E.S.E. HOSPITAL EDUARDO ARREDONDO DAZA

ESTRUCTURACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

VIGENCIA 2025 - 2028

TABLA DE CONTENIDO.

TABLA DE CONTENIDO. 2

LISTADO DE FIGURAS. 4

LISTADO DE TABLAS. 4

INTRODUCCIÓN. 6

JUSTIFICACIÓN. 7

OBJETIVOS. 8

OBJETIVOS ESPECÍFICOS. 8

MARCO NORMATIVO. 9

FASE 1 – PLANEACIÓN. 10

1. MARCO ESTRATÉGICO. 11

1.1 ALINEACIÓN CON EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI) DEL HOSPITAL EDUARDO ARREDONDO DAZA. 11

1.2 RELACIÓN CON LA POLÍTICA DE GOBIERNO DIGITAL. 12

1.3 RELACIÓN CON MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG). 12

1.4 RELACIÓN CON EL SISTEMA INSTITUCIONAL DE GESTIÓN. 12

2. CONTEXTO ORGANIZACIONAL. 14

2.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 14

2.2 CONTEXTO INTERNO. 14

2.3 CONTEXTO EXTERNO. 15

2.4 PARTES INTERESADAS. 15

2.5 FACTORES INTERNOS Y EXTERNOS. 16

2.6 ALCANCE DEL MSPI. 17

3. GOBIERNO DEL MSPI DEL HEAD. 18

3.1 GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN. 18

3.2 ROLES Y RESPONSABILIDADES. 19

3.3 COMITÉ INSTITUCIONAL DEL MSPI. 20

3.3.1 Funciones: 20

3.3.2 Integrantes sugeridos: 20

3.3.3 Reuniones: 20

3.4 POLÍTICAS DEL COMITÉ INSTITUCIONALDEL MSPI. 20
3.4.1 Principios de las políticas del MSPI: 21
4. LÍNEA BASE PARA IMPLEMENTACIÓN DEL MSPI. 22
4.1 EVALUACIÓN INICIAL DEL MSPI. 22
5. PLANIFICACIÓN DEL MSPI DEL HEAD. 23
5.1 EVALUACIÓN INICIAL DEL MSPI. 23
5.2 GESTIÓN DE ACTIVOS DE INFORMACIÓN. 23
5.3 CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS. 24
5.3.1 Clasificación: 24
5.3.2 Valoración: 24
5.3.3 Criticidad: 24
6. GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN. 26
6.1 METODOLOGÍA DE VALORACIÓN DEL RIESGO. 26
6.2 MATRIZ INSTITUCIONAL DE RIESGOS. 26
6.3 EVALUACIÓN Y ACEPTACIÓN DE LOS RIESGOS. 27
6.4 RESULTADO DEL ANÁLISIS DE RIESGOS. 28
FASE 2 – EJECUCIÓN. 30
7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI). 31
7.1 GENERALIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI). 31
7.2 DEFINICIÓN DE LOS CRITERIOS DE PRIORIZACIÓN. 32
7.3 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PTRSPI). 33
7.4 PLAN DE ACCIÓN DEL PTRSPI. 34
FASE 3 – VERIFICAR. 37
8. SEGUIMIENTO, EVALUACIÓN Y DESEMPEÑO DEL MSPI. 38
8.1 SEGUIMIENTO A LA EJECUCIÓN DEL PTRSPI. 38
8.2 MEDICIÓN DEL DESEMPEÑO DEL MSPI (INDICADORES). 40
8.2.1 Indicadores de desempeño del MSPI: 40
8.3 MONITOREO DE LOS CONTROLES DE SEGURIDAD. 41
8.4 GESTIÓN Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. 43
8.5 AUDITORÍAS Y EVALUACIONES DEL MSPI. 43

8.6 EVALUACIÓN DE LA EFICACIA DE LOS CONTROLES. 44
FASE 4 – ACTUAR. 46
9. SEGUIMIENTO, EVALUACIÓN Y DESEMPEÑO DEL MSPI. 47
9.1 ACCIONES CORRECTIVAS. 47
9.2 ACCIONES PREVENTIVAS. 48
9.3 PLAN DE MEJORAMIENTO DEL MSPI. 48
9.4 MEJORA CONTÍNUA DEL MSPI. 49
9.5 REVISIÓN POR LA ALTA DIRECCIÓN. 49
10. ARTICULACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) CON EL PLAN DE TRANSICIÓN DE IPv4 A IPv6. 52
10.1 RELACIÓN DEL MSPI CON EL PLAN DE TRANSICIÓN DE IPV4 A IPV6. 53
10.2 LINEAMIENTOS GENERALES PARA UNA TRANSICIÓN SEGURA HACIA IPV6. 53
10.3 ESTADO ACTUAL DE LA TRANSICIÓN IPV4 - IPV6 EN LA ESE HOSPITAL EDUARDO ARREDONDO DAZA. 54
10.4 CONSIDERACIONES FINALES. 55
ANEXO 1. 56
ANEXO 2. 57

LISTADO DE FIGURAS.

Ilustración 1. MSPI y políticas existentes. 11
Ilustración 2. Contexto interno. 14
Ilustración 3. Contexto externo. 15
Ilustración 4. Partes interesadas. 16
Ilustración 5. Modelo de gobierno del MSPI. 18

LISTADO DE TABLAS.

Tabla 1. Marco Normativo del MSPI. 9
Tabla 2. Factores internos y externos que afectan el MSPI. 17
Tabla 3. Roles y responsabilidades del MSPI. 19
Tabla 4. Evaluación inicial del MSPI del HEAD. 22
Tabla 5. Criterios de clasificación de activos. 24

Tabla 6. Criterios de valoración de activos. 24
Tabla 7. Criterios de evaluación de los riesgos. 27
Tabla 8. Resumen de resultados. 28
Tabla 9. Análisis de probabilidad e impacto. 28
Tabla 10. Principales amenazas identificadas. 28
Tabla 11. Generalidades PSPI. 32
Tabla 12. Tabla de lineamientos del PTRSPI. 34
Tabla 13. Plan de acción PTRSPI. 36
Tabla 14. Matriz de seguimiento del PTRSPI. 39
Tabla 15. Indicadores del MSPI. 41
Tabla 16. Monitoreo de los controles. 42
Tabla 17. Criterios de evaluación. 42
Tabla 18. Modelo de registro y seguimiento de incidentes. 43
Tabla 19. Indicadores de gestion. 43
Tabla 20. Auditorías y evaluaciones. 44
Tabla 21. Registro de hallazgos. 44
Tabla 22. Ejemplo de matriz de evaluación de eficacia de los controles. 45
Tabla 23. Modelo de control de acciones correctivas. 47
Tabla 24. Modelo de control de acciones preventivas. 48
Tabla 25. Modelo para plan de mejoramiento. 49
Tabla 26. Relación MSPI y migración a IPv6. 53
Tabla 27. Diagnóstico de la migración IPv4 a IPv6 en el HEAD. 55

INTRODUCCIÓN.

La E.S.E. Hospital Eduardo Arredondo Daza reconoce que la información constituye uno de sus activos estratégicos más importantes para garantizar la prestación continua, segura y eficiente de los servicios de salud. La creciente dependencia de las tecnologías de la información, los sistemas clínicos, las plataformas administrativas y los servicios digitales hace necesario establecer un modelo integral que permita proteger la información institucional frente a amenazas internas y externas, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

En cumplimiento de la Política de Gobierno Digital, del Modelo de Seguridad y Privacidad de la Información (MSPI) expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y de la normatividad vigente en materia de seguridad digital y protección de datos personales, la E.S.E. Hospital Eduardo Arredondo Daza adopta el presente Modelo de Seguridad y Privacidad de la Información como instrumento institucional para fortalecer la gestión de los riesgos de seguridad de la información y consolidar una cultura organizacional orientada a la protección de sus activos de información.

El Modelo se encuentra articulado con el Plan Estratégico de Tecnologías de la Información (PETI) 2025–2028, el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno y las demás políticas institucionales relacionadas con la gestión documental, la protección de datos personales, la continuidad del negocio y la administración de riesgos, permitiendo una gestión integral de la seguridad y privacidad de la información.

Con el fin de facilitar la implementación, el seguimiento y la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), su estructura se organiza bajo el ciclo Planear, Hacer, Verificar y Actuar (PHVA). Este enfoque permite desarrollar el modelo de manera ordenada, iniciando con la planeación de las estrategias y la gestión de riesgos, continuando con la implementación de los controles y planes definidos, evaluando periódicamente su desempeño mediante mecanismos de seguimiento y, finalmente, promoviendo acciones de mejora que aseguren la actualización y fortalecimiento permanente de la seguridad y privacidad de la información en la E.S.E. Hospital Eduardo Arredondo Daza.

JUSTIFICACIÓN.

La transformación digital en el sector salud ha incrementado significativamente la dependencia de las tecnologías de la información para soportar los procesos asistenciales, administrativos, financieros y de apoyo de las instituciones prestadoras de servicios de salud. En este contexto, la información se consolida como uno de los activos más valiosos de la E.S.E. Hospital Eduardo Arredondo Daza, al contener datos clínicos, administrativos, financieros, epidemiológicos y personales cuya protección resulta indispensable para garantizar la continuidad de la prestación de los servicios de salud, el cumplimiento de la normatividad vigente y la confianza de los ciudadanos.

El aumento de amenazas cibernéticas, la evolución de los mecanismos de fraude digital, la exposición permanente de los sistemas de información y la creciente utilización de plataformas tecnológicas obligan a las entidades públicas a fortalecer sus capacidades para prevenir, detectar, responder y recuperar sus servicios frente a incidentes que puedan afectar la seguridad y privacidad de la información.

En este sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido el Modelo de Seguridad y Privacidad de la Información (MSPI) como el marco de referencia para que las entidades públicas implementen un Sistema de Gestión de Seguridad de la Información basado en la gestión integral del riesgo y en la mejora continua. La E.S.E. Hospital Eduardo Arredondo Daza adopta el presente Modelo de Seguridad y Privacidad de la Información como instrumento estratégico para fortalecer la gobernanza de la seguridad digital, proteger sus activos de información y apoyar el cumplimiento de los objetivos institucionales definidos en el Plan Estratégico de Tecnologías de la Información (PETI), promoviendo una gestión responsable de la información durante todo su ciclo de vida.

OBJETIVOS.

Desarrollar el Modelo de Seguridad y Privacidad de la Información (MSPI) para la E.S.E. Hospital Eduardo Arredondo Daza como un instrumento de gestión que permita proteger la información institucional, gestionar los riesgos asociados a su uso y fortalecer las capacidades de la entidad para preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. Todo ello en armonía con el PETI institucional, la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG), la normatividad vigente y las buenas prácticas en seguridad de la información.

OBJETIVOS ESPECÍFICOS.

• Definir el marco de gestión del MSPI, estableciendo las políticas, lineamientos, roles y responsabilidades que orienten la administración de la seguridad y privacidad de la información dentro de la entidad.

• Identificar y valorar los activos de información para conocer su importancia dentro de los procesos institucionales y determinar las medidas de protección que requiere cada uno de ellos.

• Analizar los riesgos que puedan afectar la información institucional, con el propósito de priorizar acciones que reduzcan su impacto sobre la prestación de los servicios de salud.

• Diseñar las estrategias y controles necesarios para proteger la infraestructura tecnológica, los sistemas de información, las bases de datos y los demás activos críticos que soportan la operación del Hospital.

• Incorporar mecanismos que permitan proteger los datos personales y la información sensible, promoviendo el cumplimiento de la legislación vigente y el respeto por la privacidad de pacientes, funcionarios y demás grupos de interés.

• Formular el Plan de Seguridad y Privacidad de la Información (PSPI) y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) como herramientas que orienten la ejecución de las acciones de mejora definidas para el fortalecimiento del modelo.

MARCO NORMATIVO.

El presente marco normativo constituye el referente para la formulación, implementación, seguimiento y mejora continua del MSPI de la E.S.E. Hospital Eduardo Arredondo Daza. Su aplicación garantiza que las políticas, procedimientos, controles y planes definidos en este documento se encuentren alineados con la legislación colombiana, la Política de Gobierno Digital, MIPG y las buenas prácticas internacionales en seguridad de la información, contribuyendo a una gestión segura, transparente y confiable de la información institucional.

Norma	Descripción	Relación con el MSPI
Constitución Política de Colombia (1991)	Artículos 15, 20, 74 y 209.	Establece el derecho a la intimidad, el habeas data, el acceso a la información pública y los principios de la función administrativa.
Ley 527 de 1999	Define el marco jurídico de los mensajes de datos, el comercio electrónico y las firmas digitales.	Soporta la autenticidad e integridad de la información electrónica institucional.
Ley 594 de 2000	Ley General de Archivos.	Regula la administración, conservación y disposición de los documentos y archivos institucionales.
Ley 1266 de 2008	Régimen de habeas data financiero.	Complementa la protección de la información personal y el tratamiento de datos.
Ley 1273 de 2009	Modifica el Código Penal creando los delitos informáticos.	Establece la protección penal frente a ataques contra la información y los sistemas informáticos.
Ley 1341 de 2009 (modificada por la Ley 1978 de 2019)	Define los principios de la sociedad de la información y la organización del sector TIC.	Marco general para la gestión de las tecnologías de la información en entidades públicas.
Ley 1437 de 2011	Código de Procedimiento Administrativo y de lo Contencioso Administrativo.	Promueve el uso de medios electrónicos en las actuaciones administrativas.
Ley 1581 de 2012	Régimen General de Protección de Datos Personales.	Norma principal para el tratamiento de datos personales en la entidad.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.	Define principios y procedimientos para el tratamiento de datos personales.
Ley 1712 de 2014	Ley de Transparencia y Acceso a la Información Pública.	Regula el acceso a la información pública y la gestión de la información institucional.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC.	Incorpora lineamientos de Gobierno Digital y seguridad digital.
Decreto 1008 de 2018	Actualiza la Política de Gobierno Digital.	Integra la seguridad de la información como habilitador de la transformación digital.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.	Fortalece la gestión del riesgo digital y la resiliencia institucional.
Resolución 1519 de 2020 (MinTIC)	Estándares de publicación y acceso a la información pública.	Apoya la gestión segura de la información publicada por la entidad.
Resolución 500 de 2021 (MinTIC)	Lineamientos para la implementación de la Política de Gobierno Digital.	Orienta la adopción del MSPI dentro del marco de Gobierno Digital.
Decreto 767 de 2022	Actualiza la Política de Gobierno Digital.	Refuerza la seguridad digital, la arquitectura institucional y la gestión de los servicios digitales.
Modelo de Seguridad y Privacidad de la Información – MinTIC (versión vigente)	Guía metodológica para las entidades públicas.	Constituye el referente principal para el diseño e implementación del presente MSPI.
ISO/IEC 27001:2022	Sistema de Gestión de Seguridad de la Información.	Referencia internacional para la gestión basada en riesgos y la mejora continua.
ISO/IEC 27002:2022	Controles para la seguridad de la información.	Proporciona las buenas prácticas para la selección e implementación de controles de seguridad.

Tabla 1. Marco Normativo del MSPI.

FASE 1 – PLANEACIÓN.

1. MARCO ESTRATÉGICO.

Como parte del marco estratégico del presente proyecto, se muestra la correlación entre las políticas, lineamientos e instrumentos establecidos en la Política de Gobierno Digital, con el propósito de evidenciar su articulación, complementariedad y contribución al fortalecimiento de la gestión institucional, la transformación digital y el cumplimiento de los objetivos estratégicos de la E.S.E. Hospital Eduardo Arredondo Daza.



Ilustración 1. MSPI y políticas existentes.

1.1 ALINEACIÓN CON EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI) DEL HOSPITAL EDUARDO ARREDONDO DAZA.

El Modelo de Seguridad y Privacidad de la Información constituye uno de los instrumentos estratégicos complementarios del Plan Estratégico de Tecnologías de la Información (PETI) de la E.S.E. Hospital Eduardo Arredondo Daza. Su implementación contribuye al cumplimiento de los objetivos estratégicos orientados al fortalecimiento del gobierno de TI, la transformación digital, la gestión integral de riesgos tecnológicos y la protección de los activos de información institucionales.

El MSPI desarrolla los componentes de seguridad definidos en el PETI mediante la implementación de políticas, procedimientos, controles y mecanismos de seguimiento que permiten reducir la exposición a riesgos tecnológicos, fortalecer la continuidad de los servicios críticos y garantizar el uso seguro de la información institucional. Las iniciativas contempladas en el presente documento se integran con el portafolio de proyectos del PETI, permitiendo una planeación coordinada de las inversiones, la optimización de los recursos y el seguimiento unificado de las acciones relacionadas con la seguridad de la información.

Asimismo, el Plan de Seguridad y Privacidad de la Información (PSPI) y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI), incorporados en este documento, constituyen instrumentos de ejecución del PETI para materializar los objetivos institucionales relacionados con la seguridad digital y la gestión de riesgos.

1.2 RELACIÓN CON LA POLÍTICA DE GOBIERNO DIGITAL.

El presente modelo se desarrolla en concordancia con la Política de Gobierno Digital, orientando la implementación de capacidades institucionales para garantizar que los servicios digitales ofrecidos por la E.S.E. Hospital Eduardo Arredondo Daza sean confiables, seguros, interoperables y centrados en el ciudadano. La gestión de la seguridad y privacidad de la información constituye un habilitador transversal de la transformación digital, permitiendo que las iniciativas tecnológicas incorporadas por la entidad se desarrollen bajo principios de gestión del riesgo, protección de la información, continuidad operacional y mejora continua.

1.3 RELACIÓN CON MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG).

El MSPI se articula con el Modelo Integrado de Planeación y Gestión mediante la implementación de prácticas que fortalecen la gestión institucional, el control interno, la administración de riesgos y la mejora continua. En este contexto, la seguridad de la información deja de ser una responsabilidad exclusiva del área de tecnologías de la información y se convierte en un compromiso institucional que involucra a todos los procesos, dependencias, servidores públicos, contratistas y terceros que administren información de la entidad.

1.4 RELACIÓN CON EL SISTEMA INSTITUCIONAL DE GESTIÓN.

El Modelo de Seguridad y Privacidad de la Información se integra con los diferentes sistemas de gestión implementados por la E.S.E. Hospital Eduardo Arredondo Daza, fortaleciendo la administración de riesgos institucionales y apoyando el cumplimiento de los objetivos estratégicos. La articulación del MSPI comprende, entre otros, los siguientes componentes institucionales:

- Plan Estratégico Institucional.

- Plan Estratégico de Tecnologías de la Información (PETI).
- Modelo Integrado de Planeación y Gestión (MIPG).
- Sistema de Control Interno.
- Sistema Obligatorio de Garantía de Calidad en Salud.
- Programa de Gestión Documental.
- Política de Protección de Datos Personales.
- Plan Institucional de Archivos.
- Plan de Continuidad del Negocio.
- Política de Gestión del Riesgo.

2. CONTEXTO ORGANIZACIONAL.

2.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La E.S.E. Hospital Eduardo Arredondo Daza desarrolla sus actividades en un entorno donde la información clínica, administrativa, financiera y asistencial constituye uno de sus activos más valiosos. La protección de esta información resulta esencial para garantizar la continuidad de los servicios de salud, preservar la confianza de los pacientes y demás grupos de interés, cumplir con las disposiciones legales vigentes y reducir los riesgos que puedan afectar la operación institucional. En este contexto, la seguridad y privacidad de la información se convierte en un componente estratégico para fortalecer la gestión institucional y apoyar los procesos de transformación digital del Hospital.

2.2 CONTEXTO INTERNO.

Las actividades realizadas durante la construcción del PETI de la E.S.E. Hospital Eduardo Arredondo Daza, permitieron evidenciar una infraestructura tecnológica y sistemas de información que soportan sus procesos institucionales; sin embargo, se identifican oportunidades de mejora relacionadas con el fortalecimiento del gobierno de la seguridad, la formalización de políticas y procedimientos, la incorporación de capacidades especializadas en ciberseguridad y el desarrollo de una mayor cultura organizacional en torno a la protección de la información. Estos aspectos reflejan un nivel de madurez básico en seguridad de la información y constituyen el punto de partida para la implementación del MSPI, orientando las acciones necesarias para consolidar un modelo de gestión más sólido, alineado con los objetivos institucionales y basado en la mejora continua.



Ilustración 2. Contexto interno.

2.3 CONTEXTO EXTERNO.

La E.S.E. Hospital Eduardo Arredondo Daza desarrolla sus actividades en un entorno caracterizado por una creciente transformación digital del sector salud, donde la disponibilidad, integridad y confidencialidad de la información son fundamentales para la prestación de los servicios y la continuidad de la operación institucional. Este escenario exige a la entidad fortalecer permanentemente sus capacidades para gestionar los riesgos asociados al uso de las tecnologías de la información y responder de manera efectiva a las nuevas amenazas del entorno digital.

A este contexto se suman factores como el incremento de las amenazas cibernéticas, la interacción permanente con proveedores de tecnología y la necesidad de intercambiar información de forma segura con otras entidades del sector salud, organismos de control y plataformas nacionales de interoperabilidad. Estos elementos hacen necesario contar con un Modelo de Seguridad y Privacidad de la Información que permita fortalecer la gestión de riesgos, proteger los activos de información y asegurar el cumplimiento de los objetivos institucionales.



Ilustración 3. Contexto externo.

2.4 PARTES INTERESADAS.

La gestión de la seguridad y privacidad de la información requiere identificar las partes interesadas que interactúan con la E.S.E. Hospital Eduardo Arredondo Daza y comprender sus necesidades frente a la protección de la información. Cada uno de estos actores participa directa o

indirectamente en la generación, consulta, almacenamiento o intercambio de información institucional, por lo que sus expectativas constituyen un elemento clave para la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI).



Ilustración 4. Partes interesadas.

2.5 FACTORES INTERNOS Y EXTERNOS.

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) está influenciada por diversos factores internos y externos que pueden favorecer o afectar la capacidad de la E.S.E. Hospital Eduardo Arredondo Daza para proteger sus activos de información. Identificar estos factores permite comprender el entorno en el que se desarrollará el modelo y orientar la definición de estrategias, controles y acciones de mejora acordes con la realidad institucional. La siguiente matriz resume los principales factores identificados durante el diagnóstico institucional.

FACTORES INTERNOS	FACTORES EXTERNOS
Infraestructura tecnológica con oportunidades de fortalecimiento en seguridad.	Cambios permanentes en el marco normativo del sector salud y de Gobierno Digital.
Disponibilidad de talento humano para la gestión de TI, con necesidad de fortalecer capacidades en ciberseguridad.	Incremento de amenazas cibernéticas dirigidas al sector salud.
Disponibilidad de talento humano para la gestión de TI, con necesidad de fortalecer capacidades en ciberseguridad.	Evolución constante de las tecnologías de la información y las comunicaciones.
Sistemas de información que soportan la operación institucional y requieren fortalecimiento en controles de seguridad.	Requerimientos de interoperabilidad con plataformas nacionales y entidades del sector salud.

Gestión documental y administración de la información institucional en proceso de fortalecimiento.	Riesgos asociados al intercambio de información con proveedores y terceros.

Tabla 2. Factores internos y externos que afectan el MSPI.

2.6 ALCANCE DEL MSPI.

El Modelo de Seguridad y Privacidad de la Información (MSPI) de la E.S.E. Hospital Eduardo Arredondo Daza tiene como alcance la gestión de la seguridad y privacidad de la información que soporta la prestación de los servicios de salud y el desarrollo de los procesos institucionales. Su implementación comprende los activos de información, los recursos tecnológicos, el talento humano y los procesos que intervienen en la creación, procesamiento, almacenamiento, transmisión y disposición de la información institucional. El alcance del modelo aplica a todos los servidores públicos, contratistas, proveedores y terceros que, en ejercicio de sus funciones o actividades, tengan acceso a la información o a los recursos tecnológicos de la entidad, así como a los sistemas de información, bases de datos, equipos de cómputo, redes de comunicaciones y demás activos que soportan la operación institucional.

De igual forma, el MSPI cubre la información generada y administrada en los procesos estratégicos, misionales, de apoyo y de evaluación de la E.S.E. Hospital Eduardo Arredondo Daza, independientemente del medio en que esta se encuentre (físico o digital), promoviendo su protección durante todo su ciclo de vida.

3. GOBIERNO DEL MSPI DEL HEAD.

La seguridad de la información constituye un componente estratégico para la E.S.E. Hospital Eduardo Arredondo Daza, ya que permite proteger uno de los activos más importantes de la institución: la información que soporta la atención en salud, la gestión administrativa, los procesos financieros y la toma de decisiones. Su adecuada gestión no depende únicamente de la implementación de controles tecnológicos, sino de un modelo de gobierno que defina responsabilidades, establezca mecanismos de coordinación y promueva una cultura institucional orientada a la protección de la información.

3.1 GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN.

La E.S.E. Hospital Eduardo Arredondo Daza debe implementar un modelo de seguridad de la información que garantice que las actividades, estrategias y acciones relacionadas con el PETI y el MSPI de la institución se ejecuten, tengan seguimiento, cumplimiento y se generen acciones de mejoramiento continuo.



Ilustración 5. Modelo de gobierno del MSPI.

3.2 ROLES Y RESPONSABILIDADES.

La implementación y sostenibilidad del Modelo de Seguridad y Privacidad de la Información (MSPI) requiere la participación coordinada de los diferentes niveles de la organización. Cada actor tiene responsabilidades específicas orientadas a proteger los activos de información, gestionar los riesgos y garantizar el cumplimiento de las políticas institucionales de seguridad y privacidad de la información. La asignación clara de responsabilidades fortalece el gobierno del modelo, facilita la toma de decisiones y promueve una cultura de corresponsabilidad en toda la entidad.

NIVEL JERÁRQUICO	ROL / DEPENDENCIA	RESPONSABILIDAD DENTRO DEL MSPI
Estratégico	**Gerente**	Liderar el gobierno del MSPI, aprobar las políticas institucionales relacionadas, asignar los recursos necesarios y promover una cultura organizacional orientada a la protección de la información.
Estratégico	**Jefe de Tecnologías de la Información**	Coordinar la implementación técnica del MSPI, administrar los controles tecnológicos, apoyar la gestión de riesgos, liderar la atención de incidentes de seguridad y garantizar la operación segura de la infraestructura tecnológica.
Estratégico	**Comité Institucional del MSPI**	Orientar la implementación del MSPI, realizar seguimiento a su ejecución, analizar los riesgos estratégicos, aprobar planes de acción y formular recomendaciones para la mejora continua del modelo.
Táctico	**Asesor Jurídico**	Asesorar el cumplimiento del marco legal aplicable en materia de protección de datos personales, acceso a la información pública, contratación y demás disposiciones relacionadas con la seguridad de la información.
Táctico	**Líder de Talento Humano**	Integrar la seguridad de la información en los procesos de selección, inducción, reinducción y capacitación, fortaleciendo la cultura institucional de seguridad.
Táctico	**Líderes de Proceso**	Identificar y custodiar los activos de información de su proceso, participar en la gestión de riesgos y asegurar el cumplimiento de las políticas y procedimientos del MSPI.
Evaluación y Control	**Oficina de Control Interno / Calidad**	Verificar la implementación y eficacia del MSPI mediante auditorías, seguimientos y evaluaciones, promoviendo acciones correctivas y oportunidades de mejora.
Operativo	**Funcionarios de la institución**	Aplicar las políticas y procedimientos de seguridad de la información en el desarrollo de sus funciones, proteger los activos de información y reportar oportunamente incidentes o vulnerabilidades.
Operativo	**Contratistas**	Cumplir las obligaciones de seguridad de la información definidas por la entidad y proteger la información institucional a la que tengan acceso durante la ejecución de sus actividades.
Operativo	**Proveedores y Terceros**	Garantizar el tratamiento seguro de la información institucional conforme a los requisitos contractuales y a las políticas de seguridad establecidas por la entidad.

Tabla 3. Roles y responsabilidades del MSPI.

3.3 COMITÉ INSTITUCIONAL DEL MSPI.

El Comité Institucional de Seguridad y Privacidad de la Información es la instancia encargada de orientar, coordinar y realizar seguimiento a la implementación del MSPI en la E.S.E. Hospital Eduardo Arredondo Daza. Su propósito será apoyar la toma de decisiones relacionadas con la protección de los activos de información, la gestión de riesgos, el cumplimiento normativo y la mejora continua del modelo.

3.3.1 Funciones:

- Aprobar los lineamientos estratégicos del MSPI.
- Hacer seguimiento al Plan de Seguridad y Privacidad de la Información (PSPI).
- Revisar el avance del Plan de Tratamiento de Riesgos (PTRSPI).
- Analizar los incidentes relevantes de seguridad de la información.
- Revisar periódicamente el nivel de madurez del MSPI.
- Aprobar acciones de mejora y planes de fortalecimiento.
- Promover la cultura institucional de seguridad de la información.
- Presentar recomendaciones a la Alta Dirección.

3.3.2 Integrantes sugeridos:

- Gerente o designado.
- Jefe del área de sistemas.
- Asesor jurídico.
- Líder de talento humano.
- Jefe del área de calidad o control interno.
- Líderes de proceso.
- Representantes de los funcionarios y contratistas.

3.3.3 Reuniones:

Se sugiere la programación de reuniones ordinarias trimestrales y reuniones extraordinarias cuando la situación lo requiera.

3.4 POLÍTICAS DEL COMITÉ INSTITUCIONALDEL MSPI.

Es necesario definir una política que permita que el comité institucional del MSPI funcione correctamente luego de diseñado e implementado. Esta política será revisada periódicamente por la Alta Dirección y el Comité Institucional de Seguridad y Privacidad de la Información para asegurar su vigencia y alineación con los objetivos estratégicos del Hospital. Esta, debe ser una política

institucional elaborada, publicadas y con la debida apropiación por parte de todos los funcionarios y partes interesadas de la institución.

3.4.1 Principios de las políticas del MSPI:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autenticidad.
- Trazabilidad.
- Gestión basada en riesgos.
- Cumplimiento normativo.
- Mejora continua.

4. LÍNEA BASE PARA IMPLEMENTACIÓN DEL MSPI.

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la E.S.E. Hospital Eduardo Arredondo Daza parte de una evaluación inicial orientada a conocer el estado de la gestión de la seguridad de la información. Esta línea base permite identificar las capacidades existentes, establecer las necesidades prioritarias y definir las acciones que se desarrollarán durante la implementación del modelo, conforme a los lineamientos del Ministerio TIC y las buenas prácticas internacionales.

4.1 EVALUACIÓN INICIAL DEL MSPI.

Como resultado de la evaluación realizada, se evidenció que la E.S.E. Hospital Eduardo Arredondo Daza no cuenta con un Modelo de Seguridad y Privacidad de la Información formalmente implementado. Si bien existen controles tecnológicos y procedimientos administrativos que contribuyen a la protección de la información, estos funcionan de manera independiente y no hacen parte de un esquema integral de gestión de la seguridad. La entidad inicia la implementación del MSPI con el propósito de fortalecer el gobierno de la seguridad, gestionar los riesgos de manera estructurada y consolidar una cultura institucional orientada a la protección de la información.

COMPONENTE EVALUADO	ESTADO
Gestión de Incidentes	Parcial
Continuidad del Negocio	Parcial
Gobierno del MSPI	En implementación
Roles y Responsabilidades	En implementación
Política de Seguridad de la Información	No implementada
Gestión de Activos de Información	No implementada
Clasificación de la Información	No implementada
Gestión de Riesgos de Seguridad	No implementada
Auditoría y Mejora Continua	No implementadas
Indicadores del MSPI	No implementados

Tabla 4. Evaluación inicial del MSPI del HEAD.

5. PLANIFICACIÓN DEL MSPI DEL HEAD.

La planificación constituye la base para la implementación del MSPI, ya que permite definir los elementos necesarios para gestionar los riesgos, proteger los activos de información y establecer los controles que garanticen la confidencialidad, integridad y disponibilidad de la información institucional. En esta fase se identifican los activos de información, se establece su clasificación, se analizan los riesgos asociados y se formulan las estrategias que orientarán la implementación del modelo en la E.S.E. Hospital Eduardo Arredondo Daza.

5.1 EVALUACIÓN INICIAL DEL MSPI.

Los activos de información representan uno de los recursos más importantes para la E.S.E. Hospital Eduardo Arredondo Daza, ya que soportan la prestación de los servicios de salud, la gestión administrativa y la toma de decisiones institucionales. Su adecuada identificación, valoración y administración constituye el punto de partida para la gestión de riesgos y la definición de los controles de seguridad del MSPI. La gestión de activos busca garantizar que toda la información, independientemente de su formato o medio de almacenamiento, cuente con un responsable claramente definido y reciba un tratamiento acorde con su importancia para la organización.

5.2 GESTIÓN DE ACTIVOS DE INFORMACIÓN.

El inventario de activos de la ESE Hospital Eduardo Arredondo Daza comprende los activos de información asociados a los procesos estratégicos, misionales, de apoyo y de evaluación definidos en el mapa de procesos institucional. Incluye tanto los activos primarios (información que soporta la prestación de los servicios de salud y la gestión administrativa) como los sistemas de información y demás activos de soporte utilizados para su almacenamiento, procesamiento y disponibilidad. El inventario constituye el repositorio oficial para la administración de los activos de información del Hospital y será la base para la gestión de riesgos, la implementación de controles de seguridad, la continuidad del negocio y la mejora continua del MSPI.

En el Anexo 1, se muestra la tabla completa de gestión de activos de información del Hospital Eduardo Arredondo Daza.

5.3 CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS.

Se realizó la definición de los criterios institucionales para clasificar y valorar los activos de información de la E.S.E. Hospital Eduardo Arredondo Daza, garantizando que su protección sea proporcional al valor que representan para la operación institucional, el cumplimiento normativo y la prestación de los servicios de salud. La clasificación se realizó considerando el nivel de sensibilidad de la información, los requisitos legales aplicables y el impacto que tendría su divulgación, alteración o pérdida.

5.3.1 Clasificación:

CLASIFICACIÓN	DESCRIPCIÓN
Pública	Información que puede ser conocida por cualquier ciudadano sin generar afectación para la institución.
Uso Interno	Información destinada exclusivamente al funcionamiento institucional cuyo acceso está restringido al personal autorizado.
Clasificada	Información protegida por normas relacionadas con datos personales, historia clínica, información laboral o cualquier otra disposición legal que limite su divulgación.
Reservada	Información cuya divulgación, modificación o pérdida puede afectar la prestación de los servicios, la seguridad institucional o el cumplimiento de obligaciones legales.

Tabla 5. Criterios de clasificación de activos.

5.3.2 Valoración:

CLASIFICACIÓN	DESCRIPCIÓN
Confidencialidad (C)	Necesidad de restringir el acceso únicamente a personas autorizadas.
Integridad (I)	Necesidad de preservar la exactitud, consistencia y completitud de la información.
Disponibilidad (D)	Necesidad de garantizar que la información esté accesible cuando sea requerida para la operación institucional.

Tabla 6. Criterios de valoración de activos.

5.3.3 Criticidad:

La criticidad representa la importancia del activo para la continuidad de la operación institucional y la prestación de los servicios de salud. Su determinación considera:

- Impacto sobre la atención de los pacientes.
- Cumplimiento de requisitos legales y regulatorios.
- Continuidad de los procesos institucionales.
- Protección de datos personales y de la historia clínica.
- Impacto financiero, reputacional y operativo.

Los activos clasificados con criticidad alta o muy alta serán priorizados durante el proceso de gestión de riesgos y la implementación de controles de seguridad.

6. GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

El objetivo de esta sección es establecer la metodología institucional para identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información de la E.S.E. Hospital Eduardo Arredondo Daza, con el propósito de implementar controles apropiados que reduzcan la probabilidad de ocurrencia de incidentes de seguridad y garanticen la continuidad de los procesos institucionales y la adecuada prestación de los servicios de salud. La gestión del riesgo constituye uno de los pilares del Modelo de Seguridad y Privacidad de la Información (MSPI), permitiendo orientar la toma de decisiones sobre la implementación de controles de seguridad de acuerdo con el nivel de exposición de cada activo de información.

6.1 METODOLOGÍA DE VALORACIÓN DEL RIESGO.

Se presentan a continuación los criterios que se utilizaron para realizar la valoración de los riesgos de la ESE Hospital Eduardo Arredondo Daza:

- Amenazas.
- Vulnerabilidad.
- Riesgos.
- Controles existentes.
- Probabilidad.
- Impacto.
- Nivel de riesgo.
- Tratamiento.

6.2 MATRIZ INSTITUCIONAL DE RIESGOS.

La Matriz de Riesgos de Seguridad de la Información se elaboró con base en el inventario institucional de activos de información de la E.S.E. Hospital Eduardo Arredondo Daza, constituyéndose en el principal instrumento para identificar, analizar y valorar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información. Para cada activo se identificaron las amenazas, vulnerabilidades, riesgos asociados, controles existentes, probabilidad de ocurrencia, impacto, nivel de riesgo, estrategia de tratamiento y controles propuestos, permitiendo establecer una priorización objetiva de las acciones de mitigación. Los resultados de esta matriz sirven como fundamento para la formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI), la selección de controles de

seguridad y el fortalecimiento continuo del Modelo de Seguridad y Privacidad de la Información (MSPI) del Hospital. Se anexa la matriz realizada en el ANEXO 2 de este documento.

6.3 EVALUACIÓN Y ACEPTACIÓN DE LOS RIESGOS.

Con el propósito de establecer un tratamiento uniforme de los riesgos identificados durante el proceso de gestión de riesgos de seguridad de la información, la E.S.E. Hospital Eduardo Arredondo Daza define criterios para la evaluación y aceptación del riesgo, los cuales orientan la toma de decisiones sobre la implementación de controles y la priorización de acciones de mejora.

La valoración de cada riesgo se realizó considerando dos variables fundamentales: la probabilidad de ocurrencia, entendida como la posibilidad de que una amenaza explote una vulnerabilidad existente, y el impacto, que representa las consecuencias que tendría la materialización del riesgo sobre la operación institucional, la continuidad de los servicios, la información clínica y administrativa, el cumplimiento legal y la imagen del Hospital. La combinación de estas variables permitió establecer el nivel de riesgo y definir el tratamiento más apropiado. Los criterios adoptados para la aceptación del riesgo son los siguientes:

NIVEL DE RIESGO	CRITERIO INSTITUCIONAL	ACCIÓN REQUERIDA
Bajo	El riesgo se considera aceptable dentro de la operación normal de la entidad.	Mantener controles existentes y realizar seguimiento periódico.
Medio	El riesgo requiere acciones de mejora, de acuerdo con la disponibilidad de recursos y prioridades institucionales.	Implementar controles preventivos o correctivos y realizar monitoreo continuo.
Alto	El riesgo puede afectar significativamente la operación, la prestación de los servicios de salud o el cumplimiento normativo.	Priorizar su tratamiento mediante la implementación de controles específicos dentro del PTRSPI.
Crítico	El riesgo representa una amenaza inmediata para la continuidad de la operación, la confidencialidad, integridad o disponibilidad de la información institucional.	Implementar acciones inmediatas, asignar recursos prioritarios y realizar seguimiento por la Alta Dirección y el Comité Institucional de Seguridad de la Información.

Tabla 7. Criterios de evaluación de los riesgos.

6.4 RESULTADO DEL ANÁLISIS DE RIESGOS.

Como resultado de la aplicación de la metodología de gestión de riesgos de seguridad de la información, se evaluaron 64 activos de información correspondientes a los procesos estratégicos, misionales, de apoyo y de evaluación de la E.S.E. Hospital Eduardo Arredondo Daza. Para cada activo se identificó un riesgo principal, considerando las amenazas, vulnerabilidades y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información.

El análisis permitió establecer que la institución presenta una mayor concentración de riesgos en un nivel Alto, lo que evidencia la necesidad de fortalecer los controles de seguridad sobre los activos que soportan la prestación de los servicios de salud y la gestión administrativa. La valoración realizada constituye la línea base para priorizar las acciones contempladas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI). Se muestran en las siguientes tres tablas el resumen de los resultados obtenidos en el análisis de riesgos:

CONCEPTO	RESULTADO
Activos de información evaluados	**66**
Riesgos identificados	**66**
Riesgos Críticos	**2 (0,015%)**
Riesgos Altos	**40 (62,5%)**
Riesgos Medios	**24 (37,5%)**
Riesgos Bajos	**0 (0%)**
Tratamiento definido: Mitigar	**66 (100%)**

Tabla 8. Resumen de resultados.

VARIABLE	RESULTADO
Probabilidad Alta (3)	**19 activos (29,7%)**
Probabilidad Media (2)	**45 activos (70,3%)**
Impacto Muy Alto (5)	**39 activos (60,9%)**
Impacto Alto (4)	**21 activos (32,8%)**
Impacto Medio (3)	**4 activos (6,3%)**

Tabla 9. Análisis de probabilidad e impacto.

AMENAZA	FRECUENCIA
Indisponibilidad del sistema	**8**
Alteración de registros	**8**
Acceso no autorizado	**7**
Alteración de la información	**4**
Modificación no autorizada	**3**
Pérdida o alteración de la información	**3**

Tabla 10. Principales amenazas identificadas.

Los resultados de la evaluación evidencian que la E.S.E. Hospital Eduardo Arredondo Daza presenta una alta dependencia de sus activos de información para el desarrollo de sus procesos institucionales. El hecho de que el 62,5 % de los riesgos se clasifiquen en nivel Alto indica la necesidad de implementar medidas de tratamiento prioritarias orientadas a fortalecer la seguridad de los sistemas de información, proteger la información clínica y administrativa, mejorar la disponibilidad de los servicios tecnológicos y reducir la probabilidad de incidentes de seguridad. En consecuencia, la totalidad de los riesgos identificados fueron definidos con la estrategia de mitigación, constituyéndose en la base para la formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI), mediante el cual se establecerán los controles, responsables, recursos y plazos necesarios para disminuir la exposición al riesgo y fortalecer el Modelo de Seguridad y Privacidad de la Información de la entidad.

Los riesgos clasificados como Altos se concentran principalmente en activos críticos para la operación del Hospital, entre ellos:

- Sistemas de información asistenciales (SIHOS y ANNARLAB).
- Historia Clínica Electrónica.
- Facturación y cartera.
- Laboratorio Clínico.
- Bases de datos institucionales (MySQL).
- Infraestructura tecnológica (servidores, copias de seguridad, comunicaciones y switches).
- Sistemas de reporte institucional (RIPS y SISPRO).
- Información financiera y de talento humano.

La indisponibilidad o alteración de estos activos podría afectar la continuidad de la prestación de los servicios de salud, el cumplimiento de los requerimientos regulatorios, la gestión administrativa y la protección de la información sensible de pacientes y funcionarios.

FASE 2 – EJECUCIÓN.

7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI).

El Plan de Seguridad y Privacidad de la Información (PSPI) es el instrumento de planificación mediante el cual la E.S.E. Hospital Eduardo Arredondo Daza establece las acciones, estrategias e iniciativas necesarias para implementar, mantener y fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI). Su propósito es orientar la ejecución de los controles de seguridad y privacidad de la información, garantizando la protección de los activos de información, la continuidad de los procesos institucionales y el cumplimiento de los requisitos legales, regulatorios y técnicos aplicables.

El PSPI se fundamenta en los resultados de la gestión de riesgos de seguridad y privacidad de la información y articula las actividades necesarias para la implementación de controles administrativos, físicos y tecnológicos, la sensibilización del talento humano, el seguimiento al desempeño del modelo y la mejora continua. En este contexto, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) constituye el principal instrumento de ejecución del PSPI, al definir las iniciativas, actividades, responsables, recursos, plazos e indicadores orientados a reducir los riesgos identificados y fortalecer el nivel de madurez del MSPI en la Entidad.

La ejecución del PSPI estará alineada con los objetivos estratégicos institucionales, el Plan Estratégico de Tecnologías de la Información (PETI), la Política de Gobierno Digital, la Guía para la Implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y los lineamientos de la norma ISO/IEC 27001:2022, promoviendo una gestión integral, sistemática y sostenible de la seguridad y privacidad de la información en la E.S.E. Hospital Eduardo Arredondo Daza.

7.1 GENERALIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI).

El PSPI integra las iniciativas institucionales orientadas a la gestión de riesgos, la implementación de controles, el fortalecimiento de capacidades, la sensibilización de los servidores públicos, el seguimiento de indicadores y la mejora continua del sistema de gestión de seguridad de la información.

Para la E.S.E. Hospital Eduardo Arredondo Daza, el PSPI se materializa mediante la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI), el cual define las iniciativas priorizadas, las actividades, responsables, recursos, plazos e indicadores requeridos para reducir los riesgos identificados durante la evaluación institucional.

Componente del PSPI	Instrumento desarrollado en el MSPI
Gestión de Riesgos	Matriz Institucional de Riesgos
Tratamiento de Riesgos	PTRSPI
Implementación de Controles	Plan de Acción del PTRSPI
Seguimiento	Matriz de Seguimiento del PTRSPI
Medición	Indicadores del MSPI
Verificación	Auditorías y Evaluación de Controles
Mejora Continua	Plan de Mejoramiento del MSPI

Tabla 11. Generalidades PSPI.

7.2 DEFINICIÓN DE LOS CRITERIOS DE PRIORIZACIÓN.

Con base en los resultados de la evaluación de riesgos realizada para la E.S.E. Hospital Eduardo Arredondo Daza, las acciones contempladas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) fueron priorizadas con el propósito de orientar la implementación de los controles hacia aquellos riesgos que representan un mayor impacto para la institución. La priorización de las iniciativas se realizó considerando los siguientes criterios:

- Nivel de riesgo: Se priorizan los riesgos clasificados como Críticos y Altos, de acuerdo con los resultados obtenidos en la Matriz de Gestión de Riesgos de Seguridad de la Información.
- Criticidad del activo: Se otorga prioridad a los activos que soportan los procesos misionales, la atención de pacientes, los sistemas de información institucionales y la infraestructura tecnológica.
- Impacto institucional: Se priorizan las acciones que contribuyen a garantizar la continuidad de la operación, la disponibilidad de los servicios tecnológicos, la protección de la información y el cumplimiento de los objetivos institucionales.
- Cumplimiento normativo: Se consideran prioritarias las iniciativas orientadas al cumplimiento de los requisitos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y la normatividad vigente en materia de seguridad de la información y protección de datos personales.
- Cobertura del control: Se priorizan los controles cuya implementación permite reducir simultáneamente múltiples riesgos, optimizando el uso de los recursos institucionales y fortaleciendo la seguridad de manera integral.

7.3 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PTRSPI).

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) define las acciones que la E.S.E. Hospital Eduardo Arredondo Daza implementará para reducir la probabilidad de ocurrencia y el impacto de los riesgos identificados durante la evaluación de seguridad de la información. Las acciones propuestas se encuentran orientadas al fortalecimiento de los controles administrativos, técnicos y físicos, priorizando aquellos que permiten mitigar riesgos de manera transversal sobre múltiples activos de información. La ejecución del plan será progresiva y estará sujeta a la disponibilidad presupuestal, la asignación de recursos y la programación institucional, sin perjuicio de la atención inmediata de los riesgos clasificados como críticos.

Las iniciativas definidas en este plan constituyen la hoja de ruta para el fortalecimiento del Modelo de Seguridad y Privacidad de la Información y deberán integrarse con la planeación institucional, el PETI y los planes de mejoramiento derivados de auditorías internas y externas.

No.	Iniciativa de tratamiento	Riesgos que atiende	Prioridad	Responsable
L-01	Implementación de una solución de seguridad perimetral (Firewall NGFW).	Accesos no autorizados, ataques externos, propagación de malware y amenazas provenientes de Internet.	Muy Alta	Gerencia – Jefe Sistemas
L-02	Implementación de una Plataforma Institucional de Protección Antimalware	Infección por malware, ransomware, software malicioso y compromiso de estaciones de trabajo y servidores.	Muy Alta	Gerencia – Jefe Sistemas
L-03	Fortalecimiento de la gestión de identidades y control de accesos	Accesos indebidos, uso inadecuado de credenciales y privilegios excesivos.	Muy Alta	Jefe Sistemas
L-04	Implementación y actualización de políticas de seguridad de la información	Ausencia de políticas institucionales, uso inadecuado de recursos tecnológicos y dispositivos personales.	Muy Alta	Comité de Seguridad de la Información
L-05	Fortalecimiento de la protección de los sistemas de información institucionales	Riesgos asociados a SIHOS, ANNARLAB, RFAST y demás aplicaciones críticas.	Alta	Jefe Sistemas
L-06	Fortalecimiento de la estrategia de copias de seguridad y recuperación ante desastres	Pérdida de información e indisponibilidad de servicios.	Alta	Jefe Sistemas
L-07	Gestión de vulnerabilidades y actualización tecnológica	Software desactualizado y vulnerabilidades técnicas.	Alta	Jefe Sistemas

L-08	Fortalecimiento de la seguridad de servidores, bases de datos y almacenamiento	Alteración, pérdida o divulgación de información institucional.	Alta	Jefe Sistemas
L-09	Fortalecimiento de la infraestructura de red y comunicaciones	Fallas de conectividad e indisponibilidad de servicios tecnológicos.	Media	Jefe Sistemas
L-10	Programa institucional de sensibilización y capacitación en seguridad de la información	Errores humanos, ingeniería social y phishing.	Media	Talento Humano – Jefe Sistemas
L-11	Implementación del programa de monitoreo, auditoría y mejora continua del MSPI	Incumplimiento de controles y mejora continua.	Media	Comité de Seguridad de la Información

Tabla 12. Tabla de lineamientos del PTRSPI.

7.4 PLAN DE ACCIÓN DEL PTRSPI.

El presente Plan de Acción establece las actividades necesarias para implementar las iniciativas de tratamiento definidas en el PTRSPI, con el propósito de reducir el nivel de exposición a los riesgos de seguridad y privacidad de la información identificados en la E.S.E. Hospital Eduardo Arredondo Daza.

Las acciones propuestas se desarrollarán de manera progresiva durante la vigencia del Plan, considerando la disponibilidad de recursos institucionales, la prioridad de los riesgos y la capacidad técnica de la Entidad. Su ejecución será objeto de seguimiento periódico por parte del Comité Institucional de Seguridad de la Información, el cual verificará el cumplimiento de las actividades programadas y la efectividad de los controles implementados.

No.	INICIATIVA	ACTIVIDADES PRINCIPALES	RESPONSABLE	RECURSOS REQUERIDOS	PLAZO	ENTREGABLE	INDICADOR
PA-001	Implementación de seguridad perimetral (Firewall NGFW)	Elaborar estudio técnico, definir especificaciones, adquirir, instalar, configurar políticas de seguridad y poner en operación la solución.	Gerencia – Jefe Sistemas	Recursos financieros, personal TIC y proveedor especializado	Corto	Firewall implementado y configurado	% de implementación del proyecto
PA-002	Implementación de la Plataforma Institucional de Protección Antimalware	Adquirir e implementar una solución corporativa con administración centralizada para estaciones de trabajo y servidores, configurar políticas, monitoreo y actualizaciones automáticas.	Jefe Sistemas	Licencias, infraestructura, personal TIC	Corto	Plataforma implementada y operativa	% de equipos protegidos
PA-003	Fortalecimiento de la gestión de identidades y control de accesos	Revisar perfiles de usuario, depurar cuentas, definir privilegios, fortalecer autenticación y procedimientos de administración de accesos.	Jefe Sistemas	Personal TIC	Corto	Matriz de perfiles y procedimiento actualizado	% de usuarios revisados
PA-004	Actualización del marco documental de seguridad de la información	Elaborar, actualizar, aprobar y divulgar políticas, procedimientos y lineamientos del MSPI (contraseñas, BYOD, respaldo, control de accesos, gestión de incidentes, uso aceptable, entre otros).	Comité de Seguridad de la Información	Equipo MSPI	Corto	Políticas y procedimientos aprobados	% de documentos formalizados
PA-005	Fortalecimiento de la protección de los sistemas de información institucionales	Revisar configuraciones de seguridad, controles de acceso y mecanismos de protección de SIHOS, ANNARLAB, RFAST y demás aplicaciones institucionales.	Jefe Sistemas	Personal TIC y proveedores	Mediano	Sistemas fortalecidos	% de sistemas intervenidos
PA-006	Fortalecimiento de la estrategia de copias de seguridad y recuperación	Actualizar procedimientos de respaldo, automatizar copias, definir almacenamiento seguro y realizar pruebas periódicas de restauración.	Jefe Sistemas	Infraestructura de almacenamiento	Mediano	Procedimiento implementado y pruebas ejecutadas	% de respaldos exitosos
PA-007	Gestión de vulnerabilidades y actualización tecnológica	Inventariar software, aplicar parches de seguridad, eliminar vulnerabilidades críticas y establecer un procedimiento permanente de actualización.	Jefe Sistemas	Personal TIC	Permanente	Plan de actualización tecnológica	% de vulnerabilidades corregidas

PA-008	Fortalecimiento de servidores, bases de datos y almacenamiento	Implementar controles de endurecimiento (hardening), revisar configuraciones, restringir accesos y fortalecer mecanismos de protección de la información.	Jefe Sistemas	Personal TIC	Mediano	Servidores fortalecidos	% de servidores intervenidos
PA-009	Fortalecimiento de la infraestructura de red y comunicaciones	Mejorar la seguridad de dispositivos de red, segmentación, monitoreo y administración de la infraestructura tecnológica.	Jefe Sistemas	Equipos de red y personal TIC	Mediano	Infraestructura optimizada	% de dispositivos asegurados
PA-010	Programa de sensibilización y capacitación	Diseñar y ejecutar jornadas periódicas de capacitación sobre seguridad de la información, protección de datos personales, ingeniería social y buenas prácticas digitales.	Talento Humano / Jefe Sistemas	Recursos de capacitación	Permanente	Plan de capacitación ejecutado	% de funcionarios capacitados
PA-011	Gestión de incidentes de seguridad de la información	Implementar el procedimiento institucional para el reporte, análisis, atención y cierre de incidentes de seguridad de la información.	Comité de Seguridad / Jefe Sistemas	Personal TIC	Mediano	Procedimiento implementado	Tiempo promedio de atención de incidentes
PA-012	Seguimiento y mejora continua del MSPI	Revisar periódicamente la matriz de riesgos, evaluar indicadores, realizar auditorías internas y actualizar el PTRSPI conforme a los resultados obtenidos.	Comité de Seguridad de la Información	Equipo MSPI	Permanente	Informes de seguimiento y mejora	% de cumplimiento del PTRSPI

Tabla 13. Plan de acción PTRSPI.

FASE 3 – VERIFICAR.

8. SEGUIMIENTO, EVALUACIÓN Y DESEMPEÑO DEL MSPI.

El seguimiento, la evaluación y la medición del desempeño constituyen la fase de Verificar del ciclo de mejora continua del MSPI. En esta etapa, la E.S.E. Hospital Eduardo Arredondo Daza verifica la eficacia de los controles implementados, el cumplimiento de las actividades definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) y el grado de avance en el logro de los objetivos de seguridad y privacidad de la información. Para ello, se establecen mecanismos de seguimiento, indicadores de gestión, procesos de monitoreo, gestión de incidentes y auditorías internas que permiten evaluar el desempeño del modelo, identificar oportunidades de mejora y proporcionar información objetiva para la toma de decisiones por parte de la Alta Dirección y del Comité Institucional de Seguridad de la Información, garantizando la mejora continua y la sostenibilidad del MSPI en la Entidad.

8.1 SEGUIMIENTO A LA EJECUCIÓN DEL PTRSPI.

El área de sistemas de la ESE Hospital Eduardo Arredondo Daza, en coordinación con el Comité Institucional de Seguridad de la Información y los responsables de cada iniciativa, realizará el seguimiento periódico al plan mediante la revisión de evidencias, informes de avance y resultados obtenidos. Como parte del seguimiento deberán verificarse, como mínimo, los siguientes aspectos:

- Cumplimiento de las actividades establecidas en el Plan de Acción.
- Avance físico y porcentual de cada iniciativa del PTRSPI.
- Estado de implementación de los controles de seguridad.
- Riesgos mitigados y riesgos pendientes de tratamiento.
- Cumplimiento de los cronogramas establecidos.
- Disponibilidad de los recursos necesarios para la ejecución del plan.
- Dificultades o desviaciones que afecten el cumplimiento de las actividades.
- Acciones correctivas definidas para superar los incumplimientos identificados.

Los resultados del seguimiento deberán consolidarse en informes periódicos presentados al Comité Institucional de Seguridad de la Información y a la Alta Dirección, quienes evaluarán la necesidad de ajustar prioridades, asignar recursos adicionales o modificar las estrategias definidas en el PTRSPI.

CÓDIGO	INICIATIVA DEL PTRSPI	RESPONSABLE	PLAZO	ESTADO	SEMÁFORO	% AVANCE	EVIDENCIAS DE CUMPLIMIENTO	ÚLTIMO SEGUIMIENTO	OBSERVACIONES
PA-001	Implementación de seguridad perimetral (Firewall NGFW)	Gerencia / Área TIC	Corto	Pendiente		0%	-	N/A	Iniciativa programada.
PA-002	Implementación de la Plataforma Institucional de Protección Antimalware	Área TIC	Corto	Pendiente		0%	-	N/A	Iniciativa programada.
PA-003	Fortalecimiento de la gestión de identidades y control de accesos	Área TIC	Corto	Pendiente		0%	-	N/A	Iniciativa programada.
PA-004	Actualización del marco documental de seguridad de la información	Comité de Seguridad Información	Corto	En ejecución		40%	MSPI, PTRSPI, PSPI y políticas institucionales	jul-26	MSPI en ejecución
PA-005	Fortalecimiento de la protección de los sistemas de información institucionales	Área TIC	Mediano	Pendiente		0%	-	N/A	Iniciativa programada.
PA-006	Fortalecimiento de la estrategia de copias de seguridad y recuperación	Área TIC	Mediano	Pendiente		0%	-	N/A	Iniciativa programada.
PA-007	Gestión de vulnerabilidades y actualización tecnológica	Área TIC	Permanente	Pendiente		0%	-	N/A	Iniciativa programada.
PA-008	Fortalecimiento de servidores, bases de datos y almacenamiento	Área TIC	Mediano	Pendiente		0%	-	N/A	Iniciativa programada.
PA-009	Fortalecimiento de la infraestructura de red y comunicaciones	Área TIC	Mediano	Pendiente		0%	-	N/A	Iniciativa programada.
PA-010	Programa de sensibilización y capacitación	Talento Humano / Área TIC	Permanente	Pendiente		0%	-	N/A	Iniciativa programada.
PA-011	Gestión de incidentes de seguridad de la información	Comité de Seguridad / Área TIC	Mediano	Pendiente		0%	-	N/A	Iniciativa programada.
PA-012	Seguimiento y mejora continua del MSPI	Comité de Seguridad de Información	Permanente	En ejecución		30%	Matriz de riesgos institucional, PTRSPI	jul-26	MSPI en ejecución

Tabla 14. Matriz de seguimiento del PTRSPI.

8.2 MEDICIÓN DEL DESEMPEÑO DEL MSPI (INDICADORES).

La matriz construida constituye el instrumento operativo de seguimiento del PTRSPI y establece la trazabilidad entre las iniciativas del plan de acción (capítulo 7.3) y la medición del desempeño del MSPI (capítulo 8.1). La información registrada en ella servirá como fuente para el cálculo de los indicadores de cumplimiento, la elaboración de informes periódicos al Comité Institucional de Seguridad de la Información y la Alta Dirección, así como para la identificación de acciones de mejora dentro del ciclo PHVA.

8.2.1 Indicadores de desempeño del MSPI:

Código	Objetivo de medición	Indicador	Fórmula	Meta	Frecuencia	Responsable	Fuente de información
MSPI-01	Medir la ejecución del PTRSPI	**Porcentaje de iniciativas ejecutadas**	(Iniciativas finalizadas / Total de iniciativas del PTRSPI) ×100	≥90%	Trimestral	Área TIC	Matriz de Seguimiento PTRSPI
MSPI-02	Controlar el avance del PTRSPI	**Porcentaje promedio de avance del PTRSPI**	Σ(% avance de las iniciativas) / Total iniciativas	≥85%	Trimestral	Área TIC	Matriz de Seguimiento PTRSPI
MSPI-03	Verificar la implementación de controles	**Porcentaje de controles implementados**	(Controles implementados / Controles programados) ×100	≥90%	Trimestral	Área TIC	PTRSPI
MSPI-04	Evaluar la mitigación del riesgo	**Porcentaje de riesgos tratados**	(Riesgos tratados / Riesgos identificados) ×100	≥80%	Semestral	Comité de Seguridad	Matriz Institucional de Riesgos
MSPI-05	Evaluar la reducción del riesgo alto	**Riesgos altos mitigados**	(Riesgos altos mitigados / Riesgos altos identificados) ×100	≥80%	Semestral	Comité de Seguridad	Matriz de Riesgos
MSPI-06	Controlar incidentes	**Incidentes atendidos oportunamente**	(Incidentes atendidos dentro del tiempo establecido / Total incidentes) ×100	≥95%	Trimestral	Área TIC	Registro de Incidentes
MSPI-07	Fortalecer la cultura de seguridad	**Cobertura de capacitación**	(Funcionarios capacitados / Funcionarios programados) ×100	100%	Semestral	Talento Humano	Registros de capacitación
MSPI-08	Verificar el cumplimiento documental	**Documentos del MSPI actualizados**	(Documentos actualizados / Documentos programados) ×100	100%	Anual	Comité de Seguridad	Control documental
MSPI-09	Evaluar el seguimiento institucional	**Seguimientos ejecutados**	(Seguimientos realizados / Seguimientos programados) ×100	100%	Trimestral	Comité de Seguridad	Actas e informes
MSPI-10	Verificar auditorías	**Cumplimiento del programa de auditoría**	(Auditorías ejecutadas / Auditorías programadas) ×100	100%	Anual	Control Interno	Plan Anual de Auditoría

MSPI-11	Medir el cierre de acciones de mejora	**Acciones de mejora implementadas**	(Acciones cerradas / Acciones formuladas) ×100	≥90%	Semestral	Comité de Seguridad	Planes de mejoramiento
MSPI-12	Evaluar el desempeño global del MSPI	**Índice de Madurez del MSPI**	Promedio ponderado de los indicadores MSPI-01 a MSPI-11	≥85%	Anual	Comité Seguridad de información	Consolidado de indicadores

Tabla 15. Indicadores del MSPI.

8.3 MONITOREO DE LOS CONTROLES DE SEGURIDAD.

El propósito del monitoreo es identificar oportunamente desviaciones, fallas de operación, vulnerabilidades, incidentes o incumplimientos que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional. El monitoreo será realizado por el área de sistemas del HEAD con el apoyo del Comité Institucional de Seguridad de la Información y las dependencias responsables de los activos de información, utilizando como fuente los registros operativos, informes técnicos, auditorías, indicadores del MSPI, matriz de riesgos y la Matriz de Seguimiento del PTRSPI.

CÓDIGO	CONTROL DE SEGURIDAD	TIPO DE CONTROL	MECANISMO DE MONITOREO	EVIDENCIA	FRECUENCIA	RESPONSABLE
CS-01	Políticas de Seguridad de la Información	Administrativo	Verificación de vigencia, aprobación y difusión	Políticas aprobadas y control documental	Anual	Comité de Seguridad
CS-02	Gestión de usuarios y privilegios	Administrativo / Técnico	Revisión de usuarios activos, perfiles y permisos	Reportes de usuarios y registros de acceso	Trimestral	Area sistemas
CS-03	Gestión de contraseñas	Técnico	Validación de cumplimiento de la política institucional	Configuración de sistemas y registros	Trimestral	Area sistemas
CS-04	Protección antimalware	Técnico	Verificación del estado de actualización y cobertura de los equipos	Consola del antivirus e informes técnicos	Mensual	Area sistemas
CS-05	Firewall y seguridad perimetral	Técnico	Revisión de eventos, reglas y disponibilidad del firewall	Bitácoras del firewall	Mensual	Area sistemas
CS-06	Copias de seguridad institucionales	Técnico	Validación de ejecución de respaldos y pruebas de restauración	Reportes de respaldo y restauración	Mensual	Area sistemas
CS-07	Gestión de vulnerabilidades	Técnico	Revisión vulnerabilidad detectada y acción implementada	Informes de análisis de vulnerabilidades	Trimestral	Area sistemas

CS-08	Actualizaciones y parches de seguridad	Técnico	Seguimiento a la instalación de actualizaciones críticas	Reportes de actualización	Mensual	Area sistemas
CS-09	Inventario de activos de información	Administrativo	Verificación de actualización del inventario institucional	Inventario institucional de activos	Semestral	Area sistemas
CS-10	Clasificación de la información	Administrativo	Revisión de la clasificación de nuevos activos de información	Inventario y registros documentales	Semestral	Propietarios de los activos
CS-11	Capacitación y sensibilización	Administrativo	Seguimiento al cumplimiento del plan anual de capacitación	Listados de asistencia y evaluaciones	Semestral	Talento Humano / Área sistemas
CS-12	Gestión de incidentes de seguridad	Administrativo / Técnico	Revisión de incidentes reportados, tiempos de atención y cierre	Registro de incidentes	Trimestral	Area sistemas
CS-13	Cumplimiento del PTRSPI	Administrativo	Seguimiento al avance de las iniciativas del Plan de Tratamiento	Matriz de Seguimiento del PTRSPI	Trimestral	Comité de Seguridad
CS-14	Cumplimiento del MSPI	Administrativo	Evaluación de indicadores de desempeño y avance del modelo	Tablero de Indicadores del MSPI	Trimestral	Comité de Seguridad
CS-15	Cumplimiento normativo	Administrativo	Revisión del cumplimiento de los requisitos legales y regulatorios aplicables	Informes de cumplimiento	Anual	Comité de Seguridad

Tabla 16. Monitoreo de los controles.

Los resultados del monitoreo serán consolidados por el área de sistemas del HEAD y presentados trimestralmente al Comité Institucional de Seguridad de la Información. Cuando se identifiquen desviaciones, incumplimientos o fallas en la operación de los controles, se formularán las acciones correctivas correspondientes y se incorporarán al Plan de Mejoramiento del MSPI para su seguimiento dentro del ciclo PHVA.

ESTADO	CRITERIO	ACCIÓN REQUERIDA
Conforme	El control opera de acuerdo con los lineamientos definidos y existen evidencias suficientes de su funcionamiento.	Continuar con el monitoreo periódico.
Parcialmente Conforme	El control presenta debilidades menores o evidencias incompletas que no comprometen significativamente su eficacia.	Implementar acciones de mejora y realizar seguimiento.
No Conforme	El control no se encuentra implementado, no opera adecuadamente o carece de evidencias objetivas de cumplimiento.	Formular e implementar acciones correctivas prioritarias e incluirlas en el Plan de Mejoramiento del MSPI.

Tabla 17. Criterios de evaluación.

8.4 GESTIÓN Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

La E.S.E. Hospital Eduardo Arredondo Daza establecerá un proceso para la gestión de incidentes de seguridad de la información con el fin de identificar, registrar, analizar, atender y realizar seguimiento a los eventos que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad o privacidad de la información institucional. El área de sistemas del HEAD será responsable de coordinar la atención inicial de los incidentes y reportar su gestión al Comité Institucional de Seguridad de la Información, el cual evaluará la necesidad de implementar acciones correctivas, actualizar la matriz de riesgos o fortalecer los controles establecidos en el MSPI.

CÓDIGO	FECHA	ACTIVO AFECTADO	TIPO DE INCIDENTE	NIVEL	ESTADO	RESPONSABLE	ACCIONES IMPLEMENTADAS	FECHA DE CIERRE
INC-001					Abierto			
INC-002					En tratamiento			
INC-003					Cerrado			

Tabla 18. Modelo de registro y seguimiento de incidentes.

Los resultados obtenidos serán analizados trimestralmente por el Comité Institucional de Seguridad de la Información y servirán como insumo para la actualización de la matriz de riesgos, el PTRSPI y el Plan de Mejoramiento del MSPI.

INDICADOR	META	FRECUENCIA
Incidentes atendidos dentro del tiempo establecido	≥95%	Trimestral
Tiempo promedio de atención de incidentes	≤24 horas	Trimestral
Incidentes cerrados	≥90%	Trimestral
Incidentes recurrentes	≤10%	Semestral

Tabla 19. Indicadores de gestion.

8.5 AUDITORÍAS Y EVALUACIONES DEL MSPI.

La E.S.E. Hospital Eduardo Arredondo Daza realizará auditorías y evaluaciones periódicas con el propósito de verificar el cumplimiento de los requisitos del MSPI, evaluar la eficacia de los controles implementados e identificar oportunidades de mejora que contribuyan al fortalecimiento de la seguridad y privacidad de la información. Las auditorías serán desarrolladas por la Oficina de Control Interno o por quien haga sus veces, con el apoyo del Comité Institucional de Seguridad de

la Información y el área de sistemas, tomando como referencia la normativa vigente, la ISO/IEC 27001:2022 y los lineamientos del Modelo de Seguridad y Privacidad de la Información.

ACTIVIDAD	FRECUENCIA	RESPONSABLE	EVIDENCIA
Auditoría Interna del MSPI	Anual	Oficina de Control Interno	Informe de auditoría
Evaluación del PTRSPI	Trimestral	Comité de Seguridad	Informe de seguimiento
Evaluación de Indicadores del MSPI	Trimestral	Área sistemas	Tablero de indicadores
Revisión de la Matriz de Riesgos	Semestral	Comité de Seguridad	Matriz actualizada
Evaluación de Controles de Seguridad	Semestral	Área sistemas	Informe técnico

Tabla 20. Auditorías y evaluaciones.

Los resultados de las auditorías y evaluaciones serán presentados al Comité Institucional de Seguridad de la Información y a la Alta Dirección para la definición de acciones correctivas, preventivas y de mejora, las cuales alimentarán el Plan de Mejoramiento del MSPI y contribuirán al proceso de mejora continua del modelo.

Código	Auditoría	Hallazgo	Clasificación	Acción de mejora	Responsable	Estado
AUD-001			Mayor / Menor / Observación			

Tabla 21. Registro de hallazgos.

8.6 EVALUACIÓN DE LA EFICACIA DE LOS CONTROLES.

La E.S.E. Hospital Eduardo Arredondo Daza evaluará periódicamente la eficacia de los controles de seguridad de la información implementados, con el fin de verificar que estos cumplan el propósito para el cual fueron establecidos y contribuyan a reducir los riesgos identificados en la Matriz Institucional de Riesgos. La evaluación se realizará con base en los resultados del monitoreo de controles, la gestión de incidentes, las auditorías internas, el seguimiento al PTRSPI y los indicadores de desempeño del MSPI, permitiendo determinar la necesidad de fortalecer, actualizar o reemplazar los controles existentes.

Código	Control Evaluado	Fuente de Evaluación	Resultado	Eficacia	Acción Requerida	Responsable
EC-001	Políticas de Seguridad de la Información	Auditoría Interna	Conforme	Alta	Mantener control	Comité de Seguridad
EC-002	Gestión de Usuarios y Accesos	Monitoreo de controles	Conforme	Alta	Mantener control	Área sistemas
EC-003	Protección Antimalware	Indicadores y monitoreo	Parcialmente conforme	Media	Fortalecer cobertura y actualización	Área sistemas
EC-004	Copias de Seguridad	Pruebas de restauración	Conforme	Alta	Mantener procedimiento	Área sistemas
EC-005	Gestión de Incidentes	Registro de incidentes	Parcialmente conforme	Media	Optimizar tiempos de respuesta	Área sistemas
EC-006	Capacitación y Sensibilización	Indicadores de capacitación	Conforme	Alta	Continuar ejecución del programa	Talento Humano

Tabla 22. Ejemplo de matriz de evaluación de eficacia de los controles.

FASE 4 – ACTUAR.

9. SEGUIMIENTO, EVALUACIÓN Y DESEMPEÑO DEL MSPI.

La fase Actuar corresponde a la etapa de mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), en la cual la E.S.E. Hospital Eduardo Arredondo Daza analiza los resultados obtenidos durante las fases de implementación y verificación para identificar oportunidades de mejora y fortalecer la eficacia de los controles de seguridad y privacidad de la información. En esta fase se definen e implementan acciones correctivas, preventivas y de mejora orientadas a atender las no conformidades, mitigar riesgos emergentes y optimizar el desempeño del modelo.

Las actividades desarrolladas en esta etapa se fundamentan en los resultados del seguimiento al Plan de Seguridad y Privacidad de la Información (PSPI), el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI), la gestión de incidentes, las auditorías internas, el monitoreo de controles y la evaluación de indicadores. Su ejecución permite mantener actualizado el MSPI, fortalecer el cumplimiento de los requisitos legales y normativos aplicables y consolidar una cultura institucional de seguridad y privacidad de la información basada en el mejoramiento continuo.

9.1 ACCIONES CORRECTIVAS.

Las acciones correctivas corresponden a las medidas adoptadas por la E.S.E. Hospital Eduardo Arredondo Daza para eliminar las causas que originan no conformidades o incumplimientos identificados durante la implementación y operación del MSPI, evitando su recurrencia y fortaleciendo el desempeño de los controles de seguridad y privacidad de la información. Estas acciones podrán derivarse de:

- Resultados de auditorías internas o externas.
- Incidentes de seguridad de la información.
- Hallazgos del seguimiento al PSPI y al PTRSPI.
- Incumplimiento de indicadores del MSPI.
- Revisiones efectuadas por el Comité Institucional de Seguridad de la Información.
- Evaluaciones realizadas por organismos de control.

Una vez identificada la no conformidad, deberá realizarse el análisis de causa, definir la acción correctiva, asignar un responsable, establecer un plazo de ejecución y verificar posteriormente la eficacia de la acción implementada.

Código	No conformidad	Causa raíz	Acción Correctiva	Responsable	Fecha compromiso	Estado	Evidencia
AC-001							
AC-002							

Tabla 23. Modelo de control de acciones correctivas.

9.2 ACCIONES PREVENTIVAS.

Las acciones preventivas tienen como finalidad anticiparse a la ocurrencia de incidentes o incumplimientos, mediante la identificación de oportunidades de mejora y la implementación de controles que reduzcan la probabilidad de materialización de riesgos. Estas acciones podrán originarse a partir de:

- Cambios tecnológicos.
- Nuevas amenazas y vulnerabilidades.
- Actualización de la matriz de riesgos.
- Cambios normativos.
- Recomendaciones derivadas de auditorías.
- Resultados del monitoreo de controles.
- Seguimiento a indicadores del MSPI.

Código	Riesgo identificado	Acción Preventiva	Responsable	Prioridad	Fecha compromiso	Estado
AP-001				Alta		
AP-002				Media		

Tabla 24. Modelo de control de acciones preventivas.

9.3 PLAN DE MEJORAMIENTO DEL MSPI.

El Plan de Mejoramiento del MSPI consolida las acciones correctivas, preventivas y de mejora definidas por la Entidad como resultado del seguimiento y evaluación del modelo. Este plan constituye el principal instrumento para garantizar la evolución permanente del sistema de gestión de seguridad y privacidad de la información, permitiendo realizar seguimiento a los compromisos adquiridos y verificar su cumplimiento. Las acciones incluidas en este plan podrán provenir de:

- Auditorías.
- Evaluación de indicadores.
- Seguimiento al PSPI.
- Seguimiento al PTRSPI.
- Gestión de incidentes.
- Evaluación de riesgos.
- Revisión por la Alta Dirección.

Código	Fuente	Hallazgo	Acción de mejora	Responsable	Plazo	Estado	% Avance
PM-001	Auditoría						
PM-002	Incidente						
PM-003	Indicadores						

Tabla 25. Modelo para plan de mejoramiento.

9.4 MEJORA CONTÍNUA DEL MSPI.

La mejora continua constituye el principio fundamental para garantizar la sostenibilidad y evolución del Modelo de Seguridad y Privacidad de la Información en la E.S.E. Hospital Eduardo Arredondo Daza. Su finalidad es asegurar que el modelo permanezca actualizado frente a los cambios tecnológicos, organizacionales, normativos y de riesgos que puedan afectar la seguridad y privacidad de la información institucional. Como resultado de la aplicación del ciclo PHVA, la entidad realizará revisiones periódicas al MSPI con el propósito de actualizar, cuando sea necesario:

- La Política de Seguridad y Privacidad de la Información.
- El Plan de Seguridad y Privacidad de la Información (PSPI).
- El Plan de Tratamiento de Riesgos (PTRSPI).
- La Matriz de Riesgos de Seguridad y Privacidad de la Información.
- El Inventario y Clasificación de Activos de Información.
- Los controles administrativos, físicos y tecnológicos.
- Los indicadores de gestión del MSPI.
- Los programas de sensibilización y capacitación.
- Los procedimientos relacionados con la gestión de incidentes y continuidad de la operación.

El Comité Institucional de Seguridad de la Información será responsable de revisar periódicamente los resultados obtenidos, evaluar la eficacia del MSPI y recomendar las acciones necesarias para fortalecer el nivel de madurez del modelo, promoviendo una cultura institucional de seguridad y privacidad de la información.

9.5 REVISIÓN POR LA ALTA DIRECCIÓN.

La revisión por la Alta Dirección constituye un mecanismo estratégico para evaluar la eficacia, pertinencia y desempeño del Modelo de Seguridad y Privacidad de la Información (MSPI) en la E.S.E. Hospital Eduardo Arredondo Daza. Su propósito es verificar que el modelo continúe siendo adecuado para apoyar el cumplimiento de los objetivos institucionales, responder a los cambios del entorno y garantizar la protección de los activos de información de la Entidad.

Esta revisión será liderada por la Gerencia, con el apoyo del Comité Institucional de Seguridad y Privacidad de la Información y las dependencias responsables de la gestión de tecnologías de la información. Como resultado de este proceso, la Alta Dirección podrá definir lineamientos, aprobar acciones de mejora, asignar recursos y establecer prioridades para el fortalecimiento continuo del MSPI. La revisión se realizará como mínimo una (1) vez al año, o cuando se presenten cambios significativos en el contexto institucional, modificaciones normativas, incidentes de seguridad de alto impacto, cambios tecnológicos relevantes o resultados de auditorías que requieran decisiones estratégicas. Los aspectos a evaluar durante la revisión por la Alta Dirección son los siguientes:

- Estado de implementación y cumplimiento del Plan de Seguridad y Privacidad de la Información (PSPI).
- Avance en la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI).
- Resultados del seguimiento a los indicadores de gestión del MSPI.
- Estado de los riesgos de seguridad y privacidad de la información.
- Resultados del monitoreo de controles de seguridad.
- Gestión de incidentes de seguridad de la información y lecciones aprendidas.
- Resultados de auditorías internas y externas.
- Cumplimiento de los requisitos legales, regulatorios y normativos aplicables.
- Estado de las acciones correctivas, preventivas y del Plan de Mejoramiento.
- Necesidades de recursos humanos, tecnológicos, financieros y de capacitación para el fortalecimiento del MSPI.
- Resultados esperados de la revisión

Con el desarrollo de la fase Actuar, la E.S.E. Hospital Eduardo Arredondo Daza consolida el ciclo de mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), estableciendo los mecanismos necesarios para evaluar los resultados obtenidos, implementar acciones de mejora y fortalecer permanentemente la gestión de la seguridad y privacidad de la información.

Las acciones correctivas, preventivas y de mejora definidas en este capítulo permiten que el Modelo evolucione de manera sistemática, incorporando las lecciones aprendidas, los resultados de auditorías, la gestión de incidentes, el seguimiento a los indicadores y la actualización de la matriz de riesgos como insumos para la toma de decisiones y el fortalecimiento de los controles institucionales.

De esta manera, se dispone de un Modelo de Seguridad y Privacidad de la Información alineado con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Política de Gobierno Digital y las buenas prácticas establecidas en la norma ISO/IEC 27001:2022, promoviendo una gestión integral de la seguridad de la información que contribuya a la protección de los activos de información, la continuidad de los servicios institucionales y el cumplimiento de los objetivos estratégicos de la Entidad.

Finalmente, la mejora continua deberá asumirse como un compromiso permanente de la Alta Dirección, el Comité Institucional de Seguridad y Privacidad de la Información y todos los servidores y colaboradores de la E.S.E. Hospital Eduardo Arredondo Daza, garantizando que el MSPI permanezca actualizado, responda a los cambios del entorno tecnológico y normativo, y continúe fortaleciendo la capacidad institucional para gestionar los riesgos de seguridad y privacidad de la información.

10. ARTICULACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) CON EL PLAN DE TRANSICIÓN DE IPv4 A IPv6.

La transición del protocolo de Internet versión 4 (IPv4) hacia el protocolo versión 6 (IPv6) representa un proceso estratégico para todas las entidades públicas, orientado a garantizar la continuidad de los servicios institucionales, mejorar la interoperabilidad entre plataformas tecnológicas y fortalecer las capacidades de conectividad y crecimiento de la red institucional.

En este contexto, el Modelo de Seguridad y Privacidad de la Información (MSPI) constituye un elemento transversal para la implementación del Plan de Transición de IPv4 a IPv6, proporcionando el marco de gestión necesario para identificar, evaluar y tratar los riesgos asociados a dicho proceso, así como para definir los controles administrativos, físicos y tecnológicos que permitan preservar la confidencialidad, integridad, disponibilidad y autenticidad de la información durante todas las etapas de la transición.

La implementación del Plan de Transición deberá desarrollarse de manera coordinada con los procesos de gestión de riesgos, gestión de activos de información, gestión de cambios, continuidad del negocio, gestión de incidentes y monitoreo de controles establecidos en el MSPI, garantizando que la adopción de IPv6 se realice de forma planificada, segura y conforme con las necesidades institucionales.

De igual manera, las actividades contempladas en el Plan de Transición deberán articularse con el Plan Estratégico de Tecnologías de la Información (PETI), el Plan de Seguridad y Privacidad de la Información (PSPI), el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) y los demás instrumentos de gestión institucional relacionados con el Gobierno Digital, de manera que las decisiones tecnológicas contribuyan al fortalecimiento de la seguridad de la información, la continuidad de los servicios y el cumplimiento de los objetivos estratégicos de la Entidad.

En consecuencia, el presente MSPI establece los lineamientos generales que deberán ser considerados durante la planeación, implementación, seguimiento y mejora del proceso de transición hacia IPv6, mientras que el Plan de Transición de IPv4 a IPv6 se desarrollará como un documento técnico independiente, en el cual se definirán el diagnóstico de la infraestructura tecnológica, el plan de direccionamiento, las actividades de migración, el cronograma de implementación, los recursos requeridos, los mecanismos de seguimiento y los controles específicos asociados al proceso de transición tecnológica.

10.1 RELACIÓN DEL MSPI CON EL PLAN DE TRANSICIÓN DE IPV4 A IPV6.

La implementación del Plan de Transición de IPv4 a IPv6 deberá apoyarse en los procesos y componentes definidos dentro del Modelo de Seguridad y Privacidad de la Información (MSPI), garantizando que la incorporación del nuevo protocolo se realice bajo criterios de seguridad, gestión del riesgo y mejora continua. La siguiente tabla presenta la relación entre los principales componentes del MSPI y las actividades que deberán desarrollarse durante la transición hacia IPv6.

Componente del MSPI	Aplicación en la Transición IPv4/IPv6
Gestión de Activos de Información	Identificación de equipos, aplicaciones y servicios compatibles con IPv6.
Gestión de Riesgos	Identificación, análisis y tratamiento de riesgos asociados al proceso de transición.
Gestión de Cambios	Control y autorización de las modificaciones realizadas sobre la infraestructura tecnológica.
Gestión de Configuración	Actualización segura de servidores, dispositivos de red y aplicaciones institucionales.
Gestión de Incidentes	Atención y tratamiento de incidentes derivados de la implementación de IPv6.
Monitoreo de Controles	Verificación permanente del funcionamiento de los controles implementados durante la transición.
Continuidad del Negocio	Garantizar la disponibilidad de los servicios institucionales durante el proceso de migración.
Auditoría y Seguimiento	Evaluación del cumplimiento del Plan de Transición y de los controles de seguridad implementados.
Mejora Continua	Actualización permanente del proceso de transición con base en los resultados obtenidos y las lecciones aprendidas.

Tabla 26. Relación MSPI y migración a IPv6.

10.2 LINEAMIENTOS GENERALES PARA UNA TRANSICIÓN SEGURA HACIA IPV6.

Con el propósito de garantizar que la transición hacia IPv6 se desarrolle de manera organizada, controlada y alineada con los objetivos institucionales, la E.S.E. Hospital Eduardo Arredondo Daza deberá considerar, como mínimo, los siguientes lineamientos:

- Realizar el diagnóstico del estado actual de la infraestructura tecnológica y determinar el nivel de preparación para la adopción de IPv6.

- Mantener actualizado el inventario de activos tecnológicos, identificando la compatibilidad de hardware, software, aplicaciones y servicios con el protocolo IPv6.
- Incorporar la gestión de riesgos de seguridad de la información como parte integral del proceso de transición, definiendo los controles necesarios para reducir los riesgos identificados.
- Implementar la transición de manera gradual, priorizando los servicios críticos y minimizando el impacto sobre la operación institucional.
- Garantizar que los cambios realizados en la infraestructura tecnológica sean gestionados mediante procedimientos formales de gestión de cambios y gestión de configuración.
- Realizar pruebas funcionales, de interoperabilidad y de seguridad antes de la puesta en producción de los servicios que operarán bajo IPv6.
- Capacitar al personal técnico responsable de la administración de la infraestructura tecnológica en aspectos relacionados con el direccionamiento, configuración, operación y seguridad del protocolo IPv6.
- Implementar mecanismos de monitoreo permanente que permitan verificar el desempeño, disponibilidad y seguridad de los servicios implementados sobre IPv6.
- Actualizar la documentación técnica, los procedimientos operativos y los planes institucionales cuando se incorporen nuevos servicios o componentes tecnológicos basados en IPv6.
- Realizar seguimiento periódico al avance del Plan de Transición, incorporando las acciones de mejora necesarias para garantizar el cumplimiento de los objetivos definidos.

10.3 ESTADO ACTUAL DE LA TRANSICIÓN IPV4 - IPV6 EN LA ESE HOSPITAL EDUARDO ARREDONDO DAZA.

Como parte del diagnóstico de la infraestructura tecnológica realizado durante la formulación del Plan Estratégico de Tecnologías de la Información (PETI) y del Modelo de Seguridad y Privacidad de la Información (MSPI), se evaluó el estado de la red institucional, los servicios tecnológicos y la capacidad de la infraestructura para soportar la transición del protocolo IPv4 hacia IPv6.

Los resultados del análisis evidencian que, en las condiciones actuales de operación de la E.S.E. Hospital Eduardo Arredondo Daza, **no existe una necesidad inmediata de ejecutar un proceso de migración hacia IPv6, debido a que la infraestructura tecnológica, el número de servicios publicados, el esquema de direccionamiento IP y las necesidades de conectividad institucional continúan siendo adecuadamente soportados mediante el protocolo IPv4**.

No obstante, considerando los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las tendencias de evolución tecnológica, la Entidad reconoce la importancia de prepararse para una futura adopción del protocolo IPv6, garantizando

que dicho proceso se realice de manera planificada, segura y conforme a las necesidades institucionales.

ASPECTO EVALUADO	ESTADO ACTUAL
Infraestructura de red	Opera adecuadamente sobre IPv4.
Direccionamiento IP	Suficiente para las necesidades institucionales actuales.
Servicios publicados	No requieren direccionamiento IPv6 en la actualidad.
Compatibilidad tecnológica	La mayoría de los equipos soportan IPv6, pero su habilitación no es requerida actualmente.
Necesidad de migración	No prioritaria.
Recomendación	Mantener seguimiento a los lineamientos de MinTIC y revisar el diagnóstico durante las actualizaciones del PETI y del MSPI.

Tabla 27. Diagnóstico de la migración IPv4 a IPv6 en el HEAD.

10.4 CONSIDERACIONES FINALES.

La implementación del Plan de Transición de IPv4 a IPv6 deberá entenderse como un proceso gradual y continuo, que involucra aspectos tecnológicos, administrativos y de seguridad de la información. En consecuencia, su ejecución requerirá la participación coordinada de la Alta Dirección, el Área de Tecnologías de la Información, el Comité Institucional de Seguridad y Privacidad de la Información y las demás dependencias involucradas en la gestión de los servicios tecnológicos.

El Modelo de Seguridad y Privacidad de la Información proporcionará el marco de referencia para gestionar los riesgos asociados a la transición, establecer los controles necesarios y realizar el seguimiento a las actividades implementadas, asegurando que la adopción del protocolo IPv6 contribuya al fortalecimiento de la infraestructura tecnológica institucional y al cumplimiento de los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

ANEXO 1.

- Tabla de gestión de activos de información del Hospital Eduardo Arredondo Daza.

ANEXO 2.

- Matriz institucional de riesgos del Hospital Eduardo Arredondo Daza.