Sistema de Gestión de Seguridad de la Información (SGSI) para la Fundación Clínica Shaio, basado en los lineamientos de la norma ISO/IEC 27001:2022.

Escuela Superior de Guerra

Maestría de Ciberseguridad y Ciberdefensa

Gestión de Riesgos

Bogotá, Colombia
2025

Sistema de Gestión de Seguridad de la Información (SGSI) para la Fundación Clínica Shaio, basado en los lineamientos de la norma ISO/IEC 27001:2022.

Seguridad de la información Fundación Clínica Shaio

Grupo de trabajo:

Miguel Anderson Amaya Piracoca
Erika Tatiana Sánchez Gomez
Cristian Mauricio Toro Mora
Andres Felipe Parrado Camona

Docente encargado:

Ing. Jaider Ospina Navas

Escuela Superior de Guerra “Rafael Reyes Prieto”

Maestría en Ciberseguridad y Ciberdefensa
Gestión de Riesgos Cibernéticos
Bogotá, Colombia
2025

Tabla de Contenido

1. Introducción

Este documento tiene como objetivo definir los roles y responsabilidades clave relacionados con la Seguridad de la Información dentro de la organización, en cumplimiento con los requisitos de la norma ISO/IEC 27001. La estructura de roles se alinea con las necesidades del Sistema de Gestión de Seguridad de la Información (SGSI) y busca garantizar la confidencialidad, integridad y disponibilidad de la información.

2. Presidencia

Responsabilidad: Promover una cultura organizacional que priorice la Seguridad de la Información.

Colaboración: Coordinar con Dirección General y otras áreas clave las decisiones estratégicas en ciberseguridad.

3. Junta Directiva

Responsabilidad: Aprobar las políticas estratégicas de Seguridad de la Información y garantizar los recursos necesarios para su implementación.

Autoridad: Supervisar el cumplimiento de las políticas y su alineación con los objetivos organizacionales.

4. Dirección General

Responsabilidad: Asegurar la implementación y mantenimiento del SGSI en toda la organización.

Autoridad: Decidir sobre riesgos críticos y asignar recursos.

5. Chief Information Security Officer (CISO)

Responsabilidad:

- Diseñar, implementar y supervisar el SGSI.
- Evaluar y mitigar riesgos de seguridad.
- Gestionar la respuesta a incidentes de seguridad.
- Monitorear amenazas y vulnerabilidades emergentes.

Autoridad: Tomar decisiones críticas sobre mitigación de riesgos y escalación de incidentes de alto impacto.

Colaboración:

- Trabajar con el Departamento Jurídico para garantizar el cumplimiento normativo.
- Coordinar con Control Interno en auditorías de seguridad.
- Apoyar a Finanzas en la justificación de presupuestos.
- Colaborar con todas las áreas para fomentar una cultura de seguridad.

Soporte:

- Brindar asesoría técnica al equipo de TI para implementar controles.
- Capacitar a los empleados en buenas prácticas de ciberseguridad.

6. Departamento de Tecnologías de la Información

Responsabilidad: Implementar controles técnicos, gestionar incidentes y realizar monitoreos continuos.

Colaboración: Trabajar con áreas administrativas y jurídicas para cumplir con requisitos legales.

7. Jurídica

Responsabilidad: Garantizar el cumplimiento de regulaciones relacionadas con protección de datos y ciberseguridad.

Colaboración: Asesorar en contratos, políticas y cumplimiento normativo.

8. Control Interno

Responsabilidad: Auditar controles de seguridad, evaluar riesgos y monitorear el desempeño del SGSI.

Colaboración: Generar recomendaciones para mejora continua.

9. Finanzas

Colaboración: Asegurar presupuesto para iniciativas de ciberseguridad.

Soporte: Justificar inversiones en seguridad.

10. Áreas Administrativas y de Apoyo

Soporte: Garantizar que las operaciones cumplan con los lineamientos de seguridad.

Colaboración: Facilitar la implementación de políticas y controles.

11. Calidad

Responsabilidad: Alinear las iniciativas de seguridad con los estándares de calidad de la organización.

Colaboración: Supervisar el cumplimiento de normas internacionales como ISO/IEC 27001.

12. Control de Cambios

Versión	Fecha	Descripción del cambio	Aprobado por
1.0	**30/01/2025**	**Creación inicial del documento.**	**Junta Directiva**
1.1	**02/02/2025**	**Inclusión del rol del CISO y definición ampliada de responsabilidades.**	**Junta Directiva**
1.2	**05/02/2025**	**Actualización del marco de colaboración con el área Jurídica y Control Interno.**	**Junta Directiva**