

# Hospital Regional de Sogamoso E.S.E.

## Plan de servicio y/o proceso: PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

| | | |
|---|---|---|
| Hospital Regional de Sogamoso E.S.E. | **Hospital Regional de Sogamoso E.S.E.**<br><br>**Proceso**: Gestión de la información<br>**Subproceso**: Gestión de la información<br>**Plan de servicio y/o proceso**: PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION | **Código** A-GI-GI-PS-01<br>**Fecha** 2025-01-24<br>**Versión** 1 |

| Estratégico | Misional | Apoyo | Evaluación y control |
|---|---|---|---|

## OBJETIVO GENERAL

Definir y coordinar las actividades necesarias para implementar y mantener el Modelo de Seguridad y Privacidad de la Información (SPI) en el Hospital Regional de Sogamoso, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información sensible y crítica, asegurando el cumplimiento normativo y la protección de los datos personales y corporativos.

## OBJETIVOS ESPECIFICOS

1. Establecer y mantener políticas de seguridad y privacidad de la información alineadas con las normativas vigentes en Colombia, los lineamientos del MinTIC y las mejores prácticas internacionales, como la norma ISO 27001.
2. Implementar estrategias y controles específicos para garantizar la confidencialidad, integridad y disponibilidad de la información sensible y crítica del Hospital Regional de Sogamoso E.S.E.
3. Optimizar los procesos internos de gestión de la seguridad y privacidad de la información, asegurando una respuesta eficiente y efectiva ante incidentes de seguridad.
4. Realizar auditorías y evaluaciones periódicas del cumplimiento de las políticas y controles de seguridad y privacidad de la información, identificando oportunidades de mejora y aplicando medidas correctivas cuando sea necesario.
5. Diseñar e implementar programas de capacitación y sensibilización dirigidos a todos los funcionarios, enfocados en la adopción de buenas prácticas para la protección de la información y el cumplimiento de las políticas de seguridad
6. Promover una cultura organizacional sólida en torno a la seguridad y privacidad de la información, involucrando a funcionarios, personal en misión y usuarios externos en la adopción de prácticas responsables en el manejo de datos.

## ALCANCE

La política de seguridad de la información del Hospital Regional de Sogamoso E.S.E. se aplica a todas las áreas, procesos y personas que interactúan con la información y los sistemas tecnológicos de la institución.

Esta política abarca a los colaboradores, contratistas y practicantes que tienen acceso a la información, así como al uso y manejo adecuado de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación bajo la responsabilidad del hospital. También aplica a cualquier sistema, plataforma o servicio tecnológico utilizado dentro de la institución, asegurando el cumplimiento de las normativas y mejores prácticas en seguridad de la información.

## RESPONSABLES

Dentro del Hospital Regional de Sogamoso, los responsables del plan de seguridad y privacidad de la información normalmente incluyen varios roles.

- Junta Directiva y Alta Gerencia: Son responsables de establecer la política de seguridad y privacidad, asegurar su implementación y asignar los recursos necesarios para su cumplimiento.
- Gestión de la Información: Se encargan de la implementación técnica de las políticas y medidas de seguridad, incluyendo la gestión de infraestructura tecnológica, redes y sistemas.
- Recursos Humanos: Responsable de implementar programas de capacitación y concienciación sobre seguridad y privacidad de la información para todos los empleados, contratistas y practicantes. Cada uno de estos roles tiene un papel vital en la protección de la información del hospital, trabajando juntos para mantener la confidencialidad, integridad y disponibilidad de los datos.

**MARCO LEGAL Y/O TEÓRICO**

- Ley 1266 de 2008, disposiciones generales de habeas data y se regula el manejo de la información.
- Ley Estatutaria 1581 de 2012, protección de datos personales.
- Ley 1712 de 2014, Ley de transparencia y acceso a la información pública.
- Acuerdo 03 de 2015 del Archivo General de la Nación, lineamientos generales sobre la gestión de documentos electrónicos.
- Decreto reglamentario único 1081 de 2015, reglamento sobre la gestión de la información pública.
- Decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.
- Resolución 3564 de 2015, reglamenta aspectos relacionados con la Ley de Transparencia y acceso a la información pública.
- MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN –MSPI de la política de Gobierno Digital del MinTIC.

**DEFINICIONES**

**Acceso a la información pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

**Activo:** Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

**Activo de información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC27000).

**Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo (ISO/IEC27000).

**Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoria (ISO/IEC 27000).

**Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

**Bases de datos personales:** Conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, art 3).

**Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701).

**Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009).

**Criterios del riesgo:** Termino de referencia frente a los cuales la importancia de un riesgo se evalúa.

**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 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.

**Confidencialidad**: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

**Datos:** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

**Datos abiertos:** Son todos aquellos datos primarios o con sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

**Datos personales:** Cualquier información vinculada a que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

**Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información -SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001 (ISO/IEC 27000).

**Disponibilidad**: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones

**Encargado del tratamiento de datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento (Ley 1581 de 2012, art 3).

**Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

**Evaluación del riesgo**: Proceso de comparación de los resultados del análisis de riesgo, para evaluar, y determinar su magnitud o si son aceptables o tolerables.

**Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27000).

**Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

**Ley de Transparencia y Acceso a la información pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

**Monitoreo:** Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorias de los sistemas integrados de gestión.

**Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimizarían o cifrado.

**Nivel del riesgo:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la clasificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

**Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la

información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

**Política de la seguridad de la información**: Es el componente principal para la puesta en marcha del modelo de seguridad y privacidad de la información, y unos de los requisitos del Sistema de Gestión de Seguridad de la Información, es el documento que contiene objetivo, aplicabilidad, alcance, principios, nivel de cumplimiento, fundamentos, roles y responsabilidades que se requieren como requisito para la implementación del sistema de gestión de la seguridad de la información.

**Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

**Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a tratamiento que operan en el país (Ley 1581 de 2012, art 25).

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 2700).

**Seguridad:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000).

**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 y de mejora continua (ISO/IEC 27000).

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

## DIAGNÓSTICO Y/O SITUACIÓN ACTUAL

El Hospital Regional de Sogamoso E.S.E. se encuentra en una etapa inicial en la implementación de un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), alineado con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Hasta el momento, se ha avanzado únicamente en la fase de evaluación, lo que ha permitido identificar el estado actual de los controles y procesos relacionados con la seguridad y privacidad de la información. Sin embargo, las fases de planificación, implementación, evaluación de desempeño y mejora continua aún no han sido desarrolladas. A continuación, se presentan los resultados concretos de la evaluación realizada, que servirán como base para la fase de planificación:

**Resultados de la Evaluación del Estado Actual**

1. **Estado de los controles de seguridad y privacidad de la información:**

- **Nivel inicial:** La mayoría de los controles evaluados se encuentran en un estado básico o inexistente, lo que evidencia la necesidad de diseñar e implementar controles específicos para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Fortalezas identificadas:
    - Existe un compromiso inicial por parte de la alta dirección para avanzar en la implementación del SGSPI.
    - Se han identificado los activos de información más críticos para la operación del hospital.
- Debilidades identificadas:
    - No se cuenta con políticas formalizadas de seguridad y privacidad de la información.
    - Los procedimientos para la gestión de incidentes de seguridad son inexistentes o no están documentados.
    - No se han implementado controles técnicos avanzados, como cifrado de datos o monitoreo continuo.

2. **Cumplimiento normativo:**

- **Resultado del análisis:** El hospital presenta un bajo nivel de cumplimiento con la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y otras normativas aplicables. Las principales brechas incluyen:
    - Falta de publicación y actualización de las bases de datos personales en el portal de Datos Abiertos, lo que es un requisito para garantizar la transparencia y cumplimiento con las disposiciones legales sobre la gestión de información pública.
    - Aunque el hospital cuenta con formatos para el consentimiento informado, estos requieren una revisión y actualización en algunos procesos para asegurar que cumplan con los principios de la Ley 1581 de 2012, como la finalidad específica y la conservación adecuada de la información recolectada.
- **Conclusión:** Es necesario priorizar acciones para garantizar el cumplimiento normativo, incluyendo la publicación y actualización de las bases de datos personales en el portal de Datos Abiertos y la revisión de los procesos asociados al consentimiento informado, con el fin de evitar riesgos legales y asegurar la transparencia en la gestión de datos personales.

3. **Madurez de los procesos de seguridad:**

- **Resultado de la evaluación:** Los procesos relacionados con la seguridad de la información se encuentran en un nivel inicial de madurez. Esto incluye:
    - Falta de un marco formal para la gestión de riesgos de seguridad y privacidad.
    - Ausencia de un programa de capacitación y sensibilización en seguridad de la información para los funcionarios.
- **Conclusión:** Es fundamental estructurar procesos formales y establecer un plan de acción para avanzar hacia niveles intermedios y avanzados de madurez.

4. **Capacitación y sensibilización**

- **Resultado del análisis:** No se han realizado actividades de capacitación específicas en seguridad y privacidad de la información. Esto genera un bajo nivel de conciencia entre los funcionarios sobre los riesgos asociados al manejo de datos sensibles.
- **Acción requerida:** Diseñar e implementar un programa de capacitación continuo para fortalecer la cultura organizacional en torno a la seguridad y privacidad de la información.

5. **Adopción de buenas prácticas:**

- **Resultado del análisis:** Actualmente, el hospital ha comenzado a implementar algunas buenas prácticas en ciberseguridad, aunque estas se encuentran limitadas principalmente al datacenter. Los controles existentes incluyen:
    - Gestión de accesos y permisos.
    - Monitoreo de incidentes de seguridad: No se cuenta con un sistema de monitoreo continuo que permita detectar y responder de manera oportuna a incidentes de seguridad.
    - Políticas de contraseñas robustas: Aunque existen lineamientos básicos para la creación de contraseñas, no se han implementado políticas estrictas que incluyan requisitos avanzados, como autenticación multifactor o rotación periódica de contraseñas.
- **Conclusión:** Aunque se han adoptado algunos controles en el datacenter, es necesario extender estas buenas prácticas a toda la organización. Se recomienda adoptar un enfoque basado en estándares internacionales, como el NIST Cybersecurity Framework o la ISO/IEC 27001, para garantizar la protección integral de los datos y la continuidad de los servicios. Esto incluye fortalecer la gestión de accesos y permisos en todas las áreas, implementar un sistema de monitoreo continuo y establecer políticas de contraseñas más robustas.



## RECURSOS, MATERIALES, INSUMOS Y EQUIPOS

Para el desarrollo del plan de privacidad y seguridad de la información en el Hospital Regional de Sogamoso, se requieren diversos recursos materiales e insumos que aseguren la correcta implementación y funcionamiento del sistema.

- Infraestructura tecnológica: Equipos de cómputo, servidores, sistemas de almacenamiento y redes seguras que soporten la gestión de la información y la implementación de medidas de seguridad.
- Documentación y políticas: Manuales, guías, políticas y procedimientos que establezcan las directrices y normas a seguir en materia de seguridad y privacidad de la información.
- Sistemas de respaldo y recuperación: Soluciones de backup y recuperación de datos que permitan restaurar la información en caso de pérdida o ataque cibernético.
- Equipos de control de acceso: Dispositivos como lectores de tarjetas, biometría y sistemas de autenticación

multifactor para asegurar que solo el personal autorizado tenga acceso a la información y áreas críticas.
- Capacitación y formación: Programas y recursos educativos para sensibilizar y capacitar al personal en las mejores prácticas de seguridad y privacidad de la información.

**DESARROLLO DEL DOCUMENTO**

El Hospital Regional de Sogamoso E.S.E. ha diseñado un Plan de Seguridad y Privacidad de la Información (SPI) con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los datos, alineado con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y los estándares internacionales como la ISO/IEC 27001:2013. Este plan se enfoca en fortalecer los controles de seguridad y privacidad de la información, estableciendo acciones concretas para proteger los activos de información más críticos de la institución. El desarrollo del plan se estructura en cinco fases principales: diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua, las cuales se describen a continuación:

1. **Fase de Diagnóstico:**

En esta fase, se realizó una evaluación inicial del estado actual de la seguridad y privacidad de la información en el hospital, utilizando las siguientes metodologías:

- Entrevistas con responsables clave: Para identificar las prácticas actuales y las necesidades específicas de cada área.
- Auditorías internas: Para evaluar el cumplimiento de las políticas y normativas existentes.
- Análisis documental: Revisión de políticas, procedimientos y registros relacionados con la gestión de la información.

**Resultados del diagnóstico:**

- Se identificaron brechas significativas en la implementación de controles de seguridad fuera del datacenter.
- Los controles existentes en el datacenter están en un nivel intermedio de madurez, pero no se han extendido a otros sistemas críticos.
- Se evidenció la necesidad de actualizar políticas y procedimientos para alinearlos con los estándares internacionales y normativas nacionales.

2. **Fase de Planificación:**

Con base en los resultados del diagnóstico, se elaboró un Plan de Seguridad y Privacidad de la Información específico para el Hospital Regional de Sogamoso E.S.E., enfocado en abordar las brechas identificadas y fortalecer los controles de SPI. Este plan incluye los siguientes elementos clave:

- **Procesos críticos:** Priorización de procesos como la gestión de historias clínicas electrónicas, la administración de medicamentos y la atención al paciente.
- **Sistemas de información y servicios:** Identificación de los sistemas utilizados, como el sistema de gestión hospitalaria, servicios en la nube y bases de datos internas.
- **Infraestructura tecnológica:** Evaluación de servidores, redes, dispositivos médicos conectados y equipos de cómputo.
- **Terceros relacionados:** Análisis de riesgos asociados a proveedores, contratistas y otros terceros que interactúan con la información del hospital.
- **Ubicaciones físicas:** Consideración de las áreas donde se almacena o procesa información, como salas de servidores y oficinas administrativas.

El alcance del plan se define claramente para garantizar que las acciones de seguridad y privacidad se apliquen de

manera integral en toda la institución.

3. **Fase de Implementación:**

En esta fase, se ejecutan las acciones definidas en la planificación para fortalecer los controles de seguridad y privacidad de la información. Las actividades específicas incluyen:

1. Implementación de controles técnicos y administrativos:

- Configuración de firewalls, sistemas de detección de intrusos y herramientas de cifrado para proteger la información.
- Actualización y difusión de políticas internas de seguridad y privacidad.

2. Capacitación y sensibilización:

- Realización de talleres y capacitaciones dirigidas a colaboradores, contratistas y practicantes, con el objetivo de fomentar una cultura de seguridad y privacidad de la información.

3. Gestión de terceros:

- Establecimiento de acuerdos de confidencialidad y cláusulas de seguridad en los contratos con proveedores y terceros relacionados.

4. Monitoreo y control:

- Implementación de herramientas de monitoreo continuo para detectar y responder a incidentes de seguridad en tiempo real.
    - Implementación de controles técnicos y administrativos:
        - Configuración de firewalls, sistemas de detección de intrusos y herramientas de cifrado para proteger la información.
        - Actualización de políticas internas de seguridad y privacidad, asegurando su difusión entre los colaboradores.
- Capacitación y sensibilización:
    - Realización de talleres y capacitaciones dirigidas a los colaboradores, contratistas y practicantes, con el objetivo de fomentar una cultura de seguridad y privacidad de la información.
- Gestión de terceros:
    - Establecimiento de acuerdos de confidencialidad y cláusulas de seguridad en los contratos con proveedores y terceros relacionados.
- Monitoreo y control:
    - Implementación de herramientas de monitoreo continuo para detectar y responder a incidentes de seguridad en tiempo real.

4. **Fase de Evaluación de Desempeño:**

El seguimiento y monitoreo del Modelo de Seguridad y Privacidad de la Información (MSPI) se realiza mediante la evaluación de indicadores clave de desempeño (KPIs), que permiten medir la efectividad de las acciones implementadas. Los indicadores clave incluyen:

- Tasa de incidentes de seguridad: Número de incidentes detectados y gestionados en un período determinado.

- Nivel de cumplimiento normativo: Porcentaje de cumplimiento con la legislación vigente y estándares internacionales.
- Tiempo de respuesta ante incidentes: Tiempo promedio para detectar, contener y resolver incidentes de seguridad.
- Nivel de madurez de los controles: Progreso en la implementación y efectividad de los controles de seguridad.

Además, se realizarán auditorías internas periódicas para evaluar el desempeño del sistema y garantizar que las acciones implementadas estén alineadas con los objetivos del hospital.

5. **Líneas de Estrategias del Plan e Indicadores.**

El objetivo de esta sección es establecer estrategias claras para fortalecer la Seguridad y Privacidad de la Información (SPI) en el Hospital Regional de Sogamoso E.S.E., alineadas con los objetivos estratégicos institucionales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Además, se definen indicadores clave de desempeño (KPIs) que permitan medir el impacto y la efectividad de estas estrategias.

**Línea estratégica 1: Acceso y uso de la información**

- **Acceso restringido**: Solo personal autorizado puede acceder a archivos de gestión, centrales e históricos, así como a las historias clínicas, bajo condiciones específicas.
- **Uso adecuado**: Sistemas de información destinados exclusivamente para asuntos del hospital; uso personal prohibido.
- **Protección de historias clínicas**: Se prohíbe modificar la información diligenciada y el uso de comandos de copiar y pegar.

**Línea estratégica 2: Administración de contraseñas**

- **Seguridad de contraseñas**: Contraseñas de uso personal, no deben ser reveladas ni escritas. Reportar cualquier uso no autorizado.
- **Gestión de cuentas**: Controles para identificar responsables de la creación y modificaciones de cuentas.
- **Estándares de contraseñas**: Contraseñas deben cumplir con requisitos de complejidad según la criticidad de la información.

**Línea estratégica 3: Uso de cuentas para acceso a recursos tecnológicos**

- **Roles y funciones**: Definición clara para reducir usos no autorizados. Revisión semestral por el líder de gestión de recursos informáticos.

**Línea estratégica 4: Acceso a la red por terceros**

- **Uso exclusivo de equipos hospitalarios**: Acceso a la red solo para equipos autorizados.
- **Control de acceso**: Acceso a información solo con autorización formal y análisis previo. Trazabilidad de acciones garantizada.

**Línea estratégica 5: Seguridad y confidencialidad**

- **Integridad de archivos**: Verificación de condiciones físicas y técnicas de archivos clínicos.

- **Uso profesional del correo electrónico**: Precaución con destinatarios colectivos y cumplimiento de leyes de derechos de autor.
- **Notificación de riesgos**: Informar cualquier evento que comprometa la confidencialidad y seguridad de la información.
- **Aceptación de reglamentación**: Usuarios deben aceptar formalmente las políticas de acceso y tratamiento de información.
- **Control de acceso de terceros**: Restricciones para acceso de terceros hasta que se implementen controles apropiados y se firmen acuerdos.
- **Documentación formal**: Manuales y procedimientos para proteger la información compartida con terceros

**Línea estratégica 6: Gestión de medios removibles**

- **Restricción de conexión no autorizada**: Prohibición del uso de dispositivos personales no institucionales sin autorización.
- **Protección física y control**: Los medios removibles que contienen información institucional deben ser controlados y físicamente protegidos.
- **Identificación y autorización**: Cada medio removible debe estar identificado según su contenido y el tránsito de estos medios debe ser autorizado.

**Línea estratégica 7: Conservación y prevención del deterioro de la información**

- **Sistema Integrado de Conservación**: Incluye actividades como diagnóstico integral, prevención de desastres y control ambiental.
- **Copias de seguridad**: Realización de copias de seguridad diarias, semanales y mensuales.
- **Protección de información crítica**: Medidas como bloqueo de equipos y uso de contraseñas.
- **Precauciones con documentos**: No reutilizar papel sensible y retirar documentos impresos inmediatamente.

**Línea estratégica 8: Control documental (físico – digital)**

- **Confidencialidad en gestión documental**: Responsabilidad de mantener la confidencialidad y seguridad de documentos físicos y digitales.
- **Organización de archivos digitales**: Uso de estructuras de nombres para garantizar la organización.
- **Procedimientos operativos**: Instrucciones para manejo de errores y recuperación de sistemas.

**Línea estratégica 9: Control de cambios operativos**

- **Justificación y documentación de cambios**: Todos los cambios a la infraestructura deben ser justificados, documentados y sometidos a pruebas.
- **Análisis de riesgos**: Evaluación de riesgos de implementación y no implementación de cambios.

**Línea estratégica 10: Manejo de la información financiera**

- **Bloqueo automático de equipos**: Control del tiempo de inactividad.
- **Limitación de privilegios de usuario**: Reducir riesgos asociados con la instalación de software no autorizado.
- **Medidas de seguridad adicionales**: Restricciones en el uso de software no necesario, ejecución de archivos y acceso remoto.
- **Mantenimiento y actualización**: Solo personal autorizado puede realizar estas tareas.
- **Navegador único y actualizado**: Uso de un navegador configurado para máxima seguridad en transacciones financieras
- **Redes inalámbricas seguras**: Aislamiento de redes WIFI para invitados.
- **Autenticación y control**: Uso de perfiles de autorización y notificaciones en línea para transacciones

**Acciones específicas:**

| Actividades | Resultado / Soporte | Responsable | Fecha |
|---|---|---|---|
| Asegurar la interfaz entre el sistema de informacion hospitalario y los proveedores externos de Laboratorio Clínico Y De imágenes Diagnosticas RX | Documento de validación de la interfaz entre sistemas de informacion hospitalario y los proveedores externos, incluyendo pruebas realizadas. | Referente de seguridad perimetral | 31/09/2025 |
| Implementar herramientas avanzadas de monitoreo y detección de amenazas en los sistemas de información. | Registro de implementación de herramientas (facturas, contratos e informes técnicos de configuración). | Referente de seguridad perimetral | 30/06/2025<br>31/12/2025 |
| Planificar, diseñar e implementar el modelo de seguridad y privacidad de la información **(DIAGNOSTICO)** | Documento con el resultado del **diagnóstico** realizado por la entidad con la clasificación y distinción de los activos de información teniendo en cuenta la información con datos personales y aquellos que no lo son identificando la criticidad de la información clasificada o reservada. | Referente de seguridad perimetral | 31/03/2025 |
| Diseñar e implementar campañas de sensibilización dirigidas a los colaboradores, contratistas y practicantes sobre temas como el manejo de datos sensibles, ciberseguridad y protección de datos personales. | Plan de capacitaciones realizado y registro de participantes por actividad. | ingeniero apoyo TI, Referente de seguridad perimetral | 30/06/2025 |
| Realizar talleres prácticos sobre buenas prácticas en ciberseguridad y manejo de datos sensibles. | Agenda de talleres realizada, lista de asistencia y evaluación post-taller. | ingeniero apoyo TI, Referente de seguridad perimetral | 30/09/2025 |
| Optimizar el rendimiento de los sistemas tecnológicos para asegurar su funcionamiento continuo. | Informe técnico de optimización con métricas de rendimiento antes y después de la intervención. | Referente de seguridad perimetral | 30/06/2025<br>31/12/2025 |

| | | | |
|---|---|---|---|
| Renovación antivirus Hospital Regional De Sogamoso E.S.E | Estudio previo y Contrato. | Líder De Gestión De La Información | 31/07/2025 |

6. **Plan de Seguimiento.**

El seguimiento del Plan de Seguridad y Privacidad de la Información del Hospital Regional de Sogamoso E.S.E. se realizará de manera semestral, permitiendo un monitoreo constante de las acciones implementadas y la actualización del plan según las necesidades detectadas. Este proceso tiene como objetivo garantizar la efectividad del plan y su alineación con los objetivos estratégicos de la institución.

**Metodología de seguimiento:**

- **Indicadores clave de desempeño (KPIs):** Se medirán aspectos como el porcentaje de cumplimiento de las acciones planificadas, la tasa de incidentes gestionados, el tiempo promedio de respuesta ante incidentes y el nivel de cumplimiento normativo.
- **Revisión semestral:** Cada seis meses, se analizarán los resultados obtenidos, evaluando el desempeño de los controles y detectando áreas de mejora.
- **Auditorías internas:** Se realizarán auditorías periódicas para verificar la implementación de las acciones y el cumplimiento de las políticas de seguridad y privacidad.
    - **Informes de seguimiento:** Los resultados del seguimiento se documentarán en informes semestrales, que incluirán recomendaciones específicas para ajustar el plan según las necesidades detectadas.

**Responsables:**

El equipo de gestión de la información liderará el seguimiento, en coordinación con las áreas responsables de los procesos críticos.

7. **Ámbito de Aplicación.**

La Política de Seguridad de la Información del Hospital Regional de Sogamoso E.S.E. se encuentra actualmente en proceso de desarrollo y será formalizada mediante una resolución institucional. Esta política será de aplicación en toda la institución, abarcando a todos los colaboradores, contratistas y practicantes que tengan acceso a la información, así como los procesos, sistemas y recursos tecnológicos relacionados con la gestión de la información. El alcance de la política incluye el uso y manejo responsable de documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación institucionales, garantizando la protección y privacidad de la información en todos los niveles operativos del hospital.

- **Protección de datos**: Garantizar la confidencialidad, integridad y disponibilidad de la información, siguiendo las directrices del Modelo de Seguridad y Privacidad de la Información del MINTIC.
- **Uso adecuado de recursos tecnológicos**: Asegurar que todos los dispositivos y plataformas tecnológicas sean utilizados de manera segura, implementando controles de acceso y medidas de protección contra amenazas internas y externas.
- **Capacitación y concienciación:** Proveer formación continua a todos los colaboradores, contratistas y practicantes sobre prácticas seguras para el manejo de la información, promoviendo una cultura de seguridad y privacidad.
- **Monitoreo y auditoría:** Implementar mecanismos de monitoreo y auditoría continua para identificar, evaluar y mitigar riesgos de seguridad y privacidad de la información de manera proactiva.
- **Gestión de incidentes:** Establecer procedimientos claros para la gestión de incidentes de seguridad, incluyendo la detección, notificación, y respuesta efectiva a cualquier amenaza o violación de la seguridad de la información.
- **Cumplimiento normativo:** Asegurar el cumplimiento de todas las normativas y regulaciones aplicables en materia de seguridad y privacidad de la información, manteniéndose actualizados con

los cambios legislativos y mejores prácticas internacionales.

**BIBLIOGRAFÍA**


- Plan de Seguridad y Privacidad de la Información - Función Pública. Este documento proporciona una guía detallada sobre cómo implementar medidas de seguridad y privacidad en una entidad pública1.
- Plan de Seguridad y Privacidad de la Información 2023-2026 - Dirección Nacional de Inteligencia (DNI). Este plan incluye estrategias y lineamientos para la seguridad digital y la gestión de riesgos2.
- Plan de Seguridad y Privacidad de la Información - Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Este documento ofrece un enfoque integral para la seguridad y privacidad de la información, alineado con normas internacionales como la NTC-ISO 270013.1