RESOLUCIÓN No 183
(02 DE JULIO DE 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital de la E.S.E. Hospital San Juan de Dios de Pamplona".

EL GERENTE DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN JUAN DE DIOS DE PAMPLONA,

En uso de sus facultades Legales, Estatuarias y especialmente las conferidas por el Acuerdo No. 023 de diciembre 15 de 2015 y

CONSIDERANDO:

Que el artículo 209 de la Constitución Política de Colombia establece los principios de la función administrativa, entre ellos la eficiencia, la transparencia y la moralidad.

Que la Ley 1581 de 2012 regula la protección de datos personales en Colombia.

Que el Decreto 1078 de 2015 compila la normativa del sector TIC, incluyendo las directrices sobre seguridad digital y protección de la información.

Que el Decreto 1499 de 2017 adopta el Modelo Integrado de Planeación y Gestión – MIPG, estableciendo la obligación de implementar políticas institucionales de seguridad digital.

Que el Decreto 1008 de 2018 reglamenta la Política de Gobierno Digital, incluyendo lineamientos específicos sobre ciberseguridad y gestión de riesgos tecnológicos.

Que la Circular Externa 100-000002 de 2022 de la Superintendencia de Sociedades establece directrices para fortalecer la ciberseguridad y la protección de datos en entidades públicas.

Que es deber de la E.S.E. Hospital San Juan de Dios de Pamplona proteger los activos de información, sistemas y servicios digitales frente a amenazas internas y externas, garantizando la seguridad, integridad y disponibilidad de la información institucional y es así como a petición del comité de MIPG se procede a realizar por el área de sistemas la política.

Que, en mérito de lo anterior mente expuesto se:

RESUELVE

ARTÍCULO PRIMERO. Adopción de la Política: Adóptese formalmente la Política de Seguridad Digital de la E.S.E. Hospital San Juan de Dios de Pamplona, como una directriz institucional de aplicación obligatoria en todos los niveles jerárquicos y procesos organizacionales, orientada a fortalecer la protección de los activos de información, garantizar la continuidad de los servicios, y consolidar una cultura organizacional segura, confiable y resiliente frente a riesgos digitales.

ARTÍCULO SEGUNDO. Objetivos: Orientar la transformación institucional hacia un modelo de seguridad digital integral, fortaleciendo la gobernanza tecnológica, la gestión de riesgos cibernéticos, y la protección efectiva de los datos institucionales, de conformidad con el MIPG y el Plan de Desarrollo Institucional.

PARÁGRAFO: Definir los siguientes objetivos específicos:

2.1 Garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

2.2 Establecer controles de seguridad en el acceso, almacenamiento y transmisión de datos.

RESOLUCIÓN No 183
(02 DE JULIO DE 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital de la E.S.E. Hospital San Juan de Dios de Pamplona".

2.3 Fomentar la cultura de seguridad digital mediante procesos de formación continua.

2.4 Implementar medidas de protección contra amenazas internas y externas.

2.5 Asegurar el cumplimiento normativo en materia de ciberseguridad y protección de datos.

2.6 Integrar la seguridad digital en todos los procesos y proyectos institucionales**.**

ARTÍCULO TERCERO. Alcance: La presente política aplica a todos los funcionarios, contratistas, usuarios, proveedores y demás partes interesadas que accedan o administren sistemas de información, plataformas tecnológicas y datos institucionales, en todos los procesos misionales, de apoyo y estratégicos de la E.S.E.

ARTÍCULO CUARTO. Responsables:

4.1 Gerencia: Liderar la implementación, seguimiento y evaluación de la política.

4.2 Área de la Gestión de la Tecnología: Ejecutar las acciones técnicas, coordinar la gestión de incidentes y garantizar el soporte necesario.

4.3 Control Interno: Verificar el cumplimiento y formular recomendaciones de mejora.

4.4 Líderes de procesos: Aplicar los lineamientos en sus áreas, promover prácticas seguras y reportar incidentes.

4.5 Talento humano: Participar en capacitaciones y aplicar buenas prácticas de seguridad digital.

4.6 Todos los colaboradores: Acatar la política, proteger la información y reportar riesgos o anomalías.

ARTÍCULO QUINTO: La política se regirá por los siguientes principios Rectores:

5.1 Confidencialidad: La información sólo será accesible a personas autorizadas.

5.2 Integridad: Garantizar que la información no sea alterada de forma indebida.

5.3 Disponibilidad: La información estará disponible cuando sea requerida.

5.4 Trazabilidad: Se podrá conocer quién, cuándo y cómo se accedió o modificó un dato.

5.5 Legalidad: Cumplimiento de las normas vigentes en protección de datos y ciberseguridad.

5.6 Corresponsabilidad: Todos los actores institucionales comparten la responsabilidad de la seguridad digital.

5.7 Mejora continua: Aplicación del ciclo PHVA para fortalecer los controles y capacidades institucionales.

RESOLUCIÓN No 183
(02 DE JULIO DE 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital de la E.S.E. Hospital San Juan de Dios de Pamplona".

ARTÍCULO SEXTO: La política adoptada comprenderá, como mínimo, los siguientes componentes estratégicos.

6.1 Gobierno de la Seguridad de la Información: Conjunto de estructuras, políticas, roles, responsabilidades y procesos mediante los cuales se dirige, gestiona y supervisa la seguridad de la información en la organización. Permite tomar decisiones estratégicas, establecer prioridades y garantizar la alineación con los objetivos institucionales y la normativa vigente.

6.2 Identificación y Gestión de Activos de Información: Proceso mediante el cual se identifican, clasifican, valoran y protegen los activos de información (datos, documentos, sistemas, equipos, infraestructura, personal, etc.), determinando sus propietarios, niveles de criticidad y medidas de control para prevenir pérdidas, accesos no autorizados o usos indebidos.

6.3 Gestión de Riesgos Tecnológicos: Conjunto de metodologías para identificar, analizar, evaluar y mitigar los riesgos asociados al uso de tecnologías de la información y la comunicación. Incluye el análisis de amenazas, vulnerabilidades, impactos y probabilidades, con el fin de implementar controles eficaces que protejan la continuidad operativa.

6.4 Protección contra Software Malicioso y Accesos no Autorizados: Conjunto de mecanismos preventivos y reactivos destinados a detectar, bloquear o eliminar malware (virus, troyanos, ransomware, spyware, etc.) y controlar el acceso lógico y físico a los sistemas y datos institucionales, garantizando que sólo personal autorizado pueda utilizarlos.

6.5 Gestión de Incidentes de Seguridad Digital: Proceso estructurado para la detección, reporte, análisis, contención, resolución y documentación de eventos que afecten o puedan afectar la seguridad de la información. Incluye la designación de responsables, protocolos de respuesta, comunicación y acciones correctivas para prevenir reincidencias.

6.6 Concientización y Formación en Ciberseguridad: Acciones formativas y comunicativas dirigidas a los funcionarios, contratistas y demás actores institucionales, orientadas a fomentar la adopción de comportamientos seguros, el reconocimiento de amenazas digitales y el cumplimiento de la normativa sobre seguridad de la información.

6.7 Auditoría, Monitoreo y Cumplimiento Normativo: Conjunto de actividades de seguimiento, evaluación y verificación del cumplimiento de la política de seguridad digital, los controles implementados y los estándares legales aplicables. Permite identificar brechas, mejorar prácticas y garantizar la rendición de cuentas ante entes de control.

ARTÍCULO SÉPTIMO: Enfoque de Gestión: La implementación de esta política se fundamenta en el enfoque de mejora continua, bajo el ciclo PHVA (Planear, Hacer, Verificar, Actuar), garantizando una gestión sistemática, adaptable y basada en resultados para prevenir, mitigar y responder ante amenazas digitales.

7.1 PLANEAR (P): Consiste en identificar necesidades, establecer objetivos, definir políticas, procedimientos y controles necesarios para gestionar los riesgos relacionados con la seguridad de la información y las tecnologías digitales.

RESOLUCIÓN No 183
(02 DE JULIO DE 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital de la E.S.E. Hospital San Juan de Dios de Pamplona".

7.2 HACER (H): Implica la ejecución de los planes y controles definidos. Incluye la implementación de acciones técnicas y organizacionales para proteger los activos de información y cumplir los lineamientos institucionales.

7.3 VERIFICAR (V): Se refiere al seguimiento y medición del desempeño de los controles y procesos implementados, a través de auditorías internas, revisiones de cumplimiento, indicadores de gestión y evaluación de incidentes.

7.4 ACTUAR (A): Comprende la adopción de acciones correctivas, preventivas y de mejora, con base en los resultados obtenidos en la fase de verificación, buscando fortalecer continuamente la seguridad digital de la entidad.

ARTÍCULO OCTAVO: Vigencia y actualización: La presente política tendrá una vigencia indefinida y deberá revisarse cuando se presenten cambios significativos en la normativa, el contexto institucional o el direccionamiento estratégico, con el fin de garantizar su pertinencia, efectividad y alineación con los objetivos de la E.S.E. y del MIPG. El Comité de Modelo Integrado de Planeación y Gestión - MIPG será el encargado de su evaluación periódica, emitiendo recomendaciones para su actualización y mejora.

COMUNIQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Pamplona, a los dos (02) días del mes de julio (07) del año dos mil veinticinco (2025).

LUIS DANIEL VERJEL SANCHEZ
GERENTE.

FABIO ANDRES CAMARGO JEREZ
SUB DIRECTOR ADMINISTRATIVO

ELIZABETH SANCHEZ BARROSO
ASESORA JURIDICA

Proyectó: Área de Gestión de la Información
Revisó: Comité de Gestión y Desempeño
Aprobó: Comité de Gestión y Desempeño