TABLA DE CONTENIDO

PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OBJETIVO

Fortalecer la gestión institucional del Hospital Raúl Orejuela Bueno E.S.E. en materia de seguridad y privacidad de la información, mediante la implementación progresiva de un Sistema de Gestión de Seguridad de la Información (SGSI), que permita proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información, garantizando el cumplimiento normativo y considerando las capacidades técnicas, humanas y presupuestales de la entidad.

OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a ejecutar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

ALCANCE

El Plan Estratégico de seguridad y privacidad de la Información al buscar la implementación del Sistema de Gestión de Seguridad y privacidad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

El presente Plan Estratégico de Seguridad y Privacidad de la Información aplica a todos los procesos, áreas y dependencias del Hospital Raúl Orejuela Bueno E.S.E., incluyendo su Sede Principal y las más de 36 sedes y puntos de atención en el municipio de Palmira.

La estrategia se aplicará progresivamente, dando prioridad a la sede principal y a los procesos críticos relacionados con la atención en salud, la gestión administrativa y la información clínica. Las acciones contempladas en el PESI estarán condicionadas a la disponibilidad presupuestal, técnica y operativa, razón por la cual su implementación se planificará por fases de acuerdo con la capacidad institucional.

DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 de 2018, "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Resolución 00500 de 2021 – Ministerio TIC Por la cual se establecen los lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en las entidades públicas.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC Particularmente el Título 9 de la Parte 1 del Libro 2, sobre Gobierno Digital.
- Ley 1581 de 2012 – Protección de datos personales Establece el régimen general de hábeas data.
- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública
- Ley 1273 de 2009 – Delitos Informáticos Modifica el Código Penal en materia de protección de la información y los datos.
- Ley 87 de 1993 – Sistema de Control Interno Aplica para el monitoreo de cumplimiento de políticas institucionales.

ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Vigencia 2025 (basado en FURAG)

1. Gobernanza y responsabilidad

- Se cuenta con un responsable de seguridad digital, aunque vinculado como contratista.
- **Riesgo:** Falta de continuidad del rol y ausencia de institucionalización.

  Acción sugerida: Incluir formalmente el cargo dentro del manual de funciones o planta de personal.

Gestión de riesgos y continuidad

- Hay una política de respaldo y un plan de continuidad del negocio (PCN).
- No se realizaron análisis de vulnerabilidades durante el último año.
- Riesgos en infraestructura en la nube **no han sido gestionados**.

  Acciones sugeridas:

  - Programar y documentar análisis de vulnerabilidades (2026).
  - Actualizar el plan de tratamiento de riesgos (incluyendo servicios cloud).
  - Documentar y validar pruebas de continuidad y recuperación.

Infraestructura y herramientas de protección

- Se cuenta con antivirus y firewall activos.
- Se implementan políticas básicas de respaldo.
- El presupuesto TIC asignado a seguridad es **apenas del 0.07%**, lo cual es insuficiente.

  Acción sugerida: Justificar aumento progresivo del presupuesto TIC con base en necesidades de renovación, monitoreo y detección.

Gestión de incidentes

- No hay un procedimiento formal para gestión y reporte de incidentes.
- Se reconocen mecanismos técnicos básicos de protección.

  Acción sugerida: Construir un procedimiento documentado de respuesta a incidentes, socializarlo y probarlo anualmente.

Protección de datos personales

- Se indica cumplimiento parcial de la Ley 1581 de 2012.
- El Sistema de Información R-Fast contiene datos sensibles sin un procedimiento institucional completo.

Acción sugerida: Construir o actualizar el manual de protección de datos personales y el registro de actividades de tratamiento (RAT).

Cumplimiento normativo

- La entidad cumple con buenas prácticas de autenticación (DMARC, SPF, DKIM).
- No se evidencia cumplimiento integral de la Circular 01 de 2018 ni reporte a COLCERT.

Acción sugerida: Elaborar un cronograma de cumplimiento normativo y evidencias ante MinTIC/Supersalud.

Diagnóstico global (semáforo por componente)

Componente	Nivel actual	Observación clave
Gobernanza de seguridad digital	Medio	Falta institucionalización
Gestión de riesgos y continuidad	Bajo	No hay análisis ni seguimiento
Infraestructura y herramientas	Medio	Hay herramientas aunque desactualizadas, pero sin planeación
Gestión de incidentes (ciberseguridad)	Bajo	No hay procedimiento formal
Protección de datos personales	Bajo	No hay política robusta institucional
Cumplimiento normativo sectorial	Medio	Parcial, pero con avances técnicos

ESTRATEGIA DE SEGURIDAD DIGITAL

LA ENTIDAD establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad y privacidad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse y debidamente articularse al habilitador de seguridad y privacidad de la Política de Gobierno Digital. (*Ver Resolución 500 de 2021*).

Por tal motivo, ***EL HOSPITAL RAÚL OREJUELA BUENO E.S.E.,*** define las siguientes 5 estrategias específicas, adoptando los lineamientos de MINTIC, la resolución 500 de 2021 y del Anexo 1, que contiene la actualización del Modelo de Seguridad y Privacidad de la Información, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

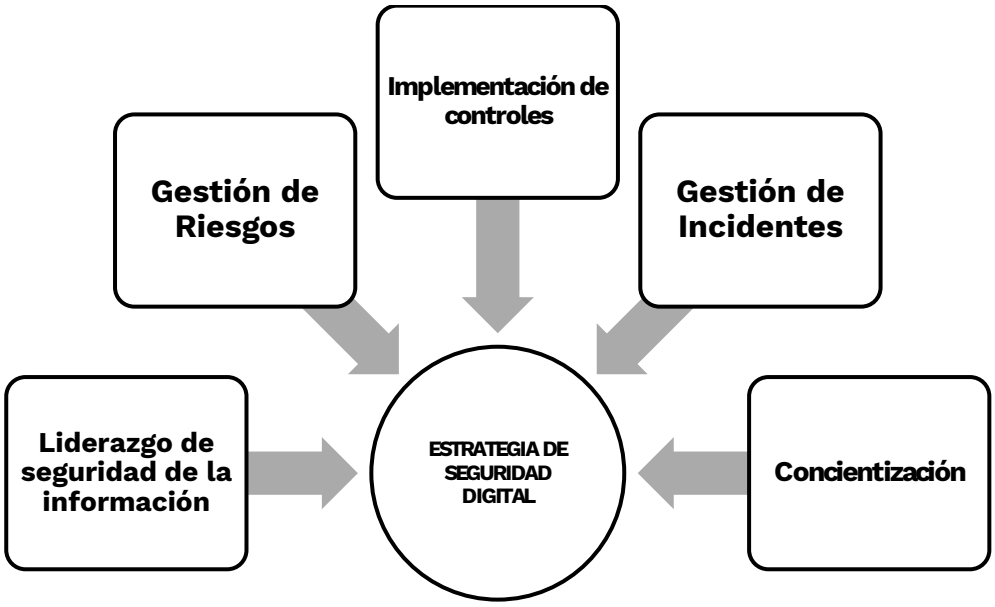

Ilustración 1 Estrategia de seguridad digital.

DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad y privacidad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo y apropiando al interior de la entidad las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, **EL HOSPITAL RAÚL OREJUELA BUENO E.S.E.** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). Los proyectos deben estar relacionados tanto con el Manual de políticas como con la política de seguridad definida en la entidad, además estos proyectos deben corresponder a la implementación de controles que permita mitigar riesgos de seguridad de la información que la entidad haya identificado

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	PROYECTO 1: Desarrollar e implementar una política de seguridad PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Política de Seguridad Formalizada e Implementada. Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de riesgos	PROYECTO 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad PROYECTO 4: Implementar manual de políticas de seguridad de la información.	Matriz de riesgos de seguridad digital Definir planes de tratamiento de riesgos Definir el manual base de políticas de la entidad y un plan de socialización efectivo.
Concientización	PROYECTO 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. PROYECTO 2: Realizar jornadas de sensibilización a todo el personal. PROYECTO 3: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas. PROYECTO 4: Medir el grado de sensibilización a toda la Entidad.	1 plan de cambio, cultura y apropiación que describa las estrategias que se implementarán en la vigencia. 2. Evidencias de las actividades desarrolladas 3. Certificaciones de cursos 4. Resultado de las encuestas de medición

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Implementación de controles	CONTROL 1 Política de respaldos de información. CONTROL 2 Procedimiento de Gestión de Cambios. CONTROL 3 Clasificación de la información. CONTROL 4 Políticas de Desarrollo Seguro CONTROL 5 Implementación de solución WAF *CONTROL 6:* Política de seguridad física y del entorno CONTROL 7: Política de escritorio limpio	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información. Políticas de Desarrollo Seguro WAF desplegado y funcional. Política de seguridad física y del entorno implementada. Socializada Seguimiento a usuarios con equipos institucionales para validar aplicación de política de escritorio limpio.
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. **PROYECTO 2:** Capacitar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.

CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

	AÑO 2026						AÑO 2027			
	TRIMESTRE 1	**TRIMESTRE 2**	**TRIMESTRE 3**	**TRIMESTRE 4**	**RESPONSABLE**	**FECHA**	**TRIMESTRE 1**	**TRIMESTRE 2**	**RESPONSABLE**	**FECHA**
ACTIVIDADES	**Realizar diagnóstico seguridad y privacidad**		Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	Capacitar al personal en la gestión de incidentes de seguridad de la información.	TIC		Actualización Diagnóstico de Seguridad	Desarrollo Sensibilización 2026	TIC	
	Identificación de activos procesos	Implementación de solución WAF		Gestión de Riesgos de Seguridad	TIC		Adquisición soluciones IPS y actualización de		TIC	

	misionales					infraestructura requerida			
	Desarrollo Plan de Sensibilización 2026	Adquisición e implementación Sistema de Análisis de Vulnerabilidades	Seguimiento de controles implementado Adopción protocolo IPV6	TIC		Actualizar plan de seguridad y plan de tratamiento de riesgos de seguridad con nuevo cronograma	Implementación Estrategias de Capacitación en Seguridad	TIC	
		Socialización e implementación de controles y políticas estipuladas en el manual de la entidad							

Nota: Al finalizar cada vigencia, LA ENTIDAD, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

ANÁLISIS PRESUPUESTAL:

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes:

AÑO 2026		AÑO 2027		AÑO 2028	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**
Construir los lineamientos técnicos e implementación de controles que se definan en el plan operacional de seguridad y privacidad de la información.		Implementar el 100% del Modelo de Seguridad y Privacidad de la Información y gestionar la auditoría interna de cumplimiento.		Mantener el funcionamiento del Modelo de seguridad y privacidad de la Información	
Implementación de solución WAF		Adquisición y despliegue de soluciones de IPS		Adquisición Servicio Ethical Hacking	
Adquisición Sistema de Análisis de Vulnerabilidades		Renovación WAF y Sistema de Análisis de Vulnerabilidades		Renovación WAF, IPS y Análisis de Vulnerabilidades	
Adopción protocolo IPV6					
TOTAL PRESUPUESTO AÑO 2026		**TOTAL PRESUPUESTO AÑO 2027**		**TOTAL PRESUPUESTO AÑO 2028**	

RESPONSABLES

1. Representante Legal de la Entidad: Aprobar los documentos de Alto Nivel
2. Junta directiva: Aprobar documentos estratégicos y disposiciones presupuestales previa revisión y aprobación del representante legal.
3. Jefe de la oficina de TI (Oficial de Seguridad Digital): Coordinar las actividades de implementación del MSPI
4. Líderes de proceso: Responsables de aplicar y vigilar el cumplimiento de las políticas en su área. También son responsables de liderar políticas al interior del SGSI.
5. Equipo TIC: Implementa controles tecnológicos.
6. Control interno: Incluye seguridad en auditorías.
7. Contratación: Aplica medidas de seguridad en relaciones con terceros.
8. Talento Humano: Sensibiliza y forma en SGSI.
9. Todos los funcionarios y colaboradores: Cumplen con las políticas y apoyan su implementación.

No. Versión	Fecha Revisión / Actualización	Pagina	Solicitante	Cambios y/o modificaciones realizadas
01	Enero 2019	Todo	Octavio Enrique Murillas Peña	Emisión del Documento
02	Enero 2020	Todo	Octavio Enrique Murillas Peña	Actualización logo símbolos ICONTEC
03	Enero 2021	Todo	Luisa Fernanda Arismendi Muñoz	Revisión y modificación
04	Enero de 2022	Todo	Luisa Fernanda Arismendi Muñoz	Se actualiza plantilla de planes de proceso. • Se actualiza nuevo esquema de codificación de documentos. PL3-TIC • Se actualiza por completo la información del plan
05	Enero de 2023	Todo	Dora Isaura López Serna	Se revisa todo el documento y no requiere actualización, lo cual continua con la misma versión 04.
06	Enero de 2024	Todo	Dora Isaura López Serna	Se revisa todo el documento y no requiere actualización, lo cual continua con la misma versión 04.

07	Enero de 2025	Todo	Octavio E. Murillas Peña	Se revisa todo el documento; se revisa la planeación estratégica y se actualiza el plan de desarrollo.
08	Enero 2026	Todo	Octavio E. Murillas Peña	Se revisa y actualiza todo el documento

	NOMBRE	***CARGO***	***FIRMA***
ELABORÓ	Octavio E. Murillas Peña	Líder de Programa (Tecnologías y Técnicas de la Información)	Ver Formato FR35-GCA Aprobación de la Información Documentada
REVISÓ	Victoria Eugenia Betancourt	Jefe Oficina Asesora de Planeación	Ver Formato FR35-GCA Aprobación de la Información Documentada
	Alexander Trujillo	Subgerente administrativo	Ver Formato FR35-GCA Aprobación de la Información Documentada
	Isabel Cristina Torres	Jefe de Calidad	Ver Formato FR35-GCA Aprobación de la Información Documentada
APROBÓ	Clara Inés Sánchez Perafán	Gerente	Ver Formato FR35-GCA Aprobación de la Información Documentada