Cruz Roja

POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

Políticas y procedimientos de seguridad

La presente política establece el compromiso de la Cruz Roja con la protección de la información que gestiona, tanto en sus operaciones internas como en sus actividades humanitarias. Esta política aplica a todo el personal fijo, voluntariado, personal médico, contratistas, proveedores tecnológicos y cualquier otra parte que acceda a sistemas o datos de la organización.

El objetivo principal de esta política es garantizar la **confidencialidad, integridad y disponibilidad** de la información sensible, médica, logística y operativa en poder de la Cruz Roja, en cumplimiento con sus principios humanitarios y con las normativas legales aplicables a nivel nacional e internacional.

Alcance

Esta política se aplica a todos los sistemas de información, plataformas digitales, bases de datos, redes, dispositivos móviles, servidores, aplicaciones internas y externas utilizadas por la Cruz Roja, sin importar la sede, nivel jerárquico o modalidad de trabajo (presencial o remoto).

Principios Rectores

- **Confidencialidad**: Solo el personal autorizado podrá acceder a información sensible.
- **Integridad**: La información debe mantenerse completa, precisa y protegida contra alteraciones no autorizadas.
- **Disponibilidad**: Los sistemas y datos deben estar accesibles cuando se requieran, especialmente en operaciones críticas o de emergencia.
- **Legalidad**: Se respetarán todas las leyes y regulaciones de protección de datos, ciberseguridad y derechos humanos.
- **Mejora continua**: El SGSI será revisado y actualizado de manera constante para adaptarse a nuevos riesgos y tecnologías.

Compromiso de la Dirección

La alta dirección de la Cruz Roja manifiesta su apoyo total a esta política y al funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando los recursos necesarios y promoviendo una cultura organizacional basada en la seguridad, responsabilidad y transparencia.

2. Control de Acceso

El acceso a la información y a los sistemas de la Cruz Roja se gestiona bajo el principio de **menor privilegio**, otorgando a cada usuario únicamente los permisos necesarios para el cumplimiento de sus funciones. Esta política busca minimizar el riesgo de accesos no autorizados, fugas de información o alteraciones indebidas de los datos.

2.1 Asignación de privilegios

- Todo acceso será autorizado previamente por el responsable del área correspondiente y registrado por el equipo de Tecnologías de la Información.
- Los privilegios se asignarán en función del **rol del usuario** (médico, voluntario, coordinador, administrativo, etc.).
- Se realizará una revisión semestral de los accesos otorgados para garantizar su vigencia y pertinencia.

2.2 Separación de funciones

- Las tareas críticas estarán divididas entre diferentes usuarios para evitar conflictos de interés o abuso de poder (por ejemplo: quien autoriza pagos no puede ejecutar transferencias).
- En áreas sensibles (como donaciones, datos médicos o logística humanitaria), los sistemas contarán con doble aprobación o validación cruzada.

3. Política de Contraseñas

La gestión segura de contraseñas es un componente esencial de la protección de la información dentro de la Cruz Roja. Esta política establece los requisitos mínimos que deben cumplir todas las contraseñas utilizadas para acceder a los sistemas y recursos digitales de la organización.

3.1 Requisitos mínimos

- Las contraseñas deberán tener una **longitud mínima de 12 caracteres**.
- Deben incluir al menos:
    - Una letra mayúscula
    - Una letra minúscula
    - Un número
    - Un carácter especial (por ejemplo: @, #, $, %)

- No se permite el uso de contraseñas comunes o fácilmente predecibles (ej. “123456”, “admin”, “cruzroja2023”).

3.2 Periodicidad de cambio

- Las contraseñas deberán cambiarse al menos cada **90 días**.
- El sistema impedirá la reutilización de las últimas **5 contraseñas anteriores**.

3.3 Gestión de contraseñas

- Las contraseñas deben mantenerse en **estricta confidencialidad** y **nunca compartirse**.
- Si se sospecha que una contraseña ha sido comprometida, el usuario deberá cambiarla de inmediato y notificar al equipo de TI.
- Los sistemas críticos utilizarán, además, **autenticación multifactor (2FA)**.

3.4 Bloqueo de cuentas

- Después de **5 intentos fallidos consecutivos**, la cuenta será bloqueada automáticamente por motivos de seguridad.
- El desbloqueo solo podrá ser realizado por el personal autorizado de TI, previa verificación de identidad.

2.3 Suspensión y revocación de accesos

- Las cuentas de usuarios inactivos por más de 30 días serán bloqueadas temporalmente.
- El acceso de personal desvinculado se revocará **de forma inmediata** al finalizar la relación laboral o voluntaria.
- Se llevará un registro de todos los cambios de privilegios y accesos revocados.

2.4 Acceso remoto

- El acceso a recursos institucionales fuera de las instalaciones físicas de la Cruz Roja solo estará permitido mediante el uso de **VPN cifrada y autenticación multifactor (2FA)**.
- Queda prohibido el uso de equipos personales para acceder a información crítica sin autorización explícita del área de TI.

4. Gestión de Incidentes de Seguridad

La Cruz Roja reconoce la importancia de detectar, registrar, responder y aprender de los incidentes de seguridad de la información, con el objetivo de minimizar su impacto operativo y reputacional, y de garantizar la continuidad de las actividades humanitarias.

4.1 Definición de incidente

Se considerará **incidente de seguridad** cualquier evento que comprometa, o pueda comprometer, la **confidencialidad, integridad o disponibilidad** de la información, incluyendo (pero no limitado a):

- Accesos no autorizados a sistemas o datos.
- Pérdida, robo o daño de equipos informáticos.
- Divulgación no autorizada de información personal o médica.
- Infecciones por malware, ransomware o ataques de denegación de servicio (DoS).
- Errores humanos con impacto en la información (envío de datos al destinatario equivocado, borrado accidental).

4.2 Proceso de gestión de incidentes

Los incidentes serán gestionados según el siguiente procedimiento estructurado:

1. **Detección e identificación**: Cualquier usuario que detecte un incidente deberá **reportarlo inmediatamente** al equipo de TI o al correo seguridad@cruzroja.org.
2. **Clasificación y priorización**: El equipo de TI clasificará el incidente según su gravedad e impacto.
3. **Contención**: Se tomarán medidas inmediatas para detener o limitar el alcance del incidente.
4. **Análisis y resolución**: Se investigará la causa raíz y se aplicarán acciones correctivas.
5. **Documentación**: Cada incidente será registrado en un **registro central de incidentes**, incluyendo fecha, impacto, responsables y acciones tomadas.
6. **Lecciones aprendidas**: Se generará un informe de análisis posterior (post mortem) para evitar recurrencias.

4.3 Roles y responsabilidades

- **Usuarios finales**: Detectar y notificar incidentes.

- **Equipo de TI**: Investigar, contener y resolver incidentes técnicos.
- **Dirección de la sede**: Coordinar la respuesta cuando haya impacto operativo o reputacional.
- **Área de comunicación**: Gestionar la comunicación externa si el incidente afecta a donantes, beneficiarios o socios.

4.4 Evaluación continua

- Se realizarán **simulacros de incidentes de seguridad** al menos una vez al año.
- Se revisará el procedimiento tras cada incidente crítico para identificar mejoras.

5. Copias de Seguridad y Recuperación

La Cruz Roja establece esta política para asegurar la protección y recuperación de sus activos de información ante cualquier evento que pueda ocasionar pérdida, corrupción o inaccesibilidad de los datos, garantizando la continuidad de las operaciones humanitarias en todos los contextos.

5.1 Alcance

Esta política aplica a todos los sistemas críticos, bases de datos, archivos administrativos, históricos médicos y plataformas digitales que almacenen información operativa o sensible.

5.2 Frecuencia de respaldo

- **Bases de datos médicas y de beneficiarios:** Respaldo **diario** automático.
- **Sistemas administrativos y financieros:** Respaldo **semanal**.
- **Documentación institucional y de proyectos:** Respaldo **mensual**.

Los respaldos serán almacenados en formato cifrado, tanto en una nube privada (infraestructura de Cruz Roja Internacional o proveedor validado) como en dispositivos de almacenamiento físico externo (off-site), ubicados en instalaciones seguras.

5.3 Verificación y restauración

- Todos los respaldos se **verificarán automáticamente** mediante comprobaciones de integridad (hashes).
- Se realizarán **pruebas de restauración** completas **al menos una vez al mes**, para garantizar la funcionalidad de los archivos respaldados.

- Se mantendrá un **registro de verificación y pruebas** disponible para auditorías internas y externas.

5.4 Gestión de versiones

- Se mantendrán **versiones históricas** de los respaldos por un período mínimo de **90 días**, con posibilidad de ampliación según el tipo de información.
- Se establecerá un procedimiento para la **recuperación granular** de archivos específicos si es necesario.

5.5 Responsabilidades

- El **equipo de TI de la sede central** será responsable de la implementación, automatización y monitoreo de los respaldos.
- Cada **oficina regional** deberá designar un responsable de supervisar que los procedimientos de copia y recuperación se apliquen localmente.
- La **dirección del SGSI** validará la efectividad de los respaldos y reportará a la alta dirección cualquier fallo o debilidad.

6. Concienciación y Capacitación

La Cruz Roja reconoce que el factor humano es clave en la protección de la información. Por ello, se establece un programa estructurado de **formación y concienciación en seguridad de la información**, dirigido a todo el personal, incluyendo trabajadores permanentes, voluntarios y colaboradores externos.

6.1 Objetivos del programa

- Asegurar que todo el personal comprenda sus responsabilidades en relación con la seguridad de la información.
- Promover el cumplimiento de las políticas internas y la normativa legal vigente.
- Reducir la probabilidad de incidentes causados por error humano, ingeniería social o negligencia.
- Fomentar una **cultura de seguridad continua** dentro de la organización.

6.2 Formación obligatoria

- Todo nuevo integrante de la organización deberá completar una **formación básica en seguridad de la información** durante su proceso de incorporación.

- Se realizará una **capacitación anual obligatoria**, con contenidos actualizados y adaptados a la función de cada empleado o voluntario (por ejemplo, sanitarios, administrativos, logísticos).
- Los contenidos incluirán temas como:
    - Uso seguro del correo electrónico
    - Identificación de intentos de phishing
    - Gestión segura de contraseñas
    - Uso adecuado de dispositivos móviles y portátiles
    - Manejo responsable de datos personales y sensibles

6.3 Campañas de sensibilización

- Se realizarán campañas internas cada trimestre, con materiales como:
    - Infografías y carteles en sedes
    - Correos educativos
    - Boletines digitales
    - Simulacros de ataques de phishing
- Estas campañas reforzarán comportamientos seguros y recordarán las buenas prácticas cotidianas.

6.4 Evaluación y seguimiento

- Se realizarán evaluaciones breves tras cada capacitación para medir la comprensión de los contenidos.
- El área de seguridad de la información mantendrá un **registro actualizado de participación y cumplimiento**, el cual podrá ser auditado en cualquier momento.
- Las áreas con mayor nivel de riesgo o historial de incidentes recibirán **formación adicional especializada**.