Manual del Sistema de Gestión de Seguridad de la Información (SGSI)

Cruz Roja

Manual del SGSI

Introducción

El presente Manual del Sistema de Gestión de Seguridad de la Información (SGSI) ha sido desarrollado para la Cruz Roja con el propósito de establecer una estructura formal que permita gestionar y proteger eficazmente la información crítica en todas sus operaciones, tanto internas como de campo.

La información gestionada por la Cruz Roja abarca datos personales de beneficiarios, información médica sensible, logística de misiones humanitarias, informes financieros, bases de datos de voluntariado, así como comunicaciones estratégicas. La protección de esta información no solo responde a principios éticos y legales, sino que resulta esencial para la **continuidad operativa y la confianza de los donantes, los beneficiarios y el público en general**.

Este documento presenta los fundamentos del SGSI basado en los principios establecidos por la norma **ISO/IEC 27001**, e incluye políticas, procedimientos, roles y controles definidos para minimizar los riesgos asociados a la seguridad de la información.

El SGSI es una herramienta **viva**, que se adapta a los cambios del entorno operativo, tecnológico y normativo. Su correcta implementación garantiza que la Cruz Roja pueda cumplir su misión humanitaria en un entorno digital cada vez más complejo y amenazante.

1.1 Principios Humanitarios y Éticos Aplicados al SGSI

El Sistema de Gestión de Seguridad de la Información de la Cruz Roja no se fundamenta únicamente en normas técnicas, sino también en los principios humanitarios que guían a la organización a nivel global. Estos principios son integrados en el diseño y la ejecución del SGSI como marco ético transversal:

- **Humanidad:** Toda acción de protección de datos se orienta a preservar la dignidad, la vida y el bienestar de las personas afectadas por crisis humanitarias.
- **Imparcialidad:** La gestión de la información debe evitar cualquier forma de discriminación, garantizando la protección equitativa de todos los datos, sin distinción por raza, religión, condición social o política.

- **Neutralidad:** El SGSI protege la información de forma objetiva, evitando que sea utilizada con fines políticos, ideológicos o militares.
- **Independencia:** Las políticas de seguridad responden exclusivamente a las necesidades de protección de la información y no están sujetas a intereses externos.
- **Voluntariado:** Se promueve la capacitación en ciberseguridad de todo el personal voluntario, garantizando su participación activa y segura en el ecosistema digital.
- **Unidad y Universalidad:** La protección de la información se aplica de manera homogénea en todas las delegaciones, sin importar su ubicación o tamaño, con una visión global de seguridad solidaria.

Estos principios refuerzan la visión del SGSI como una herramienta ética, legal, técnica y humana.

2. Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la Cruz Roja abarca todas las unidades operativas, procesos, sistemas y personas que manejan información sensible dentro del marco de las actividades humanitarias, administrativas y logísticas de la organización.

Este alcance ha sido definido para cubrir todos los elementos críticos que podrían representar un riesgo para la seguridad de la información y, por ende, para la misión humanitaria de la organización.

2.1 Activos cubiertos

- **Información médica y de beneficiarios:** Historias clínicas, bases de datos personales, formularios de registro.
- **Sistemas informáticos:** Servidores, aplicaciones internas, plataformas de gestión de voluntariado y donaciones.
- **Redes de comunicación:** Intranet institucional, VPNs, servidores de correo.
- **Infraestructura física:** Centros de operaciones, oficinas administrativas, almacenes y unidades móviles.
- **Dispositivos móviles:** Tablets, laptops y teléfonos usados en terreno por personal y voluntarios.

2.2 Ubicaciones físicas incluidas

- Sede central y regionales.

- Delegaciones operativas nacionales.
- Almacenes de insumos médicos y humanitarios.
- Centros móviles de respuesta.

2.3 Ambientes digitales

- Plataformas en la nube (internacionales o contratadas).
- Bases de datos en servidores físicos y virtualizados.
- Sistemas compartidos con filiales de la Cruz Roja Internacional.

2.4 Partes interesadas

Parte interesada	Rol en el SGSI
Dirección general	Responsable final del cumplimiento
CISO / Seguridad TI	Gestión y supervisión técnica
Personal administrativo	Usuarios operativos y custodios de datos
Voluntarios y técnicos	Manipulación de datos en campo
Donantes y aliados	Interacción con datos públicos y financieros

3. Objetivos y Metas del SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) de la Cruz Roja tiene como propósito establecer un entorno seguro, resiliente y confiable para la protección de todos los activos de información que respaldan su labor humanitaria, administrativa y operativa.

Los objetivos del SGSI se alinean con los principios éticos y humanitarios de la organización, así como con las buenas prácticas internacionales en ciberseguridad, especialmente la norma **ISO/IEC 27001**.

3.1 Objetivos generales

1. **Proteger la confidencialidad, integridad y disponibilidad** de la información médica, personal, logística, financiera y operativa de la Cruz Roja.
2. **Prevenir y mitigar los riesgos de seguridad de la información** mediante la identificación oportuna de amenazas y vulnerabilidades.
3. **Garantizar la continuidad de las operaciones** ante incidentes de seguridad, fallos tecnológicos o desastres naturales.

4. **Fomentar una cultura organizacional orientada a la seguridad**, basada en la concienciación, la formación y la responsabilidad compartida.
5. **Cumplir con las leyes, reglamentos y compromisos internacionales** relacionados con la protección de datos personales, privacidad y derechos humanos.

3.2 Metas específicas del SGSI (medibles)

Meta	Indicador de Cumplimiento	Plazo de Evaluación
Implementar control de acceso por roles en todos los sistemas críticos	100% de usuarios con permisos asignados por rol	6 meses
Capacitar al 100% del personal en políticas de seguridad de la información	Registro de formación actualizado	Anualmente
Realizar una copia de seguridad completa de los datos críticos diariamente	Registro de respaldos automáticos verificados	Mensual
Ejecutar al menos un simulacro de incidente de seguridad por sede al año	Informe de simulacro y plan de mejora	Anual
Realizar revisión de accesos y privilegios en todos los sistemas	Registro de auditoría y verificación de accesos	Trimestral

Estas metas permitirán **medir el avance real** del SGSI, justificar la inversión en seguridad y evidenciar el cumplimiento de los compromisos adquiridos por la Cruz Roja ante sus beneficiarios, donantes y autoridades.

4. Estructura Organizativa del SGSI

El éxito de un Sistema de Gestión de Seguridad de la Información (SGSI) depende en gran medida de la definición clara de roles y responsabilidades. La Cruz Roja establece una estructura organizativa que permite distribuir, supervisar y ejecutar las actividades relacionadas con la protección de la información de manera coordinada, descentralizada y alineada con su modelo operativo internacional.

4.1 Comité de Seguridad de la Información

Este comité se encarga de liderar la implementación, evaluación y mejora del SGSI. Está compuesto por representantes de las áreas clave de la organización y liderado por la Dirección General.

Miembros:

- Director General o su delegado
- Responsable de Tecnologías de la Información (TI)
- Oficial de Protección de Datos (DPO)
- Coordinador de Operaciones Humanitarias
- Representante del equipo de voluntariado
- Responsable de logística y almacenes

- Auditor interno

4.2 Roles clave y responsabilidades

Rol	**Función principal en el SGSI**
Director General	Garantizar el respaldo institucional del SGSI, aprobar políticas, asignar recursos
Responsable de TI / CISO	Coordinar la implementación técnica del SGSI, liderar evaluaciones de riesgos, responder a incidentes.
Oficial de Protección de Datos (DPO)	Velar por el cumplimiento legal en protección de datos personales y privacidad.
Encargados de sede/delegación	Aplicar las políticas del SGSI a nivel local, capacitar al personal y reportar incidentes.
Voluntarios capacitados	Cumplir las políticas y reportar eventos sospechosos.
Auditor de Seguridad	Evaluar la efectividad del SGSI, realizar auditorías periódicas, identificar oportunidades de mejora.
Médicos y personal de salud	Proteger la información médica de los beneficiarios, aplicar prácticas seguras en el manejo de historiales y sistemas clínicos.
Voluntarios capacitados	Cumplir las políticas y reportar eventos sospechosos durante sus tareas en terreno o en actividades digitales.
Encargados de proyectos humanitarios	Garantizar que los sistemas y datos utilizados en campo estén alineados con las políticas del SGSI y se gestionen con criterios de seguridad.
Voluntarios capacitados	Cumplir las políticas y reportar eventos sospechosos durante sus tareas en terreno o en actividades digitales.

4.3 Coordinación multinivel

Debido a su presencia global, la Cruz Roja implementa un modelo de seguridad distribuido:

- **Nivel central (sede internacional):** Define políticas, estándares y herramientas comunes.

- **Nivel regional (delegaciones):** Aplica los controles y políticas en función del contexto operativo.
- **Nivel local (terreno):** Ejecuta procedimientos básicos, garantiza la protección física y digital de los datos recolectados, y reporta a los niveles superiores.

5. Evaluación de Riesgos

La evaluación de riesgos es el proceso mediante el cual la Cruz Roja identifica, analiza y prioriza los riesgos que podrían afectar la seguridad de la información. Este análisis permite establecer medidas de control adecuadas para proteger los datos, garantizar la continuidad de las operaciones humanitarias y cumplir con las obligaciones legales y éticas.

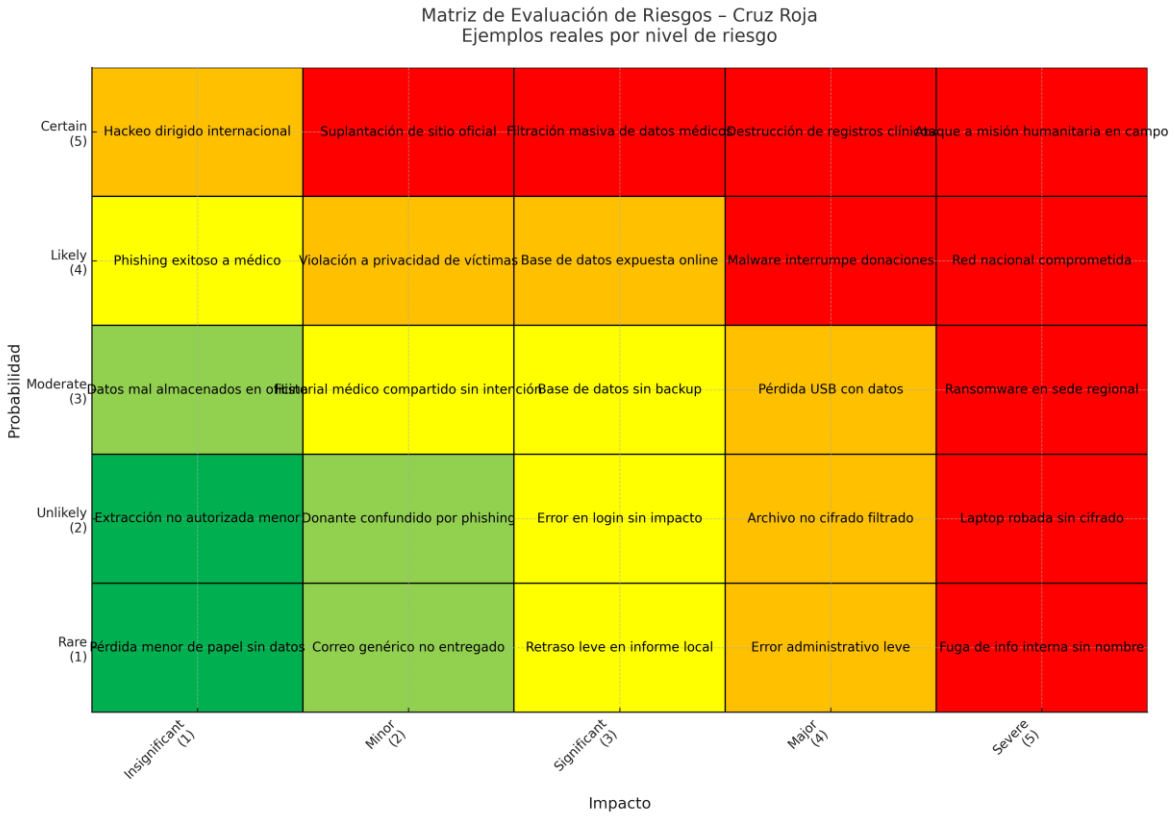
5.1 Metodología utilizada

La evaluación se realiza siguiendo los principios de ISO/IEC 27005 y se basa en los siguientes pasos:

1. **Identificación de activos**
2. **Identificación de amenazas**
3. **Identificación de vulnerabilidades**
4. **Evaluación del impacto potencial**
5. **Evaluación de la probabilidad de ocurrencia**
6. **Cálculo del nivel de riesgo = Impacto x Probabilidad**
7. **Clasificación y priorización del riesgo**

Se utiliza la **Matriz de Evaluación de Riesgos** con cinco niveles de impacto y cinco niveles de probabilidad, lo que permite clasificar los riesgos en niveles Bajo, Medio, Alto o Crítico.

5.2 Ejemplo de análisis de riesgos de activos críticos



5.3 Priorización de riesgos

Los riesgos con una puntuación superior a 15 se consideran **Críticos** y requieren tratamiento inmediato. Aquellos entre 10 y 15 se consideran **Altos**, y deben ser mitigados a corto plazo. Los **riesgos medios y bajos** se monitorean y se gestionan con controles básicos o medidas preventivas.

6. Controles Seleccionados

Los controles seleccionados por la Cruz Roja han sido definidos con base en los riesgos identificados, los activos críticos y los requisitos de la norma **ISO/IEC 27001 (Anexo A)**. Estos controles están diseñados para garantizar una protección adecuada y proporcional, teniendo en cuenta la naturaleza humanitaria de la organización, su alcance internacional y los recursos disponibles.

Los controles están organizados en tres categorías principales:

6.1 Controles técnicos

Control	Objetivo	Riesgo mitigado

Autenticación multifactor (2FA)	Proteger accesos a sistemas críticos	Phishing, acceso no autorizado
Cifrado de discos en portátiles	Prevenir el acceso a datos tras robo o pérdida	Robo de dispositivos, filtración de datos
Firewalls y sistemas antimalware	Detener amenazas externas y software malicioso	Infección por malware, ransomware
Segmentación de red	Aislar áreas críticas y limitar propagación de ataques	Ataques laterales en red
Copias de seguridad automáticas	Garantizar la recuperación de datos ante pérdida	Fallos del sistema, ransomware

6.2 Controles organizativos

Control	Objetivo	Riesgo mitigado
Revisión de accesos por rol Política de contraseñas robusta	Limitar privilegios innecesarios Aumentar la dificultad de accesos no autorizados	Escalada de privilegios, abuso interno Ataques de diccionario/brute-force
Capacitación obligatoria en ciberseguridad	Sensibilizar al personal y voluntariado	Errores humanos, phishing, pérdida de info
Procedimiento de gestión de incidentes	Responder y contener amenazas rápidamente	Cualquier incidente de seguridad
Clasificación de la información	Tratar los datos según su nivel de sensibilidad	Filtración accidental o negligente

6.3 Controles físicos

Control	Objetivo	Riesgo mitigado

Control de acceso físico a servidores	Proteger el hardware de accesos no autorizados	Sabotaje, robo de datos
Almacenamiento cerrado de documentos impresos	Evitar fugas por manipulación física	Pérdida de formularios, divulgación
Vigilancia en sedes (CCTV)	Monitorear áreas críticas	Robo, intrusión

6.4 Criterios para la selección de controles

Los controles han sido seleccionados considerando:

- El nivel de riesgo (según la matriz del Punto 5).
- Los recursos disponibles en cada sede.
- Las exigencias legales (protección de datos, normas internacionales).
- La viabilidad técnica en entornos de operación humanitaria.

Cada control tendrá un responsable designado y será documentado en un plan de implementación, monitoreo y revisión.

7. Resumen de Políticas de Seguridad

Como parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI), la Cruz Roja ha definido un conjunto de políticas formales que guían el comportamiento de su personal, voluntariado y aliados frente al uso, almacenamiento y transmisión de la información. Estas políticas reflejan los valores de la organización y están alineadas con los objetivos del SGSI.

A continuación, se presenta un resumen de las políticas más relevantes:

7.1 Política General de Seguridad de la Información

Establece los **principios rectores** del SGSI (confidencialidad, integridad, disponibilidad) y el **compromiso institucional** con la protección de los datos. Define el alcance, objetivos generales y la responsabilidad compartida entre todas las partes interesadas.

7.2 Política de Control de Accesos

Garantiza que solo el personal autorizado acceda a información específica según su función. Define el uso de roles, autenticación segura (2FA), y procedimientos de alta, baja y modificación de usuarios.

7.3 Política de Contraseñas

Establece los requisitos mínimos de robustez para las contraseñas utilizadas en los sistemas de la Cruz Roja: longitud, complejidad, renovación periódica y prohibición de reutilización o compartición entre usuarios.

7.4 Política de Gestión de Incidentes

Describe el procedimiento para **identificar, reportar, contener y aprender** de incidentes de seguridad. Incluye los canales de notificación y las responsabilidades en cada fase del proceso.

7.5 Política de Copias de Seguridad

Garantiza la disponibilidad de la información crítica mediante respaldos programados, almacenamiento cifrado y pruebas periódicas de restauración de datos.

7.6 Política de Concienciación y Formación

Promueve una cultura organizacional orientada a la ciberseguridad mediante formación obligatoria, campañas de sensibilización y simulacros periódicos dirigidos a todo el personal y voluntariado.

7.7 Revisión y actualización de políticas

Todas las políticas serán **revisadas anualmente** o tras incidentes críticos, cambios legales o modificaciones operativas. La actualización será liderada por el Comité de Seguridad y aprobada por la Dirección General.

8. Procedimientos Clave

Los procedimientos clave del SGSI permiten aplicar de manera práctica las políticas de seguridad de la Cruz Roja. Están diseñados para ser claros, ejecutables y adaptables tanto en sedes administrativas como en contextos de operaciones humanitarias.

A continuación, se describen los más relevantes:

8.1 Procedimiento para el Control de Accesos

Objetivo: Garantizar que cada usuario tenga acceso únicamente a la información y sistemas necesarios para sus funciones.

Pasos principales:

1. Solicitud de alta de usuario firmada por el responsable de área.
2. Asignación de rol y permisos específicos por el equipo de TI.
3. Revisión de privilegios cada 3 meses.
4. Baja inmediata al finalizar relación laboral o voluntaria.

8.2 Procedimiento para el Uso de Contraseñas

Objetivo: Asegurar contraseñas fuertes y seguras en todos los sistemas.

Pasos principales:

1. Creación de contraseña con mínimo 12 caracteres (mayúsculas, minúsculas, número, símbolo).
2. Cambio obligatorio cada 90 días.
3. Prohibición de compartir o almacenar contraseñas visibles.
4. Uso recomendado de gestores de contraseñas seguros.

8.3 Procedimiento de Gestión de Incidentes

Objetivo: Actuar de forma rápida y eficiente ante cualquier incidente de seguridad.

Pasos principales:

1. Identificación del incidente por cualquier usuario.
2. Notificación inmediata al equipo de seguridad (correo: seguridad@cruzroja.org).
3. Contención y análisis por parte del equipo técnico.
4. Comunicación interna y externa (si aplica).
5. Documentación del caso y plan de mejora.

8.4 Procedimiento de Copias de Seguridad y Recuperación

Objetivo: Garantizar que la información crítica pueda recuperarse ante cualquier pérdida.

Pasos principales:

1. Copia diaria automática de sistemas críticos.
2. Verificación semanal de integridad de los backups.
3. Prueba mensual de restauración parcial.
4. Almacenamiento cifrado en nube segura y dispositivo externo (off-site).

8.5 Procedimiento de Formación y Concienciación

Objetivo: Asegurar que todo el personal conoce sus responsabilidades en seguridad de la información.

Pasos principales:

1. Formación obligatoria al ingresar a la organización.
2. Cursos anuales según el rol (salud, técnico, voluntario, administrativo).
3. Campañas visuales en sedes (afiches, pantallas, boletines).
4. Simulacros periódicos de seguridad (phishing, incidentes simulados).

9. Monitoreo y Revisión del SGSI

El monitoreo y la revisión periódica del Sistema de Gestión de Seguridad de la Información (SGSI) permiten garantizar que las políticas, controles y procedimientos establecidos sean efectivos y estén alineados con los objetivos de la Cruz Roja. Esta actividad es esencial para adaptarse a cambios tecnológicos, organizacionales, legales y operativos.

9.1 Actividades de monitoreo

La Cruz Roja implementa mecanismos de monitoreo continuo para identificar desviaciones, vulnerabilidades y posibles incidentes:

- **Revisión de logs** en servidores y sistemas críticos.
- **Monitoreo de tráfico de red** en sedes y plataformas digitales.
- **Alertas automáticas** ante accesos sospechosos, uso indebido de privilegios o malware.
- **Seguimiento del cumplimiento** de las políticas (por ejemplo, vencimiento de contraseñas o caducidad de accesos).

Todo el monitoreo técnico es gestionado por el equipo de seguridad de TI, con informes mensuales enviados al Comité de Seguridad.

9.2 Indicadores clave de desempeño (KPIs)

Para evaluar la efectividad del SGSI, se miden los siguientes indicadores:

Indicador	Meta esperada
% de usuarios con capacitación anual completa	≥ 95%
Número de incidentes gestionados por trimestre	≤ 3 críticos, ≤ 10 en total
Tasa de éxito en restauración de respaldos	100% en pruebas mensuales
Revisión de accesos completada a tiempo	100% en cada período trimestral
Simulacros de seguridad realizados	≥ 1 por sede al año

9.3 Revisión del SGSI

Al menos una vez al año se realiza una **revisión formal del SGSI** liderada por el Comité de Seguridad, que incluye:

- Revisión del cumplimiento de objetivos y KPIs.
- Evaluación de la adecuación de los controles aplicados.
- Análisis de los incidentes ocurridos y las lecciones aprendidas.
- Revisión de las auditorías internas y externas.
- Propuestas de mejora o actualización del SGSI.

9.4 Auditorías internas y externas

- **Auditorías internas:** Se realizan semestralmente, coordinadas por el auditor de seguridad y revisadas por el Comité de Seguridad.
- **Auditorías externas:** Se llevan a cabo cada 2 años o cuando se requiera para certificar el cumplimiento normativo (por ejemplo, ISO 27001 o normas de protección de datos europeas).

10. Mejora Continua del SGSI

La Cruz Roja adopta un enfoque de mejora continua como principio fundamental para mantener la eficacia, actualidad y pertinencia del Sistema de Gestión de Seguridad de la Información (SGSI). Este enfoque permite responder proactivamente a los cambios en el entorno tecnológico, normativo y operativo, y asegurar que la protección de la información siga siendo sólida y confiable a lo largo del tiempo.

10.1 Modelo PDCA (Plan-Do-Check-Act)

El ciclo **PDCA**, también conocido como el ciclo de Deming, es la base sobre la que se estructura la mejora continua del SGSI:

Fase	Descripcion
Planific	Definir objetivos, políticas, controles y procesos en base al análisis de riesgos.

Hacer (Do)	Implementar los controles y procedimientos definidos.
Verificar (Check)	Monitorear y evaluar el desempeño del SGSI, auditorías internas y KPIs.
Actuar (Act)	Tomar acciones correctivas, actualizar procesos y reforzar las políticas.

10.2 Mecanismos de retroalimentación

El SGSI incorpora canales estructurados de retroalimentación que permiten detectar oportunidades de mejora:

- Resultados de auditorías internas y externas.
- Informes de incidentes de seguridad y análisis post-mortem.
- Revisión de indicadores de desempeño (KPIs).
- Encuestas internas de satisfacción y concienciación del personal.
- Cambios en el entorno legal, tecnológico o de amenazas.

10.3 Actualización del sistema

Toda actualización del SGSI será:

- **Documentada formalmente** y aprobada por el Comité de Seguridad.
- **Comunicada a todos los niveles** de la organización.
- **Acompañada de formación** específica si implica cambios operativos.

Se establece una **revisión anual obligatoria del SGSI**, con posibilidad de revisiones extraordinarias en caso de:

- Incidentes graves o repetitivos.
- Cambios normativos.
- Modificaciones estructurales o tecnológicas.

10.4 Compromiso organizacional

La mejora continua es una **responsabilidad colectiva**. Desde la Dirección General hasta el voluntariado en terreno, cada miembro de la Cruz Roja está llamado a:

- Reportar debilidades, fallos o sugerencias.
- Cumplir los procedimientos establecidos.
- Contribuir activamente a una cultura de seguridad y mejora constante.

Conclusión

La protección de la información en la Cruz Roja no es solo una necesidad técnica, sino una responsabilidad ética y humanitaria. A través de este Manual del SGSI, la organización establece un marco sólido para identificar, mitigar y gestionar los riesgos relacionados con la seguridad de la información, en un contexto operativo que frecuentemente incluye situaciones críticas, entornos vulnerables y datos altamente sensibles.

Este manual representa una herramienta viva que evoluciona junto con los desafíos del entorno digital. Su implementación no depende únicamente del área de tecnología, sino del compromiso colectivo de todas las personas que forman parte de la Cruz Roja: personal administrativo, voluntariado, profesionales de la salud, responsables de proyectos y aliados estratégicos.

A través del ciclo de mejora continua, el sistema será revisado, fortalecido y adaptado permanentemente para asegurar que la información esté protegida con el mismo nivel de dedicación y cuidado que caracteriza a la labor humanitaria de la organización.