# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

**Fecha de Aprobación:** 19 de febrero 2025
**Ente Aprobador:** Junta Directiva / Gerente General

## 1. Propósito:

El propósito de esta política es establecer el marco de gobierno para la gestión de la seguridad de la información en CENTRARSE, con el fin de preservar la **confidencialidad, integridad y disponibilidad** de los activos de información, así como de los sistemas que los procesan. Esta política demuestra nuestro compromiso con la protección de la información de nuestra organización, nuestros socios, donantes y beneficiarios, en línea con los más altos estándares éticos y los requerimientos de la cooperación internacional **y de la legislación vigente en materia de privacidad.**

## 2. Alcance:

Esta política es de obligatorio cumplimiento para todos los colaboradores (empleados, voluntarios, pasantes, consultores y miembros de la junta directiva) que tengan acceso a los sistemas de información o a los activos de información de CENTRARSE, independientemente de su modalidad de contratación o ubicación física.

**Esto incluye explícitamente a los colaboradores que operan en modalidades de trabajo remoto o híbrido, así como en dispositivos personales autorizados que se conectan a la red corporativa o acceden a información clasificada (BYOD).**

## 3. Objetivos:

a Proteger la información contra el acceso no autorizado, la divulgación, modificación, destrucción o uso indebido.

b. Establecer responsabilidades en la gestión de la seguridad de la información.

c. Cumplir con los requisitos legales, contractuales y de los cooperantes internacionales en materia de protección de datos y privacidad.

d. Crear una cultura de seguridad entre todos los colaboradores.

e. Minimizar el impacto de los incidentes de seguridad mediante una respuesta rápida y efectiva.
f. Asegurar el cumplimiento de las normativas de privacidad y protección de datos personales aplicables, protegiendo los derechos de los titulares de los datos (Socios, Donantes, Beneficiarios).

## 4. Principios Fundamentales:

Nuestra estrategia de seguridad se rige por los principios de:

- **Confidencialidad:** La información solo debe ser accesible para personas y sistemas autorizados.
- **Integridad:** La información debe ser exacta, completa y protegida contra modificaciones no autorizadas.
- **Disponibilidad:** La información y los sistemas deben ser accesibles para los usuarios autorizados cuando se requieran.
- **Modelo de Confianza Cero (Zero Trust):** Nunca confiar, siempre verificar. El acceso a los recursos de la organización debe ser verificado en cada punto, independientemente de la ubicación del usuario o del dispositivo.

## 5. Designación de Usuarios y Control de Accesos:

**a. Principio de Mínimo Privilegio:** A cada usuario se le asignarán los permisos de acceso estrictamente necesarios para el desempeño de sus funciones laborales.

**b. Gestión de Cuentas de Usuario:**

- La creación, modificación y desactivación de cuentas de usuario se realizará de forma formal, previa solicitud y autorización del supervisor inmediato y del área de Administración y Finanzas/TI.
- Las cuentas de usuarios que se desvinculen de la organización serán desactivadas en un plazo no mayor a **4 horas laborables** para mitigar riesgos de acceso post-laboral.

**c. Credenciales de Acceso:**

- Se prohíbe compartir contraseñas o credenciales de acceso.
- **Se exige el uso de un Administrador de Contraseñas (Password Manager) corporativo para almacenar y generar credenciales robustas y únicas para cada sistema.**
- Las contraseñas deben ser robustas, cumplir con los estándares de complejidad definidos internamente y se recomienda el uso de **frases de contraseña (passphrases)** largas y únicas.
- **Se implementará y exigirá la Autenticación Multi-Factor (MFA) para el acceso a la mayoría de los sistemas, siendo obligatoria para el correo institucional, VPN, plataformas financieras y de almacenamiento en la nube.**

## 6. Clasificación y Confidencialidad de la Información

a. Toda la información será clasificada según su sensibilidad y criticidad. Los niveles de clasificación incluyen:

- **Pública:** Información autorizada para divulgación general (ej.: comunicados de prensa).
- **Uso Interno:** Información para uso dentro de la organización (ej.: manuales de procesos internos no sensibles).
- **Confidencial:** Información sensible (ej.: datos personales, estados financieros internos, propuestas a donantes, **información relacionada con la privacidad**) cuyo acceso no autorizado podría causar un daño moderado.
- **Restringida:** Información altamente sensible (ej.: expedientes de personal, contratos, informes de auditoría, claves de acceso, **información de salud o financiera de beneficiarios**) cuyo acceso está limitado a un grupo muy específico de personas y cuyo compromiso causaría un daño grave o reputacional.

b. Toda la información clasificada como Confidencial o Restringida debe estar claramente marcada y ser manejada con las medidas de seguridad correspondientes (ej.: cifrado, almacenamiento en ubicaciones seguras, control de acceso estricto).

## 7. Políticas Internas para Salvaguardar la Información

### a. Equipos y Dispositivos (Versión Ajustada)

- Todos los equipos informáticos (laptops y teléfonos) deben contar con medidas de seguridad adecuadas.
    - Las laptops deben tener una **solución Antivirus/Anti-malware** actualizada que idealmente ofrezca funciones de **Protección de Endpoints (EDR)** o equivalente.
    - El **firewall** del sistema operativo (u otro interno) debe estar **activado y configurado** para proteger la red local.
    - **Se recomienda fuertemente el Cifrado de Disco Completo (Full Disk Encryption - FDE)** en todas las laptops que contengan información clasificada como Confidencial o Restringida, para proteger los datos en caso de pérdida o robo del equipo.
- Está prohibido instalar software no autorizado en los equipos de la organización.
- Los dispositivos móviles que accedan al correo institucional o a la red deben cumplir con las políticas de seguridad (código de desbloqueo, biometría, cifrado básico).

## 8. Capacitación y Concientización:

Todos los colaboradores recibirán capacitación obligatoria sobre esta política y las mejores prácticas de seguridad de la información, incluyendo **simulacros de phishing**, al momento de su ingreso y de forma periódica (**mínimo semestralmente**),

para mantener un nivel alto de concientización y preparación ante amenazas persistentes.

**9. Respuesta a Incidentes:**
Cualquier incidente de seguridad (pérdida de información, acceso no autorizado, infección por *malware*, intento de *phishing*) debe ser reportado de inmediato al **Equipo de Respuesta a Incidentes (ERT)**, liderado por el [Responsable de TI / Director Financiero].

**Se activará el Protocolo de Respuesta a Incidentes (IRP) formal de la organización para contener el incidente, erradicar la causa y recuperar la operatividad en el marco del Plan de Continuidad del Negocio (BCP).** En caso de violación de datos personales (brecha de seguridad), se procederá a la **notificación legal a los afectados y a las autoridades competentes** en el plazo establecido por la normativa aplicable.

**10. Sanciones:**
El incumplimiento de esta política será considerado una falta grave y puede dar lugar a medidas disciplinarias, que pueden incluir desde una amonestación formal hasta la terminación de la relación contractual, dependiendo de la gravedad y del impacto de la falta, sin perjuicio de las acciones legales que pudieran corresponder.

**11. Revisión y Actualización:**
Esta política será revisada **anualmente**, o de manera inmediata tras un incidente de seguridad grave o un cambio regulatorio significativo, por el Comité de Seguridad de la Información o, en su defecto, por la Dirección Ejecutiva y el área financiera-administrativa, para asegurar su vigencia y efectividad.

Aprobado por:

Connie de Paiz
Presidenta de Junta Directiva
CentraRSE

Juan Pablo Morafaya
Gerente General y Representante Legal
CentraRSE