1. Nombre de la política	POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

Seguridad
de la Información

2. SLOGAN DE LA POLÍTICA: "PENSANDO EN TI, DOY LO MEJOR DE MI"

3. REFERENCIAS NORMATIVAS

- **ISO/IEC 27001:2022**: Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), bajo un enfoque de gestión del riesgo. Constituye el estándar de referencia base del SGSI del Hospital Susana López de Valencia.

- **ISO/IEC 27002:2022:** Proporciona directrices para la selección, implementación y gestión de los controles de seguridad de la información. Es la guía de implementación de los controles del Anexo A de la ISO/IEC 27001:2022.
- **ISO/IEC 27005:2022:** Proporciona directrices para el proceso de gestión del riesgo de seguridad de la información (establecimiento del contexto, identificación, análisis, evaluación y tratamiento), en apoyo de los requisitos de la ISO/IEC 27001.
- **ISO/IEC 27035 (serie):** Orienta la gestión de incidentes de seguridad de la información: detección, reporte, evaluación, respuesta y aprendizaje. Comprende las partes 27035-1:2023 y 27035-2:2023 (principios/proceso y planeación de la respuesta) y 27035-3:2020 (operaciones de respuesta a incidentes TIC).
- **ISO 31000:2018:** Establece principios, marco y proceso para la gestión del riesgo, aplicables a cualquier tipo de riesgo en la organización. Es el marco general que complementa a la ISO/IEC 27005 para el riesgo de seguridad de la información.
- **ISO 22301:2019:** Especifica los requisitos para implementar y mantener un Sistema de Gestión de la Continuidad del Negocio (SGCN), que permita a la organización mantener y restablecer sus actividades críticas ante interrupciones.
- **ISO 19011:2018:** Proporciona directrices para auditar sistemas de gestión: principios de auditoría, gestión del programa de auditoría, realización de auditorías y evaluación de la competencia de los auditores.
- **MSPI (Modelo de Seguridad y Privacidad de la Información, MinTIC):** Componente de la Política de Gobierno Digital que imparte lineamientos a las entidades públicas para la adopción de buenas prácticas, orientando el ciclo de vida de la seguridad de la información (planeación, implementación, evaluación y mejora continua) bajo el ciclo PHVA. Está basado en la ISO/IEC 27001.
- **LEY 1273 DE 2009 (delitos informáticos):** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado, denominado 'de la protección de la información y de los datos', y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."
- **LEY 1581 DE 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales."**

- **LEY 1712 DE 2014 (Transparencia y Acceso a la Información Pública):** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."
- **LEY 1751 DE 2015 (Estatutaria de Salud):** "Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones."
- **LEY 2015 DE 2020 (Historia Clínica Electrónica Interoperable):** "Por medio de la cual se crea la Historia Clínica Electrónica interoperable y se dictan otras disposiciones."
- **DECRETO 1074 DE 2015 (Decreto Único Reglamentario del sector Comercio, Industria y Turismo):** compila el régimen reglamentario de protección de datos personales de la Ley 1581 de 2012, incluido el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio (SIC).
- **DECRETO 1078 DE 2015 (Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones):** compila la reglamentación del sector TIC, incluida la Política de Gobierno Digital.
- **DECRETO 1008 DE 2018:** Establece los lineamientos generales de la Política de Gobierno Digital (antes Estrategia de Gobierno en Línea) y subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015.
- **DECRETO 338 DE 2022:** Adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015 para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.
- **DECRETO 1081 DE 2015 (Decreto Único Reglamentario del sector Presidencia de la República):** compila la reglamentación de la Ley 1712 de 2014 (transparencia y acceso a la información pública), incluidas la clasificación y reserva de la información y los instrumentos de gestión de información (compila el Decreto 103 de 2015).
- **RESOLUCIÓN 1995 DE 1999 (Ministerio de Salud, manejo de la historia clínica):** "Por la cual se establecen normas para el manejo de la Historia Clínica."
- **RESOLUCIÓN 839 DE 2017 (Ministerio de Salud y Protección Social, historia clínica):** "Por la cual se modifica la Resolución 1995 de 1999 y se dictan otras disposiciones."

4. DEFINICIONES

- **SGSI (Sistema de Gestión de Seguridad de la Información):** Marco estructurado y documentado que, bajo un enfoque de gestión del riesgo, permite a la organización establecer, implementar, mantener y mejorar la seguridad de la información, preservando la confidencialidad, integridad y disponibilidad de sus activos de información.
- **SGCN (Sistema de Gestión de Continuidad del Negocio)**: Define y mantiene las medidas que permiten a la organización seguir operando durante y después de una interrupción o crisis.
- **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:** Componente del marco institucional que establece la postura, los principios, objetivos y responsabilidades de la entidad para proteger la información en todas sus formas.
- **POLÍTICA DE SEGURIDAD DIGITAL:** Conjunto de directrices estratégicas para preservar la confidencialidad, integridad y disponibilidad de los activos de información frente a riesgos tecnológicos y amenazas cibernéticas, orientando el comportamiento de los usuarios.
- **POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN:** Directrices que protegen el derecho de las personas a controlar sus datos personales y previenen la salida o divulgación no autorizada de información, conforme a la normativa vigente.
- **PRINCIPIO DE CONFIDENCIALIDAD**: Propiedad que asegura que la información solo sea accesible para las personas o entidades autorizadas, evitando su divulgación no autorizada.
- **PRINCIPIO DE INTEGRIDAD:** Propiedad que asegura que la información se mantenga exacta, completa y confiable a lo largo de todo su ciclo de vida.
- **PRINCIPIO DE DISPONIBILIDAD:** Propiedad de que la información y los servicios que la soportan sean accesibles y utilizables por las personas autorizadas cuando lo requieran. Es crítico en la prestación de servicios de salud.

- **ACTIVO DE INFORMACIÓN:** Todo dato o recurso con valor para la entidad que debe protegerse, como historias clínicas, bases de datos, documentos, sistemas y equipos.
- **AMENAZA:** Causa potencial de un incidente no deseado que puede dañar la información o los sistemas que la soportan.
- **VULNERABILIDAD**: Debilidad de un activo o control que puede ser explotada por una amenaza para comprometer la información.
- **RIESGO:** Combinación de la probabilidad de que una amenaza explote una vulnerabilidad y del impacto resultante sobre la confidencialidad, integridad o disponibilidad de la información.
- **CONTROL:** Medida que permite reducir o mitigar un riesgo.
- **INCIDENTE:** Ocurrencia de uno o varios eventos no deseados o inesperados que comprometen la confidencialidad, integridad o disponibilidad de la información y violan la política de seguridad de la información.
- **DATO PERSONAL:** Cualquier información vinculada o asociable a una persona natural determinada o determinable (Ley 1581 de 2012).
- **DATO SENSIBLE:** Dato personal que afecta la intimidad o cuyo uso indebido puede generar discriminación, como los datos de salud (Ley 1581 de 2012).
- **COPIAS DE SEGURIDAD:** Copias de información, software y configuraciones que se generan, almacenan y prueban periódicamente para restaurar los datos ante pérdida, corrupción o incidente, preservando disponibilidad e integridad.
- **CONTROL DE ACCESO:** Conjunto de políticas y mecanismos que regulan quién accede a qué recursos, bajo mínimo privilegio y necesidad de conocer. Comprende identificación, autenticación, autorización y trazabilidad.
- **MONITOREO:** Observación, registro y análisis continuo de redes, sistemas y usuarios para detectar anomalías, eventos e incidentes de forma oportuna y permitir reaccionar ante ellos.

- **HISTORIA CLÍNICA:** Documento privado, obligatorio y sometido a reserva, en el que se registran cronológicamente las condiciones de salud del paciente y los actos del equipo de salud que interviene en su atención. Constituye el principal activo de información reservada del Hospital.

5. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información del Hospital Susana López de Valencia, en cualquier soporte, se clasifica según su nivel de sensibilidad. Cada activo tiene un responsable (propietario) que lo clasifica y lo registra en el Inventario de Activos y, cuando corresponde, en el Índice de Información Clasificada y Reservada. El Hospital adopta tres niveles, conforme a la Ley 1712 de 2014 y su reglamentación (Decreto 1081 de 2015, que compila el Decreto 103 de 2015), y a la Ley 1581 de 2012 para los datos personales.

- **Pública (nivel Bajo):** Información sometida al principio de publicidad, que puede conocerse y divulgarse sin restricción. Ejemplos: actos administrativos, datos abiertos e información del sitio web. Acceso: libre.
- **Pública Clasificada / Uso Interno (nivel Medio):** Información cuyo acceso puede restringirse para proteger derechos de terceros o el ámbito interno del Hospital (Ley 1712, art. 18). Ejemplos: documentos internos de gestión y datos personales no sensibles. Acceso: personal autorizado, según necesidad de conocer.
- **Pública Reservada / Confidencial (nivel Alto):** Información de máxima sensibilidad, incluida la historia clínica y los datos sensibles. Se protege como información pública clasificada por afectar la intimidad y la salud (Ley 1712, art. 18) y como dato sensible (Ley 1581). Acceso: estrictamente autorizado y trazable.

Cuando el Hospital custodie información cuya reserva proceda por daño a intereses públicos (Ley 1712, art. 19), esta se tratará como información pública reservada, conforme a la norma que la ampara.

El etiquetado, el manejo por nivel, el control de acceso y la desclasificación de la información documental se realizan a través del proceso de Gestión Documental y sus instrumentos: las Tablas de Retención Documental (TRD), las Tablas de Control de

Acceso para Documentos y el Índice de Información Clasificada y Reservada, que constituyen la fuente operativa de clasificación del Hospital.

6. RESPONSABLES

- Gerente: Responsable de la aprobación de la presente política, la asignación de recursos financieros, técnicos y humanos para el Sistemas de Gestión de Seguridad de la Información (SGSI), y la revisión por la dirección para asegurar su conveniencia, adecuación y eficacia.
- Comité Institucional de Gestión y Desempeño: Responsable de apoyar la dirección estratégica de la seguridad, aprobar metodologías de riesgo y tomar decisiones frente a incidentes de alto impacto.
- Comité de Gobierno Digital: instancia de gobierno de la seguridad y privacidad de la información; orienta estratégicamente el SGSI, aprueba la metodología de riesgos y la Declaración de Aplicabilidad, y decide frente a incidentes de alto impacto. En su seno opera el Comité de Seguridad de la Información, que realiza el seguimiento técnico del SGSI, revisa los hallazgos de auditoría, los riesgos y los incidentes, y propone las acciones correctivas.
- Oficina Asesora de Planeación (Planeación y Gestión Integral de Calidad): articula el SGSI con el MIPG y el sistema de calidad, y coordina el seguimiento de indicadores y la mejora continua.
- Subdirección Administrativa y Financiera, Proceso de Gestión de Sistemas de Información: diseña, implementa, opera y mantiene los controles de seguridad digital y la infraestructura tecnológica, gestiona los incidentes y designa al responsable de Seguridad de la Información.
- Subdirección Científica (Gobierno Clínico): vela por la protección de la historia clínica y de los datos sensibles en los procesos asistenciales, como información clasificada y reservada.
- Proceso de Gestión Documental: clasifica y etiqueta la información documental, administra las TRD, las Tablas de Control de Acceso y el Índice de Información Clasificada y Reservada, y controla la disposición final.

- Talento Humano y Seguridad y Salud en el Trabajo: gestiona la concientización y los compromisos de seguridad en la vinculación, permanencia y desvinculación del personal.
- Oficina Asesora Jurídica y Contratación: incorpora cláusulas de confidencialidad y de protección de datos personales en los contratos con contratistas y terceros.
- Oficina de Control Interno: realiza la evaluación independiente y la auditoría interna del SGSI.
- Líderes de Procesos: aseguran que su personal cumpla las directrices y clasifican la información propia de su área.
- Funcionarios, Contratistas y Terceros: cumplen la política, firman los acuerdos de confidencialidad y reportan los eventos e incidentes de seguridad.

7. OBJETIVO

Garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información del Hospital Susana López de Valencia E.S.E., mediante la implementación y el mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado a la norma ISO/IEC 27001:2022, al Modelo de Seguridad y Privacidad de la Información (MSPI) y a los lineamientos de seguridad digital, gestionando los riesgos físicos, tecnológicos y humanos para asegurar la prestación continua de los servicios de salud, la protección de los datos personales y el cumplimiento del marco legal vigente.

El Hospital Susana López de Valencia se compromete a cumplir los requisitos legales, reglamentarios y contractuales aplicables, a comunicar esta política a todo su personal y partes interesadas, y a mejorar continuamente el SGSI. Esta política constituye el marco para establecer, revisar y hacer seguimiento a los objetivos de seguridad de la información, que se desarrollan a través de las líneas de acción y del Plan de Acción.

8. ALCANCE

Esta política aplica a toda la información del Hospital Susana López de Valencia en cualquier soporte o medio, y a todos los procesos, sedes, sistemas, funcionarios, contratistas y terceros que la generen, accedan, gestionen o custodien.

9. LÍNEAS DE ACCIÓN

9.1. Gobernanza y Cultura de Seguridad de la Información.

9.2. Seguridad Digital y Protección de la Infraestructura Tecnológica.

9.3. Privacidad y Prevención de Fugas de Información.

9.4. Gestión de Riesgos, Incidentes y Continuidad de Operaciones.

10. EVALUACIÓN:

La evaluación del cumplimiento y eficacia de esta política se realizará de forma anual (o cuando se presenten cambios significativos en la infraestructura o normatividad) utilizando los siguientes mecanismos:

10.1. Indicadores de gestión. Se mide un indicador global de madurez del SGSI y los indicadores priorizados en el Plan de Acción de cada vigencia, en función de la capacidad operativa disponible:

- Indicador global: (N° de controles en nivel "repetible" o superior / N° total de controles aplicables del MSPI) × 100. El nivel de madurez se valora según la escala del instrumento de evaluación del MSPI (inexistente, inicial, repetible, efectivo, gestionado y optimizado).
- Indicadores por línea: los definidos y priorizados en el Plan de Acción (por ejemplo, cobertura de capacitación, activos clasificados, vulnerabilidades remediadas o riesgos tratados), que se incorporan de forma progresiva conforme madura el SGSI.

10.2. Listas de chequeo (rondas de seguridad). Verificación aleatoria de: el bloqueo automático de pantalla por inactividad y la ausencia de contraseñas visibles; la vigencia de los controles de acceso; la ejecución de copias de seguridad; y el estado del inventario y la clasificación de activos.

10.3. Simulacros o pruebas. Pruebas de restauración de copias de seguridad, simulacros de incidentes de seguridad o ejercicios de continuidad de los servicios de información, según corresponda.

10.4. Auditoría interna y revisión por la dirección. El SGSI se somete a auditoría interna. Sus resultados, junto con el seguimiento de indicadores y el avance de los controles, se revisan en el Comité de Gobierno Digital, que analiza los hallazgos y define las acciones correctivas y las oportunidades de mejora. Esta instancia soporta la revisión por la dirección del SGSI.

10.5. Encuesta de percepción de cultura de seguridad. Aplicación anual para medir el nivel de apropiación de la cultura de seguridad de la información por parte de funcionarios, contratistas y terceros.

11. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
0	26/03/2024	Creación de la Política General de Seguridad de La Información.
1	Abril 2026	Actualización integral de la Política General De Seguridad De La Información: Se alinean los lineamientos a la norma ISO/IEC 27001:2022, se integra el componente de Seguridad Digital y Privacidad de la Información conforme al MSPI y MIPG.

12. ANEXO PLAN DE ACCIÓN

OBJETIVO ESTRATEGICO HSLV O EJE (si aplica)	LINEAS DE ACCIÓN	ACTIVIDADES	META DE LA ACTIVIDAD	INDICADOR DE MEDICIÓN	CANAL Y/O METODOLOGIA	MECANISMO DE EVALUACIÓN Y MONITOREO	TIPO DE PRODUCTO	EVIDENCIA
SER LA MEJOR EXPERIENCIA EN SALUD	9.1 GOBERNANZA Y CULTURA DE SEGURIDAD DE LA INFORMACIÓN Resp: J. Silva Chávez — R. Camacho	Sodialización de la Política General de Seguridad de la Información (SLV-SIF-GSI-62) al personal del HSLV.	100% del personal informado sobre el contenido, el alcance y las responsabilidades de la política.	(N° colaboradores con socialización / Total colaboradores) × 100	Presentación en el Comité de Gobierno Digital (24 de junio de 2026) y difusión al personal por correo institucional (Google Workspace), SPARK y demás canales de comunicación institucional.	Acta del Comité de Gobierno Digital y registro de envío de las comunicaciones al personal por correo, SPARK y demás canales institucionales; acuse de recibo cuando el canal lo permita.	Informe de socialización de la política.	Acta del Comité de Gobierno Digital (24 de junio de 2026), correos institucionales y mensajes de SPARK enviados al personal, y acuses de recibo cuando el canal lo permita.
		Elaboración y aprobación formal de la Declaración de Aplicabilidad (SOA) y adopción del MSPI	Declaración de Aplicabilidad (SOA) aprobada y MSPI adoptado por el Comité de Seguridad de la Información durante la vigencia 2026.	Acta del Comité de Seguridad de la Información con aprobación del SOA y adopción del MSPI (Sí/No).	Sesión del Comité de Seguridad de la Información, que opera en el marco del Comité de Gobierno Digital.	Acta del Comité de Seguridad de la Información (Comité de Gobierno Digital) firmada.	Declaración de Aplicabilidad (SOA) aprobada (código pendiente de asignación por Gestión Documental)	Acta del Comité de Seguridad de la Información y SOA firmado
		Programa de concientización en ciberseguridad: Cultura de Ciberseguridad HSLV.	≥70% de funcionarios y contratistas capacitados en ciberseguridad al cierre de la vigencia 2026	(N° colaboradores capacitados / Total colaboradores) × 100 ; ≥70%.	Boletines digitales semestrales, talleres presenciales o virtuales anuales, e-learning en Google Workspace y campañas de seguridad (phishing y manejo de contraseñas).	Evaluación pre y post, listas de asistencia e informe bimestral de resultados al Comité de Seguridad de la Información (Comité de Gobierno Digital).	Informe anual de concientización.	Listas de asistencia, evaluaciones de conocimiento (pre y post) y certificados de participación.
	9.2 SEGURIDAD DIGITAL Y PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA Resp: J. Silva Chávez — R. Camacho	Revisión por la dirección del SGSI.	revisión por la dirección del SGSI ejecutada y documentada en acta durante la vigencia 2026.	N° de revisiones por la dirección ejecutadas con acta / N° planificadas (meta: 1).	Sesión del Comité de Seguridad de la Información, en el marco del Comité de Gobierno Digital, con informe de gestión del SGSI : indicadores, resultados de auditoría, avance de controles, riesgos e incidentes.	Acta de revisión por la dirección con decisiones, compromisos y acciones de mejora.	Informe del SGSI y acta de revisión por la dirección.	Informe del SGSI y acta de revisión por la dirección firmada.
		Actualización del Inventario de Activos de Información del HSLV.	Inventario de activos de información de los procesos priorizados (misionales y críticos: SIAU, historia clínica, servidores y bases de datos) levantado y clasificado, con cobertura ≥70% al cierre de 2026; ampliación progresiva en las siguientes vigencias.	(N° de activos documentados y clasificados / N° de activos identificados en los procesos priorizados) × 100. Meta: ≥70%.	Levantamiento por procesos priorizados, con el instrumento (matriz) de inventario de activos y apoyo de los líderes de proceso para identificar y clasificar los activos de su área.	Revisión y actualización del inventario por el responsable de Seguridad de la Información, con reporte del avance de cobertura al Comité de Seguridad de la Información (Comité de Gobierno Digital).	Inventario de activos de información actualizado (procesos priorizados)	Matriz de inventario de activos diligenciada, clasificada y firmada por el responsable.
		Gestión de vulnerabilidades técnicas: análisis semestral con Sophos y ESET Protect.	2 análisis semestrales ejecutados, cada uno con informe de hallazgos y plan de remediación.	N° de informes de vulnerabilidades entregados / N° de análisis planificados (meta: 2).	Sophos XGS 136 (SFOS 21.5.1) y ESET Protect v11.0; revisión de CVE críticos y priorización por CVSS.	Informe semestral de vulnerabilidades	Informe técnico semestral de vulnerabilidades	Informes semestrales con hallazgos (CVSS) y acciones de remediación
	9.3 PRIVACIDAD Y PREVENCIÓN DE FUGAS DE INFORMACIÓN Resp: J. Silva Chávez	Actualización y firma de acuerdos de confidencialidad de funcionarios, contratistas y terceros.	100% de funcionarios, contratistas y terceros con acceso a información con acuerdo firmado	(N° acuerdos firmados / Total funcionarios + contratistas + terceros con acceso) × 100	Gestión documental con Talento Humano (Farith Obando) y Contratación (Sergio Ángel)	Registro y control de acuerdos firmados con verificación periódica por RRHH y SI	Acuerdos firmados y archivados	Acuerdos de confidencialidad firmados, archivados en hojas de vida y contratos
	9.4 GESTIÓN DE RIESGOS, INCIDENTES Y CONTINUIDAD DE OPERACIONES Resp: J. Silva Chávez — R. Camacho	Actualización del Registro de Riesgos de Seguridad de la Información (MSPI / ISO 27005)	Registro actualizado anualmente y articulado con la matriz de riesgos institucional del HSLV	N° actualizaciones del Registro de Riesgos presentadas al HSLV / Meta: 1 por vigencia	Metodología gestión de riesgos MSPI MinTIC e ISO 27005; valoración por activo y amenaza	Revisión semestral del registro y presentación de resultados IICSI actualizado al CGDI	Registro de riesgos actualizado	Registro de riesgos SI actualizado y firmado, articulado con matriz de riesgos institucional HSLV
		Registro y atención de incidentes de seguridad de la información	100% de los incidentes de seguridad reportados, registrados y atendidos según su criticidad, durante la vigencia 2026.	(N° de incidentes atendidos y cerrados / N° de incidentes reportados) × 100.	Bitácora de incidentes y atención conforme a la guía de gestión de incidentes (ISO 27035 / MSPI).	Informe de incidentes presentado al Comité de Seguridad de la Información (Comité de Gobierno Digital).	Bitácora de incidentes e informe de gestión.	Registro de incidentes con acciones, lecciones aprendidas y cierre.

Elaboró:	Revisó:	Revisó:	Revisó:	Aprobó:
Julián Silva Chávez Profesional Sistemas de Información-Afiliado participe ASIES	**Hulber Enrique Acosta Porras** Planeación y Calidad - Afiliado participe ASIES	**Jessica L. Valencia Rodríguez** Jefe Oficina Asesora de Planeación	**Diego Herney Campo S.** Subdirector Administrativo	**Lucy Ximena Ibarra** Gerente
Fecha de aprobación 30 abril 2026		**Vigencia:** por gestión documental 5 años y/o si existen cambios normativos o en el proceso		