1. INTRODUCCIÓN

El presente documento define un modelo, y se elabora en virtud del cumplimiento de la estrategia de gobierno en línea como requisito para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo hacia el desarrollo del Modelo de Seguridad y Privacidad de la Información

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Dentro de La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, se tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la **ESE Hospital San Juan de Dios de Ituango Antioquia** está determinado, entre otros, por las necesidades y objetivos, los requisitos de seguridad y los procesos misionales.

El plan de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se proyectarán un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales se convertirán en políticas de cumplimiento de la institución, a fin, como ya se ha dicho, de mejoras mejorar nuestros estándares de seguridad de la información.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

De otro lado el MSPI especifica los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. A través del mismo se pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

2. JUSTIFICACIÓN

La **ESE Hospital San Juan de Dios de Ituango Antioquia** requiere avanzar dentro de la estrategia de Gobierno en línea, a través de las directrices exigidas por el Ministerio TIC, al cumplir con la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, a fin de contribuir dentro de la construcción de un Estado más eficiente, más transparente y participativo.

La adopción de un plan de Seguridad y Privacidad de la Información para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea, permitirá un mejor aprovechamiento de las TIC, a lo cual se trabajará en el fortalecimiento de la seguridad de la información dentro de la institución, pues se hace más que necesario garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, acorde con lo expresado en la legislación Colombiana.

3. MARCO NORMATIVO

3.1 Marco conceptual

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma. En este sentido, el Sistema de Gestión de Seguridad de la Información ISO 27001 persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada.

Los términos seguridad de la información, seguridad informática y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la

confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Entre dichos términos existen pequeñas diferencias, y dichas diferencias proceden del enfoque que le dé, las metodologías usadas y las zonas de concentración.

La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. Estos pueden ser:

☐ Electrónicos
☐ En papel
☐ Audio y vídeo, etc.

Los gobiernos, las instituciones financieras, los hospitales y las organizaciones privadas tienen enormes cantidades de información confidencial sobre sus empleados, productos, investigación, clientes, etc. La mayor parte de esta información se debe clasificar como reservada o pública según estipula norma. Si se da el caso de que información confidencial de la organización, de sus clientes, de sus decisiones, de sus cuentas, etc. caen en manos no autorizadas, esto podría acarrear demandas o sanciones para la institución.

3.2 Definiciones

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

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a

los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

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

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

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

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

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

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

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

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

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

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

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

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

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

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

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

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

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la

información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

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

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

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

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

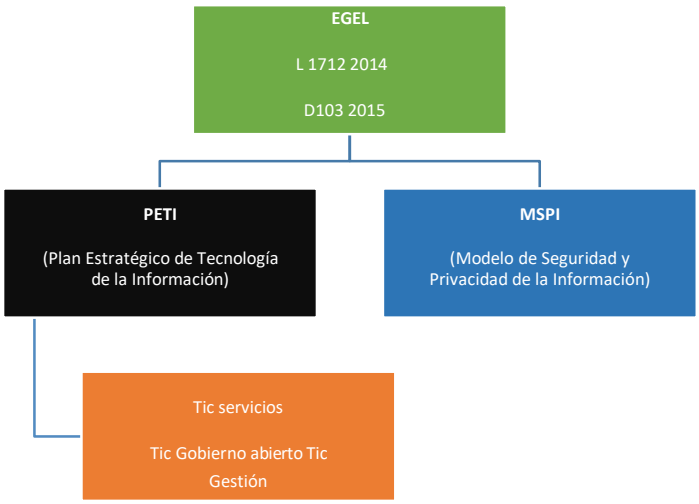
Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

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

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

3.3 Estructura y marco normativo general



4. Marco Legal

NORMATIVIDAD	DEFINICIÓN
Ley 1581 de 2012	Establece disposiciones generales para la protección de datos personales y los principios rectores para su tratamiento.
Decreto 1377 de 2013	Reglamenta aspectos relacionados con la autorización y tratamiento de datos personales.
Sentencia C-748 de 2011	Define el habeas data y la protección constitucional de los datos personales.
Decreto 1008 de 2018	Adopta la Política de Gobierno Digital en Colombia.
Política de Seguridad y Privacidad de la Información – MinTIC (MSPI)	Lineamientos para la gestión de riesgos, seguridad y privacidad en entidades públicas.
Guía de Gestión de Riesgos de Seguridad y Privacidad MinTIC	Instrumento obligatorio para la gestión de riesgos en el sector público.

NORMATIVIDAD	DEFINICIÓN
(2022)	
Ley 594 de 2000 – Ley General de Archivos	Define disposiciones para la administración, conservación y custodia de documentos físicos y electrónicos.
Acuerdo AGN 006 de 2015	Lineamientos para documentos electrónicos de archivo y gestión de riesgos asociados a su preservación.
Ley 1712 de 2014	Regula el derecho al acceso a la información pública y determina obligaciones asociadas a la clasificación y reserva de la información.
Decreto 1081 de 2015	Reglamenta parcialmente la Ley 1712.
Ley 2015 de 2020	Regula la Historia Clínica Electrónica Interoperable (HCEI).
Resolución 1995 de 1999	Regula la historia clínica, su manejo, custodia, acceso y reserva.
Resolución 5109 de 2015	Establece lineamientos de seguridad para la información del sistema de salud.
ISO/IEC 27001:2022	Estándar internacional para establecer un Sistema de Gestión de Seguridad de la Información (SGSI).

5. OBJETIVO GENERAL

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

5.1. OBJETIVOS ESPECIFICOS

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Implementar mejores prácticas de seguridad que permita identificar infraestructuras críticas.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Desarrollar mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de la **ESE Hospital San Juan de Dios de Ituango Antioquia**.
- Migrar de lPv4 a IPv6 con la utilización de las guías disponibles para tal fin.

- Aplicar, dentro del tratamiento de la información de usuarios, la legislación relacionada con la protección de datos personales (Ley estatutaria 1266 de 2008).
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.
- Mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Facilitar la labor de acceso a la información pública relacionada con la **ESE Hospital San Juan de Dios de Ituango Antioquia.**
- Promover los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.
- Forma parte integral de la estrategia GEL A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones. Se definen 5 fases: Diagnóstico, Planificación, implementación, evaluación de desempeño, mejoramiento continuo

6. ALCANCE

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

7. GUÍA METODOLÓGICA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la **ESE Hospital San Juan de Dios de Ituango Antioquia**, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y el ciclo de operaciones que determinan los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de sus decretos.

Para cada una de las fases del proceso se plantea una descripción detallada de los mismos junto a sus objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de la entidad.

Acorde a lo anterior se definen las siguientes 5 fases:

- Diagnóstico
- Planeación
- Implementación
- Evaluación
- Mejora continua

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

MATRIZ DOFA		
D2 Falta de un programa continuo de capacitación en seguridad y privacidad para personal asistencial y administrativo.	**DO 2 Gestionar proyectos ante la Gobernación o MinTIC para modernizar infraestructura y adquirir SIEM.**	**DA 2 Priorizar recursos en infraestructura esencial y servicios de misión crítica.**
D3 Dependencia de infraestructura tecnológica con soporte próximo a vencer.	**DO 3 Documentar y actualizar el inventario de activos de información y sus riesgos.**	**DA 3 Realizar seguimientos periódicamente la matriz de riesgos institucional y los planes de tratamiento según cambios del entorno.**
D4 Falta de consolidación de una cultura institucional orientada a la protección de la información.	**DO4 Integrar la seguridad digital en la planeación estratégica y en los comités de gestión y control.**	**DA 4 Dar continuidad y mejora a las evaluaciones anuales de cumplimiento del MSPI y políticas de seguridad, en articulación con Control Interno.**

8. RESPONSABLE DEL PLAN

Gestión TICs

9. DESARROLLO DEL PLAN

Fase de Diagnóstico Objetivos

- Identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad.
- Proceder al desarrollo se la fase de planificación una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez en la **ESE Hospital San Juan de Dios de Ituango Antioquia.**
- Revisar y socializar con las partes interesadas dentro de la institución, los resultados asociados a la fase de diagnóstico previas a la implementación

Figura 2 – Etapas previas a la implementación

Metas a alcanzar:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.

- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en Ciberseguridad.

Actividades

- Diligenciar una herramienta de diagnóstico que permita determinar el estado actual de la seguridad y privacidad de la información
- Diligenciar una herramienta para determinar el nivel de madurez de los controles de seguridad de la información
- Efectuar pruebas de vulnerabilidad y elaborar documento con los hallazgos encontrados
- Evaluar el avance de la implementación del ciclo de operaciones al interior de la entidad
- Evaluar el nivel de cumplimiento con la legislación vigente, relacionado con protección de datos personales.
- Evaluar el uso frente a prácticas de Ciberseguridad

Instrumentos a utilizar:

- Herramientas de diagnostico
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad

Fase de planificación Objetivos

- Utilizar los resultados de la fase de Diagnóstico para elaborar la política de seguridad y privacidad de la información alineada con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, y a través de una metodología de gestión del riesgo.
- Determinar el alcance del MSPI, extendiéndolo por procesos a todas las dependencias de la institución, teniendo en cuenta los procesos que impacten directamente la consecución de los objetivos misionales, todos los demás procesos relacionados, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelacionados

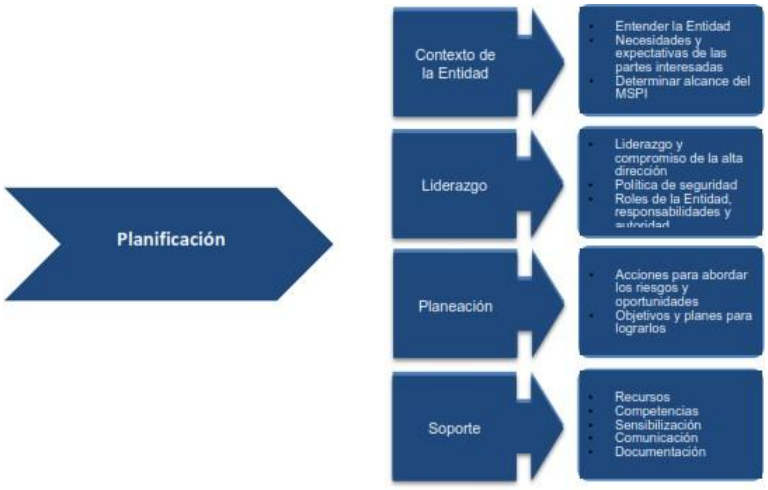


Figura 3 - Fase de planificación[1]

Metas, resultados e instrumentos de la fase de planificación

Metas	Resultados
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta dirección y socializado al interior de la entidad
Política de seguridad y Privacidad de la Información	Manual con la política de seguridad de la información, debidamente aprobado por la alta dirección y socializado al interior de la entidad
Procedimientos de seguridad de la información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.

Metas	Resultados
Inventario de activos de información	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.
Identificación, Valoración tratamiento de riesgo.	• Documento con la metodología de gestión de riesgos. • Documento con el análisis y evaluación de riesgos. • Documento con el plan de tratamiento de riesgos. • Documento con la declaración de aplicabilidad. • Documentos revisados y aprobados por la alta Dirección.
Plan de comunicación	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

Fase de implementación

Objetivo

Llevar a cabo la implementación acorde con los preceptos de planificación realizados en la etapa anterior

Procesos

Figura 4 - Fase de implementación[2]

Metas, resultados e instrumentos de la fase de implementación

Metas	Resultados
Planificación y control operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.

Actividades a realizar en la fase de implementación

- Planificación y control operacional
- Implementación del plan de tratamiento de riesgos
- Indicadores de gestión para medir:

1. Efectividad de los controles
2. Eficiencia del MSPI al interior de la entidad
3. Proveer estados de seguridad que sirvan de guía en las revisiones y las mejoras continuas
4. Comunicar valores de seguridad al interior de la entidad
5. Servir como insumo al plan de control operacional

- Plan de transición de IPV4 a IPV6

Fase evaluación de desempeño

Objetivos

- Realizar un proceso de monitoreo y desempeño del MSPI con base a los resultados que arrojan los indicadores de seguridad propuestos para verificación de efectividad, eficiencia y la eficacia de las acciones implementadas
- Permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas mediante el análisis de causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

Figura 5 - Fase de Evaluación de desempeño[3]

Metas	Resultados
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

Actividades

Meta: Plan de revisión y seguimiento a la implementación del MSPI

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.

- Revisión de la evaluación de los niveles de y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI
- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI) Meta: Plan de ejecución de auditorías
- Documentar el plan de auditorías para MSPI especificando la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes
- Llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz.
- Difundir a las partes interesadas los resultados de la ejecución de auditorías
- Conservar la información documentada como evidencia de los resultados de las auditorías

Fase de mejoramiento continuo

Objetivo

- Consolidar los resultados obtenidos de la fase de evaluación de desempeño para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.
- Definir y ejecutar un plan de mejora continua con base en los resultados de la evaluación del desempeño

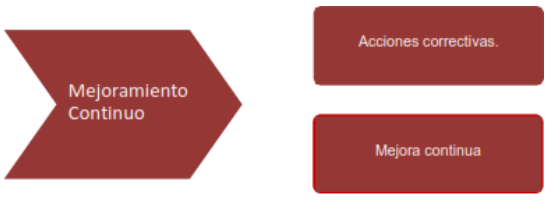


Figura 6 - Fase de mejoramiento continúo[4]

Metas	Resultados
Plan de mejora continua	• Documento con el plan de mejoramiento. • Documento con el plan de comunicación de resultados.

Actividades

- Obtener los resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI
- Obtener los resultados del plan de ejecución de auditorías y revisiones independientes al MSPI
- Efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI
- Plan de mejoramiento y de comunicación de mejora continua revisados y aprobados por la alta dirección para que se revisen las decisiones, cambios, prioridades, etc., tomadas en comités y que impacten en el MSPI.

Entregables

- Acta de reunión y/o conformación del comité
- Informe de evaluación del componente Seguridad y Privacidad de la información donde se especifiquen el nivel de los indicadores de cumplimiento acorde con el artículo 10 del decreto 1078 de 2015
- Producto de cada etapa

10. PUNTOS DE CONTROL

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

Nº	Actividad / Estrategia	Control Asociado	Responsable	Frecuencia	Evidencia
	Seguridad y Privacidad.		Seguridad de la información		
4	Actualizar el Plan de Contingencia y DRP para cubrir incidentes cibernéticos y fallas críticas.	Continuidad del negocio	Gestión de la información	Anual	Versión actualizada del DRP, simulacros
5	Realizar campañas internas de protección de datos y cultura digital segura.	Protección de datos personales	Gestión de la información / Oficial de la seguridad de la información	Trimestral	Material de campaña, registros de difusión
6	Priorizar la renovación de infraestructura tecnológica próxima a vencer soporte.	Ciclo de vida de activos	Subgerencia Administrativa / Gestión de la información	Semestral	Cotizaciones, actas, plan de renovación
9	Implementar herramientas EDR/XDR para detección temprana de amenazas.	Detección y respuesta	Oficial de la seguridad de la información	Trimestral	Reportes EDR, registros de alertas
10	Realizar seguimiento continuo a la matriz de riesgos y su plan de tratamiento.	Monitoreo de riesgos	Oficial de la seguridad de la información	Trimestral	Matriz actualizada, informes de seguimiento
11	Actualizar las políticas institucionales de seguridad y privacidad según normativa (MSPI, Ley 1581).	Políticas y normatividad	Gestión de la información / Oficial de la seguridad de la información	Anual	Políticas revisadas, resoluciones, actas
12	Mantener indicadores de gestión de seguridad y privacidad para evaluar la eficacia de los controles.	Indicadores MSPI	Gestión de la información / Oficial de la seguridad de la información	Trimestral	Tablero de indicadores, informes
13	Evaluar periódicamente la efectividad del firewall perimetral y mecanismos de respaldo.	Seguridad perimetral / Backups	Oficial de la seguridad de la información	Trimestral	Logs de firewall, reportes de respaldo

Nº	Actividad / Estrategia	Control Asociado	Responsable	Frecuencia	Evidencia
14	Formalizar acuerdos SLA con proveedores críticos (ERP, hosting, soporte).	Gestión de proveedores	Gestión de la información	Semestral	Contratos actualizados, informes SLA
15	Integrar evidencia documental al sistema de gestión documental electrónico para auditorías.	Gestión documental	Gestión de la información	Trimestral	Evidencias cargadas, actas, reportes de auditoría

11. INDICADORES Y METAS

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

NOMBRE	FORMULA	META	FRECUENCIA	RESPONSABLE
Porcentaje de ataques informáticos Controlados al sistema de información	número de ataques controlados en el periodo/ Total de ataques informáticos en el periodo*100	99%	Mensual	Mesa de servicio
Porcentaje de Inspecciones o Rondas de seguridad de la información realizadas en el periodo	Cantidad de inspecciones de seguridad realizadas / total de inspecciones de seguridad programadas*100	98%	Mensual	Mesa de servicio
Porcentaje de cumplimiento del programa de capacitación y entrenamiento de TI	Número de actividades del plan de capacitación institucional ejecutadas en el período / Número de actividades del plan de capacitación institucional programadas en el período *100	80%	Mensual	Mesa de servicio
Porcentaje de gestión de la calidad Dato de la **ESE Hospital San Juan de Dios de Ituango Antioquia**	Número de inconsistencias encontradas / Total de reportes revisados *100.	10%	Mensual	Mesa de servicio
Porcentaje de daños de los equipos tecnológicos no biomédicos.	Número de equipos dañados no biomédicos / Total de equipos no biomédicos en el área *100	1%	Mensual	Mesa de servicio

Notas:

Control de Cambios:

VERSION	Fecha	Descripción de los cambios realizados	Responsable
V-01	30/01/2025	Creación del MDC-21 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Control Interno
V-02	30/01/2026	Actualización MDC-21 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Asesora de Control Interno

Mariell Carolina Ramírez Quintero
Gerente
ESE Hospital San Juan de Dios de Ituango Antioquia