


|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |


# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



**E.S.E HOSPITAL DEPARTAMENTAL SAN  
ANTONIO PITALITO HUILA**

**2026**

| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 1     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## CONTROL DE DOCUMENTO Y DISTRIBUCIÓN:


### Control del Documento

|            | Nombre                                      | Cargo                                    | Dependencia                             | Fecha                   |
|------------|---|--|---|-------------------------|
| Autor      | Gerardo Gómez Cortes                        | Asesor Sistemas de Información           | Sistemas de Información                 | 15 de diciembre de 2025 |
|            | Michael Brayan Rojas Bermeo                 | Especialista seguridad de la Información | Mesa de ayuda LIAN BPO                  |                         |
| Revisión   | Jorge Eliecer Tovar Valencia                | Subgerente Administrativa y Financiera   | Subgerencia Administrativa y Financiera | 18 de diciembre de 2025 |
| Aprobación | Comité Institucional de Gestión y Desempeño |  |   |                         |
|            | Acta No. 001 del 22 de enero de 2026        |  |   |                         |
|            | Diana Marcela Conde Martín                  |  | Gerente                                 |                         |
| Adopción   | Resolución Gerencial No. 020                |  | Fecha: 22 de enero de 2026              |                         |

### Control de los Cambios


| Versión No. | Fecha de Aprobación |         |                | Descripción de los Cambios  |
|-------------|---------------------|---------|----------------|---|
| 1.0         | Resolución          | No. 042 | del 28/01/2020 | Levantamiento del procedimiento   |
| 2.0         | Resolución          | No. 053 | del 29/01/2021 | Actualización del documento   |
| 3.0         | Resolución          | No. 177 | del 26/7/2021  | Actualización del documento   |
| 4.0         | Resolución          | No. 027 | del 27/01/2022 | Actualización del documento   |
| 5.0         | Resolución          | No. 037 | del 27/01/2023 | Revisión y ajuste del Plan en concordancia con los avances y actividades propuestas |
| 6.0         | Resolución          | No.049  | del 30/1/2024  | Actualización del documento   |

|        |                             |  |                                   |          |       |
|--------|-----------------------------|--|-----------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                          | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del 22/01/2026 | 8.0      | 2     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

|     |                                   |                             |
|-----|-----------------------------------|-----------------------------|
| 7.0 | Resolución No. 034 del 27/01/2025 | Actualización del documento |
| 8.0 | Resolución No. 020 del 22/01/2026 | Actualización del documento |


|               |                                    |  |  |                 |              |
|---------------|------------------------------------|--|--|-----------------|--------------|
| <b>FECHA:</b> | <b>Elaboración:</b><br>26/01/2020  | <b>Aprobación</b>  | <b>Adopción</b>                              | <b>Versión:</b> | <b>Hoja:</b> |
|               | <b>Modificación:</b><br>16/01/2026 | <b>Acta No. 001 del 22/01/2026<br/>Comité Institucional de Gestión y<br/>Desempeño</b> | <b>Resolución No. 020 del<br/>22/01/2026</b> | <b>8.0</b>      | <b>3</b>     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:<br/>HSP-GI-SI-PL03<br/>22/01/2026<br/>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## TABLA DE CONTENIDO

|   |    |
|---|----|
| 1. OBJETIVO.....  | 5  |
| 2. ALCANCE .....  | 5  |
| 3. TERMINOS Y DEFINICIONES.....   | 5  |
| 4. MARCO LEGAL Y/O CONCEPTUAL .....   | 9  |
| 6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ..... | 12 |
| 6. PLAN DE ACCIÓN Y PUNTOS DE CONTROL .....   | 12 |
| 6.1 MATRIZ DE RIESGOS INSTITUCIONAL.....  | 14 |
| 7. ESTRATEGIAS Y/O LINEAS DE ACCION .....   | 1  |
| 8. INDICADORES Y METAS .....  | 1  |
| 9. DOCUMENTOS Y REGISTROS RELACIONADOS .....  | 2  |
| 10.RESPONSABLES .....   | 3  |
| 11. REFERENCIAS BIBLIOGRAFICAS.....   | 3  |
| 12. PARTICIPACIÓN CIUDADANA, APROBACIÓN Y PUBLICACIÓN DEL PLAN ..                   | 3  |

|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 4     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## 1. OBJETIVO

Presentar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información (SGSI) de la E.S.E Hospital Departamental San Antonio de Pitalito, de tal forma que se definen y aplican los controles con los cuales se busca mitigar la materialización de los riesgos de seguridad de la información en la entidad. De esta forma, se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información dentro de la institución, se mantenga la integridad, confidencialidad y disponibilidad de la información.

## 2. ALCANCE


El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los procesos de la E.S.E. Hospital Departamental San Antonio de Pitalito y es obligatorio para todos los colaboradores, independientemente de su nivel o rol. Su alcance comprende la gestión de los riesgos relacionados con la seguridad digital y la protección de la información presentes en las plataformas tecnológicas, sistemas de información y servicios de TIC que soportan la operación institucional. Este plan cubre todas las actividades derivadas del modelo de operación por procesos, garantizando la identificación, valoración, mitigación y seguimiento de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

## 3. TERMINOS Y DEFINICIONES

Para facilitar la comprensión del presente documento, se definen los siguientes términos:

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Aceptación del riesgo:** Decisión informada de tomar un riesgo particular.
- **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan


|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 5     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización.
- **Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- **Asumir/Aceptar el riesgo:** La entidad acepta el riesgo en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección y lo asume conociendo los efectos de su posible materialización.
- **Causa:** Origen, comienzo de una situación determinada que genera un efecto o consecuencia.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Resultado de un evento que afecta los objetivos.
- **Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.
- **Control:** Medida que modifica el riesgo.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO31000:2013.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.


|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 6     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- **HDSAP:** Hospital Departamental San Antonio de Pitalito.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **Información:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- **MSPI:** Modelo de Seguridad y privacidad.
- **Política de seguridad de información:** Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.
- **Probabilidad:** Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 7     |




|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
- **Riesgos de seguridad digital:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- **Riesgo Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información:** Parte del sistema de gestión general del Instituto, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo” (Icontec Internacional, 2011).
- **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información.

|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 8     |




|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

#### 4. MARCO LEGAL Y/O CONCEPTUAL

| NORMATIVIDAD  | DEFINICIÓN  |
|---|---|
| <b>Ley 1581 de 2012</b>   | Establece disposiciones generales para la protección de datos personales y los principios rectores para su tratamiento.                 |
| <b>Decreto 1377 de 2013</b>   | Reglamenta aspectos relacionados con la autorización y tratamiento de datos personales.   |
| <b>Sentencia C-748 de 2011</b>  | Define el habeas data y la protección constitucional de los datos personales.   |
| <b>Decreto 1008 de 2018</b>   | Adopta la Política de Gobierno Digital en Colombia.   |
| <b>Política de Seguridad y Privacidad de la Información – MinTIC (MSPI)</b> | Lineamientos para la gestión de riesgos, seguridad y privacidad en entidades públicas.  |
| <b>Guía de Gestión de Riesgos de Seguridad y Privacidad MinTIC (2022)</b>   | Instrumento obligatorio para la gestión de riesgos en el sector público.  |
| <b>Ley 594 de 2000 – Ley General de Archivos</b>                            | Define disposiciones para la administración, conservación y custodia de documentos físicos y electrónicos.                              |
| <b>Acuerdo AGN 006 de 2015</b>  | Lineamientos para documentos electrónicos de archivo y gestión de riesgos asociados a su preservación.                                  |
| <b>Ley 1712 de 2014</b>   | Regula el derecho al acceso a la información pública y determina obligaciones asociadas a la clasificación y reserva de la información. |
| <b>Decreto 1081 de 2015</b>   | Reglamenta parcialmente la Ley 1712.  |
| <b>Ley 2015 de 2020</b>   | Regula la Historia Clínica Electrónica Interoperable (HCEI).  |
| <b>Resolución 1995 de 1999</b>  | Regula la historia clínica, su manejo, custodia, acceso y reserva.  |
| <b>Resolución 5109 de 2015</b>  | Establece lineamientos de seguridad para la información del sistema de salud.   |
| <b>ISO/IEC 27001:2022</b>   | Estándar internacional para establecer un Sistema de Gestión de Seguridad de la Información (SGSI).                                     |

|        |                             |  |                                      |          |       |
|--------|-----------------------------|--|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 9     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## 5. Análisis DOFA

El análisis DOFA permitió identificar los factores internos y externos que influyen en la gestión de la seguridad y privacidad de la información en la E.S.E. Hospital Departamental San Antonio de Pitalito, brindando una visión integral sobre la situación actual y los principales retos institucionales frente al cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el MinTIC.


Se evidencian fortalezas asociadas al compromiso directivo, la existencia de políticas formalizadas, los controles tecnológicos implementados y la experiencia del talento humano del área TIC. Asimismo, se identifican debilidades vinculadas con la necesidad de fortalecer la cultura institucional en protección de datos, la capacitación continua del personal y la modernización de la infraestructura tecnológica.

Del entorno externo surgen oportunidades derivadas de los programas nacionales de fortalecimiento digital y las políticas de Gobierno Digital, que facilitan la gestión de proyectos de inversión y modernización tecnológica. No obstante, también se presentan amenazas relevantes, como el incremento de los ciberataques dirigidos al sector salud, las restricciones presupuestales y la dependencia de proveedores externos.

Con base en este diagnóstico, se definieron estrategias orientadas a fortalecer la seguridad institucional, consolidar la cultura de protección de datos personales y garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando la continuidad de los servicios hospitalarios y el cumplimiento de la normativa vigente en materia de seguridad y privacidad de la información.


Siguiendo los lineamientos recibidos por parte de la Gobernación del Huila, se hace inclusión de la matriz DOFA del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. Hospital Departamental San Antonio de Pitalito, con el propósito de realizar un análisis integral de la situación actual en materia de gestión de riesgos asociados a la seguridad y privacidad de la información, identificando los factores internos y externos que pueden influir en la implementación, sostenibilidad y mejora continua del plan.

|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 10    |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:<br/>HSP-GI-SI-PL03<br/>22/01/2026<br/>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

| MATRIZ DOFA  |  |  |
|--|--|--|
| <div>FACTORES EXTERNOS</div> <div>FACTORES INTERNOS</div>  | Oportunidades (O)  | Amenazas (A)   |
|  | O1 Lineamientos del MSPI y la Resolución 500/2021: Refuerzan los estándares y requisitos para mejorar la seguridad digital institucional.      | A1 Incremento de ciberataques al sector salud: Aumentan amenazas como ransomware, phishing y robo de bases de datos.                             |
|  | O2 Programas nacionales de apoyo: Ofrecen oportunidades de financiación para modernizar infraestructura y tecnología.                          | A2 Riesgos legales por incumplir la Ley 1581/2012: Las fallas en el tratamiento de datos pueden generar sanciones y procesos administrativos.    |
|  | O3 Tecnologías avanzadas de ciberseguridad: Herramientas como EDR, SIEM y firewalls modernos permiten detectar y responder mejor a incidentes. | A3 Dependencia de proveedores externos: El hosting, ERP y el soporte crítico dependen de terceros, aumentando el riesgo operacional.             |
|  | O4 Políticas de Gobierno Digital: Impulsan la transformación digital y fortalecen la gestión de la información en el sector salud.             | A4 Riesgos tecnológicos, naturales o estructurales: Fallas técnicas o eventos ambientales pueden afectar la disponibilidad de los servicios TI.  |
|  | O5 Mayor conciencia sobre protección de datos: Crece el compromiso institucional y ciudadano con la ciberseguridad y la privacidad.            |  |
| Fortalezas (F)   | ESTRATEGIAS FO   | ESTRATEGIAS FA   |
| F1 Políticas y procedimientos formalizados: La institución cuenta con lineamientos claros de confidencialidad, respaldos, accesos y continuidad. | FO 1 Aprovechar los programas del MinTIC y MinSalud para fortalecer la madurez institucional en seguridad y privacidad                         | FA 1 Reforzar la seguridad perimetral y los mecanismos de respaldo para mitigar amenazas externas.   |
| F2 Compromiso directivo: El Comité Institucional y la Subgerencia Administrativa apoyan activamente la seguridad de la información.              | FO 2 Fortalecer el componente tecnológico incorporando herramientas de monitoreo y detección temprana de incidentes.                           | FA 2 Actualizar y armonizar las políticas de seguridad y privacidad conforme a la normativa vigente.   |
| F3 Controles físicos y lógicos implementados: Se dispone de firewall, antivirus, respaldos y procedimientos técnicos consolidados.               | FO 3 Impulsar la formación continua en ciberseguridad apoyándose en la experiencia del personal TIC.   | FA 3 Mantener y consolidar los indicadores de gestión que evalúan la eficacia de los controles institucionales                                   |
| F4 Personal TIC capacitado: El equipo posee experiencia operativa en seguridad y continuidad del servicio.                                       |  |  |
| F5 Matriz de riesgos e indicadores institucionales: Existe un sistema de seguimiento y control anual sobre riesgos e indicadores.                | FO 4 Desarrollar campañas internas que refuercen la cultura de protección de datos y seguridad digital.  | FA 4 Implementar protocolos estrictos de acceso y manejo de información sensible en los sistemas hospitalarios.                                  |
| F6 Comité de Seguridad de la Información: Se cuenta con un órgano formal que orienta y supervisa la gestión de seguridad.                        |  |  |
| Debilidades (D)  | ESTRATEGIAS DO   | ESTRATEGIAS DA   |
| D1 Ausencia de herramientas centralizadas para el monitoreo integral de eventos y alertas de seguridad de la información.                        | DO 1 Incluir dentro del Plan Institucional capacitaciones continuas en seguridad digital y protección de datos personales.                     | DA 1 Diseñar un Plan de Contingencia y Recuperación ante Desastres (DRP) que contemple incidentes cibernéticos y fallas críticas.                |
| D2 Falta de un programa continuo de capacitación en seguridad y privacidad para personal asistencial y administrativo.                           | DO 2 Gestionar proyectos ante la Gobernación o MinTIC para modernizar infraestructura y adquirir SIEM.   | DA 2 Priorizar recursos en infraestructura esencial y servicios de misión crítica.   |
| D3 Dependencia de infraestructura tecnológica con soporte próximo a vencer.  | DO 3 Documentar y actualizar el inventario de activos de información y sus riesgos.  | DA 3 Realizar seguimientos periódicamente la matriz de riesgos institucional y los planes de tratamiento según cambios del entorno.              |
| D4 Falta de consolidación de una cultura institucional orientada a la protección de la información.  | DO4 Integrar la seguridad digital en la planeación estratégica y en los comités de gestión y control.  | DA 4 Dar continuidad y mejora a las evaluaciones anuales de cumplimiento del MSPI y políticas de seguridad, en articulación con Control Interno. |

| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                             | Versión: | Hoja: |
|--------|-----------------------------|--|--------------------------------------|----------|-------|
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 11    |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## 6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información a cargo de la E.S.E Hospital Departamental San Antonio de Pitalito, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados.

## 7. PLAN DE ACCIÓN Y PUNTOS DE CONTROL

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos de la E.S.E Hospital Departamental San Antonio de Pitalito, estas actividades se estructuraron siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

| Nº | Actividad / Estrategia  | Control Asociado                       | Responsable   | Frecuencia | Evidencia                                    |
|----|---|--|---|------------|--|
| 1  | Implementar una solución SIEM para centralizar el monitoreo de eventos de seguridad.        | Monitoreo y correlación de eventos     | Gestión de la información / Oficial de la seguridad de la información | Trimestral | Reportes SIEM, logs, acta de implementación  |
| 2  | Actualizar y fortalecer el inventario de activos de información y su evaluación de riesgos. | Gestión de activos / Matriz de riesgos | Oficial de la seguridad de la información                             | Trimestral | Inventario actualizado, matriz revisada      |
| 3  | Diseñar e implementar un Programa Continuo de Capacitación en                               | Formación y concienciación             | Talento Humano / Gestión de la información / Oficial de la            | Trimestral | Listas de asistencia, evaluaciones, material |

|        |                             |  |                                   |          |       |
|--------|-----------------------------|--|-----------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                          | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del 22/01/2026 | 8.0      | 12    |



E.S.E Hospital Departamental  
San Antonio de Pitalito

**EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL  
SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2**

**PROCESO: GESTIÓN DE LA INFORMACIÓN**


**SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN**

**NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE  
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**CÓDIGO:  
HSP-GI-SI-PL03  
22/01/2026  
Versión: 8.0**

|    |  |                                |   |            |   |
|----|--|--------------------------------|---|------------|---|
|    | Seguridad y Privacidad.  |                                | seguridad de la información   |            |   |
| 4  | Actualizar el Plan de Contingencia y DRP para cubrir incidentes cibernéticos y fallas críticas.      | Continuidad del negocio        | Gestión de la información   | Anual      | Versión actualizada del DRP, simulacros     |
| 5  | Realizar campañas internas de protección de datos y cultura digital segura.                          | Protección de datos personales | Gestión de la información / Oficial de la seguridad de la información | Trimestral | Material de campaña, registros de difusión  |
| 6  | Priorizar la renovación de infraestructura tecnológica próxima a vencer soporte.                     | Ciclo de vida de activos       | Subgerencia Administrativa / Gestión de la información                | Semestral  | Cotizaciones, actas, plan de renovación     |
| 9  | Implementar herramientas EDR/XDR para detección temprana de amenazas.                                | Detección y respuesta          | Oficial de la seguridad de la información                             | Trimestral | Reportes EDR, registros de alertas          |
| 10 | Realizar seguimiento continuo a la matriz de riesgos y su plan de tratamiento.                       | Monitoreo de riesgos           | Oficial de la seguridad de la información                             | Trimestral | Matriz actualizada, informes de seguimiento |
| 11 | Actualizar las políticas institucionales de seguridad y privacidad según normativa (MSPI, Ley 1581). | Políticas y normatividad       | Gestión de la información / Oficial de la seguridad de la información | Anual      | Políticas revisadas, resoluciones, actas    |
| 12 | Mantener indicadores de gestión de seguridad y privacidad para evaluar la eficacia de los controles. | Indicadores MSPI               | Gestión de la información / Oficial de la seguridad de la información | Trimestral | Tablero de indicadores, informes            |
| 13 | Evaluar periódicamente la efectividad del firewall perimetral y mecanismos de respaldo.              | Seguridad perimetral / Backups | Oficial de la seguridad de la información                             | Trimestral | Logs de firewall, reportes de respaldo      |

| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                          | Versión: | Hoja: |
|--------|-----------------------------|--|-----------------------------------|----------|-------|
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del 22/01/2026 | 8.0      | 13    |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

|    |   |                        |                           |            |   |
|----|---|------------------------|---------------------------|------------|---|
| 14 | Formalizar acuerdos SLA con proveedores críticos (ERP, hosting, soporte).                   | Gestión de proveedores | Gestión de la información | Semestral  | Contratos actualizados, informes SLA              |
| 15 | Integrar evidencia documental al sistema de gestión documental electrónico para auditorías. | Gestión documental     | Gestión de la información | Trimestral | Evidencias cargadas, actas, reportes de auditoría |

## 6.1 MATRIZ DE RIESGOS INSTITUCIONAL

La entidad ha establecido un procedimiento para la gestión integral del riesgo y como producto de su aplicación ha elaborado la matriz de riesgos institucional, la cual se encuentra identificada dentro del SGSI (Sistema de gestión de seguridad de la Información). La matriz muestra el consolidado de los riesgos del proceso de Gestión de Información, clasificados de la siguiente manera:


**Tabla 1. Riesgos de proceso**

| RIESGOS DE PROCESO  |
|---|
| Subregistros asistenciales y administrativos                                  |
| No disponibilidad de Servicios TI   |
| Perdida de la información   |
| Usuarios insatisfechos con el servicio de soporte técnico de la mesa de ayuda |
| Software desarrollado desalineado con el proceso                              |
| No disponibilidad de capital para invertir en recursos de TI                  |
| Uso de software ilegal  |
| Falla tecnológica y de redes  |
| Inapropiado almacenamiento y custodia de historias clínicas y documentación   |

**Tabla 2. Riesgos de sistemas de información**

| RIESGOS DE SISTEMAS DE INFORMACIÓN   |
|--|
| Daño por calentamiento en el cuarto del servidor principal                         |
| Colapso estructural por movimiento sísmico que pueda causar daño en los servidores |
| Espionaje remoto de bases de datos de historias clínicas y financiera              |
| Pérdida de información vital para la operación del negocio                         |
| Incumplimiento en la disponibilidad del personal de soporte                        |

|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 14    |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

Para efectos del presente Plan de Tratamiento de Riesgos, tomamos los riesgos de sistemas de información y haciendo énfasis en los riesgos que en el mapa de calor se encuentren en naranja y rojo, producto de este estudio da como resultado la siguiente matriz de riesgos.

|               |                                    |  |  |                 |              |
|---------------|------------------------------------|--|--|-----------------|--------------|
| <b>FECHA:</b> | <b>Elaboración:</b><br>26/01/2020  | <b>Aprobación</b>  | <b>Adopción</b>                              | <b>Versión:</b> | <b>Hoja:</b> |
|               | <b>Modificación:</b><br>16/01/2026 | <b>Acta No. 001 del 22/01/2026<br/>Comité Institucional de Gestión y<br/>Desempeño</b> | <b>Resolución No. 020 del<br/>22/01/2026</b> | <b>8.0</b>      | <b>15</b>    |





E.S.E Hospital Departamental  
San Antonio de Pitalito

# EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITILITO HUILA NIT: 891.180.134-2

PROCESO: GESTIÓN DE LA INFORMACIÓN


SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE  
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO:  
HSP-GI-SI-PL03  
22/01/2026  
Versión: 8.0


| RIESGO   | CAUSAS  | CONSECUENCIAS   | CONTROLES ACTUALES   | P  | I   | ZONA DE RIESGO     | NUEVOS CONTROLES PROPUESTOS  | RESPONSABLE                                       | PLAZO | INDICADOR   | SEGUIMIENTO                                  |
|--|---|---|--|----|-----|--------------------|--|---|-------|---|--|
| Falla en la seguridad e integridad de la información | 1. Insuficiencia de infraestructura tecnológica que garantice custodia, accesibilidad e integridad del dato.<br>2. Falta de priorización de la compra de herramientas informáticas.<br>3. Ataques informáticos. | Fallas en la oportunidad de la atención que puede generar insatisfacción, deserción del paciente e implicaciones legales<br>Insatisfacción del cliente interno y externo. | El proceso de Gestión de la Información cuenta con los siguientes mecanismos que permitirá mitigar el riesgo así:<br>- Plan anual de adquisiciones.<br>- Manual de Seguridad de la Información.<br>- Procedimiento de Uso y apropiación. | 40 | 100 | <b>RIESGO ALTO</b> | 1. Monitoreo y configuración de Firewall perimetral SONICWALL.<br>2. Utilización de herramientas para protección de correos institucionales.<br>3. Aplicación de las políticas de seguridad de la información.<br>4. Despliegue y educación en temas de seguridad de la información.<br>5. Cumplimiento del plan anual de adquisición.<br>6. Priorizar las según lo estipulado en el Manual de contratación. | Integrantes del proceso Gestión de la Información | 2026  | <b>Indicador 1.</b> Porcentaje de ataques informáticos Controlados al sistema de información: número de ataques controlados en el periodo/ Total de ataques informáticos en el periodo*100. (Meta: 99%).<br><br><b>Indicador 2.</b> porcentaje Inspecciones Realizadas de seguridad de la información: Cantidad de inspecciones de seguridad realizadas / total de inspecciones programadas*100 (Meta: 98%).<br><br><b>Indicador 3.</b> Porcentaje de cumplimiento del programa de capacitación y entrenamiento de TI: Número de actividades del plan de capacitación institucional ejecutadas en el periodo / Número de actividades del plan de capacitación institucional programadas en el periodo *100. (Meta: 80%) | Líder del proceso Gestión de la Información. |

|        |                             |  |                                   |          |       |
|--------|-----------------------------|--|-----------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                          | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del 22/01/2026 | 8.0      | 1     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |


|  |  |   |  |    |    |                     |   |   |      |  |  |
|--|--|---|--|----|----|---------------------|---|---|------|--|--|
| Manejo inadecuado de la protección de datos personales que afectan la confidencialidad de la información . | 1. El personal involucrado en la recopilación e ingreso de datos clínicos no salvaguarda la confidencialidad del dato.<br>2. La información que se filtra confidencial de los pacientes puede afectar su entorno social. | Violación a la privacidad del usuario y su familia e implicaciones legales. | El proceso de Gestión de la Información cuenta con los siguientes mecanismos que permitirá mitigar el riesgo así:<br>• POLÍTICA DE CONFIDENCIALIDAD, PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES.<br>• ACUERDO DE CONFIDENCIALIDAD PERSONAL DE PLANTA.<br>• ACUERDO DE CONFIDENCIALIDAD-CONTRATISTA Y/O AFILIADOS PARTICIPES.<br>• PROCEDIMIENTO : SOLICITUD COPIA DE HISTORIAS CLÍNICAS.<br>• PROCEDIMIENTO DE CONTROL DE ACCESOS LÓGICOS. | 40 | 60 | <b>RIESGO MEDIO</b> | 1. Actualizaciones continuas del sistema de información.<br><br>2. Planes de contingencia para prevenir eventos adversos relacionados con la información.<br><br>3. Despliegue y educación en temas de seguridad de la información. | Integrantes del proceso Gestión de la Información . | 2026 | <b>Indicador 1.</b> porcentaje Inspecciones Realizadas de seguridad de la información: Cantidad de inspecciones de seguridad realizadas / total de inspecciones programadas*100 (Meta: 98%). | Líder del proceso Gestión de la Información. |
| Falta de Calidad en la captura de datos de   | 1. Dificultad en la programación de auditorías que se deben realizar en  | Toma de decisiones inadecuadas a nivel directivo.                           | El proceso de Gestión de la Información cuenta con el siguiente  | 40 | 40 | <b>RIESGO MEDIO</b> | 1. Capacitación a usuarios responsables   | Integrantes del proceso Gestión de la               | 2026 | <b>Indicador:</b> 1. Porcentaje de gestión de la calidad Dato del HDSAP  | Líder del proceso Gestión de la Información. |

|        |   |  |  |                 |              |
|--------|---|--|--|-----------------|--------------|
| FECHA: | <b>Elaboración:</b><br><b>26/01/2020</b>  | <b>Aprobación</b>  | <b>Adopción</b>                          | <b>Versión:</b> | <b>Hoja:</b> |
|        | <b>Modificación:</b><br><b>16/01/2026</b> | <b>Acta No. 001 del 22/01/2026</b><br><b>Comité Institucional de Gestión y Desempeño</b> | <b>Resolución No. 020 del 22/01/2026</b> | <b>8.0</b>      | <b>2</b>     |

|   |  |  |  |   |
|---|--|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL</b><br><b>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>            |  |  |   |

|  |  |  |  |    |    |             |  |   |      |  |  |
|--|--|--|--|----|----|-------------|--|---|------|--|--|
| los registros clínicos y administrativos.              | las Historias clínicas para asegurar calidad del dato.<br>2. Constante cambio de normatividad que generan solicitudes de información que no se ha capturado.   |  | mecanismo para asegurar la calidad en la captura del dato.<br>• PROCEDIMIENTO GESTION DEL DATO.<br>• Comité de historias clínicas.   |    |    |             | del registro de información.<br><br>2. Validación de fuentes de información.                                 | Información                                       |      | Formula: Número de inconsistencias encontradas / Total de reportes revisados *100.(Meta:10%)   |  |
| Manejo y uso inadecuado de la tecnología no biomédica. | 1. Falta de planeación para la gestión de la tecnología en términos de actualización, parametrización, capacidad, copias de seguridad y capacitación.<br>2. Falta de conocimiento de uso de la tecnología y cambio de normatividad del sector salud. | Deficiencia en los procesos misionales y apoyo que generan baja productividad. | El proceso de Gestión de la Información cuenta con el siguiente mecanismo para hacer el seguimiento del uso adecuado de la tecnología no biomédica:<br>• PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD.<br>• Rondas de capacitaciones. | 20 | 40 | RIESGO BAJO | 1. copias de seguridad y equipos de contingencia.<br><br>2.Sensibilización sobre buen manejo de los equipos. | Integrantes del proceso Gestión de la Información | 2026 | <b>Indicador:</b> 1. Porcentaje de daños de los equipos tecnológicos no biomédicos.<br><br>Número de equipos dañados no biomédicos / Total de equipos no biomédicos en el área *100 (Meta: 1.0%) | Líder del proceso Gestión de la Información. |

|        |                             |  |                                   |          |       |
|--------|-----------------------------|--|-----------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                          | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del 22/01/2026 | 8.0      | 3     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## 7. ESTRATEGIAS Y/O LINEAS DE ACCION

La ejecución de este plan consiste en llevar a cabo la implementación de los controles propuestos en la matriz anterior, procurando que se realicen dentro de los tiempos establecidos y sean desarrolladas por los responsables asignados.


Para poder realizar con éxito la ejecución de las actividades estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal.

## 8. INDICADORES Y METAS

Como se observa en la tabla de la matriz anterior, por cada riesgo y por cada control propuesto se han fijado indicadores individuales, pero a nivel general es pertinente establecer un indicador que agrupe todas las actividades el cual quedaría de la siguiente manera y sirve para medir la eficacia en la ejecución del plan:

| NOMBRE  | FORMULA   | META | FRECUENCIA | RESPONSABLE      |
|---|---|------|------------|------------------|
| Porcentaje de ataques informáticos Controlados al sistema de información                    | número de ataques controlados en el periodo/ Total de ataques informáticos en el periodo*100  | 99%  | Mensual    | Mesa de servicio |
| Porcentaje de Inspecciones o Rondas de seguridad de la información realizadas en el periodo | Cantidad de inspecciones de seguridad realizadas / total de inspecciones de seguridad programadas*100   | 98%  | Mensual    | Mesa de servicio |
| Porcentaje de cumplimiento del programa de capacitación y entrenamiento de TI               | Número de actividades del plan de capacitación institucional ejecutadas en el período / Número de actividades del plan de capacitación institucional programadas en el período *100 | 80%  | Mensual    | Mesa de servicio |


|        |                                    |  |  |                 |              |
|--------|------------------------------------|--|--|-----------------|--------------|
| FECHA: | <b>Elaboración:</b><br>26/01/2020  | <b>Aprobación</b>  | <b>Adopción</b>                              | <b>Versión:</b> | <b>Hoja:</b> |
|        | <b>Modificación:</b><br>16/01/2026 | <b>Acta No. 001 del 22/01/2026<br/>Comité Institucional de Gestión y Desempeño</b> | <b>Resolución No. 020 del<br/>22/01/2026</b> | <b>8.0</b>      | <b>1</b>     |

|   |  |     |         |   |
|---|--|-----|---------|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |     |         | <b>CÓDIGO:<br/>HSP-GI-SI-PL03<br/>22/01/2026<br/>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |     |         |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |     |         |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |     |         |   |
| Porcentaje de gestión de la<br>calidad Dato del HDSAP   | Número de inconsistencias<br>encontradas / Total de reportes<br>revisados *100.                              | 10% | Mensual | Mesa de servicio  |
| Porcentaje de daños de los<br>equipos tecnológicos no<br>biomédicos.  | Número de equipos dañados no<br>biomédicos / Total de equipos no<br>biomédicos en el área *100               | 1%  | Mensual | Mesa de servicio  |

## 9. DOCUMENTOS Y REGISTROS RELACIONADOS

- Política de Confidencialidad, Privacidad y Tratamiento de Datos Personales
- Política General de Seguridad y Privacidad de la Información
- Política Desarrollo Seguro de Software
- Política Claves de Acceso Usuarios
- Política de seguridad física y del entorno
- Política de seguridad para relación con proveedores
- Políticas De Buenas Prácticas En Seguridad De La Información
- Política De Respaldo De Información
- Procedimiento de responsabilidad de la seguridad de la información
- Procedimiento de gestión de activos
- Procedimiento de seguridad ligada a los recursos humanos
- Procedimiento de seguridad en las comunicaciones y operaciones
- Procedimiento de control de acceso lógico
- Procedimiento de adquisición, desarrollo y mantenimiento de sistemas informáticos
- Procedimiento para publicación de información en la página web institucional
- Procedimiento de gestión de incidentes de seguridad
- Procedimiento de gestión de la continuidad del negocio
- Procedimiento de cumplimiento
- Procedimiento de Instalación de software
- Procedimiento de copias de seguridad base de datos
- Procedimiento de copias de seguridad de equipos de cómputo usuarios
- Procedimiento de mantenimiento de equipos de computo
- Procedimiento de restauración de base de datos
- Procedimiento de acceso a la data center
- Procedimiento de aceptación de pruebas para actualización o liberación

|        |                             |  |                                   |          |       |
|--------|-----------------------------|--|-----------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación   | Adopción                          | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y Desempeño | Resolución No. 020 del 22/01/2026 | 8.0      | 2     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

## 10. RESPONSABLES

- Subgerencia Administrativa y financiera.
- Asesor de Sistemas de información.
- Mesa de servicio de TI.
- Profesional Especializada en Seguridad Informática.
- Coordinadores de procesos


## 11. REFERENCIAS BIBLIOGRAFICAS

- **ISO/IEC 27001:2018** – Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27005:2011** – Gestión de Riesgos de Seguridad de la Información.
- **ISO/IEC 27002:2018** – Controles de Seguridad de la Información.
- **MinTIC (2021)**. Modelo de Seguridad y Privacidad de la Información – MSPI.
- **MinTIC (2022)**. Guía para la Gestión de Riesgos de Seguridad y Privacidad de la Información.
- **Ley 1581 de 2012** – Protección de Datos Personales.
- **Ley 594 de 2000** – Ley General de Archivos (soporta preservación, custodia y riesgos documentales).
- **Ley 1712 de 2014** – Transparencia y Acceso a la Información Pública.

## 12. PARTICIPACIÓN CIUDADANA, APROBACIÓN Y PUBLICACIÓN DEL PLAN

Con el fin de garantizar la participación ciudadana, el presente plan fue publicado en el mes de diciembre de 2025 en el enlace de la página web institucional: <https://hospitalpitalito.gov.co/menu-transparencia/planeacion/plan-de-accion/2555-planes-estrategicos-2026-con-el-objeto-que-la-comunidad-efectue-observaciones/>, con el propósito de recibir comentarios, sugerencias y observaciones por parte de la ciudadanía, durante el periodo comprendido entre el 26 de diciembre de 2025 al 07 de enero de 2026.

|        |                             |   |                                      |          |       |
|--------|-----------------------------|---|--------------------------------------|----------|-------|
| FECHA: | Elaboración:<br>26/01/2020  | Aprobación  | Adopción                             | Versión: | Hoja: |
|        | Modificación:<br>16/01/2026 | Acta No. 001 del 22/01/2026<br>Comité Institucional de Gestión y<br>Desempeño | Resolución No. 020 del<br>22/01/2026 | 8.0      | 3     |

|   |  |  |   |
|---|--|--|---|
| <br>E.S.E Hospital Departamental<br>San Antonio de Pitalito | <b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL<br/>SAN ANTONIO DE PITALITO HUILA NIT: 891.180.134-2</b> |  | <b>CÓDIGO:</b><br><b>HSP-GI-SI-PL03</b><br><b>22/01/2026</b><br><b>Versión: 8.0</b> |
|   | <b>PROCESO: GESTIÓN DE LA INFORMACIÓN</b>  |  |   |
|   | <b>SUBPROCESO: SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN</b>  |  |   |
|   | <b>NOMBRE DEL DOCUMENTO: PLAN DE TRATAMIENTO DE RIESGOS DE<br/>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>  |  |   |

Posterior al cumplimiento del plazo establecido para la publicación del presente plan en la página web institucional (del 26 de diciembre de 2025 al 07 de enero de 2026), no se recibieron observaciones, comentarios ni sugerencias por parte de la ciudadanía. En consecuencia, el presente Plan fue sometido a consideración y aprobación por parte del Comité Institucional de Gestión y Desempeño – MIPG, mediante Acta No. 01 del 22 de Enero de 2026. Finalmente, el Plan quedó adoptado en su versión definitiva y fue publicado en el enlace de transparencia institucional de La E.S.E. Hospital Departamental San Antonio de Pitalito, disponible en: <https://hospitalpitalito.gov.co/menu-transparencia/planeacion/plan-de-accion/2556-planes-estrategicos-y-plan-de-accion-para-la-vigencia-2026/>

|               |                                    |  |  |                 |              |
|---------------|------------------------------------|--|--|-----------------|--------------|
| <b>FECHA:</b> | <b>Elaboración:</b><br>26/01/2020  | <b>Aprobación</b>  | <b>Adopción</b>                              | <b>Versión:</b> | <b>Hoja:</b> |
|               | <b>Modificación:</b><br>16/01/2026 | <b>Acta No. 001 del 22/01/2026<br/>Comité Institucional de Gestión y<br/>Desempeño</b> | <b>Resolución No. 020 del<br/>22/01/2026</b> | <b>8.0</b>      | <b>4</b>     |