PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024
HOSPITAL SAN JUAN BAUTISTA ESE

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA ACTUALIZACIÓN
2	28/01/2019	Revisión y actualización general del documento
3	23/01/2012	6. Objetivos del Sistema de Gestión de Seguridad de la Información 9. Actividades de Seguridad y Privacidad de la Información
4	28/01/2021	9. Actividades de Seguridad y Privacidad de la Información
5	09/12/2021	1.Objetivos, Alcance 4. Marco Normativo. 5.Politica de Seguridad de la Información. 10. Estado Actual. 12 actividades de Seguridad y Privacidad de la Información
6	01/01/2023	10. Estado Actual. 12 actividades de Seguridad y Privacidad de la Información
7	25/01/2024	Introducción. Justificación. 12 actividades de Seguridad y Privacidad de la Información

Elaboró: Líder de Gestión de Sistemas Informaticos	**Actualizó:** Líder de Gestión de Sistemas Informaticos	**Revisó**: Comité de Gestión y Desempeño MIPG	**Aprobó**: Comité de Gestión y Desempeño MIPG
Cargo: Técnico Administrativo de Sistemas	**Cargo:** Profesional Universitario	**Cargo:** Comité de Gestión y Desempeño MIPG	**Cargo:** Comité de Gestión y Desempeño MIPG
Fecha:06/06/2018	**Fecha**:24/01/2024	**Fecha**: 25/01/2024	**Fecha**: 25/01/2024

TABLA DE CONTENIDO

INTRODUCCIÓN

El Hospital San Juan Bautista E.S.E, reconoce y determina la Información como un activo de gran valor e importancia que permite el desarrollo y ejecución de los procesos de planeación estratégica, misionales, de apoyo administrativo, evaluación y control, permitiendo que los objetivos descritos en el plan de gestión y de desarrollo de la alta gerencia sean ejecutados de acuerdo con los lineamientos establecidos, garantizando los principios de Seguridad – Integridad y disponibilidad de la información.

El presente Plan de Seguridad y Privacidad de la Información permite establecer la adopción del Instrumento Modelo de Seguridad y Privacidad de la Información y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de la ESE un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; este modelo consta de cinco fases (Diagnóstico, Planificación, Operación, Evaluación de desempeño, Mejoramiento Continuo), las cuales permite que la ESE puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información.

JUSTIFICACIÓN

En el contexto actual, la información se constituye como el activo más valioso y vulnerable de cualquier organización. La creciente complejidad del avance tecnológico y la sofisticación de las amenazas cibernéticas y riesgos en la seguridad de la información demandan una respuesta estratégica sólida y proactiva por parte de la ESE. La implementación de un plan de seguridad y privacidad de la información no solo es una necesidad que predomina en la actualidad, sino una inversión estratégica crucial para garantizar la sostenibilidad y el crecimiento de la ESE frente a la toma de decisiones basadas en las fuentes de información y caracterización de los servicios prestados.

La información que gestionamos a través de los diferentes procesos contempla desde datos sensibles de usuarios y pacientes hasta la propiedad intelectual que impulsa el mejoramiento de la calidad de la prestación de nuestros servicios hacia la comunidad. Un plan de seguridad y privacidad robusto garantizará la protección de estos activos críticos, evitando la pérdida, el robo o la alteración no autorizada de la información que es esencial para el cumplimiento de las estrategias establecidas en el plan de desarrollo y de gestión definidas en la ESE.

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2022-2024.

1.1. OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Adoptar el modelo de seguridad y privacidad de la información MSPI MINTIC.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

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

El plan de Seguridad y Privacidad de la Información se aplica a todos los procesos y funcionarios, Contratistas, terceros que tienen relación alguna o hacen parte del hospital San Juan Bautista E.S.E.

3. TERMINOS Y 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/IEC27000).

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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

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

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

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

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

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 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.

4. MARCO NORMATIVO

- Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

- Manual de Gobierno Digital – MINTIC.

- Modelo de Seguridad y Privacidad de la Información – MINTIC.

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.

- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.

- Ley 594 de 2000 - Ley General de Archivos.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

- Decreto 2364 de 2012 - Firma electrónica.
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.
- Ley 527 de 1999 - Ley de Comercio Electrónico.
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
- Ley Estatutaria 1581 de 2012 - Protección de datos personales.
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

5. POLITICA DE TRATAMIENTO DE LA INFORMACION

El HOSPITAL SAN JUAN BAUTISTA E.S.E., en cumplimiento de la ley estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013, sobre la privacidad y protección de datos personales en Colombia, asegura el manejo adecuado de la información que obtenga, registra, use, transmita y actualice mediante la autorización previa, expresa y voluntaria del titular de la información y actúa como responsable del tratamiento y custodia de los datos personales que por virtud de sus funciones y competencias legales establecidas le han sido suministradas a la entidad, con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (Civil, Comercial y/o Laboral etc.), incluyendo pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas).

En virtud de los procesos misionales y administrativos del Hospital San Juan Bautista E.S.E, enmarcados en los modelos de atención tratamientos médicos, se compromete que la información recolectada, almacenada, usada, transferida o eliminada tendrá los procesos adecuados y documentados con las descripciones de acuerdo a las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso que establezca la ley y normatividad vigente.

Dado en el municipio de chaparral, a los 9 días del mes enero de 2018.

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de _HOSPITAL SAN JUAN BAUTISTA E.S.E. con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El HOSPITAL SAN JUAN BAUTISTA E.S.E., para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de
- seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios,
- terceros, aprendices, practicantes y clientes del HOSPITAL SAN JUAN BAUTISTA E.S.E.
- Garantizar la continuidad de los servicios frente a incidentes.

6.1. Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del HOSPITAL SAN JUAN BAUTISTA E.S.E. y los usuarios en general.

6.2. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI del HOSPITAL SAN JUAN BAUTISTA E.S.E.:

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. protegerá su información de las amenazas originadas por parte del personal.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. implementará control de acceso a la información, sistemas y recursos de red.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• El HOSPITAL SAN JUAN BAUTISTA E.S.E. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• HOSPITAL SAN JUAN BAUTISTA E.S.E. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

• HOSPITAL SAN JUAN BAUTISTA E.S.E. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7. OBJETIVOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

- Adoptar Modelo de Seguridad y Privacidad de la información MSPI de acuerdo con los lineamientos de la Política de Gobierno Digital para la implementación del Sistema de Gestión de Seguridad de la Información SGSI.
- Implementar el SGSI y fortalecer los controles de protección de los activos de la información.
- Minimizar los riesgos de seguridad de la información mediante la ejecución de las políticas de seguridad.
- Garantizar la Seguridad, Confidencialidad y Disponibilidad de la información de acuerdo con el SGSI y normas vigentes que lo reglamente.
- Prevenir y controlar los incidentes de seguridad de la información.
- Construir una cultura en seguridad de la información en los procesos misionales, administrativos y financieros de la E.S.E.
- Mejorar continuamente el SGSI, mediante las acciones de mejoras y lecciones aprendidas en la ejecución de la política de gobierno digital.

8. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI

Aplicable a todos los activos de información, talento humano de los procesos misionales, técnicos, administrativos, Financieros de Apoyo y demás, verificando y ajustándolo a la Institución, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad avalada por el Comité de Seguridad de la Información o política de tratamiento de datos, establecida en el documento Análisis de Contexto de Seguridad y Privacidad.

9. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que el Modelo Integrado de Planeación y Gestión MPIG, permite la integración de todos los procesos, planes y orientación de Misional y de apoyo de la Institución se nombra como integrantes del Comité De Seguridad de la Información a los integrantes del Comité de gestión y Desempeño, sus integrantes son las personas que tienen los siguientes cargos:

- Gerente o su delegado, quien lo presidirá.
- Profesional Universitario del área Financiera.
- Profesional Universitario área de Personal.
- Coordinador Área Asistencial.
- Coordinador Área de Sistemas de Información.
- Coordinador área de Calidad.
- Contador.
- Asesor Jurídico.
- Asesor de Planeación.
- Invitados: Control Interno; quien tendrán voz, pero no voto.

Las funciones del Comité de Seguridad de la Información son:

- Impulsar la implementación del Sistema de Gestión de Seguridad de la Información SGSI en la E.S.E.
- Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI de los procesos institucionales de la E.S.E.
- Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema Integrado de Gestión de la Información.
- Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la presidencia de la República.
- Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos de la seguridad de la información para la E.S.E, con el fin de tomar y establecer las medidas necesarias.
- Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de Información de la entidad.
- Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.

- Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- Las demás funciones inherentes a la naturaleza del Comité.

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

A través de la adopción del instrumento MSPI Modelo de Seguridad y Privacidad de la Información suministrado por MINTIC, la E.S.E. se encuentra en un nivel de madurez Intermedio, de acuerdo con la tabla de valor suministrada por el instrumento.

La E.S.E de acuerdo con el avance del ciclo PHVA del 40% de avance esperado para el año 2021 se obtuvo un 31% en el componente de Planificación, del 20% de avance esperado para el año de 2022 se obtuvo el 15% del componente de Implementación, y para el 20% de avance esperado en la vigencia de 2023 se evidencia el cumplimiento total del avance, lo que indica que se realizaron los respectivos controles y seguimientos a los componentes y actividades establecidas en las vigencias anteriores.

Dado los resultados anteriormente descritos para esta vigencia se debe fortalecer con las actividades ya desarrolladas en los diferentes componentes y avanzar con el cumplimiento del porcentaje pendiente definido en ciclo PHVA del instrumento Modelo de Seguridad y Privacidad de la Información.

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2021	Planificación	31%	40%
2022	Implementación	15%	20%
2023	Evaluación de desempeño	20%	20%
2024	Mejora continua	0%	20%
TOTAL		66%	100%

Frente a los dominios de mayor cumplimiento se hace referencia al Ítem No A.5 **POLITICAS DE SEGURIDAD DE LA INFORMACIÓN.**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO

A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	67	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	21	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	27	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	8	100	**INICIAL**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	1	100	**INEXISTENTE**
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	**INEXISTENTE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	**INEXISTENTE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	**INEXISTENTE**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	**INEXISTENTE**
A.18	CUMPLIMIENTO	0	100	**INEXISTENTE**
PROMEDIO EVALUACIÓN DE CONTROLES		**16**	**100**	**INICIAL**

Con relación al avance realizado en la vigencia 2022 frente a la 2023, encontramos que el componente de Planificación se mantuvo actual frente a lo esperado, el cual se encuentra en proceso de desarrollo la actividad faltante **Procedimientos de control documental del MSPI**, sin embargo el aumento de 8% adicional del componente de Implementación y la totalidad del avance esperado en el componente Evaluación de desempeño ha evidenciado que la brecha de la aplicación del instrumento MSPI no estableció cambios en la evaluación e implementación de los dominios establecidos en el instrumento

MSPI, lo que refiere que para la actual vigencia se debe repetir la gestión e implementación de las actividades requeridas para ejercer un avance optimo frente a la implementación del Sistema de Gestion de Seguridad de la Información..

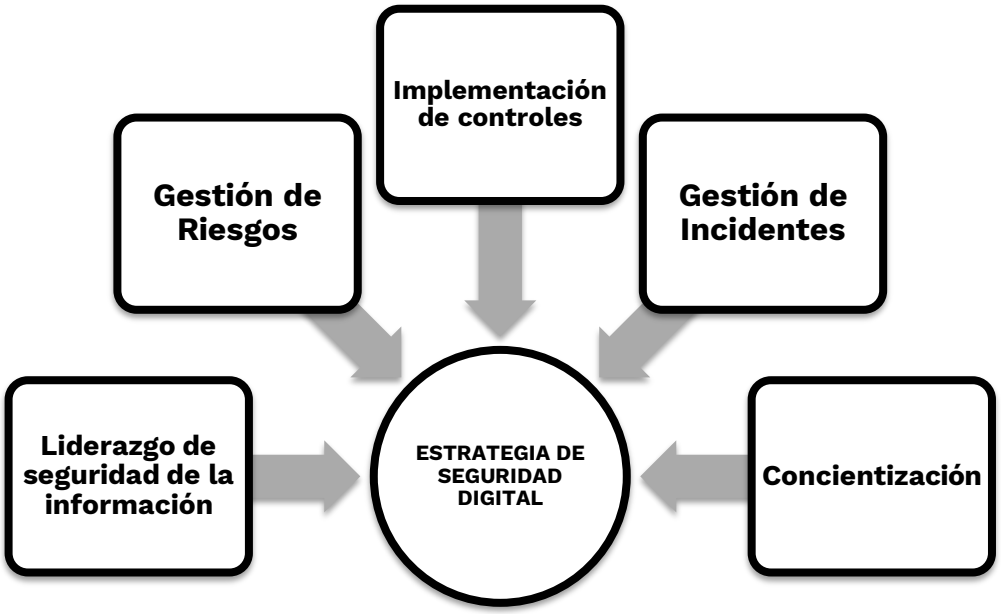
Frente a los dominios de mayor cumplimiento para la vigencia 2023 nos existen cambios o novedades.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	67	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	21	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	27	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	8	100	**INICIAL**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	1	100	**INEXISTENTE**
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	**INEXISTENTE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	**INEXISTENTE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	**INEXISTENTE**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	**INEXISTENTE**
A.18	CUMPLIMIENTO	0	100	**INEXISTENTE**
PROMEDIO EVALUACIÓN DE CONTROLES		**16**	**100**	**INICIAL**

11. ESTRATEGIA DE SEGURIDAD DIGITAL

LA E.S.E. establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse.

Por tal motivo, la E.S.E. define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



11.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

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

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

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

12. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las actividades para realizar se definen de acuerdo con el instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC en su componente de Planificación e Implementación y serán aplicadas a la vigencia 2024 fortaleciendo las metas trazadas de las vigencias anteriores de acuerdo con el Plan de Acción Institucional aumentando en un 10% la meta.

Nombre	Descripción	Calculo	Meta	Frec. Medición
A2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de actividades Realizadas /Número de Actividades del Ítem	50%	Semestral
AD.3. SEGURIDAD DE LOS RECURSOS HUMANOS	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de actividades Realizadas /Número de Actividades del Ítem	50%	Semestral
AD.4. GESTIÓN DE ACTIVOS	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de actividades Realizadas /Número de Actividades del Ítem	50%	Semestral
T.1. CONTROL DE ACCESO	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Técnicas.	Número de actividades Realizadas /Número de Actividades del Ítem	60%	Semestral
T.3. SEGURIDAD FÍSICA Y DEL ENTORNO	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Técnicas.	Número de actividades Realizadas /Número de Actividades del Ítem	60%	Semestral

13. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

14. DOCUMENTOS ASOCIADOS

CÓDIGO	TITULO
PE-PE-MIPG-PL6	Plan Estratégico de Tecnologías de la Información - PETI
PE-PE-MIPG-PL7	Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
Articles-5482 MINTIC	Instrumento Evaluación MSPI MINTIC
PA-GSI-ARI-M1 (V1)	Manual Políticas de Seguridad y Privacidad
	Análisis de Contexto de Seguridad y Privacidad.