Evaluación de Riesgos – SGSI Cruz Roja

Este documento contiene la identificación, clasificación y evaluación de los riesgos asociados a los activos definidos en el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización Cruz Roja. Se consideran tanto amenazas internas como externas, así como las vulnerabilidades correspondientes y su posible explotación.

1. Identificación y Clasificación de Activos

- Hardware:
  - Servidores centrales
  - Equipos de escritorio y portátiles
  - Dispositivos móviles (tabletas y smartphones)
  - Equipamiento de red (routers, switches)
- Software:
  - Sistemas operativos de servidores y estaciones
  - Aplicaciones internas (gestión de voluntariado, emergencias, etc.)
  - Sistemas de gestión de donaciones
  - Plataformas de videoconferencia y correo
- Datos:
  - Información personal de beneficiarios
  - Datos de donantes
  - Informes financieros y contables
  - Historial de intervenciones y proyectos
- Personal:
  - Empleados contratados
  - Voluntarios
  - Proveedores de servicios externos

2. Amenazas y Vulnerabilidades

A continuación se identifican amenazas potenciales y las vulnerabilidades asociadas que podrían exponer a los activos:

- Amenaza: Acceso no autorizado
  - Vulnerabilidad: Contraseñas débiles, falta de autenticación multifactor
- Amenaza: Malware / Ransomware

    - Vulnerabilidad: Sistemas desactualizados, falta de antivirus
- Amenaza: Pérdida o robo de dispositivos
    - Vulnerabilidad: Falta de cifrado de disco
- Amenaza: Errores humanos
    - Vulnerabilidad: Capacitación insuficiente, ausencia de políticas claras
- Amenaza: Desastres naturales
    - Vulnerabilidad: Falta de respaldo remoto y continuidad operativa
- Amenaza: Violaciones de datos
    - Vulnerabilidad: Configuración insegura de bases de datos y redes

3. Evaluación y Priorización de Riesgos

Cada riesgo ha sido evaluado considerando su probabilidad de ocurrencia y el impacto que tendría sobre la organización:

Riesgo	Probabilidad	Impacto	Calificación
Acceso no autorizado a datos sensibles	Alta	Alto	Alto
Infección por malware en sistemas internos	Media	Alto	Alto
Pérdida de dispositivos móviles sin cifrado	Alta	Media	Alto
Errores humanos en el manejo de información	Media	Media	Medio
Daños por desastres naturales	Baja	Alto	Medio
Fuga de datos por configuración insegura	Media	Alto	Alto