad digital	www.eff.org
Amnistía Internacional	Security Lab contra ataques digitales	www.amnesty.org
Tactical Tech	Capacitación en seguridad digital	www.tacticaltech.org
Derechos Digitales	ONG regional en América Latina	www.derechosdigitales.org

Mensaje final

La seguridad digital no es complicada si se aprende paso a paso. Empieza con contraseñas seguras, luego añade autenticación en dos pasos, usa aplicaciones de comunicación cifrada y navegadores seguros. Con el tiempo, podrás implementar respaldos cifrados y VPN comunitarias. La clave es la práctica y el aprendizaje constante.