SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

HOSPITAL-CLÍNICA SAN AGUSTÍN

POLÍTICA DE SEGURIDAD DE LA INFORMACION
HCSA-SGSI-POL-02

Ver.01

ELABORADO	REVISADO	APROBADO
Abg. José Rodríguez	Dr. David Romo R.	Dr. David Romo R.
DELEGADO DE PROTECCION DE DATOS	**GERENTE GENERAL**	**GERENTE GENERAL**
13 de junio de 2025	**16 de junio de 2025**	**16 de junio de 2025**

HISTORIAL DE VERSIONES			
Nro. DE VERSIÓN:	**FECHA:**	**CAMBIOS REALIZADOS EN LOS DOCUMENTOS:**	**MOTIVO DE LA REVISIÓN:**
01	16 de junio 2025	De acuerdo con requisito 5.2 ISO 27001	Emisión
VIGENCIA A PARTIR DE: JUNIO 2025			

POLÍTICA DE SEGURIDAD DE LA INFORMACION

1. Propósito

El propósito de esta política es establecer las directrices generales para la protección de la información gestionada por el Hospital Clínica San Agustín, asegurando su confidencialidad, integridad y disponibilidad, conforme a los requisitos establecidos en la norma ISO/IEC 27001:2022, específicamente el requisito 5.2, y los controles sugeridos en la ISO/IEC 27002:2022.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que acceden o manipulan información del Hospital Clínica San Agustín, independientemente del medio en que se almacene, transmita o procese.

3. Declaración de la Política (Requisito 5.2 - ISO/IEC 27001:2022)

La Alta Dirección de [Nombre de la Organización] se compromete a:

- Asegurar que la seguridad de la información esté alineada con la dirección estratégica de la organización.
- Integrar los objetivos de seguridad de la información dentro de los procesos de negocio.
- Satisfacer los requisitos aplicables de las partes interesadas, así como los requisitos legales, reglamentarios y contractuales relacionados con la seguridad de la información.
- Abordar los riesgos y oportunidades que puedan afectar a la seguridad de la información.
- Asignar los recursos necesarios para implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).
- Promover una cultura de seguridad entre todos los colaboradores, fomentando la concienciación y la formación continua.
- Apoyar el cumplimiento de los controles establecidos en los dominios de la norma ISO/IEC 27002:2022.

4. Principios de Seguridad de la Información

El Hospital Clínica San Agustín, adoptara los siguientes principios:

- Confidencialidad: la información solo será accesible a las personas autorizadas.
- Integridad: se protegerá la exactitud y completitud de la información.
- Disponibilidad: los usuarios autorizados tendrán acceso a la información cuando lo requieran.

5. Controles por Dominio (basado en ISO/IEC 27002:2022)

5.1. Controles Organizativos (Cláusula 5)

El Hospital Clínica San Agustín, implementará, mantendrá y dará seguimiento al cumplimiento de los siguientes controles administrativos:

- Definición de roles y responsabilidades.
- Aplicación de políticas, procedimientos y estándares.
- Revisión y actualización continua de la gestión de riesgos.
- Ejecución de planes de continuidad de negocio.
- Administración de activos de información.

5.2. Controles de Personas (Cláusula 6)

El Hospital Clínica San Agustín, implementará, mantendrá y dará seguimiento al cumplimiento de los siguientes controles aplicado al personal:

- Implementación de planes de concienciación y formación en seguridad.
- Implementación de controles de ingreso, permanencia y salida del personal.
- Implementación de procedimientos disciplinarios ante incumplimiento de los principios de seguridad de la información.

5.3. Controles Físicos (Cláusula 7)

El Hospital Clínica San Agustín, implementará, mantendrá y dará seguimiento al cumplimiento de los siguientes controles aplicado al control físico:

- Implementación de controles de acceso físico a instalaciones.
- Implementación de protección contra amenazas sobre los activos de la información.
- Implementación de medios de almacenamiento y disposición segura de medios.

5.4. Controles Tecnológicos (Cláusula 8)

El Hospital Clínica San Agustín, implementará, mantendrá y dará seguimiento al cumplimiento de los siguientes controles aplicado a controles tecnológicos:

- Implementación de controles de acceso lógico.
- Implementación de protección mediante firewalls y cifrado.
- Implementación de respaldo y recuperación de datos.
- Implementación de actualización de sistemas y gestión de vulnerabilidades.
- Implementación de gestión segura del trabajo remoto y dispositivos móviles.

6. Cumplimiento y Supervisión

El cumplimiento de esta política será supervisado regularmente mediante auditorías internas, revisiones de seguridad y seguimiento de incidentes. Todo incumplimiento será investigado y gestionado conforme a los procedimientos disciplinarios de acuerdo con lo establecido en el respectivo reglamento interno del Hospital Clínica San Agustín.

7. Mejora Continua

Esta política será revisada anualmente o ante cambios significativos en el contexto organizacional, la tecnología o los requisitos legales. Se fomentará la mejora continua del Sistema de Gestión de Seguridad de la Información SGSI para mantener su eficacia y adecuación.

8. Implementación y cumplimiento normativo (Ley de Protección de Datos Personales)

En cumplimiento de la Ley orgánica de Protección de Datos Personales y su Reglamento, el Hospital Clínica San Agustín se compromete a:

- Establecer canales adecuados, accesibles y eficaces para garantizar el ejercicio de los derechos de los titulares de datos personales, en especial los derechos de acceso, rectificación, actualización, eliminación, oposición, portabilidad y suspensión del tratamiento, conforme a la LOPDP.

- Designar y contar formalmente con un Delegado de Protección de Datos (DPD), quien actuará como punto de contacto para los titulares, así como entre el Hospital Clínica San Agustín y la Autoridad de Protección de Datos Personales, conforme a lo establecido en el artículo 48 de la LOPDP y el reglamento.
- Implementar procedimientos claros y documentados para la atención de solicitudes de derechos, garantizando su resolución dentro de los plazos legales establecidos.
- Establecer mecanismos para la identificación, gestión y notificación de incidentes de seguridad y brechas de datos personales, incluyendo registros de los mismos, en cumplimiento del principio de proactividad y responsabilidad, así como de los artículos 43 y 46 del Reglamento General.
- Adoptar y mantener actualizado un Registro de Actividades de Tratamiento (RAT), que contenga la información mínima requerida en el artículo 38 del reglamento a la LOPDP, incluyendo la finalidad del tratamiento, bases legales, plazos de conservación, medidas de seguridad, y transferencias realizadas.
- Incluir cláusulas informativas y mecanismos de obtención de consentimiento libre, informado, específico e inequívoco, especialmente cuando se traten datos sensibles o de salud, conforme a los artículos 7, 8 y 26 de la LOPDP.
- Capacitar periódicamente al personal en materia de protección de datos personales y concienciación sobre la seguridad de la información, como parte de una estrategia integral de cumplimiento normativo y cultura organizacional.

9. Aprobación y Difusión

La presente política ha sido aprobada por la Alta Dirección y será difundida a todos los niveles del Hospital Clínica San Agustín, para su conocimiento y cumplimiento obligatorio.

Dr. David Romo Rodríguez
Gerente General