

CATALIZADOR.SOCIAL, A.C.

Gestión de la NoViolencia · Metodología Ahimsa®

Protocolo para el Manejo Ético y Seguro de Información

Criterios de minimización, acceso, desidentificación, conservación, eliminación segura y respuesta ante incidentes

Catalizador.Social, A.C. · sostenibilidad@catalizador.social

Versión 1.1 · septiembre de 2026

Autoría de la metodología Ahimsa®: Daniela Sepúlveda Ruiz

1. Presentación y objetivo

Catalizador.Social genera y resguarda información sensible en el curso de su trabajo: diagnósticos organizacionales, testimonios relacionados con violencia, datos de contacto de personas defensoras y colaboradoras, y evidencia de proyectos que se comparte con financiadores. Este Protocolo establece los criterios de minimización, acceso, desidentificación, conservación, eliminación segura y respuesta ante incidentes que aplicamos para manejar esa información de forma ética y segura, tomando como referencia nuestro propio Manual de Seguridad Integral y los estándares de seguridad digital feminista adoptados por organizaciones aliadas de la región.

2. Alcance

Este Protocolo aplica a toda la información que Catalizador.Social recopila, produce o resguarda en el marco de su trabajo, incluyendo: datos personales de colaboradoras y participantes; datos personales sensibles (ver Aviso de Privacidad Integral); testimonios y documentación relacionada con situaciones de violencia; información institucional de las organizaciones y colectivas acompañadas; y datos administrativos, financieros y de donantes.

3. Principios que aplicamos

- **Minimización:** recopilamos únicamente la información necesaria para el propósito específico de cada actividad, proyecto o proceso, y evitamos solicitar datos “por si acaso” son útiles en el futuro.
- **Necesidad de conocimiento:** el acceso a la información se otorga solo a quien lo requiere para cumplir su función, no por jerarquía ni por defecto.
- **Proporcionalidad:** las medidas de seguridad deben ser adecuadas al nivel de sensibilidad de la información y al contexto de riesgo, sin ser insuficientes ni desproporcionadamente restrictivas para el trabajo cotidiano.
- **Redundancia:** existe siempre una alternativa de respaldo para la información crítica y para los canales de comunicación institucionales.
- **No hacer daño:** ninguna práctica de gestión de información debe, en sí misma, incrementar el riesgo de exposición de una persona o comunidad.

4. Clasificación de la información

Nivel	Ejemplos	Tratamiento
Pública	Materiales de infoactivismo, informes agregados y anonimizados, contenidos publicados en redes y el sitio web.	Sin restricción de acceso; se revisa antes de publicar conforme al

Nivel	Ejemplos	Tratamiento
		Enfoque Centrado en Personas Sobrevivientes.
Interna	Documentos de planeación, actas, comunicación operativa del equipo.	Acceso restringido al equipo y personas colaboradoras autorizadas.
Confidencial	Datos de contacto de personas y organizaciones, información contractual y financiera.	Acceso restringido por rol; se comparte solo con necesidad de conocimiento.
Sensible	Testimonios de violencia, datos sobre orientación sexual, identidad de género, salud, origen étnico u opiniones políticas.	Acceso mínimo e individualizado; requiere consentimiento expreso conforme al Aviso de Privacidad; almacenamiento cifrado cuando la herramienta lo permita.
Diagnóstico anónimo	Respuestas a instrumentos de diagnóstico grupal (p. ej. violentómetro laboral).	Anonimato garantizado técnicamente desde el diseño del formulario; resultados entregados únicamente en forma agregada.

5. Criterios de acceso

- Cada persona colaboradora accede únicamente a la información necesaria para las actividades que tiene asignadas.
- Las cuentas y carpetas institucionales (Google Workspace, Classroom, hojas de cálculo de proyectos) se organizan con permisos diferenciados por área o proyecto, y no se comparten credenciales personales.
- Se activa autenticación multifactor en las cuentas institucionales que lo permitan (correo institucional, WordPress, PayPal), priorizando aplicaciones autenticadoras sobre SMS cuando sea posible.
- Cuando una persona deja de colaborar con la organización, se revocan sus accesos y se transfieren las cuentas o carpetas institucionales a quien continúe la actividad, a más tardar en los días siguientes a su salida.
- Se mantiene, en un lugar seguro y con acceso restringido, un registro de administradoras, dominios, servicios contratados y métodos de recuperación de las cuentas institucionales.

6. Desidentificación y anonimización

Antes de usar información en informes, estadísticas, materiales de comunicación o solicitudes de financiamiento, la desidentificamos siempre que el propósito no requiera identificar a la persona: sustituimos nombres por códigos o seudónimos, agregamos los datos a nivel de grupo en lugar de caso individual, y removemos detalles de contexto (ubicación exacta, fechas específicas, descripciones físicas) que permitan identificar a alguien por deducción. Cuando identificar a una

persona es indispensable para el propósito del material —por ejemplo, un testimonio público de incidencia—, se hace únicamente con su consentimiento expreso y por escrito.

En instrumentos de diagnóstico grupal como el violentómetro laboral que se aplica en el *Taller de Diagnóstico de Expresiones de Violencias en el Espacio de Trabajo* de la Metodología Ahimsa® el anonimato se garantiza de forma técnica, no solo se promete de palabra: los formularios se configuran para que las respuestas no puedan vincularse a quien las emitió, ni por correo electrónico, ni por dispositivo, ni cruzando la marca de tiempo con las listas de asistencia. Los resultados se comparten con la organización acompañada únicamente de forma agregada; nunca se entregan de manera individualizada ni se usan para sancionar a una persona específica.

7. Conservación y retención

- **Información de proyectos y financiadores:** se conserva por el plazo que exijan las obligaciones contractuales y fiscales aplicables.
- **Testimonios y datos sensibles:** se conservan únicamente el tiempo necesario para el propósito por el que se recabaron; se revisan al concluir cada proceso o proyecto para decidir si corresponde anonimizarlos, archivarlos de forma restringida o eliminarlos.
- **Datos de personas que ya no colaboran o participan:** se revisan periódicamente y se eliminan cuando ya no exista una finalidad ni una obligación legal que justifique conservarlos.

8. Eliminación segura

Cuando la información debe eliminarse, se hace de forma que no pueda recuperarse: se vacían las papeleras de los servicios en la nube, se sobrescriben o destruyen los respaldos físicos, y se revoca el acceso desde todos los dispositivos y cuentas vinculadas. La eliminación de credenciales o el formateo de un dispositivo solo se realiza después de documentar cualquier incidente de seguridad relacionado, para no destruir evidencia útil sobre lo ocurrido.

9. Línea base de seguridad digital

Toda persona colaboradora sigue, como mínimo, estas prácticas:

- Mantener sistemas operativos, navegadores y aplicaciones actualizados.
- Usar contraseñas únicas y robustas, almacenadas en un gestor de contraseñas confiable, y activar la autenticación multifactor donde esté disponible.
- Conservar los códigos de recuperación de cuentas fuera del dispositivo principal.
- Cifrar los dispositivos de trabajo y configurar bloqueos de pantalla robustos.

- Verificar por un segundo canal cualquier solicitud sensible (transferencias, contraseñas, información de personas sobrevivientes) antes de actuar, incluso si parece provenir de una persona conocida.
- Evitar el uso de redes wifi públicas sin protección adicional para acceder a cuentas institucionales o información sensible.
- Proteger los metadatos, la ubicación y la identidad de las personas sobrevivientes, defensoras o fuentes que compartieron información con la organización.

Estas prácticas son un punto de partida, no una garantía absoluta: ninguna herramienta ofrece seguridad o anonimato total, y la seguridad digital es un proceso continuo de mejora, no un estado que se alcanza una sola vez.

10. Respuesta ante incidentes

Ante la sospecha o confirmación de un acceso no autorizado, pérdida, robo o filtración de información, se siguen estos pasos:

1. Aislar el acceso comprometido sin destruir evidencia (por ejemplo, cerrar sesión en dispositivos desconocidos antes que borrar archivos).
2. Identificar con precisión qué información quedó expuesta y a qué personas podría afectar.
3. Notificar cuanto antes a las personas cuya integridad, seguridad o privacidad pueda verse comprometida por la filtración, priorizando a quienes enfrenten mayor riesgo.
4. Solicitar apoyo técnico externo especializado cuando sea necesario.
5. Documentar el incidente completo y, solo después de documentarlo, cambiar credenciales y revocar accesos comprometidos.
6. Revisar y reforzar, a partir de lo aprendido, la política de accesos y respaldos institucionales.

Campo	Contenido
Fecha y hora de detección	
Información o cuentas afectadas	
Personas potencialmente afectadas	
Acciones tomadas de inmediato	
Persona que documenta y da seguimiento	
Medidas de mejora derivadas del incidente	

11. Roles y responsabilidades

Rol	Responsabilidad principal
Persona responsable del tratamiento de datos	Atiende solicitudes de derechos ARCO, coordina la aplicación del Aviso de Privacidad Integral y de este Protocolo.
Coordinación de cada área o proyecto	Define quién necesita acceso a qué información dentro de su equipo y revisa los permisos de forma periódica.
Toda persona colaboradora	Aplica la línea base de seguridad digital, reporta incidentes de inmediato y sigue los criterios de clasificación de la información.

12. Vigencia y revisión

Este Protocolo se revisa al menos cada dos años, o de inmediato después de un incidente de seguridad relevante. Dudas, reportes de incidentes o sugerencias pueden dirigirse a sostenibilidad@catalizador.social.