PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN PARA ORGANIZACIONES

GUÍA PRÁCTICA

datagéner

La presente guía tiene como objetivo compartir los principales elementos y buenas prácticas relativas a la protección y seguridad de los activos de información por parte de organizaciones.

Equipo

Coordinación General
Mailén García

Redacción de contenidos
Facundo Benítez Piloni

Año: octubre 2025

DataGénero. Observatorio de datos con perspectiva de Género
datagenero.org | info@datagenero.org

CONTENIDOS

1. INTRODUCCIÓN

Las organizaciones de la sociedad civil suelen trabajar con información sensible y confidencial. Es decir, suelen almacenar datos personales de beneficiarios/as, donantes, equipos de voluntariado y/o de las comunidades a las que acompañan. Además, suelen tener datos bancarios, contratos y convenios entre partes, así como también información financiera sensible.

Un descuido puede significar que se pierdan datos, que alguien sin permiso acceda a información de uso interno que se haga un mal uso de la misma.

La buena noticia es que no se necesitan grandes presupuestos ni equipos especializados para dar pasos firmes en este tema, con pequeñas acciones cotidianas se puede lograr mucho.

2. CONCEPTOS BÁSICOS

2.1 Seguridad de la información

La seguridad de la información es el conjunto de prácticas, medidas y herramientas que protegen los datos frente a accesos no autorizados, modificaciones indebidas o pérdidas accidentales. Su objetivo es garantizar que la información esté protegida en todo momento.

2.2 Privacidad

La privacidad se refiere al derecho de las personas a controlar cómo se utilizan sus datos personales. Implica que cualquier información que identifique o pueda identificar a una persona debe ser manejada con respeto, transparencia y únicamente para los fines autorizados.

2.3 Ciclo de vida de los datos

1. Recolección: solo lo necesario.
2. Almacenamiento: protegido y accesible solo a quienes corresponda.
3. Uso: según los fines autorizados.
4. Intercambio: con medidas de protección.
5. Eliminación segura: cuando ya no sea necesaria.

3. PRINCIPOS BÁSICOS DE SEGURIDAD

Presentamos algunos principios orientan la forma en que las organizaciones deben tratar los datos:

- ***Confidencialidad**: la información sensible solo debe estar disponible para personas autorizadas.*
- ***Integridad**: los datos deben mantenerse correctos y completos, sin alteraciones no autorizadas.*
- ***Disponibilidad**: la información debe estar accesible para quienes la necesitan en el momento oportuno.*
- ***Minimización**: solo se deben recolectar y conservar los datos estrictamente necesarios para cumplir los objetivos de la organización.*
- ***Transparencia**: las personas deben conocer de manera clara para qué se utilizan sus datos y cómo se protegen.*
- ***Responsabilidad**: la organización tiene la obligación de implementar medidas adecuadas para cumplir con estos principios a partir de diferentes medidas.*

4. BUENAS PRÁCTICAS

A continuación, se enumeran una serie de prácticas fáciles de aplicar en el día a día para la gestión de información de manera segura.

Contraseñas

- Las contraseñas constituyen la primera barrera de protección: son como las llaves de tu casa. Si son débiles o compartidas sin cuidado, cualquiera puede entrar.
- Se recomienda robustecer las contraseñas con frases largas o combinaciones robustas que incluyan caracteres como letras, números y símbolos. Las contraseñas pueden ser fáciles de recordar, pero difíciles de adivinar.
- Evitar repetir y reutilizar la misma contraseña en todos los sistemas o aplicativos.
- Considerar el uso de gestores de contraseñas gratuitos, como Bitwarden.

Accesos y permisos

- No todas las personas de la organización necesitan ver toda la información. Se recomienda desarollar una matriz de acceso en base a roles o personales y dar acceso solo a quienes realmente lo requieran.
- Implementar un proceso de revisión y auditoría periódica: revisar de vez en cuando quién tiene acceso a documentos y activos de información compartidos.

Protección de dispositivos

- Celulares y computadoras suelen ser la puerta de entrada a la información.
- Bloquea siempre los dispositivos con contraseña o PIN.
- Instala antivirus gratuitos y confiables como Avast o usa el que ya trae Windows.

Respaldos

- Los respaldos son como tener un duplicado de tus llaves. Se recomienda hacer copias periódicas de la información importante.
- Guardar una copia en un disco externo y otra en la nube (Google Drive, OneDrive).
- Muchas filtraciones empiezan con un simple clic en un enlace sospechoso.
- Desconfiar de correos que piden datos urgentes, traen archivos inesperados o no conoces al usuario remitente.
- Evita enviar información muy sensible sin protección

5. ENFOQUE ORGANIZACIONAL

- Definir un/a responsable de seguridad de la información.
- Redactar políticas internas simples (contraseñas, dispositivos, correos).
- Promover una cultura organizacional de cuidado y confianza.

6. GLOSARIO

Phishing: engaño por correo para robar datos.

Malware: software malicioso.

Ransomware: secuestro de archivos a cambio de dinero.

Cifrado: proceso que protege la información para que solo pueda ser leída por quienes tienen la clave.

7. RECURSOS RECOMENDADOS

- Access Now: https://www.accessnow.org/help-es/
- APC: Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género: Herramienta de evaluación https://www.apc.org/es/pubs/marco-para-el-desarrollo-de-una-politica-de-ciberseguridad-que-responda-las-cuestiones-de-1

8. *CHECK LIST* FINAL

- [ ] Uso contraseñas seguras y 2FA
- [ ] Defino accesos según roles
- [ ] Actualizo y protejo dispositivos
- [ ] Hago respaldos cifrados regularmente
- [ ] Tengo políticas internas de seguridad y protección de datos escritas
- [ ] Capacito a mi equipo en detectar fraudes
- [ ] Sé cómo eliminar datos de forma segura