



ALIANZA
HUMEDALES
ANDINOS

PROTOCOLO PARA DEFENSOR@S AMBIENTALES

CUIDADOS DIGITALES, SEGURIDAD
FÍSICA Y ORGANIZACIONAL



ALIANZA
HUMEDALES
ANDINOS

ÍNDICE

1. Introducción y Fundamentos.....	4
1.1 Contexto regional y principales desafíos.....	4
1.2 Objetivos del protocolo.....	6
1.3 Alcance y destinatarios.....	7
1.4 Definición de personas defensoras ambientales.....	7
1.5 Principios rectores del protocolo.....	8
 2. Identificación de Riesgos y Respuestas Asociadas.....	 9
2.1 Riesgos digitales, reputacionales y mediáticos.....	9
2.1.1 Seguridad de los dispositivos de trabajo.....	10
2.1.2 Seguridad de las cuentas y datos.....	19
2.1.3 Seguridad en las redes sociales y páginas web institucionales....	21
2.1.4 Ataques digitales.....	24
 2.2 Seguridad Física y Organizacional.....	 25
2.2.1 Vigilancia, seguimiento y hostigamiento en el territorio.....	25
2.2.1.1 Identificación y registro de incidentes.....	25
2.2.1.2 Comunicación inmediata y activación de redes.....	26
2.2.1.3 Medidas preventivas en terreno.....	26
2.2.1.4 Protección ante el Estado y las empresas.....	26
2.2.1.5 Protección vinculada a investigaciones y monitoreos ambientales.....	27
2.2.1.6 Principio de seguridad colectiva.....	27
2.2.1.7 Evaluación de riesgo territorial.....	27
2.2.2 Amenazas verbales o escritas.....	28
2.2.2.1 Tipos de amenazas y supuestos de riesgo.....	28
2.2.2.2 Medidas preventivas y recomendaciones generales.....	28
2.2.2.3 Procedimiento ante la recepción de una amenaza.....	29
2.2.3 Represión en protestas.....	29
2.2.4 Seguridad en salidas a terreno.....	30
2.2.5 Ingreso no autorizado a sede o domicilio.....	32

1. INTRODUCCIÓN Y FUNDAMENTOS

1.1 Contexto regional y principales desafíos.

América Latina y el Caribe concentran una gran proporción de los conflictos socioambientales a nivel global debido a la vasta riqueza en biodiversidad, ecosistemas estratégicos y bienes naturales presentes en la región. La expansión de actividades extractivas —como la minería, la explotación de hidrocarburos, la generación hidroeléctrica, la industria forestal y la agroindustria a gran escala— ha generado crecientes tensiones territoriales entre proyectos económicos y las comunidades que habitan y dependen de estos ecosistemas.

Diversos informes internacionales han documentado que América Latina es actualmente la región más peligrosa del mundo para las personas defensoras del medio ambiente y de los derechos humanos. Según el informe anual de Global Witness, al menos 196 personas defensoras de la tierra y del medio ambiente fueron asesinadas en 2023, registrándose que aproximadamente el 85% de estos casos ocurrieron en América Latina. Países como Colombia, Brasil, México y Honduras concentran la mayor parte de estos ataques, muchos de ellos vinculados a conflictos por la explotación de recursos naturales,

minería, expansión agroindustrial y proyectos de infraestructura¹.

La evidencia también muestra que las agresiones contra personas defensoras no se limitan a la violencia física, sino que incluyen criminalización judicial, campañas de estigmatización, vigilancia, amenazas y hostigamiento, especialmente en contextos de disputa territorial asociados a actividades extractivas. Informes de Front Line Defenders² indican que las personas defensoras vinculadas a la tierra, los territorios indígenas y el medio ambiente constituyen uno de los grupos más expuestos a ataques, detenciones arbitrarias y persecución judicial a nivel global.

En este escenario, los pueblos indígenas y las comunidades rurales se encuentran particularmente expuestos. Diversos estudios muestran que los pueblos indígenas representan una proporción desproporcionadamente alta de víctimas de violencia contra defensores ambientales, debido a que sus territorios suelen coincidir con áreas de alta biodiversidad y con importantes reservas de recursos naturales, lo que intensifica los conflictos socioambientales en torno a proyectos extractivos.

¹ Global Witness. (2024). Standing firm: The land and environmental defenders on the frontlines of the climate crisis. Global Witness.

² Front Line Defenders. (2023). Global Analysis 2022/2023: The situation of human rights defenders at risk worldwide. Front Line Defenders

La oposición o cuestionamiento a proyectos extractivos que involucran intereses económicos de gran escala puede situar a las personas defensoras en contextos de alta vulnerabilidad. Estas situaciones suelen incluir hostigamiento, intimidación, vigilancia territorial o digital, estigmatización pública y, en algunos casos, agresiones físicas o procesos judiciales destinados a debilitar la defensa ambiental.

Estas dinámicas resultan particularmente visibles en territorios asociados a la explotación de minerales críticos para la transición energética, especialmente en el denominado “**triángulo del litio**”, que comprende zonas de Bolivia, Argentina y Chile. En estos territorios altoandinos, donde se ubican importantes sistemas salinos como el Salar de Atacama, Maricunga, Ascotán, Salinas Grandes, el Salar del Hombre Muerto, Uyuni y Coipasa, la creciente presión por la extracción de litio ha intensificado los conflictos socioambientales y los riesgos para comunidades indígenas, campesinas y organizaciones territoriales.

Las comunidades que habitan estos ecosistemas dependen directamente de los salares, humedales altoandinos y aguas subterráneas para su subsistencia cultural, económica y espiritual. La defensa de estos territorios ha generado escenarios de tensión con actores estatales y privados, incrementando la exposición de defensores y defensoras a diversas

formas de violencia, vigilancia y criminalización.

Frente a este escenario, resulta fundamental fortalecer mecanismos institucionales y sociales que garanticen condiciones seguras para la defensa del medio ambiente y los derechos humanos.

Uno de los instrumentos más relevantes en esta materia es el **Acuerdo de Escazú**,³ el primer tratado ambiental regional de América Latina y el Caribe que establece obligaciones para los Estados en materia de acceso a la información ambiental, participación pública en la toma de decisiones y acceso a la justicia en asuntos ambientales. Asimismo, constituye el primer tratado internacional que incorpora disposiciones específicas para la protección de las personas defensoras de derechos humanos en asuntos ambientales.

El artículo 9 del Acuerdo de Escazú establece que los Estados deben garantizar un entorno seguro y propicio para que las personas defensoras puedan actuar sin amenazas, restricciones ni inseguridad, reconociendo su rol fundamental en la protección del medio ambiente y en el fortalecimiento de la democracia ambiental.

3 CEPAL. (2018). Acuerdo Regional sobre Acceso a la Información, Participación Pública y Acceso a la Justicia en Asuntos Ambientales en América Latina y el Caribe (Acuerdo de Escazú). Naciones Unidas.

1.2. Objetivos del protocolo.

OBJETIVO GENERAL:

Establecer lineamientos y recomendaciones que permitan fortalecer la seguridad digital, física y organizacional de las personas y organizaciones integrantes de la **Alianza de Humedales Andinos** (AHA), reduciendo los riesgos asociados a amenazas, ataques o vulneraciones vinculadas a su labor de defensa ambiental.

OBJETIVOS ESPECÍFICOS:

- **Proteger** la información sensible vinculada a las causas ambientales, territorios y personas defensoras.
- **Promover** el uso de herramientas seguras de comunicación y gestión de información.
- **Prevenir y mitigar** riesgos asociados a ataques digitales, filtraciones de datos y campañas de hostigamiento o desinformación.
- **Proponer** medidas preventivas y de respuesta para resguardar la seguridad física y la integridad de las personas defensoras ambientales.

1.3. Alcance y destinatarios.

El presente protocolo tiene como finalidad entregar orientaciones y herramientas destinadas a fortalecer la seguridad digital, física y organizacional de quienes participan en la defensa del medio ambiente y de los territorios.

Este documento está dirigido principalmente a:

- **Personas** defensoras del medio ambiente.
- **Comunidades** indígenas y organizaciones territoriales.
- **Organizaciones** no gubernamentales (ONG) vinculadas a la defensa socioambiental.
- **Equipos** técnicos y asesores legales que acompañan procesos de defensa territorial.

El protocolo posee un carácter regional, con foco en los territorios de Bolivia, Chile y Argentina, donde la expansión de actividades extractivas —como la minería de litio, la minería metálica, proyectos energéticos y otras iniciativas de gran escala— ha intensificado los conflictos socioambientales y los riesgos para las personas defensoras.

Asimismo, el documento reconoce la especial vulnerabilidad que enfrentan las defensoras indígenas, comunitarias y territoriales, quienes muchas veces experimentan riesgos diferenciados asociados a desigualdades de género, discriminación estructural y violencia territorial.

1.4 Definición de personas defensoras ambientales

Para efectos del presente protocolo, se entiende por personas defensoras de derechos humanos en asuntos ambientales a aquellas personas, grupos u organizaciones que promueven y defienden los derechos humanos vinculados a la protección del medio ambiente, los territorios y los bienes naturales.

El Acuerdo de Escazú define a los y las defensoras ambientales y de derechos humanos como “personas, grupos y organizaciones que promueven y defienden los derechos humanos en asuntos ambientales”⁴. La Corte Interamericana de Derechos Humanos ha definido a los y las defensoras de derechos humanos como “cualquier persona que realice una actividad de promoción y defensa de algún derecho humano, y se autodenomina como tal o tenga reconocimiento social de su defensa”, siendo los y las defensoras ambientales aquellas que se dedican a asuntos ambientales⁵. Este estatus se deriva de la labor de defensa realizada, y no requiere de un reconocimiento formal ni de que dicha actividad sea permanente.⁶

⁴ Acuerdo de Escazú, artículo 9.1

⁵ Baraona Bray vs Chile [2023] Corte Interamericana de Derechos Humanos, Serie C 481, párr. 71.

⁶ Ídem, párr. 70

1.5. Principios rectores del protocolo

El presente protocolo se fundamenta en los siguientes principios orientadores:

Enfoque de Derechos Humanos

Reconoce que la defensa del medio ambiente constituye una dimensión fundamental de la protección de los derechos humanos, especialmente en relación con el derecho a la vida, la salud, el agua, el territorio y un medio ambiente sano.

Perspectiva de género

Reconoce que la defensa del medio ambiente constituye una dimensión fundamental de la protección de los derechos humanos, especialmente en relación con el derecho a la vida, la salud, el agua, el territorio y un medio ambiente sano.

Interculturalidad y reconocimiento de Pueblos Originarios

Reconoce el rol fundamental de los pueblos indígenas en la protección de los territorios, ecosistemas y bienes naturales, así como la importancia de respetar sus sistemas de conocimiento, organización y gobernanza territorial.

Principio precautorio

En contextos de incertidumbre o riesgo potencial para la seguridad de las personas defensoras, se deberán adoptar medidas preventivas orientadas a evitar o reducir posibles daños.

Derecho a defender derechos

Este protocolo reconoce el derecho de toda persona a promover y defender los derechos humanos y el medio ambiente en condiciones de seguridad y sin amenazas ni represalias.

El Acuerdo de Escazú establece la obligación para los Estados de garantizar “un entorno seguro y propicio” para que las personas defensoras ambientales “puedan actuar sin amenazas, restricciones e inseguridad”.⁷ Esta protección cobra aún más relevancia en el caso de aquellos y aquellas defensoras ambientales que pertenecen a grupos que sufren discriminación estructural, como es el caso de las mujeres, disidencias sexogenéricas, pueblos indígenas y personas racializadas.

En este contexto, resulta fundamental identificar los principales riesgos que enfrentan las personas defensoras ambientales y establecer mecanismos de prevención y respuesta que permitan fortalecer su seguridad y la de las organizaciones que acompañan estos procesos.

2. IDENTIFICACIÓN DE RIESGOS Y RESPUESTAS ASOCIADAS

Las personas defensoras del medio ambiente enfrentan una diversidad de riesgos que pueden clasificarse en riesgos digitales, reputacionales, físicos, jurídicos y organizacionales. Estos riesgos suelen presentarse de manera combinada y escalonada, comenzando frecuentemente con vigilancia o campañas de difamación y escalando hacia amenazas directas, criminalización judicial o agresiones físicas.

Diversos estudios muestran que las amenazas contra defensores ambientales suelen seguir patrones identificables de escalamiento del conflicto, especialmente en contextos de industrias extractivas o disputas territoriales (Global Witness, 2023; Front Line Defenders, 2022).

Reconocer tempranamente estos patrones permite activar medidas de prevención, protección colectiva y documentación, fortaleciendo la resiliencia organizacional frente a ataques.

A continuación, se desarrollarán las distintas situaciones de riesgo abordadas por este protocolo, divididas en dos bloques fundamentales: la Parte 1, centrada en los riesgos digitales, reputacionales y mediáticos, donde se entregan pautas para proteger dispositivos, cuentas y la identidad digital de la organización; y la Parte 2, dedicada a la seguridad física y organizacional, que detalla las medidas de respuesta ante incidentes de vigilancia territorial, amenazas, represión en protestas, riesgos en salidas a terreno e ingresos no autorizados a sedes o domicilios.

2.1 RIESGOS DIGITALES, REPUTACIONALES Y MEDIÁTICOS

El trabajo de defensa ambiental depende cada vez más de herramientas digitales para comunicarse, documentar impactos ambientales, coordinar acciones legales y difundir información pública. Sin embargo, esta exposición digital también genera vulnerabilidades que pueden ser aprovechadas por actores interesados en acceder a información sensible, desacreditar a las organizaciones o interrumpir su funcionamiento.

Diversos informes han documentado que las personas defensoras del ambiente son objetivo frecuente de vigilancia digital, campañas de difamación y ataques informáticos, especialmente en contextos de conflictos socioambientales vinculados a proyectos extractivos (Front Line Defenders, 2022; Global Witness, 2023).

Por esta razón, la seguridad digital debe ser entendida como una parte integral de la protección de las personas defensoras y de la seguridad organizacional.

2.1.1 Seguridad de los dispositivos de trabajo.

Los **dispositivos electrónicos** —como teléfonos móviles, computadores personales o tabletas— almacenan información estratégica relacionada con la labor de defensa ambiental, incluyendo:

- Comunicaciones internas
- Bases de datos de comunidades
- Documentos legales
- Registros de monitoreo ambiental
- Contactos de aliados y organizaciones

La pérdida, robo o acceso no autorizado a estos dispositivos puede comprometer información sensible y exponer a las organizaciones y comunidades a situaciones de riesgo.

Además, el uso intensivo de dispositivos móviles en terreno (protestas, monitoreo ambiental, reuniones comunitarias) aumenta la probabilidad de extravío, confiscación o robo.

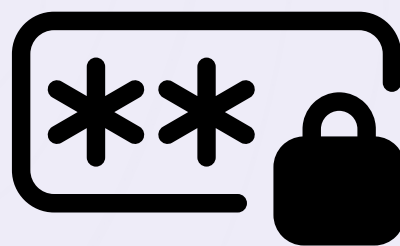
Teléfonos móviles y tabletas.

Recomendaciones Preventivas.

Como recomendaciones generales para el cuidado de nuestro celular podemos mencionar:

a. Cuida tus contraseñas de acceso.

- Claves alfanuméricas (lo más recomendado).
- Mezclar idiomas.
- Utilizar frases.
- No utilizar la misma contraseña para todo.



b. Activa el bloqueo de tu pantalla.

- Contraseñas para bloqueo de pantalla.
- Bloqueo automático de dispositivos cuando no lo estamos usando.

c. Cifrar los dispositivos para proteger la información.

El cifrado de dispositivos consiste en convertir la información almacenada en el equipo en un código ilegible para terceros. De esta forma, aunque un dispositivo sea robado o extraviado, los datos no podrán ser leídos sin la clave de acceso correspondiente.

Actualmente, la mayoría de los sistemas operativos incluyen funciones de cifrado automático que pueden activarse desde la configuración del dispositivo.

Actualmente, la mayoría de los sistemas operativos incluyen funciones de cifrado automático que pueden activarse desde la configuración del dispositivo. Esto añade una capa adicional de seguridad frente al acceso no autorizado.

Recomendaciones: Activar el cifrado completo del dispositivo desde las opciones de seguridad del sistema.

Utilizar claves de acceso robustas para desbloquear el equipo.

Evitar almacenar información sensible en dispositivos que no tengan cifrado activado.

Ejemplo: Si un teléfono celular que contiene contactos de comunidades o información de una investigación ambiental es robado, el cifrado impide que terceros puedan acceder a esos datos aunque retiren la tarjeta SIM o intenten acceder al almacenamiento del dispositivo.

d. Instala un antivirus para tu celular.

Los antivirus o programas de seguridad permiten detectar y bloquear software malicioso (malware) que puede instalarse en los dispositivos mediante aplicaciones, enlaces o archivos adjuntos.

Este tipo de programas monitorea permanentemente el sistema para identificar comportamientos sospechosos, proteger la información almacenada y evitar accesos no autorizados.

Recomendaciones: Instalar un antivirus confiable desde el sitio oficial del proveedor o desde las tiendas oficiales de aplicaciones.

Mantener el antivirus actualizado para asegurar la detección de nuevas amenazas.

Evitar instalar más de un antivirus simultáneamente, ya que pueden interferir entre sí.

Ejemplo: Un archivo enviado por correo electrónico puede contener un programa malicioso que intente copiar contactos o documentos del teléfono. Un antivirus actualizado puede detectar este archivo antes de que se instale en el dispositivo.



e. Utiliza sólo aplicaciones de sitios oficiales.

Las aplicaciones descargadas desde sitios no oficiales pueden contener software malicioso que permita a terceros acceder al dispositivo o recopilar información personal.

Las tiendas oficiales de aplicaciones (como Google Play o App Store) realizan controles de seguridad que reducen significativamente el riesgo de instalar programas maliciosos.

Recomendaciones: Descargar aplicaciones únicamente desde tiendas oficiales.

Revisar la reputación de la aplicación y los comentarios de otros usuarios antes de instalarla.

Evitar instalar aplicaciones enviadas por enlaces en mensajes o correos electrónicos.

Ejemplo: En algunos casos, aplicaciones falsas que imitan plataformas conocidas pueden instalarse en el dispositivo y registrar contraseñas o información personal ingresada por el usuario.

f. Cuídate de las redes de Wifi abiertas.

Las redes WiFi abiertas o públicas suelen carecer de sistemas adecuados de seguridad. Esto permite que personas conectadas a la misma red puedan interceptar información transmitida por otros usuarios.

Este tipo de riesgo es conocido como interceptación de tráfico de datos.

Recomendaciones: Evitar acceder a cuentas sensibles (correo electrónico, plataformas de almacenamiento o redes sociales institucionales) desde redes WiFi públicas.

Preferir conexiones mediante datos móviles o redes seguras.

Utilizar servicios VPN cuando sea necesario conectarse a redes públicas.

Ejemplo: Si una persona se conecta a una red WiFi abierta en un café y accede a su correo institucional, un tercero podría interceptar la información transmitida y obtener datos de acceso.

Preferir conexiones mediante datos móviles o redes seguras.

Utilizar servicios VPN cuando sea necesario conectarse a redes públicas.

Ejemplo: Si una persona se conecta a una red WiFi abierta en un café y accede a su correo institucional, un tercero podría interceptar la información transmitida y obtener datos de acceso.



g. Aplicaciones de seguridad para teléfonos celulares.

Existen diversas aplicaciones que permiten reforzar la seguridad de los dispositivos móviles y proteger la información almacenada.

Estas herramientas pueden ofrecer funciones como:

- Generación de claves dinámicas de acceso
- Autenticación en dos pasos
- Bloqueo remoto del dispositivo
- Rastreo de ubicación en caso de pérdida o robo
- Almacenamiento seguro de contraseñas.

Recomendaciones:

- Utilizar aplicaciones de autenticación para la verificación en dos pasos.
- Activar funciones de rastreo del dispositivo.
- Utilizar gestores de contraseñas para proteger accesos a cuentas sensibles.

Ejemplos de herramientas recomendadas:

- Authy o Google Authenticator (verificación en dos pasos)
- Bitwarden (gestor de contraseñas)
- Find My Device o Find My iPhone (rastreo de dispositivos)

Situaciones de riesgo y medidas de respuesta**a. ¿Qué hacer en caso de robo de nuestro celular de trabajo?**

El robo o extravío de dispositivos electrónicos constituye uno de los incidentes de seguridad más frecuentes en el trabajo de organizaciones sociales y ambientales. Los teléfonos móviles suelen contener información sensible, contactos, documentos y acceso a diversas cuentas institucionales.

Ante la pérdida o robo de un celular de trabajo se recomienda actuar rápidamente para proteger la información y evitar accesos no autorizados.

Las acciones primarias para resguardar nuestros datos o las de nuestras organizaciones pueden ser las siguientes:

- Bloquear el dispositivo de forma remota, utilizando herramientas de rastreo del sistema operativo (por ejemplo, “Buscar mi dispositivo” o “Find my iPhone”).
- Cerrar la sesión del dispositivo en las cuentas vinculadas (correo electrónico, servicios en la nube, redes sociales).
- Cambiar las contraseñas de las cuentas asociadas al dispositivo.
- Informar inmediatamente al equipo de la organización para prevenir posibles accesos indebidos a información institucional.

Acciones secundarias que podemos identificar, que tengan la finalidad de recuperar datos, contraseñas o información pueden ser las siguientes:

- Realizar la denuncia ante las autoridades competentes, especialmente si el dispositivo contenía información sensible.
- Intentar localizar el dispositivo mediante las herramientas de rastreo disponibles (iCloud, Find My Device u otras aplicaciones).
- Resguardar información sensible desde otros dispositivos seguros.
- Si existe riesgo de uso indebido del dispositivo, informar públicamente a las redes de la organización para advertir sobre posibles mensajes o comunicaciones fraudulentas.

b. Hackeo o acceso no autorizado a un celular

El hackeo corresponde al acceso no autorizado a un dispositivo o cuenta digital con el objetivo de obtener información, manipular datos o controlar sistemas informáticos.

Este tipo de incidentes puede manifestarse mediante señales como:

- Mensajes enviados sin autorización
- Aplicaciones desconocidas instaladas
- Cambios en configuraciones del dispositivo
- Actividad inusual en cuentas vinculadas.

Medidas de respuesta

En caso de sospecha o confirmación de hackeo se recomienda:

1. **Informar inmediatamente al equipo de la organización** para activar medidas de seguridad.
2. **Desconectar el dispositivo de internet** (datos móviles y WiFi) para evitar la propagación del ataque.
3. **Cambiar todas las contraseñas** asociadas al dispositivo desde un equipo seguro.
4. **Activar la verificación en dos pasos** en las cuentas más importantes.
5. **Revisar las aplicaciones instaladas** y eliminar cualquier software sospechoso.
6. **Evaluar el respaldo y restauración del dispositivo** si se confirma la intrusión.
7. En casos graves, **considerar la denuncia ante autoridades competentes.**



Computadores portátiles y de escritorio

Recomendaciones de carácter preventivo.

Las siguientes recomendaciones aplican tanto a computadores portátiles (notebooks) como a computadores de escritorio. No obstante, los equipos portátiles presentan mayores riesgos de pérdida o robo durante desplazamientos, mientras que los computadores de escritorio requieren especial atención al control de acceso físico al lugar donde se encuentran instalados.



a. Seguridad de acceso

- Utilizar contraseñas robustas (mínimo 12 caracteres combinando letras, números y símbolos).
- Evitar utilizar datos personales como fechas de nacimiento, direcciones o nombres de familiares.
- Activar el bloqueo automático de pantalla tras 5–10 minutos de inactividad.
- Siempre que sea posible, habilitar autenticación en dos pasos⁸ (2FA) para acceder a cuentas.

Uso de gestores de contraseñas

Se recomienda utilizar gestores de contraseñas como Bitwarden⁹, que permiten almacenar de manera segura múltiples contraseñas en una única “caja fuerte digital”.

Esto facilita el uso de contraseñas robustas y diferentes para cada cuenta sin necesidad de memorizarlas.

b. Actualizaciones y mantenimiento.

Mantener el sistema actualizado es una de las medidas más efectivas para prevenir ataques informáticos.

Se recomienda:

- Mantener actualizado el sistema operativo
- Activar actualizaciones automáticas
- Actualizar periódicamente los programas instalados.

⁸ La autenticación de dos factores (2FA) es un método de seguridad que requiere dos formas de identificación para acceder a cuentas, combinando una contraseña con un segundo factor como un código SMS, una app de autenticidad ([Google Authenticator](#), [Authy](#)) o notificación push.

⁹ La autenticación de dos factores (2FA) es un método de seguridad que requiere dos formas de identificación para acceder a cuentas, combinando una contraseña con un segundo factor como un código SMS, una app de autenticidad ([Google Authenticator](#), [Authy](#)) o notificación push.

Eliminación de software innecesario

Cada programa instalado en el computador representa un posible punto de vulnerabilidad.

Por esta razón se recomienda eliminar aplicaciones que no sean necesarias para el trabajo de la organización.

c. Protección contra malware (virus informáticos).

Para proteger el equipo contra virus informáticos se recomienda:

- Instalar un antivirus confiable y mantenerlo actualizado¹⁰
- Evitar instalar más de un antivirus simultáneamente
- Activar el firewall¹¹ del sistema operativo.
- Instalación de programas únicamente debe realizarse desde sitios oficiales o tiendas reconocidas (Microsoft Store, App Store, páginas oficiales de los sistemas operativos).

d. Navegación y comunicación seguras.

Para reducir riesgos durante la navegación en internet se recomienda:

- Utilizar navegadores actualizados
- Instalar bloqueadores de rastreo y publicidad.

Un navegador recomendado por su nivel de privacidad es Mozilla Firefox, complementado con extensiones como uBlock Origin.

Uso de VPN, cuando se utilicen redes públicas o compartidas, se recomienda conectarse mediante una VPN¹² (Red Privada Virtual), que cifra la conexión y protege la navegación frente a interceptaciones.

e. Gestión de Información Sensible.

Para proteger la información almacenada en los equipos se recomienda:

- Separar el uso personal del uso laboral del computador
- Cifrar carpetas o discos duros que contengan información sensible.

Cifrado de discos

En sistemas Windows se puede utilizar BitLocker, mientras que en sistemas macOS o Linux se recomienda VeraCrypt.¹³

El cifrado impide que terceros puedan acceder a la información incluso si el dispositivo es robado.

Copias de seguridad, se recomienda realizar copias de seguridad periódicas en:

- Discos externos cifrados
- Servicios de nube segura.¹⁴

¹⁰ Para equipos con Windows, Microsoft Defender ofrece una protección básica y gratuita. Recomendamos Norton y Bitdefender como los mejores antivirus de pago.

¹¹ Un firewall es una barrera que controla el tráfico de red que entra y sale del equipo. Permite bloquear conexiones no solicitadas y limitar qué aplicaciones pueden comunicarse por la red. Es una línea de defensa complementaria al antivirus.

¹² Una VPN (Red Privada Virtual) cifra la conexión a internet y oculta la dirección IP. Proton VPN (<https://protonvpn.com/es-419>) asoma como una de las mejores opciones gratuitas.

¹³ Si tienes Windows, te recomendamos BitLocker. Si tienes otros sistemas operativos, te recomendamos VeraCrypt.

¹⁴ Se recomienda utilizar servicios que ofrecen cifrado de extremo a extremo, cifrado de conocimiento cero, autenticación en dos pasos (2FA) y políticas de privacidad transparentes. Asoman como las mejores opciones Proton Drive (<https://proton.me/es-419/drive>), Tresorit (<https://tresorit.com/>) y Sync (<https://www.sync.com/>).

Entre los servicios recomendados se encuentran Proton Drive, Tresorit y Sync, que ofrecen cifrado de extremo a extremo.

f. Uso físico del equipo.

Los dispositivos electrónicos no deben quedar desatendidos en espacios públicos o compartidos. En el caso de computadores portátiles se recomienda utilizar candados de seguridad tipo Kensington cuando el equipo deba permanecer en oficinas u otros espacios.

Para computadores de escritorio existen kits de seguridad que permiten fijar la torre y el monitor a una superficie.

g. Mantener activo un servicio de rastreo de dispositivos.

Los principales sistemas operativos permiten activar funciones de rastreo del dispositivo en caso de pérdida o robo.

- Windows: Find My Device
- macOS: Find My

Se recomienda verificar periódicamente que esta función se encuentre activada.

Situaciones de riesgo y medidas de respuesta

a. ¿Qué hacer en caso de robo de nuestro computador?

En caso de pérdida o robo de un equipo institucional o personal que contenga información vinculada al trabajo de la organización, se deberán seguir las siguientes recomendaciones:

- **Informar de inmediato a la organización**, detallando las circunstancias del hecho (lugar, hora, tipo de dispositivo y, si es posible, número de serie o cualquier característica extra que sirva para identificar el dispositivo).
- **Cambiar todas las contraseñas** asociadas a las cuentas que pudieran haber estado abiertas o guardadas en el equipo (correo electrónico, servicios en la nube, redes sociales, etc.).
- **Revocar el acceso remoto a las cuentas** sincronizadas o vinculadas al dispositivo (por ejemplo, desde Google, Microsoft o Bitwarden).
- **Notificar a las autoridades policiales** y realizar la denuncia formal, adjuntando antecedentes identificatorios del equipo.
- **Intentar ubicar el equipo mediante servicios de rastreo**. Inicia sesión desde otro dispositivo en el servicio de rastreo de tu equipo. Consulta la ubicación actual, o la última conocida. Activa el modo perdido o bloquea el equipo de forma remota. Considera la opción de borrado remoto sólo si se confirma que no es posible la recuperación segura.

Es muy importante no intentar recuperar el equipo por cuenta propia si la ubicación sugiere riesgo. Informa a la policía y proporcionarles la información de localización.

- **Monitorear actividad sospechosa** en las cuentas personales e institucionales durante los días siguientes.
- **Informar al equipo interno** si existía información sensible o datos de terceros en el dispositivo, para que se adopten medidas preventivas o de contención.

b. ¿Qué hacer en caso de hackeo de nuestro computador?

Si se sospecha o confirma que un computador ha sido comprometido por un acceso no autorizado (hackeo), se deberán seguir los siguientes pasos:

- **Aislar el equipo inmediatamente.** Desconecta el computador de internet (Wi-Fi y cable de red) y de cualquier dispositivo externo. No lo utilices ni intentes repararlo por cuenta propia, ya que podrías eliminar evidencia o facilitar la propagación del ataque.
- **Notificar al responsable institucional de seguridad digital.** Informa de inmediato el incidente, indicando la fecha, hora y síntomas observados (mensajes anómalos, lentitud inusual, archivos cifrados, ventanas emergentes, etc.). Si el equipo contenía información sensible, específica claramente de qué tipo de información se trata.
- **Preservar evidencia y registrar la situación.** Anota los hechos relevantes y conserva cualquier elemento que pueda servir como evidencia (mensajes, correos, pantallazos, nombres de archivos). No borres datos ni formatees el equipo hasta recibir indicaciones del área técnica o de seguridad.
- **Dar aviso a las autoridades competentes.** De existir indicios de delito informático, filtración de información sensible o daño a sistemas institucionales, se debe presentar una denuncia formal ante la autoridad que corresponda, aportando toda la información recopilada.
- **Cambiar contraseñas desde un dispositivo seguro.** Utilizando otro equipo no afectado, cambia las contraseñas de todas las cuentas que hayan sido utilizadas en el computador comprometido (correo, servicios en la nube, redes sociales, gestores de contraseñas). Recuerda tener activada la autenticación en dos pasos (2FA) para mayor seguridad.

2.1.2 Seguridad de las cuentas y datos

Las cuentas digitales y plataformas de gestión de información, como correos electrónicos, servicios en la nube y aplicaciones de mensajería, constituyen los entornos críticos donde circula y se almacena el capital informativo de la organización.

El robo de credenciales o el acceso no autorizado a estos espacios permite que terceros intercepten comunicaciones, sustraigan documentos confidenciales o suplanten identidades, comprometiendo la seguridad de quienes integran la defensa ambiental.

Recomendaciones de carácter preventivo:

Se deberán implementar medidas que aseguren la correcta identificación y autenticación de las personas usuarias que acceden a los sistemas de información de la organización. Para ello, se establecerán mecanismos que permitan una identificación inequívoca y personalizada de toda persona que intente acceder a los sistemas de información, verificando además que cuente con la debida autorización.

Estas medidas deben ser observadas de manera estricta y permanente:

- Utiliza siempre un nombre de usuario y contraseña para acceder a los sistemas informáticos.
- Crea contraseñas seguras, con un mínimo de 12 caracteres, combinando letras, números y símbolos o utilizando frases largas fáciles de recordar.
- Evita usar datos personales obvios en tus contraseñas, como tu nombre, nombre de usuario, fechas de nacimiento o número de documento.
- Cambia tu contraseña al menos una vez al año, o de inmediato si sospechas que ha sido comprometida.
- Nunca compartas tu contraseña con otras personas y no la anotes en lugares visibles.
- Utiliza gestores de contraseñas. Estas herramientas permiten almacenar de forma segura los nombres de usuario y contraseñas de distintas cuentas en un único lugar protegido. De esta manera es posible utilizar contraseñas robustas y diferentes para cada servicio sin necesidad de memorizarlas.¹⁶
- Asegúrate de que las contraseñas se almacenen de forma segura y que no sean fácilmente legibles.
- Activar la verificación en dos pasos en dispositivos y cuentas institucionales y personales vinculadas al trabajo de la organización.

Situaciones de riesgo y de respuesta:

La detección temprana de accesos no autorizados permite reducir el impacto de incidentes de seguridad y evitar la exposición de información sensible. Con el fin de orientar a las y los usuarios en la detección temprana de incidentes de seguridad, se presentan a continuación algunos ejemplos de situaciones que pueden evidenciar el robo de credenciales o el acceso indebido a cuentas y plataformas:

- **Correo electrónico personal o institucional:** el/la usuario/a no puede acceder a su cuenta, recibe notificaciones de inicio de sesión desde ubicaciones desconocidas u observa que se han enviado correos a sus contactos sin su autorización. Esta situación constituye un posible robo de credenciales y acceso no autorizado.
- **Plataformas de almacenamiento en la nube:** el/la usuario/a recibe una notificación de actividad inusual y, al ingresar, identifica descargas de archivos confidenciales o modificaciones en documentos compartidos que no realizó. Este hecho indica un acceso indebido a la plataforma.
- **Aplicaciones de mensajería** (ej. WhatsApp): el/la usuario/a es expulsado/a repentinamente de la aplicación en su dispositivo y se le solicita verificar nuevamente el número de teléfono. Esto puede ocurrir cuando otra persona activa la cuenta en un dispositivo distinto, evidenciando un posible robo de acceso.

En caso de detectar un posible robo de credenciales o un acceso no autorizado a cuentas de correo electrónico, plataformas de almacenamiento en la nube, aplicaciones de mensajería o espacios de comunicación virtual, los/las usuarios/as deberán aplicar de inmediato las siguientes medidas de protección:

- **Cambio inmediato de contraseña:** Actualizar la contraseña comprometida siguiendo los criterios de seguridad establecidos en este protocolo.
- **Cierre de sesiones activas:** Revisar la configuración del servicio afectado y cerrar todas las sesiones abiertas que no correspondan. En aplicaciones como WhatsApp Web, Instagram u otras plataformas vinculadas, verificar los dispositivos conectados y cerrar aquellos desconocidos.
- **Revisión de actividad reciente:** En plataformas de almacenamiento de datos, revisar los registros de descargas, modificaciones y accesos recientes para identificar el alcance del incidente.
- **Revisión de configuración:** Verificar si existen accesos delegados, reglas de reenvío automático o configuraciones de seguridad alteradas, y eliminarlos en caso de que no hayan sido autorizados por el usuario.

- **Notificación interna:** Informar de inmediato al área responsable de seguridad informática de la organización para activar medidas adicionales, como bloqueo temporal de la cuenta, auditoría de accesos o recuperación de información.
- **Seguridad en reuniones virtuales:** En plataformas de comunicación, reforzar la seguridad de las reuniones habilitando salas de espera, controles de admisión y contraseñas de acceso.
- **Comunicación preventiva:** Si desde la cuenta se enviaron mensajes fraudulentos, informar a los contactos para que no abran enlaces sospechosos ni descarguen archivos adjuntos.
- **Monitoreo posterior:** Durante los días siguientes, revisar la actividad de la cuenta y reforzar las medidas de seguridad descritas en este protocolo (por ejemplo, activar la verificación en dos pasos si la plataforma lo permite).

2.1.3 Seguridad en las redes sociales y páginas web institucionales

Las redes sociales y páginas web de las organizaciones territoriales son ventanas al mundo: nos permiten comunicar nuestras luchas, convocar a acciones y generar redes de apoyo. Pero también pueden ser puertas de entrada para quienes buscan vigilarnos, desacreditarnos o hacernos daño. Por eso, cuidar estos espacios es parte de la defensa del territorio.

Recomendaciones de carácter preventivo:

- **Reducción de la exposición innecesaria:** Es fundamental minimizar la información personal que se comparte en línea para reducir riesgos.
 - Evitar publicar datos personales como teléfonos, direcciones, DNI, correos personales o información familiar.
 - No compartir en tiempo real la ubicación de actividades, reuniones o de personas defensoras, para prevenir riesgos de seguimiento o ataques.
 - Crear cuentas colectivas con identidad organizativa, que representen al colectivo u organización y no a personas individuales, de modo que la comunicación sea más segura.
- **Protección de accesos:** Los accesos a cuentas y plataformas deben estar cuidadosamente protegidos. Se recomienda:
 - Usar contraseñas largas, únicas y seguras que combinen letras, números y símbolos. Cambiarlas periódicamente.
 - Activar la verificación en dos pasos (2FA), preferentemente con aplicaciones como Authy o Google Authenticator (ver anexo 1.2)
 - Usar correos electrónicos seguros y exclusivos para gestionar redes sociales y páginas, no mezclar correos personales con instituciones o colectivas.

- **Roles y control de accesos:** Para prevenir filtraciones o uso indebido de nuestras cuentas:
 - Definir claramente quiénes administran las redes y páginas del colectivo. No todas las personas necesitan tener acceso completo.
 - Se recomienda limitar los accesos y asignar roles según funciones, como en Facebook Business Manager, de modo que nadie comparta contraseñas y se pueda mantener un registro claro de las acciones realizadas por cada administrador.
- **Cuidado con enlaces y archivos sospechosos:** Los ataques de *phishing*¹⁷ y malware son frecuentes. Por eso deben tomarse las siguientes precauciones.
 - Nunca se debe hacer clic en enlaces extraños o no solicitados, especialmente si llegan por mensajes privados, comentarios o correos sospechosos.
 - Es útil verificar si la cuenta ha sido filtrada o comprometida mediante servicios como [HaveIBeenPwned](#) / [Firefox Monitor](#)
 - No descargar archivos de remitentes desconocidos, incluso si parecen legítimos, y confirmar siempre la fuente antes de abrir cualquier documento.
- **Revisar y ajustar configuraciones de privacidad:** Revisar y configurar la privacidad de cada plataforma permite controlar quién puede ver, comentar, etiquetar o compartir el contenido publicado. En sitios web, se recomienda utilizar protocolos HTTPS y limitar los formularios que recopilan datos personales innecesarios. Revisar guías de privacidad específicas:
 - Facebook: [Centro de privacidad de Meta](#)
 - Instagram: [Cómo desactivar geolocalización](#)
 - TikTok: [Privacidad en TikTok](#)
 - Twitter (X): [Centro de privacidad y seguridad](#)
- **Resguardos ante suplantaciones:** Es importante verificar regularmente si existen cuentas falsas que usen el nombre del colectivo o de personas integrantes, y denunciarlas colectivamente en las plataformas.
- En casos donde se comparta información personal sensible, se puede solicitar la eliminación de datos personales a través de formularios oficiales, por ejemplo: [Google - Solicitud de eliminación de datos](#)
- Estas medidas ayudan a proteger la reputación digital del colectivo y la seguridad de quienes participan en él.

¹⁷ El phishing es una técnica de engaño digital que busca robar información personal o contraseñas a través de mensajes falsos que simulan ser de fuentes confiables, como bancos, redes sociales o servicios de correo electrónico.

¹⁸ HTTPS (protocolo de transferencia de hipertexto seguro) es una versión más segura de HTTP que cifra la comunicación entre tu navegador y un sitio web. Esto protege la información sensible que envías y recibes, como credenciales de inicio de sesión, datos bancarios o información personal, manteniéndola privada y segura. Puedes identificarlo porque la URL comienza con https://

Situaciones de riesgo y de respuesta:

- **En caso de hackeo o pérdida de control de la cuenta:** Si una cuenta individual o del colectivo es vulnerada, es fundamental actuar rápidamente para minimizar daños.
 - Intentar recuperar el acceso usando las herramientas de recuperación de la plataforma (correo alternativo, número de teléfono registrado, preguntas de seguridad).
 - Notificar al equipo y cambiar inmediatamente las contraseñas de cuentas vinculadas.
 - Denunciar el incidente a la plataforma y, si es grave, considerar acciones legales.
 - Informar públicamente que la cuenta fue vulnerada en caso de que se haya publicado contenido falso, dañino o desinformación, dejando claro que la información no proviene del colectivo.
- **En caso de suplantación de identidad:** Cuando alguien crea una cuenta falsa usando el nombre del colectivo o de sus integrantes.
 - Denunciar la cuenta desde varias cuentas aliadas, ya que la denuncia colectiva suele tener más peso ante las plataformas.
 - Contactar directamente con soporte de la plataforma si no hay respuesta automática.
 - Emitir un comunicado aclarando la situación, sin compartir el contenido falso.
- **En caso de ataque coordinado o campaña de difamación:** Los ataques organizados, ya sea mediante comentarios, publicaciones o campañas de desinformación, requieren respuesta estratégica y colectiva.
 - No responder de forma impulsiva. Evaluar colectivamente cómo actuar y qué mensajes emitir.
 - Documentar todo con capturas de pantalla de mensajes, publicaciones o perfiles de agresores para posibles acciones legales o de seguimiento.
 - Solicitar apoyo a organizaciones aliadas o redes de defensa digital como Vita Activa o María da Judá.
 - Delegar temporalmente el manejo de redes a alguien del equipo que pueda sostener la comunicación sin sobrecarga emocional, evitando que la presión afecte la seguridad de las personas.
- **En caso de intento de “phishing”:** Para protegerse de correos, mensajes o enlaces falsos que buscan robar información.
 - No hacer clic en mensajes que pidan ingresar contraseñas, datos personales o financieros.
 - Verificar cuidadosamente la dirección del remitente y los enlaces, sin abrirllos directamente.

- Reportar el mensaje como phishing en el servicio de correo o plataforma utilizada.
- Cambiar contraseñas inmediatamente si se hizo clic o se ingresaron datos.

2.1.4 Ataques digitales

Los ataques digitales pueden dirigirse tanto a personas de manera individual como a organizaciones en su conjunto. Estos ataques buscan comprometer la seguridad, la reputación y la integridad de la información. A continuación, se describen los principales tipos de ataques y las medidas de respuesta sugeridas.

- **Ataques individuales:** Se trata de acciones dirigidas contra una persona en específico, que pueden incluir el robo de contraseñas, suplantación de identidad, acceso indebido a cuentas personales o difusión de información privada
- **Ataques organizacionales:** Estos ataques buscan afectar a una organización en su conjunto, comprometiendo correos institucionales, plataformas de almacenamiento de datos, sitios web o sistemas internos.
- **Campañas de difamación:** Acciones organizadas para dañar la reputación de una persona u organización, mediante publicaciones masivas de contenido negativo o falso en redes sociales y otros medios digitales.
- **Noticias falsas, engañosas o tendenciosas en medios:** Difusión de información errónea o manipulada, ya sea en redes sociales, páginas web o medios de comunicación tradicionales, con el fin de confundir, manipular o dañar la credibilidad.



¡Cuidar nuestras redes y páginas es cuidar nuestras voces!

Así como defendemos la tierra y el agua, defendamos también nuestros canales de comunicación.

2.2 SEGURIDAD FÍSICA Y ORGANIZACIONAL

2.2.1 Vigilancia, seguimiento y hostigamiento en el territorio.

La vigilancia, el seguimiento y el hostigamiento en los territorios habitados por comunidades indígenas y organizaciones ambientales constituyen una de las principales amenazas a la seguridad física de las y los defensores de los derechos humanos y de la naturaleza.

Los territorios altoandinos del norte de Chile, el noroeste argentino y el altiplano boliviano son zonas que actualmente concentran un creciente interés por parte de la minería del cobre, la industria del hidrógeno verde y la extracción de litio en sistemas salinos como el Salar de Atacama, Salinas Grandes, el Salar del Hombre Muerto, Uyuni, Coipasa, Maricunga, Salar de Ascotán y Pastos Grandes, entre otros. En estas zonas, se han intensificado los riesgos para las comunidades indígenas y las personas defensoras del medio ambiente.

Así, la expansión de proyectos mineros y energéticos, junto con la creciente presión sobre las aguas subterráneas y los ecosistemas frágiles, ha generado tensiones territoriales, conflictos socioambientales y situaciones de vigilancia y hostigamiento hacia quienes defienden los salares, humedales y derechos de la naturaleza en estos ecosistemas altoandinos.

La Alianza de Humedales Andinos reconoce la necesidad de establecer medidas preventivas, colectivas y coordinadas que garanticen la integridad física y psicológica de quienes defienden los derechos de participación y los derechos de la naturaleza.

2.2.1.1 Identificación y registro de incidentes.

Todo episodio de vigilancia, seguimiento, presencia sospechosa de personas y/o vehículos, sobrevuelo de drones, toma de fotografías o rondas inusuales en las inmediaciones de las comunidades y/o los salares deberá ser registrado en una bitácora de seguridad territorial.

El registro debe incluir:

- Fecha, hora y lugar exacto del incidente.
- Descripción detallada de los hechos.
- Identificación posible de los involucrados (personas, vehículos, empresas).
- Testigos presentes.

La información deberá almacenarse de forma segura y cifrada, con una copia de respaldo en la coordinación regional de la Alianza o en un lugar de resguardo designado por la comunidad.

2.2.1.2 Comunicación inmediata y activación de redes.

Ante cualquier indicio de hostigamiento, el o la defensora deberá notificar de inmediato al equipo de coordinación de la Alianza de Humedales Andinos, utilizando los canales de comunicación definidos en este protocolo (mensajería cifrada o contacto de emergencia).

En casos de riesgo grave o inminente, se deberá informar también a:

- Autoridades competentes: Carabineros o Fiscalía local.
- Instituciones de protección: Programa de Protección de Defensores de Derechos Humanos del INDH.
- Redes aliadas: CEJIL, CIDH, Observatorio de Conflictos Mineros de América Latina (OCMAL) u otras organizaciones de acompañamiento.

Esta comunicación debe priorizar la protección inmediata de las personas y la salvaguarda de la información sensible asociada a investigaciones o denuncias.

2.2.1.3 Medidas preventivas en terreno.

Antes de realizar actividades en zonas de riesgo, como sectores aledaños a proyectos extractivos, se deberán implementar las siguientes medidas:

- Elaborar un plan de visita con rutas, horarios y puntos de control.
- Evitar desplazamientos individuales y mantener comunicación constante con la base comunitaria.
- Coordinar previamente con autoridades tradicionales o representantes de los pueblos originarios.
- Variar itinerarios en caso de vigilancia sistemática y limitar la exposición pública de información sensible.
- Evitar publicaciones georreferenciadas en redes sociales durante las actividades de terreno.

2.2.1.4 Protección ante el Estado y las empresas.

El hostigamiento, la vigilancia o criminalización de defensores y comunidades constituye una vulneración al derecho de participación pública y de defensa del medio ambiente, reconocido en el Acuerdo de Escazú (artículo 9).

Las organizaciones y comunidades deberán:

- Documentar los hechos con respaldo audiovisual y testigos.
- Presentar denuncias ante el INDH y organismos internacionales pertinentes.
- Solicitar medidas de protección colectivas cuando el riesgo afecte a más de una comunidad.
- Activar mecanismos de alerta y acompañamiento jurídico mediante las redes de la Alianza y organizaciones aliadas.

2.2.1.5 Protección vinculada a investigaciones y monitoreos ambientales.

Cuando las situaciones de riesgo se relacionan con investigaciones, monitoreos o denuncias impulsadas por la Alianza o sus comunidades, se deberá:

- Evaluar los niveles de exposición pública de las y los voceros.
- Resguardar las identidades de informantes, denunciantes y miembros de las comunidades.
- Asegurar la circulación cifrada de informes, mapas y datos técnicos.
- Mantener la custodia segura de materiales sensibles en plataformas protegidas y con acceso restringido.

2.2.1.6 Principio de seguridad colectiva.

Todas las medidas deberán entenderse bajo un enfoque de seguridad colectiva, intercultural y preventiva, donde el cuidado mutuo, la comunicación oportuna y la cooperación entre comunidades sean los pilares centrales. El objetivo es que la defensa de los salares, humedales y de los derechos de la naturaleza se realice sin temor, sin represalias y en pleno ejercicio del derecho a participar en asuntos ambientales, conforme a los estándares del Acuerdo de Escazú y los principios de justicia ambiental.

2.2.1.7 Evaluación de riesgo territorial.

Antes de realizar actividades de defensa ambiental, monitoreo comunitario o visitas a zonas en conflicto socioambiental, se recomienda realizar una evaluación básica de riesgos territoriales. Esta evaluación permite anticipar posibles amenazas y adoptar medidas preventivas adecuadas.

La evaluación deberá considerar:

- presencia de empresas extractivas o contratistas en la zona
- antecedentes de conflictos socioambientales
- episodios previos de hostigamiento o vigilancia
- condiciones de aislamiento geográfico o falta de conectividad
- capacidad de respuesta de redes de apoyo locales.

Cuando el riesgo sea elevado, se recomienda:

- evitar desplazamientos individuales
- coordinar acompañamiento comunitario
- limitar la exposición pública de las actividades en terreno
- informar previamente a redes de apoyo y organizaciones aliadas.

2.2.2 Amenazas verbales o escritas.

Es una prioridad para la Alianza de Humedales Andinos proteger a quienes defienden los derechos de los pueblos indígenas y del medio ambiente. Dado el riesgo que enfrentan las y los defensores frente a la industria extractiva, se establece el siguiente marco de prevención y actuación ante amenazas verbales, escritas o de otro tipo. Este protocolo busca resguardar la integridad física, emocional y digital de integrantes de la organización, así como de dirigentes y miembros de las comunidades indígenas con las que se trabaja, fortaleciendo la respuesta colectiva y promoviendo una cultura de cuidado y apoyo mutuo.

2.2.2.1 Tipos de amenazas y supuestos de riesgo.

Se consideran amenazas:

- **Amenazas verbales:** intimidaciones realizadas por teléfono, en reuniones, mensajes de voz o mediante terceras personas. Ejemplo: llamadas o comentarios de terceros con advertencias directas o indirectas sobre la labor del defensor.
- **Amenazas escritas:** comunicaciones hostiles por correo electrónico, mensajes de texto, redes sociales o notas dejadas en domicilios, vehículos o lugares de trabajo.
- **Amenazas indirectas o simbólicas:** actos destinados a intimidar sin expresar una amenaza explícita, como seguimientos reiterados, presencia intimidatoria cerca del domicilio o lugar de trabajo, daño a bienes personales, o difusión de información personal con intención de generar temor.

El **supuesto de riesgo** se define como cualquier situación en que la integridad física, psicológica o la reputación de una persona o grupo se vea comprometida debido a su labor en la defensa ambiental, territorial y/o comunitaria. Toda amenaza debe ser considerada una alerta y tratada con seriedad, sin subestimarse.

2.2.2.2 Medidas preventivas y recomendaciones generales.

Con el objetivo de reducir la exposición a amenazas, se recomiendan las siguientes acciones preventivas:

- Mantener comunicación interna constante, informando sobre situaciones inusuales o comportamientos sospechosos.
- Evitar la exposición innecesaria de información sobre líneas de trabajo, lugares de residencia, rutinas y/o desplazamientos.
- Establecer redes de apoyo y acompañamiento con organizaciones aliadas y personas de confianza.

2.2.2.3 Procedimiento ante la recepción de una amenaza.

En caso de recibir una amenaza grave, incluyendo amenazas de muerte, se deben seguir los siguientes pasos:

- No confrontar ni responder directamente a la amenaza. Mantener la calma.
- Registrar evidencia de la amenaza: mensajes, capturas de pantalla, notas, fotos o grabaciones.
- Informar de inmediato a la organización o al equipo de coordinación.
- Activar el protocolo interno de seguridad y, si corresponde, notificar a las autoridades competentes y solicitar acompañamiento legal en la organización.
- Evaluar medidas de protección personal: modificar rutinas, trayectos o lugares de residencia si el riesgo es permanente.
- Solicitar apoyo psicológico para enfrentar el impacto emocional de la amenaza.
- Coordinar cualquier comunicación externa, resguardando la seguridad y confidencialidad de los involucrados.

Nota final: La seguridad es un esfuerzo colectivo. Ningún defensor o defensora debe enfrentar amenazas en soledad. La coordinación, la prevención y el acompañamiento son fundamentales para proteger la vida, la integridad y la labor en defensa de los territorios y los derechos de las comunidades.

2.2.3 Represión en protestas.

La protesta social es un derecho protegido por el derecho internacional de los derechos humanos, vinculado a la libertad de expresión, reunión y participación pública. La represión durante manifestaciones o acciones públicas es una de las principales amenazas para defensores y defensoras del medioambiente y de los pueblos indígenas en América Latina. Este protocolo orienta la actuación frente a situaciones de uso excesivo de la fuerza o criminalización durante la protesta.

- **Antes de la protesta:** evaluar los riesgos, definir los roles (seguridad, primeros auxilios, comunicación), portar identificación y contactos de apoyo legal, informar a las personas de confianza, y reconocer las rutas de escape o puntos seguros.
- **Durante la protesta:** mantener una actitud pacífica, evitar la confrontación, documentar los hechos de violencia sin exponerse y, en caso de detención, exigir hablar con algún abogado o abogada de la organización.
- **Después de la protesta:** registrar y denunciar los actos de violencia ante los organismos de derechos humanos, ofrecer acompañamiento psicológico y legal, y sistematizar los hechos para fortalecer la defensa colectiva.

Como señala el CEJIL¹⁹(2019), “la represión busca debilitar los procesos de defensa territorial; por ello, la respuesta debe basarse en la protección inmediata, la denuncia pública y el cuidado mutuo. La protesta es un derecho legítimo y esencial para la defensa del territorio y del medio ambiente”.

2.2.4 Seguridad en salidas a terreno.

Las actividades de campo en territorios de la Puna y humedales andinos pueden implicar riesgos específicos vinculados a la geografía, el clima, las distancias, la conectividad limitada y, en algunos casos, a contextos de tensión social y territorial. Para resguardar la seguridad de las personas que forman parte de la Alianza por los Humedales Andinos, se proponen los siguientes lineamientos:

Recomendaciones de carácter preventivo.

• Planificación previa

- Informar el itinerario completo (fechas, lugares de visita, medios de transporte, contactos de referencia) a la organización de pertenencia;
- Designar una persona de enlace dentro de su organización responsable de recibir actualizaciones y dar seguimiento en caso de emergencia;
- Evaluar posibles riesgos en la zona de visita (restricciones de acceso, cortes de ruta, etc.).

• Comunicación y monitoreo

- Mantener comunicación periódica con la persona de enlace, informando novedades y confirmando llegada a cada destino (a través de una simple comunicación por teléfono o email, indicando que se encuentra bien);
- Avisar con anticipación si se prevé estar sin señal de celular, indicando tiempos estimados de desconexión y reconexión;
- Informar de cualquier cambio en el itinerario ni bien entre en su conocimiento;
- Contar con un medio de comunicación y llevar al menos un cargador externo para la batería del celular.

• Transporte y desplazamientos

- Utilizar medios de transporte confiables y seguros, y verificar que los vehículos estén preparados para caminos de altura.
- Siempre que sea posible viajar acompañado y con una persona que conozca el territorio.

- **Seguridad personal y de la información**

- Priorizar siempre espacios públicos y comunitarios, espacios de confianza;
- A los fines de minimizar riesgos, debe procurarse precaución al momento de dar información personal y/o de algún integrante de su organización de pertenencia o de la Alianza sin su consentimiento (número de celular, e-mail, dirección, etc);
- La información a la que se tenga acceso en razón del trabajo en las organizaciones miembro o por intermedio de la Alianza, sean datos internos, contactos, proyectos o cualquier otra, debe ser mantenida confidencial, salvo se indique expresamente lo contrario, con la finalidad de proteger a la Alianza y organizaciones en su conjunto.

- **Condiciones de salud y ambiente**

- Prever insumos básicos para la altura y el clima, e informar al equipo si alguna persona tiene condiciones médicas preexistentes relevantes;
- En caso de viajar con personas invitadas por la Alianza o por una organización miembro, se deberá prever que también informen con antelación sobre estas condiciones para poder tomar recaudos básicos de cuidado y prevención;
- Siempre que sea posible, se recomienda contratar un seguro de viaje que cubra eventualidades médicas, accidentes o traslados de emergencia.

Situaciones de riesgo y medidas de respuesta

En los territorios altoandinos, las actividades de terreno pueden implicar riesgos adicionales asociados a la altura geográfica, temperaturas extremas, deshidratación, radiación solar intensa y largas distancias entre centros poblados. Estas condiciones deben ser consideradas en la planificación de cualquier visita o monitoreo ambiental.

Considerar además, que muchas zonas de la Puna y de los salares andinos la cobertura de telefonía móvil es limitada o inexistente. Por esta razón, se recomienda planificar previamente los puntos de comunicación disponibles, informar los horarios estimados de contacto y considerar el uso de dispositivos de comunicación satelital cuando sea posible.

- Definir canales de alerta en caso de accidente, hostigamiento o pérdida de contacto (ej. avisar a coordinación de su organización);
- Documentar incidentes de forma segura para su eventual seguimiento legal o de protección.

2.2.5 Ingreso no autorizado a sede o domicilio.

Recomendaciones de carácter preventivo

Control de llaves y accesos

- Mantener un registro actualizado de quiénes poseen llaves o contraseñas de ingreso
- Cambiar cerraduras o códigos de acceso ante cualquier sospecha de pérdida, robo o filtración de llaves.
- Limitar el acceso a espacios con información sensible únicamente a personas autorizadas por la organización.
- No brindar información sobre la ubicación exacta de sedes, domicilios o archivos a personas ajenas sin justificación.

Protección de información y equipos

- Guardar bajo llave documentos, discos duros y dispositivos que contengan información sensible.
- Utilizar contraseñas seguras y, siempre que sea posible, cifrado de disco o protección por PIN.
- Mantener copias de seguridad (backups) cifradas en espacios externos o en la nube.
- Evitar dejar computadoras o dispositivos encendidos y sin supervisión.
- No dejar claves escritas a la vista ni en lugares de fácil acceso.

Comunicación y discreción organizacional

- En contextos de tensión territorial o riesgo para la seguridad de las personas defensoras, se recomienda evaluar la conveniencia de limitar la señalización visible de la sede o de las actividades de la organización.
- Minimizar la difusión pública de direcciones, horarios o rutinas de trabajo.

Situaciones de riesgo y de respuesta

Acciones inmediatas ante un ingreso o intento de ingreso

- Priorizar la integridad personal por sobre los bienes materiales.
- Si se cuenta con posibilidad segura de hacerlo, dar aviso inmediato a la coordinación de la organización y/o a contactos de emergencia designados. Asegurar que los contactos de emergencia estén visibles y disponibles para todas las personas de la organización.
- Contactar a las autoridades locales o a redes de apoyo de confianza, según la valoración del riesgo.

- En caso de sospecha de seguimiento, vigilancia o allanamiento irregular, registrar la hora, circunstancias y testigos, e informar a la coordinación de la organización para activar medidas de acompañamiento o asesoramiento legal.

Registro y documentación del incidente

- Documentar el hecho lo antes posible (fotos, videos, lista de objetos sustraídos, descripción de daños o personas involucradas) sin comprometer la seguridad de quien lo hace.
- Guardar los registros en un lugar seguro o enviarlos a la persona designada para seguimiento de incidentes de seguridad.
- No divulgar públicamente la información hasta coordinar con la organización la estrategia de comunicación y protección adecuada.

Revisión posterior y contención

- Después del incidente, realizar una reunión interna para revisar lo ocurrido, identificar vulnerabilidades y actualizar medidas preventivas.
- Procurar apoyo psicosocial para quienes se vean afectados por el hecho.
- Evaluar la necesidad de reforzar la seguridad física, digital o incluso de reubicar temporalmente la sede o el personal, según el riesgo.



PROTOCOLO PARA DEFENSOR@S AMBIENTALES

CUIDADOS DIGITALES, SEGURIDAD
FÍSICA Y ORGANIZACIONAL



ALIANZA
HUMEDALES
ANDINOS



WWW.HUMEDALESANDINOS.ORG