



# Manual del Sistema de Gestión de Seguridad de la Información (SGSI) - UNICEF

---

## Índice

1. Introducción
2. Objetivo
3. Alcance
4. Términos y definiciones
5. Política de Seguridad de la Información
6. Contexto de la organización
  - 6.1. Entendimiento de la organización y su contexto
  - 6.2. Entendimiento de las necesidades y expectativas de las partes interesadas
7. Liderazgo
  - 7.1. Compromiso de la alta dirección
  - 7.2. Roles, responsabilidades y autoridades
  - 7.3. Comité de Seguridad de la Información
  - 7.4. Aprobación y revisión de la política de seguridad
8. Planificación
  - 8.1. Proceso de identificación de activos
  - 8.2. Evaluación de riesgos y oportunidades
  - 8.3. Objetivos de seguridad de la información
  - 8.4. Tratamiento de riesgos
  - 8.5. Evaluación continua y revisión de riesgos
9. Apoyo
  - 9.1. Recursos
  - 9.2. Competencia y asignación de roles clave
  - 9.3. Formación y concienciación sobre seguridad de la información
  - 9.4. Comunicación interna y externa
  - 9.5. Control documental y gestión de la información
10. Operación del SGSI
  - 10.1. Procedimiento de identificación y gestión del riesgo
  - 10.2. Implementación de controles de seguridad basados en ISO/IEC 27001
  - 10.3. Gestión de incidentes de seguridad de la información
  - 10.4. Planificación de la continuidad del negocio
  - 10.5. Protección de la privacidad y datos personales
11. Evaluación del desempeño
  - 11.1. Monitorización y medición de la efectividad del SGSI
  - 11.2. Auditoría interna y revisión de cumplimiento
  - 11.3. Revisión por la dirección
  - 11.4. Mecanismos de evaluación de riesgos emergentes
12. Mejora continua
  - 12.1. No conformidades y acciones correctivas

- 12.2. Mejora continua y actualización del SGSI

### 13. Anexos

- 13.1. Anexo A: Controles de seguridad de la información (ISO 27001 - Anexo A)
- 13.2. Anexo B: Política de control de acceso
- 13.3. Anexo C: Documentación técnica del SGSI
- 13.4. Anexo D: Glosario de términos de seguridad de la información

## 1. Introducción

Este manual del Sistema de Gestión de Seguridad de la Información (SGSI) para UNICEF proporciona una guía estructurada y completa para la protección de los activos de información críticos de la organización. Basado en la norma **ISO/IEC 27001**, este manual permite gestionar, controlar y mitigar los riesgos relacionados con la seguridad de la información, asegurando que los objetivos de UNICEF se cumplan de manera eficaz sin comprometer la integridad, confidencialidad o disponibilidad de la información.

Este documento describe los procesos, controles y políticas que forman parte del SGSI y que son aplicables a todas las áreas operativas de UNICEF, desde sus oficinas centrales hasta sus proyectos sobre el terreno, considerando las diversas ubicaciones geográficas en las que opera.

## 2. Objetivo

El objetivo principal del SGSI es proteger los activos de información de UNICEF frente a amenazas, tanto internas como externas. Esto implica minimizar el riesgo de pérdida, robo, corrupción o acceso no autorizado a la información crítica. Además, el SGSI permite que UNICEF cumpla con las normativas internacionales y locales de privacidad y protección de datos, tales como el **Reglamento General de Protección de Datos (RGPD)** en la Unión Europea.

Los objetivos clave del SGSI son los siguientes:

- Asegurar que la información sensible se gestione de manera segura y eficiente.
- Prevenir y mitigar los impactos de posibles incidentes de seguridad.
- Aumentar la conciencia de seguridad de la información entre todos los empleados y colaboradores de UNICEF.
- Mejorar continuamente los procesos y controles de seguridad para hacer frente a amenazas emergentes.

## 3. Alcance

El alcance del SGSI cubre todas las operaciones en España de UNICEF, incluyendo :

- **Infraestructura de tecnología:** Servidores, redes, estaciones de trabajo y dispositivos móviles.
- **Servicios en la nube:** Plataformas como **Microsoft 365**, **Google Workspace**, y sistemas de colaboración en línea.
- **Sistemas de gestión de datos:** Bases de datos que contienen información de beneficiarios, donantes, empleados y proyectos.
- **Personal y contratistas:** Incluyendo todos los niveles de la organización, tanto en oficinas centrales como en proyectos de campo.

El SGSI también abarca la protección de datos personales y confidenciales, como los historiales médicos de los beneficiarios y los datos financieros de los donantes, asegurando que su manejo se realice

conforme a las regulaciones aplicables.

## 4. Términos y definiciones

Para asegurar una comprensión clara de los términos utilizados a lo largo de este manual, a continuación se presentan algunas definiciones importantes:

- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Activos de información:** Recursos como datos, sistemas, hardware o personas que son críticos para las operaciones de la organización.
- **Amenaza:** Potencial causa de un incidente no deseado que puede generar un daño o interrupción de las operaciones.
- **Vulnerabilidad:** Debilidad en un activo que podría ser explotada por una amenaza para causar daño.
- **Riesgo:** La combinación de la probabilidad de que ocurra una amenaza y el impacto potencial que puede generar.
- **Incidente de seguridad de la información:** Un evento que compromete la confidencialidad, integridad o disponibilidad de la información.

## 5. Política de Seguridad de la Información

### 5.1. Propósito de la política

La política de seguridad de la información de UNICEF establece un marco claro para proteger los activos de información. Se aplicará a todos los empleados, contratistas y terceros con acceso a los sistemas de información de UNICEF. El objetivo es asegurar que toda la información se maneje de manera que garantice su protección adecuada contra amenazas tanto internas como externas.

### 5.2. Principios clave

- **Confidencialidad:** La información será accesible solo para las personas debidamente autorizadas.
- **Integridad:** Los datos se mantendrán precisos y completos, y cualquier cambio o modificación será autorizado.
- **Disponibilidad:** Los sistemas de información estarán disponibles para su uso cuando sea necesario.

### 5.3. Cumplimiento normativo

UNICEF se compromete a cumplir con las normativas de protección de datos locales e internacionales, incluyendo **el RGPD (Reglamento General de Protección de Datos)**, la **Ley de Protección de Datos Personales** y cualquier otra regulación aplicable en los países donde opere.

### 5.4. Revisión y aprobación

La política de seguridad de la información será revisada y aprobada por la alta dirección anualmente. Cualquier cambio significativo en los procesos operativos, tecnológicos o regulatorios será motivo de una revisión extraordinaria.

## 6. Contexto de la organización

### 6.1. Entendimiento de la organización y su contexto

UNICEF opera en un entorno global, lo que implica que sus sistemas de información están sujetos a una amplia variedad de riesgos que varían según las condiciones locales y las capacidades tecnológicas. En países en desarrollo, por ejemplo, UNICEF enfrenta riesgos adicionales relacionados con la infraestructura débil y la falta de personal capacitado en tecnologías avanzadas.

A nivel global, también existen amenazas cibernéticas, como ataques dirigidos a datos confidenciales, ransomware y otras formas de explotación maliciosa de vulnerabilidades en la red.

## 6.2. Entendimiento de las necesidades y expectativas de las partes interesadas

Las partes interesadas que dependen de la correcta gestión de la seguridad de la información de UNICEF incluyen:

- **Donantes:** Exigen que la información financiera esté protegida y que se les informe si ocurre una violación de datos que pueda comprometer su privacidad.
- **Beneficiarios:** Sus datos médicos y personales deben estar protegidos en todo momento, especialmente en situaciones vulnerables.
- **Reguladores:** Los gobiernos nacionales y organismos internacionales que supervisan el cumplimiento de las regulaciones de privacidad y protección de datos.
- **Proveedores y terceros:** UNICEF trabaja con diversos socios y proveedores, quienes esperan que los sistemas compartidos y los datos intercambiados estén protegidos adecuadamente.

## 7. Liderazgo

### 7.1. Compromiso de la alta dirección

La alta dirección de UNICEF está comprometida con la creación, implementación y mantenimiento de un SGSI eficaz. Esto se evidencia en la asignación de recursos, la capacitación de personal y el apoyo continuo a las iniciativas de seguridad de la información. La alta dirección también se compromete a participar activamente en la revisión y mejora del SGSI mediante informes periódicos y auditorías.

### 7.2. Roles, responsabilidades y autoridades

Cada miembro de UNICEF tiene un papel clave en la seguridad de la información. Se identifican los siguientes roles y responsabilidades específicos:

- **Director de seguridad de la información (CISO):** Responsable de la estrategia y supervisión del SGSI.
- **Equipo de IT:** Implementa y gestiona los controles técnicos necesarios para proteger los activos de información.
- **Oficiales de cumplimiento:** Supervisan el cumplimiento con las normativas aplicables y auditan el sistema regularmente.

### 7.3. Comité de Seguridad de la Información

El Comité de Seguridad de la Información está compuesto por miembros de varias áreas, incluyendo TI, operaciones y recursos humanos. Este comité se reunirá trimestralmente para evaluar el estado del SGSI, revisar incidentes y proponer mejoras.

### 7.4. Aprobación y revisión de la política de seguridad

La política de seguridad de la información se revisará anualmente o cuando se produzcan cambios importantes en el entorno operativo o regulatorio. La revisión será dirigida por el Comité de Seguridad y aprobada por la alta dirección.

## 8. Planificación

### 8.1. Proceso de identificación de activos

El proceso de planificación comienza con la identificación de los activos de información críticos para las operaciones de UNICEF. Esto incluye hardware (servidores, estaciones de trabajo), software (sistemas operativos, aplicaciones críticas), datos sensibles (información de donantes, beneficiarios, empleados) y los procesos asociados.

### 8.2. Evaluación de riesgos y oportunidades

El proceso de evaluación de riesgos sigue un enfoque basado en ISO/IEC 27005, utilizando herramientas de análisis de riesgo como:

- **Matriz de impacto-probabilidad:** Se utiliza para clasificar los riesgos en función de su severidad y la probabilidad de ocurrencia.
- **Software de gestión de riesgos:** Automatiza la identificación y seguimiento de riesgos.

Se desarrollan estrategias de mitigación basadas en la priorización de los riesgos identificados.

### 8.3. Objetivos de seguridad de la información

Se establecerán objetivos medibles para mejorar la seguridad de la información en UNICEF, incluyendo:

- **Reducción del tiempo de respuesta ante incidentes:** Minimizar el tiempo promedio de resolución de incidentes de seguridad críticos en un 20%.
- **Aumento de la capacitación en seguridad:** Lograr que el 100% de los empleados de UNICEF completen el curso de concienciación de seguridad anual.

### 8.4. Tratamiento de riesgos

Los riesgos se abordarán mediante las siguientes acciones:

- **Mitigación:** Implementar controles para reducir la probabilidad o el impacto del riesgo.
- **Transferencia:** Contratar seguros que cubran posibles pérdidas financieras derivadas de incidentes.
- **Aceptación:** Algunos riesgos menores serán aceptados con base en su baja probabilidad y bajo impacto.

(Continuará en las siguientes secciones...)

## Conclusión

Este manual proporciona una base sólida y detallada para el SGSI de UNICEF, cubriendo desde la planificación inicial hasta la mejora continua.

**Tú dijiste:**

continualo

**ChatGPT Plus**

ChatGPT

Aquí está la continuación del manual, ampliando las secciones operativas, de evaluación de desempeño, mejora continua y anexos, con suficiente detalle para alcanzar el nivel de extensión que necesitas:

## 9. Apoyo

### 9.1. Recursos

La implementación y mantenimiento del SGSI requiere una asignación adecuada de recursos, tanto humanos como tecnológicos. Esto incluye:

- **Personal especializado:** Recursos dedicados a la gestión de la seguridad de la información, como administradores de sistemas, analistas de seguridad, auditores internos y responsables del cumplimiento normativo.
- **Herramientas tecnológicas:** Inversión en herramientas como **firewalls**, sistemas de detección de intrusiones (**IDS/IPS**), cifrado, herramientas de monitoreo de red y software para la gestión de incidentes.
- **Capacitación continua:** Los recursos destinados a la formación deben asegurar que el personal esté preparado para manejar riesgos emergentes, identificar amenazas y reaccionar ante incidentes.

### 9.2. Competencia y asignación de roles clave

Es esencial que todo el personal involucrado en la gestión y operación del SGSI tenga las competencias necesarias. Se establecerá un **plan de formación** que incluirá:

- **Capacitación técnica para el personal de TI:** Esto incluye entrenamiento en herramientas de seguridad, análisis forense, y respuesta a incidentes.
- **Concienciación en seguridad para todos los empleados:** Formación en la identificación de amenazas comunes, como el phishing, y en el uso correcto de las herramientas de autenticación multifactor (MFA).

El equipo de seguridad debe estar conformado por:

- **CISO:** Responsable de la estrategia general del SGSI y supervisión de su cumplimiento.
- **Responsable de la gestión de riesgos:** Encargado de evaluar los riesgos de seguridad, establecer controles y monitorear su efectividad.
- **Auditores internos:** Revisan el sistema y realizan auditorías periódicas para asegurar el cumplimiento.

### 9.3. Formación y concienciación sobre seguridad de la información

Los empleados y colaboradores de UNICEF recibirán formación obligatoria anual en seguridad de la información, con módulos adaptados según el rol de cada trabajador. Las áreas clave incluyen:

- **Gestión de contraseñas y autenticación.**

- **Reconocimiento de amenazas cibernéticas** (phishing, ransomware, malware).
- **Buenas prácticas en el manejo de datos confidenciales.**
- **Procedimientos para la notificación de incidentes.**

## 9.4. Comunicación interna y externa

La correcta comunicación es fundamental para la implementación eficaz del SGSI. Se establecerán **protocolos de comunicación** que incluyan:

- **Comunicación interna:** Informes periódicos sobre incidentes, cambios en políticas y campañas de sensibilización. Las alertas de seguridad se comunicarán por correo electrónico y canales internos.
- **Comunicación externa:** En caso de incidentes que afecten a partes externas (donantes, beneficiarios, reguladores), UNICEF seguirá un protocolo de notificación alineado con las normativas locales e internacionales, garantizando que las partes afectadas reciban la información necesaria de forma clara y oportuna.

## 9.5. Control documental y gestión de la información

La correcta gestión de la documentación es clave para el éxito del SGSI. Se implementarán políticas para asegurar que toda la documentación relacionada con la seguridad de la información esté actualizada, disponible y sea accesible solo para las personas autorizadas. Los procedimientos incluirán:

- **Control de versiones:** Se utilizarán sistemas automatizados para el control de versiones de políticas, procedimientos y manuales de seguridad.
- **Archivado seguro:** Toda la documentación relacionada con incidentes de seguridad y auditorías será almacenada en sistemas cifrados y con acceso restringido.

# 10. Operación del SGSI

## 10.1. Procedimiento de identificación y gestión del riesgo

La identificación y gestión de riesgos es un proceso continuo dentro del SGSI. UNICEF utilizará un ciclo de **identificación, evaluación, tratamiento y monitoreo de riesgos**. Los procedimientos clave incluyen:

- **Análisis de riesgos inicial:** Realizado al implementar el SGSI, para identificar las principales amenazas, vulnerabilidades y activos críticos.
- **Monitoreo continuo:** Evaluaciones trimestrales que permiten identificar nuevos riesgos o cambios en los riesgos existentes.
- **Respuesta rápida a incidentes:** Establecer un plan de respuesta que permita detectar y mitigar rápidamente cualquier incidente.

## 10.2. Implementación de controles de seguridad basados en ISO/IEC 27001

UNICEF implementará un conjunto de controles de seguridad basados en las recomendaciones del **Anexo A de ISO/IEC 27001**. Estos controles cubrirán:

- **Control de acceso:** Implementación de autenticación multifactor (MFA) en todos los sistemas críticos y uso de políticas estrictas de contraseñas.
- **Cifrado de datos:** Protección de datos sensibles tanto en tránsito como en reposo mediante el uso de cifrado AES-256.
- **Gestión de vulnerabilidades:** Utilización de herramientas automatizadas de escaneo de vulnerabilidades para asegurar que los sistemas y software reciban parches de seguridad regulares.

- **Protección física de los activos:** Controles de acceso físico a servidores, almacenamiento y redes para prevenir accesos no autorizados.

### 10.3. Gestión de incidentes de seguridad de la información

UNICEF establecerá un **plan de gestión de incidentes** que incluya:

- **Detección temprana de incidentes:** Implementación de un sistema de detección de intrusos (IDS/IPS) para identificar actividad sospechosa en tiempo real.
- **Proceso de notificación:** Todos los empleados y colaboradores serán capacitados en la notificación inmediata de incidentes de seguridad. Se implementarán canales de comunicación específicos para este propósito.
- **Análisis forense:** En caso de incidentes graves, el equipo de seguridad realizará análisis forenses para identificar las causas del incidente, su impacto y las medidas necesarias para evitar su recurrencia.
- **Informe post-incidente:** Al finalizar la gestión de un incidente, se generará un informe detallado con recomendaciones para mejorar los controles y evitar futuros incidentes.

### 10.4. Planificación de la continuidad del negocio

La planificación de la continuidad del negocio es esencial para garantizar que las operaciones de UNICEF no se vean gravemente afectadas en caso de un incidente grave. El **Plan de Continuidad del Negocio (BCP)** incluirá:

- **Identificación de servicios críticos:** Procesos y sistemas que son esenciales para el funcionamiento de UNICEF y que deben priorizarse en situaciones de emergencia.
- **Plan de recuperación ante desastres (DRP):** Descripción de los procedimientos a seguir para restaurar los servicios críticos en el menor tiempo posible, incluyendo copias de seguridad y redundancias en infraestructuras clave.
- **Pruebas regulares del BCP/DRP:** Realización de simulaciones y pruebas anuales para asegurar que el personal esté preparado y los sistemas de respaldo funcionen correctamente.

### 10.5. Protección de la privacidad y datos personales

UNICEF gestionará los datos personales de donantes, empleados y beneficiarios conforme a las normativas de privacidad vigentes, incluyendo el **Reglamento General de Protección de Datos (RGPD)** y otras leyes locales aplicables. Las medidas incluirán:

- **Consentimiento explícito:** Asegurar que se obtenga el consentimiento adecuado para la recolección y tratamiento de datos personales.
- **Derechos de los titulares de los datos:** Establecer procedimientos para que los interesados puedan acceder, rectificar o eliminar sus datos, conforme a los requisitos legales.
- **Evaluaciones de impacto de privacidad:** Realizar evaluaciones de impacto para nuevos proyectos que involucren el tratamiento de datos personales, para asegurar que se implementen las salvaguardias adecuadas.

## 11. Evaluación del desempeño

### 11.1. Monitorización y medición de la efectividad del SGSI

La monitorización del desempeño del SGSI será continua, con indicadores clave de rendimiento (KPIs)



que incluyan:

- **Número de incidentes de seguridad reportados.**
- **Tiempo promedio de respuesta ante incidentes.**
- **Porcentaje de empleados capacitados en seguridad de la información.**

## 11.2. Auditoría interna y revisión de cumplimiento

Se realizarán auditorías internas del SGSI al menos una vez al año, o tras la ocurrencia de incidentes críticos. Las auditorías revisarán:

- **Conformidad con ISO/IEC 27001** y otras normativas aplicables.
- **Efectividad de los controles de seguridad implementados.**
- **Cumplimiento con las políticas internas de seguridad.**

El informe de auditoría incluirá recomendaciones de mejora y acciones correctivas.

## 11.3. Revisión por la dirección

La alta dirección de UNICEF revisará el desempeño del SGSI de forma periódica, tomando en cuenta:

- **Resultados de las auditorías internas.**
- **Cambios en el entorno de amenazas.**
- **Revisión de los objetivos de seguridad de la información.**

Se documentará cualquier decisión o recomendación para mejorar el SGSI.

## 11.4. Mecanismos de Evaluación de Riesgos Emergentes

Es crucial contar con mecanismos efectivos para evaluar y gestionar los riesgos emergentes que puedan afectar la seguridad de la información. UNICEF implementará procedimientos continuos de monitoreo y evaluación de los riesgos que surjan debido a cambios tecnológicos, amenazas externas, o situaciones imprevistas. Esto puede incluir:

- **Monitoreo activo de amenazas:** Utilizar herramientas de inteligencia de amenazas cibernéticas para identificar vulnerabilidades emergentes.
- **Revisiones periódicas:** Evaluaciones de riesgos a intervalos regulares para adaptarse a nuevas amenazas.
- **Análisis de tendencias:** Identificación de patrones en incidentes de seguridad que podrían indicar una amenaza creciente.

La mejora continua se logrará al integrar los resultados de estas evaluaciones en el proceso de gestión de riesgos y al ajustar las políticas de seguridad cuando se detecten riesgos nuevos o emergentes.

## Mejora Continua

La mejora continua del SGSI se basará en el ciclo PDCA (Plan-Do-Check-Act) para asegurar que el sistema evoluciona de acuerdo con los desafíos y necesidades cambiantes de seguridad. Esto se logrará mediante:

- **Monitoreo constante** de los controles de seguridad y su efectividad.
- **Auditorías internas** y externas para identificar brechas de seguridad.

- **Entrenamiento regular** del personal para que se mantenga actualizado en las mejores prácticas.

## 12.1. No Conformidades y Acciones Correctivas

Cuando se identifiquen no conformidades dentro del SGSI, UNICEF tomará medidas correctivas para abordar y remediar la situación de manera oportuna. El proceso incluirá:

1. **Identificación de la no conformidad:** Esto puede suceder mediante auditorías internas, quejas de empleados o incidentes de seguridad.
2. **Investigación y análisis de causa raíz:** Determinar las causas subyacentes para evitar que se repita.
3. **Implementación de acciones correctivas:** Establecer medidas correctivas adecuadas para remediar las deficiencias.
4. **Seguimiento de la eficacia:** Evaluar si las acciones correctivas implementadas fueron eficaces.

## 12.2. Mejora Continua y Actualización del SGSI

Además de las acciones correctivas, UNICEF llevará a cabo una **actualización periódica del SGSI**. Esto se basará en:

- **Revisión de políticas y procedimientos** a medida que se identifican áreas de mejora.
- **Evaluación de cambios en el entorno externo e interno** (como legislación y amenazas).
- **Incorporación de lecciones aprendidas** de incidentes de seguridad y auditorías para optimizar los controles de seguridad.

Las actualizaciones deben reflejar las mejores prácticas de seguridad y adaptarse a los riesgos emergentes.

## Anexos

### 13.1. Anexo A: Controles de Seguridad de la Información (ISO 27001 - Anexo A)

En el Anexo A de la ISO 27001 se especifican los **controles de seguridad** que deben ser implementados en el SGSI. Estos controles se agrupan en 14 áreas clave, que incluyen:

1. Política de seguridad de la información.
2. Organización de la seguridad de la información.
3. Gestión de activos.
4. Seguridad de recursos humanos.
5. Gestión de accesos.
6. Criptografía.
7. Seguridad física y ambiental.
8. Seguridad de las operaciones.
9. Gestión de incidentes de seguridad de la información.
10. Gestión de continuidad del negocio.
11. Cumplimiento.

UNICEF debe cumplir con estos controles para garantizar la seguridad de la información en todos sus procesos.

### 13.2. Anexo B: Política de Control de Acceso

El control de acceso es fundamental para proteger la información sensible. La **Política de Control de Acceso** establecerá:

1. **Normas de acceso a sistemas:** Definir quién tiene acceso a qué información y bajo qué condiciones.
2. **Control de privilegios:** Minimizar los accesos a datos sensibles según el principio de menor privilegio.
3. **Autenticación y autorización:** Implementación de métodos de autenticación robustos (como contraseñas fuertes, autenticación multifactor).
4. **Monitoreo de accesos:** Registro y seguimiento de accesos a sistemas críticos para detectar actividades no autorizadas.

### 13.3. Anexo C: Documentación Técnica del SGSI

Este anexo incluirá toda la **documentación técnica** necesaria para la implementación y mantenimiento del SGSI, que puede incluir:

- **Diagramas de flujo** para procesos de seguridad.
- **Configuraciones de infraestructura de TI** que cumplen con los estándares de seguridad.
- **Protocolos de comunicaciones seguras.**
- **Listas de verificación de seguridad** y procedimientos de control.

### 13.4. Anexo D: Glosario de Términos de Seguridad de la Información

El glosario incluirá definiciones clave relacionadas con la seguridad de la información, tales como:

- **Confidencialidad:** Asegurar que la información esté accesible solo a personas autorizadas.
- **Integridad:** Garantizar que la información no sea alterada sin autorización.
- **Disponibilidad:** Asegurar que la información esté disponible cuando se necesite.
- **Incidente de seguridad:** Cualquier evento que comprometa la seguridad de la información.