

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código:	POL-AAI-11
	Versión:	02
	Página:	Página 1 de 17

Política General de Seguridad y Privacidad de la Información



 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	2 de 17

1. OBJETIVO

Proteger la confidencialidad, integridad y disponibilidad de la información del Hospital Universitario San José de Popayán y de sus sistemas de información, minimizando los riesgos asociados y garantizando la continuidad de los servicios.

2. ALCANCE Y POBLACIÓN OBJETO

La política se aplica a toda la información generada, procesada o administrada por el Hospital Universitario San José de Popayán, dentro de sus recursos de información y sus procesos misionales (Core) de la organización, incluyendo datos clínicos, administrativos, redes, equipos de cómputo, servidores y equipos portátiles, conforme a la Ley 1581 de 2012 sobre protección de datos personales y al estándar ISO/IEC 27001. Cubre todos los procesos asistenciales, los servicios de apoyo y las áreas administrativas, y se extiende a todo el personal, incluidos médicos, enfermeras, administrativos, contratistas y terceros autorizados. Además, tiene como objetivo establecer y mantener controles y directrices que preserven la integridad, confidencialidad y disponibilidad de la información.

Se define el ámbito y alcance del SGSI para el Área administración y almacenamiento de la información, aplicando a todos sus procesos, procedimientos y funciones, determinados de la siguiente manera:

- ✓ Procedimiento de conservación y custodia de la historia clínica.
- ✓ Procedimientos soporte a software y demás aplicaciones.
- ✓ Procedimiento de soporte técnico a equipo de cómputo e impresoras
- ✓ Procedimiento de soporte técnico ante fallas de redes
- ✓ Procedimiento de realización de copias de seguridad
- ✓ Procedimiento de desarrollo de aplicativos
- ✓ Procedimiento de adopción de tecnologías de la información y las comunicaciones
- ✓ Procedimiento de planificación de la gestión de la información
- ✓ Procedimiento de gestión y minería de datos
- ✓ Procedimiento para el manejo de la historia clínica electrónica
- ✓ Procedimiento uso seguro de las TIC
- ✓ Procedimiento de adquisición de tecnología, medicamentos, dispositivos médicos y mobiliario de los diferentes procesos
- ✓ Procedimiento de gestión y evaluación de la tecnología de sistemas de información del HUSJ de Popayán
- ✓ Procedimiento de Contingencia de la información
- ✓ Procedimiento de Confidencialidad
- ✓ Procedimiento para solicitar acceso a la VPN del HUSJ
- ✓ Otros procedimientos que se definen como necesarios

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	3 de 17

3. RESPONSABLES

Toda la organización del Hospital Universitario San José de Popayán es responsable de cumplir las políticas de seguridad de la información, desde el personal médico, asistencial y administrativo hasta contratistas, proveedores y terceros autorizados, quienes deben aplicar las políticas de seguridad en sus actividades diarias. La implementación y supervisión de las políticas están a cargo del Área de Administración y Almacenamiento de la Información, con apoyo del Comité de Seguridad de la Información, que gestiona los riesgos y propone mejoras. La Gerencia aprueba las políticas y toma decisiones estratégicas relacionadas con la seguridad de la información. Adicionalmente, la Oficina Asesora de Planeación o la Auditoría interna es responsable de realizar auditorías internas y evaluaciones periódicas para verificar el cumplimiento de las directrices establecidas, asegurando así la mejora continua y la protección integral de los activos de información institucionales.

4. NORMATIVIDAD VIGENTE

Nº	NORMA	EXPEDIDA POR	DESCRIPCIÓN
1	Constitución Política de Colombia (1991)	Congreso de la República	Establece los derechos fundamentales, incluido el derecho a la intimidad y el habeas data.
2	Ley 1581 de 2012	Congreso de la República	Por la cual se dictan disposiciones generales para la protección de datos personales.
3	Ley 23 de 1981	Congreso de la República	Normas en materia de ética médica que regulan la confidencialidad de la información del paciente.
4	Ley 527 de 1999	Congreso de la República	Define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales.
5	Decreto 1377 de 2013	Presidencia de la República	Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales.

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	4 de 17

6	ISO/IEC 27001:2013 (adoptada en Colombia como NTC-ISO/IEC 27001:2013)	ICONTEC	Norma que especifica los requisitos para un sistema de gestión de seguridad de la información.
7	Resolución 1995 de 1999	Ministerio de Salud y Protección Social	Reglamenta el manejo de la historia clínica.
8	Circular Externa 005 de 2017	Superintendencia de Industria y Comercio	Instrucciones sobre la implementación de medidas para la protección de datos personales.

5. DEFINICIONES

Información: Toda información, independientemente de su forma, que es creada, almacenada o procesada por los recursos de información, redes de comunicaciones y datos o medios de almacenamiento."

Recursos de Información (RI): Todo equipo de cómputo, impresiones, recursos en línea, medios de almacenamiento magnético y todas las actividades relacionadas a sistemas de cómputo, incluyendo cualquier dispositivo capaz de recibir e-mails, navegación en la Web, o con capacidad de recepción, almacenamiento, manejo o transmisión electrónica de datos (servidores, computadores personales, portátiles, smartphones, redes de datos, equipos de fax, impresoras). Adicionalmente, procedimientos, equipos, instalaciones físicas, software y data diseñados para crear, recolectar, procesar, almacenar o transmitir información.

Activos de información: son todos los datos, sistemas, equipos y recursos utilizados para almacenar, procesar y transmitir información en una organización, incluyendo registros digitales, documentos físicos, software y hardware.

Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado

Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	5 de 17

de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

6. POBLACIÓN OBJETO

Esta política aplica a todo el personal del Hospital Universitario San José de Popayán (médicos, enfermeras, administrativos, técnicos), así como a contratistas, proveedores y terceros autorizados que interactúen con los sistemas de información de la organización. No aplica a dispositivos personales no autorizados.

7. DESARROLLO DE LA POLITICA

7.1 JUSTIFICACIÓN DE LA POLÍTICA:

Esta política se implementa para proteger la información, el activo más crítico del hospital, frente a amenazas como ciberataques, errores humanos u otros riesgos, salvaguardando su confidencialidad, integridad y disponibilidad. Se rige con leyes nacionales (Ley 1581, 1273) y estándares internacionales (ISO 27001), y contribuye a la continuidad de los servicios de salud, así como la promoción de una cultura organizacional de seguridad entre colaboradores, contratistas y terceros.

7.2 ORIENTACION ESTRATÉGICA:

En el Hospital Universitario San José de Popayán, la información es uno de los activos más valiosos. Las historias clínicas de los pacientes, los datos administrativos y los sistemas tecnológicos que se usan diariamente son esenciales para brindar una atención médica de calidad. Sin embargo, esta información está expuesta a diferentes riesgos como robos de información, ataques cibernéticos o incluso errores humanos que podrían comprometer la continuidad de los servicios o afectar el funcionamiento del hospital.

Por esta razón, se desarrolló la política de seguridad y privacidad de la información, la cual debe ser cumplida por todos los médicos, enfermeras, personal administrativo, contratistas y proveedores. Su objetivo principal es proteger la información bajo tres principios básicos:

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	6 de 17

- **Confidencialidad:** Que solo las personas autorizadas puedan acceder a los datos.
- **Integridad:** Que la información sea exacta y no se modifique indebidamente.
- **Disponibilidad:** Que los sistemas estén funcionando cuando se necesiten.

Esta política no es solo un requisito legal (como lo exigen la Ley 1581 de protección de datos o la ISO 27001), sino un compromiso con los pacientes y con la calidad del servicio. Ayudan a prevenir problemas que podrían interrumpir la atención médica, poner en riesgo la privacidad de las personas o generar sanciones para el hospital.

Cada uno de nosotros tiene un papel importante: desde bloquear el computador al levantarnos del puesto de trabajo, hasta reportar cualquier situación sospechosa. La seguridad de la información no es solo responsabilidad del área de tecnología, es una tarea de todos los días en la que todos participamos para cuidar lo que más importa: la salud y la confianza de nuestra comunidad.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se definió en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- ✓ La gestión de los riesgos de los activos de información estará a cargo del proceso de Administración y Almacenamiento de la Información teniendo en cuenta el nivel de tolerancia al riesgo de la institución.
- ✓ La implementación de políticas de seguridad de la información y de políticas complementarias por cada procedimiento o proceso a cargo del área de Administración y Almacenamiento de la Información, para preservar la confidencialidad, integridad y disponibilidad de la información institucional.
- ✓ El fomento de la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información
- ✓ Minimizar el riesgo en las funciones y procedimientos a cargo de Administración y Almacenamiento de la Información.
- ✓ Cumplir con los principios de seguridad de la información
- ✓ Mantener la confianza de sus clientes, usuarios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos CORE de la organización.

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	7 de 17

Esta política estará regida por los siguientes principios.

- ✓ **Protección de recursos de información:** Proteger los recursos de información y tecnología administrados por el proceso de Administración y Almacenamiento de la Información frente a amenazas internas o externas, deliberadas o accidentales.
- ✓ **Seguridad desde el diseño:** Incorporar medidas de seguridad en los sistemas de información desde su desarrollo, implementación y mantenimiento, reduciendo los riesgos de errores humanos y eventos naturales.
- ✓ **Gestión de acceso:** Implementar controles de acceso que impidan el ingreso no autorizado a los sistemas, bases de datos, servicios y recursos de red.
- ✓ **Concienciación y responsabilidad del personal:** Sensibilizar y capacitar permanentemente al personal sobre el uso adecuado de contraseñas y la protección de la información, estableciendo responsabilidades claras, compartidas y aceptadas por colaboradores, proveedores, socios de negocio y terceros autorizados.
- ✓ **Revisión y actualización de la política:** La política será revisada anualmente por el oficial de seguridad de la información o su delegado, y actualizada cuando se presenten cambios tecnológicos, incidentes de seguridad o modificaciones normativas relevantes.
- ✓ **Gestión de riesgos de terceros:** Proteger la información y activos ante los riesgos asociados a accesos otorgados a terceros (afiliados, proveedores, clientes), o resultantes de servicios contratados (outsourcing).
- ✓ **Gestión de incidentes de seguridad:** Establecer procedimientos para la identificación, reporte, análisis y respuesta a incidentes de seguridad de la información.
- ✓ **Gestión de activos y copias de seguridad:** Inventariar y clasificar los activos de información; mantener y probar copias de seguridad conforme a las necesidades del hospital.
- ✓ **Control de medios removibles:** Restringir y controlar el uso de medios de almacenamiento removibles (USB, discos externos), asegurando su escaneo con antivirus antes de su uso.
- ✓ **Gestión de cambios:** Controlar y autorizar los cambios en los sistemas de información para minimizar impactos en la seguridad.
- ✓ **Cumplimiento normativo:** Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables.
- ✓ **Protección de infraestructuras:** Salvaguardar las instalaciones de procesamiento

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	8 de 17

y la infraestructura tecnológica que soporta los procesos críticos.

- ✓ **Gestión y uso seguro de contraseñas:** Establecer y aplicar manuales o procedimientos o guías para la creación, uso, almacenamiento y renovación de contraseñas, garantizando que sean robustas, confidenciales y únicas. Las contraseñas deben cumplir con criterios mínimos de complejidad, no ser compartidas, y renovarse periódicamente según las directrices definidas por el área de Administración y Almacenamiento de la Información. Se promoverá el uso de autenticación multifactor (MFA) en los sistemas críticos.

Objetivos del Sistema de Gestión de Seguridad de la información:

- ✓ Proteger los activos de información y la tecnología utilizada para su procesamiento, bajo responsabilidad del proceso de Administración y Almacenamiento de la Información, con el fin de preservar la confidencialidad, integridad y disponibilidad, y salvaguardándolos frente a amenazas internas o externas, ya sean deliberadas o accidentales.
- ✓ Mantener un sistema actualizado de políticas, procedimientos, estándares y planes de tratamiento de riesgos que permita minimizar el nivel de exposición al riesgo de los activos de información bajo la responsabilidad de la Administración y Almacenamiento de la Información.
- ✓ Fomentar la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información
- ✓ Preservar la continuidad de los servicios críticos mediante la implementación de planes de contingencia, recuperación ante desastres y continuidad del negocio relacionados con los activos de información.
- ✓ Promover la gestión adecuada de los accesos a la información y a los sistemas, asegurando que solo las personas autorizadas puedan acceder a los recursos pertinentes, de acuerdo con sus roles y responsabilidades
- ✓ Establecer el seguimiento, la documentación, el análisis y la comunicación de los incidentes de seguridad de la información reportados, garantizando su adecuada gestión y notificación a los responsables correspondientes, bajo la coordinación de la Oficina de Administración y Almacenamiento de la Información y las Comunicaciones.
- ✓ Revisar periódicamente las vulnerabilidades y debilidades técnicas de los sistemas de información y la infraestructura tecnológica, mediante el uso de herramientas de software especializadas, en pruebas de penetración, detección de vulnerabilidades y verificación de controles.

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	9 de 17

Aplicación de las Políticas: El Hospital Universitario San José protegerá todos los Recursos de Información de la organización de acuerdo con las políticas definidas.

Específicamente, la organización aplicará políticas, procedimientos, buenas prácticas, estándares, y guías para proteger las funciones de los recursos de información de datos internos, errores de programación, mal manejo por individuos dentro de o fuera de la empresa. Esto con la finalidad de proteger a la organización de riesgos que comprometan la Integridad de los programas, violación de los derechos individuales a la privacidad y confiabilidad, violación del derecho penal, o de potenciales daños a la seguridad pública.

Todos los Programas de seguridad de los recursos de información de la organización serán responsables y adaptables a los cambios tecnológicos que afecten los Recursos de Información.

Roles y Responsabilidades: Área de Administración y Almacenamiento de la Información. Área responsable de la gestión y administración de los recursos de información del Hospital Universitario San José, La designación del Área de Administración y Almacenamiento de la Información está dirigida a establecer la responsabilidad de diseñar e implementar políticas para el manejo de los recursos de información, proveer una mejor coordinación de las actividades que involucren acceso, procesamiento y administración de la información dentro de la organización, y para asegurar una mejor orientación de tales actividades dentro y fuera de la misma. El área de Administración y Almacenamiento de la Información tiene la autoridad y responsabilidad para implementar Políticas de Seguridad, Procedimientos, Prácticas Estándares y Guías para proteger los Recursos de Información de la empresa.

Propietario: Es el gerente, coordinador o usuario responsable de las funciones que tiene que ver con el manejo y soporte de los recursos, las personas a los cuales se les responsabiliza de llevar a cabo los programas que utilizan los recursos de información. El propietario es responsable de establecer los controles que provean la seguridad. Dependiendo sea el caso, la propiedad puede ser compartida por gerentes o coordinadores de diferentes áreas de servicio y/o procesos.

Usuario: Tiene la responsabilidad de (1) usar los recursos sólo para los propósitos establecidos por el propietario y la organización, (2) cumplir con los controles establecidos por el propietario y la organización, y (3) prevenir declaraciones de información confidencial o sensible. El usuario es la persona que ha sido autorizada para leer, ingresar o actualizar información por al propietario de la información. El usuario cumple el más simple control efectivo para proveer adecuada seguridad.

Mejores Prácticas:

1. Los controles de seguridad de los recursos de información (RI) no deben ser ignorados, desactivados ni eludidos.
2. La conciencia de seguridad de la información del personal debe ser continua,

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	10 de 17

reforzada, actualizada y validada.

3. Todo el personal es responsable del manejo y uso adecuado de los recursos de información (RI), así como de las acciones relacionadas con la seguridad de dichos recursos. Asimismo, cada persona tiene la obligación de reportar cualquier sospecha o confirmación de violaciones o manejo inapropiado de las políticas de seguridad de la información.
4. Las contraseñas, números de identificación de personal (PIN), claves de seguridad, y otros procedimientos y dispositivos de seguridad en los sistemas de informáticos deben ser protegidos por el usuario. Toda violación de seguridad debe ser reportada al responsable o coordinador encargado y/o al área de Administración y Almacenamiento de la Información.
5. El acceso, uso y modificación de los recursos de información (RI) deben realizarse de forma estrictamente segura. La autorización de acceso a la información para cada usuario debe revisarse periódicamente, especialmente en casos de cambios en la situación laboral, como transferencias, promociones, desvinculación o finalización de sus actividades.
6. El uso de los Recursos Informáticos (RI) debe estar oficialmente autorizado y se permite únicamente para propósitos de la organización. No se garantiza la privacidad personal en el uso de herramientas como el correo electrónico, la navegación por Internet y otras plataformas de comunicación electrónica. El uso de estos medios puede ser monitoreado para atender reclamos o apoyar procesos de investigación. Las áreas responsables de la gestión de los equipos informáticos deben asegurar el uso adecuado de los RI, gestionarlos de manera eficiente y reportar su estado y uso.
7. Cualquier información utilizada en un sistema de los recursos de información (RI), debe ser mantenida con confidencialidad y seguridad por el usuario. El hecho de que la información sea almacenada electrónicamente no cambia el requerimiento de mantener la información segura y confiable. Más bien, el tipo o clasificación de la información por sí misma es la base para determinar si la información debe guardarse en forma confidencial y segura. Adicionalmente, si esta información es almacenada en un papel o un formato electrónico, o si la información es copiada, impresa o transmitida electrónicamente debe ser protegida como confidencial y segura.
8. Al finalizar la relación laboral con el hospital, los usuarios deberán entregar todos los bienes y recursos de información (RI) que les hayan sido asignados. Durante este proceso, se aplicarán todas las políticas de seguridad de la información vigentes, hasta completar la devolución de los recursos. Esta política también establece la terminación formal de cualquier vínculo entre el usuario y el hospital.
9. La ejecución de copias de seguridad de los equipos de cómputo debe ser solicitada formalmente por el Coordinador del área, mediante el formato establecido para tal fin. Esta solicitud debe ser remitida al Área de Administración y Almacenamiento de

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	11 de 17

la Información, el cual será responsable de ejecutar la copia de seguridad conforme a lo estipulado en el procedimiento de Copias de Seguridad de Equipos de Cómputo.

10. El propietario del proyecto debe coordinar con el Área de Administración y Almacenamiento de la Información y obtener su aprobación antes de iniciar cualquier proyecto de adquisición de hardware, compra o desarrollo de software para la organización. Los costos asociados a la adquisición, desarrollo y operación de hardware y software deberán ser autorizados por la Gerencia, la Subgerencia y los Coordinadores, según corresponda. La Gerencia, las áreas de servicio y/o los procesos solicitantes deberán actuar dentro de los límites de aprobación establecidos en las políticas de compras de la organización. Se publicará una lista de hardware y software estándar que podrá adquirirse sin necesidad de aprobación previa.
11. El área de servicio y/o el proceso que requiera o autorice una aplicación informática deberá seguir los procedimientos adecuados para garantizar la integridad y seguridad de todos los programas y archivos de información creados u obtenidos mediante dichas aplicaciones.
12. La red de datos es de propiedad y está bajo el control del Área de Administración y Almacenamiento de la Información. Será necesario obtener la aprobación de dicha área antes de conectar a la red cualquier recurso que no cumpla con las guías o estándares publicados. El Área de Administración y Almacenamiento de la Información se reserva el derecho de desconectar de la red cualquier recurso que no cumpla con los estándares establecidos o que no se considere adecuadamente seguro.
13. La integridad en el uso de software, utilidades, sistemas operativos, redes y archivos de información es responsabilidad de cada una de las áreas de servicio y/o procesos en los que se encuentra dividida la organización. El uso de datos con fines de prueba o investigación deberá ser autorizado por el Coordinador del Área de Administración y Almacenamiento de la Información.
14. Todos los cambios o modificaciones en los sistemas de recursos de información (RI), redes de datos, programas o datos deben ser aprobados por el proceso encargado el cual es responsable de su integridad.
15. El área de Administración y Almacenamiento de la Información debe proveer controles de acceso adecuados para monitorear los sistemas y proteger la información y los programas contra usos indebidos, conforme a las necesidades definidas por los propietarios o usuarios de la información. Todo acceso debe encontrarse debidamente documentado, autorizado y controlado.
16. Todos los contratos relacionados con sistemas o aplicaciones informáticas, incluyendo alquileres, licencias u otros acuerdos, deberán ser autorizados y firmados por el Gerente y el Área de Administración y Almacenamiento de la Información y/o

	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	12 de 17

el usuario autorizado de la organización. Estos contratos deben incluir los términos aprobados por el área legal. Asimismo, se debe notificar a los proveedores o contratistas de recursos de información (RI) de la organización sobre la obligación de respetar los derechos de propiedad de los sistemas de información, programas y datos requeridos.

17. Los sistemas informáticos, los recursos de información (RI) y los equipos asociados que se utilicen para fines de la organización, pero que sean operados y administrados por terceros fuera del control directo de la empresa, deben cumplir con los requisitos contractuales establecidos y estarán sujetos a monitoreo; como también conocer la Política General de Seguridad y Privacidad de la información.
18. El acceso externo desde y hacia los recursos de información (RI) debe cumplir con las guías de seguridad apropiadas y publicadas por la organización.
19. Todo software comercial utilizado en los sistemas informáticos debe contar con un acuerdo de licencia que describa los derechos de uso y las restricciones del producto. El personal debe cumplir con todos los términos de dichas licencias y no debe realizar copias no autorizadas del software. El Área de Administración y Almacenamiento de la Información se reserva el derecho de remover cualquier software sin licencia de los recursos de información (RI).
20. El Área de Administración y Almacenamiento de la Información se reserva el derecho de eliminar cualquier software o archivo de los sistemas informáticos que no esté relacionado con las actividades o fines de la organización. Algunos ejemplos de este tipo de software son: juegos, programas de mensajería instantánea o chat, herramientas para eludir restricciones de navegación, archivos de música, fotografías y programas freeware o shareware.
21. Todo el personal que acceda a información clínica de los pacientes, incluyendo historias clínicas electrónicas, deben garantizar la confidencialidad, integridad y disponibilidad de dicha información. Queda estrictamente prohibido divulgar, compartir o utilizar información clínica sin autorización expresa y justificación laboral. Se deben aplicar controles de acceso por rol y registro de auditoría de accesos.
22. La información almacenada en medios físicos o electrónicos (USB, discos duros, CDs, impresos) debe ser manejada de forma segura. Los medios que contengan información confidencial deben ser cifrados, controlados y eliminados de forma segura (borrado seguro, destrucción física certificada) al finalizar su uso.
23. El acceso a las áreas donde se encuentran equipos que procesan o almacenan información crítica (servidores, centros de datos, archivos físicos) debe ser restringido mediante mecanismos de control físico (tarjetas, biometría, cerraduras) y registrado.

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	13 de 17

24. El uso de redes inalámbricas (Wi-Fi) dentro del Hospital debe cumplir con estándares de cifrado robusto, segmentación de red (separación de redes para pacientes, visitantes y personal) y mecanismos de autenticación segura. Está estrictamente prohibida la instalación de puntos de acceso o dispositivos de red no autorizados, tales como routers personales, repetidores inalámbricos, swiches u otros equipos que permitan compartir conexión sin la aprobación del Área de Administración y Almacenamiento de la Información
25. El acceso a Internet desde los sistemas informáticos de la organización estará restringido únicamente a los sitios web autorizados y aprobados por el Área de Administración y Almacenamiento de la Información. Cualquier intento de acceder a sitios no permitidos será bloqueado automáticamente por los sistemas de filtrado y monitoreo de navegación implementados. La lista de sitios autorizados se revisará y actualizará periódicamente de acuerdo con las necesidades de la organización. Se prohíbe el uso de herramientas o programas destinados a eludir estas restricciones de navegación.
26. Todo dispositivo de almacenamiento extraíble, incluyendo memorias USB, discos duros portátiles y tarjetas de memoria, deberá ser escaneado con el software antivirus autorizado por el Área de Administración y Almacenamiento de la Información antes de ser conectado a cualquier equipo de cómputo de la organización. El uso de estos dispositivos estará sujeto a la autorización y supervisión del área correspondiente, y únicamente se permitirá cuando sea estrictamente necesario para fines laborales. Queda prohibido el uso de dispositivos de almacenamiento personal no autorizados. El Área de Administración y Almacenamiento de la Información se reserva el derecho de bloquear o restringir el uso de puertos USB en los equipos, según lo considere necesario para preservar la seguridad de los recursos de información (RI).
27. El acceso remoto a los sistemas y recursos de información (RI) de la organización solo podrá realizarse mediante las soluciones de Red Privada Virtual (VPN) previamente autorizadas y administradas por el Área de Administración y Almacenamiento de la Información. Está estrictamente prohibido el uso de cualquier otro software, servicio o herramienta de conexión remota que no haya sido aprobado formalmente por dicha área. El acceso por VPN debe cumplir con los controles de autenticación, cifrado y monitoreos establecidos. Todo acceso remoto no autorizado será considerado una violación grave a las políticas de seguridad de la organización y estará sujeto a sanciones.
28. Los equipos de cómputo estarán bajo la responsabilidad del Coordinador del área y no podrán ser trasladados a otras dependencias sin la autorización previa del Área de Administración y Almacenamiento de la Información. Además, dicho traslado deberá contar con la respectiva asignación de cambio emitida por el área de Almacén, encargada de la gestión del inventario de los equipos.

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	14 de 17

29. Ningún funcionario ni contratista podrá retirar equipos de cómputo fuera de las instalaciones del Hospital Universitario San José sin contar previamente con la autorización del Coordinador del área correspondiente y del Coordinador del Área de Administración y Almacenamiento de la Información.

30. El cumplimiento de todas las políticas, mejores prácticas, procedimientos y guías que respaldan esta política de seguridad de la información es obligatorio.

Violaciones: Cualquier evento que resulte en robo, pérdida o uso desautorizado, declaración no autorizada, modificaciones desautorizadas, destrucciones desautorizadas, o acceso a los recursos de información (RI) denegados, constituyen una brecha de seguridad y a su confidencialidad. Estas violaciones pueden incluir, pero no limitarse, a los siguientes:

- ✓ Exponer a la organización a actuales o potenciales pérdidas monetarias
- ✓ comprometiendo la Seguridad de los RI.
- ✓ Involucra las declaraciones de información sensible o confidencial o el uso no autorizado de datos o recursos de la organización.
- ✓ Incluye el uso de los RI para beneficio personal, no ético, dañino o con propósitos ilícitos.

Acciones Disciplinarias:

El incumplimiento a la política General de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a General de Seguridad y Privacidad de la Información se refiere, la violación de estas Políticas puede resultar en acciones disciplinarias inmediatas, pero no limitadas a:

- ✓ Reprimendas Formales.
- ✓ Suspensión o acceso restringido a los Recursos de Información de la institución
- ✓ Restitución o indemnización por cualquier daño o apropiación ilícita de cualquier propiedad de la institución,
- ✓ Suspensión sin pago, Término de empleo, Término de contrato, Despido.
- ✓ Proceso Civil.
- ✓ Proceso Penal.

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	15 de 17

Asistencia: Cualquier solicitud relacionada con esta política o la aplicación de esta debe ser referida al jefe del área de Administración y Almacenamiento de la Información

7.3 POLITICA:

En coherencia con la misión y visión institucional, el Hospital Universitario San José asume un compromiso firme con la Seguridad de la Información, entendida como un elemento estratégico para garantizar la confianza, la continuidad y la calidad en la prestación de los servicios de salud.

Este compromiso se materializa mediante la implementación de un modelo integral y sostenible del Sistema de Gestión de Seguridad de la Información (SGSI), basado en los principios de confidencialidad, integridad y disponibilidad, conforme a los lineamientos de la norma ISO/IEC 27001, la Ley 1581 de 2012 y demás normativas aplicables.

El SGSI se fundamenta en la gestión de riesgos, la aplicación de controles seguros, el uso de tecnologías confiables y la capacitación continua del talento humano, promoviendo una cultura organizacional orientada a la mejora continua y a la protección efectiva de la información de pacientes, colaboradores y procesos institucionales.

8. REFERENCIAS BIBLIOGRÁFICAS

1. Organización Internacional de Normalización (ISO). (2022). *ISO/IEC 27001:2022 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos* (3a ed.). Ginebra, Suiza: ISO. 62 p. ISBN 978-92-67-11275-4.
2. Congreso de la República de Colombia. (2017, 17 de octubre). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá, Colombia: Diario Oficial No. 48.587. 12 p.
3. Ministerio de Salud y Protección Social. (2021). Resolución 3100 de 2019. Por la cual se reglamenta la Historia Clínica Electrónica. Bogotá, Colombia: Diario Oficial No. 50.909.

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	16 de 17

9. CONTROL DE REGISTROS

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN		Anexo al procedimiento OPL-PD04		OPL-PD04-FO11	
		FORMATO DE CONTROL DE REGISTROS			
			Tiempo de retención		
Nombre registro	Código	Recuperación	Almacenamiento	Conservación	Disposición
N/A					

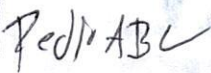
10. ANEXOS

- N/A

11. CONTROL DE CAMBIOS

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN		Anexo al procedimiento OPL-PD04		OPL-PD04-FO12
FORMATO DE CONTROL DE CAMBIOS				
Código	Versión	Fecha	Descripción del Documento	
AAI-POL-11	01	Septiembre de 2023	Creación del documento	
Define Planeación	02	Junio 2025	Se integró la información contenida en la Política del Sistema de Gestión de Seguridad de la Información, la Política General de Seguridad de la Información y la Política de Privacidad y Seguridad de la Información, con el propósito de consolidar en una única Política General de Seguridad y Privacidad de la Información	

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO PORDUEN	Proceso:	Gestión de la información y Comunicaciones	Código:	POL-AAI-11
	Subproceso:	Administración y almacenamiento de la información	Versión:	02
	Nombre del documento:	Política General de Seguridad y Privacidad de la información	Página:	17 de 17

Elaboró y/o actualizó	Pedro Alejandro Bonilla Valencia	Revisó	Juan David Uribe Ordoñez Juan Francisco Mora Obando	Aprobó	Juan Carlos Arteaga Cifuentes
Cargo	-Profesional SGSI de la administración y almacenamiento de la información – Afiliado partícipe Assesalud.OC	Cargo	-Coordinador de administración y almacenamiento de la información –Afiliado partícipe Assesalud.OC Subgerente Administrativo y Financiero Gr-1	Cargo	Gerente Gr-2 / HUSJ
Firma		Firma		Firma	
Fecha	08 JUL 2025	Fecha	08 JUL 2025	Fecha	08 JUL 2025
GESTIÓN DOCUMENTAL					
Nombre	Jesús Hernán Guerrero Erazo	Cargo	Auxiliar Administrativo Gr-3	Firma	