# CONTENIDO

Tabla de contenido

[CONTENIDO 1](#_Toc135205354)

[1. INTRODUCCION 2](#_Toc135205355)

[2. JUSTIFICACIÓN 2](#_Toc135205356)

[3. OBJETIVO GENERAL 3](#_Toc135205357)

[3.1 OBJETIVOS ESPECÍFICOS 3](#_Toc135205358)

[4. ALCANCE 4](#_Toc135205359)

[5. RESPONSABLE 4](#_Toc135205360)

[6. PARTES INTERESADAS 5](#_Toc135205361)

[7. MARCO LEGAL 6](#_Toc135205362)

[8. DEFINICIONES 10](#_Toc135205363)

[9. MODELO SE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION MSPI 14](#_Toc135205364)

[10. CICLO DE OPERACIÓN DEL MSPI 15](#_Toc135205365)

[10.1 FASE PREVIA DE DIAGNOSTICO DEL MSPI 16](#_Toc135205366)

[Estado actual 18](#_Toc135205367)

[Nivel de Madurez 18](#_Toc135205368)

[10.2 FASE DE PLANIFICACIÓN 20](#_Toc135205369)

[10.2.1 PRESENTACIÓN DE LA ENTIDAD 23](#_Toc135205370)

[Misión 23](#_Toc135205371)

[Visión 24](#_Toc135205372)

[Valores corporativos 24](#_Toc135205373)

[Organigrama 25](#_Toc135205374)

[Mapa de Procesos 26](#_Toc135205375)

[10.2.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 27](#_Toc135205376)

[10.2.3 MANUAL DE POLÍTICAS 27](#_Toc135205377)

[General: 27](#_Toc135205378)

[Especificas: 28](#_Toc135205379)

[10.2.4 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 28](#_Toc135205380)

[10.2.5 ROLES Y RESPONSABILIDADES 28](#_Toc135205381)

[Gerencia de la E.S.E. Hospital Santa Isabel 29](#_Toc135205382)

[Líder de la Oficina de Gestión de la Información 30](#_Toc135205383)

[Sub Mesa de Gobierno Digital 31](#_Toc135205384)

[Responsable de los riesgos de seguridad de la información 31](#_Toc135205385)

[Responsabilidades de las partes interesadas 32](#_Toc135205386)

[Responsabilidades de proveedores 32](#_Toc135205387)

[Gestión integral de la Calidad y Planeación 32](#_Toc135205388)

[Grupo de Infraestructura Tecnológica 33](#_Toc135205389)

[*10.2.6* INTEGRACIÓN DEL MSPI CON EL SISTEMA DE GESTIÓN DOCUMENTAL*.* 33](#_Toc135205390)

[10.2.7 GESTIÓN DE RIESGOS 34](#_Toc135205391)

[10.2.8 PLAN DE COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN 35](#_Toc135205392)

[10.2.9 PLAN DE TRANSICIÓN DE IPV4 A IPV6 35](#_Toc135205393)

[10.3 FASE DE IMPLEMENTACIÓN 36](#_Toc135205394)

[10.3.1 PLANIFICACIÓN Y CONTROL OPERACIONAL 37](#_Toc135205395)

[10.3.2 IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS 37](#_Toc135205396)

[10.3.3 INDICADORES DE GESTIÓN 38](#_Toc135205397)

[10.3.4 PLAN DE TRANSICIÓN DE IPV4 A IPV6 42](#_Toc135205398)

[10.4 FASE DE EVALUACIÓN DE DESEMPEÑO 42](#_Toc135205399)

[10.4.2 PLAN DE EJECUCIÓN DE AUDITORIAS 46](#_Toc135205400)

[10.5 FASE DE MEJORA CONTINUA 47](#_Toc135205401)

[11. BIBLIOGRAFIA 48](#_Toc135205402)

# INTRODUCCION

Mediante la adopción del Modelo de Seguridad y Privacidad (MSPI) por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

La implementación del Modelo de Seguridad y Privacidad de la Información en la Entidad está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

La información es el activo más importante y relevante para las organizaciones, siendo un recurso indispensable para el desarrollo y cumplimiento misional junto con los compromisos del negocio. La información puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesaria, para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

En atención a las situaciones de riesgo expuestas anteriormente, se genera entonces por parte de la E.S.E. Hospital Santa Isabel, la iniciativa de establecer, implementar y mantener un modelo de gestión de la seguridad de la información que propenda por alcanzar y mantener una cultura y conciencia en el acceso y uso adecuado de la información de la entidad.

El presente documento identifica y recopila buenas prácticas para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información, a partir de una evaluación de diagnóstico, planeación, implementación, gestión y mejora continua del mismo.

# JUSTIFICACIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI), pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital y busca garantizar un adecuado manejo de la información pública en poder de las entidades, la cual es uno de los activos más valiosos para la toma de decisiones. El modelo propende por un doble enfoque a desarrollar, a nivel de seguridad marcando un derrotero para que la E.S.E. Hospital Santa Isabel construya unas políticas de seguridad sobre la información, a fin de salvaguardar la misma física y lógicamente, de manera que en todo momento se pueda garantizar su integridad, disponibilidad y autenticidad.

En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o a salvaguardar los secretos profesionales, del negocio de información privilegiada de particulares en poder de la administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva.

Para lograr el éxito del modelo se requiere que el componente de seguridad de la información vaya estrechamente relacionado con la privacidad, siguiendo el mismo ciclo de operación consistente en cinco fases o etapas así: Diagnóstico, Planeación, Implementación, Evaluación de Desempeño y Mejora continua.

El Modelo 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 estos.

# OBJETIVO GENERAL

Implementar el Modelo de Seguridad y Privacidad de la Información de la

E.S.E. Hospital Santa Isabel alineado con la NTC/IEC ISO 27001:2013, el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG), la Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, requerimientos del negocio y la Política de Seguridad Digital y privacidad de la información, en cumplimiento de las disposiciones legales vigentes, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y de los activos de información que soportan a la Entidad.

# 3.1 OBJETIVOS ESPECÍFICOS

* Apoyar la operación, mejora continua y sostenibilidad del Sistema de Administración de Riesgos en materia de Seguridad de la Información de la

E.S.E..

* Mantener los lineamientos establecidos para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
* Apalancar la implementación de un Sistema de Gestión de Seguridad de la Información en la E.S.E., de acuerdo con los requerimientos establecidos en el modelo de seguridad y privacidad de la información bajo los estándares que exige la estrategia de Gobierno Digital de MINTIC.
* Contribuir al incremento de la transparencia en la gestión pública.
* Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
* Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.
* Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.

# ALCANCE

El presente documento identifica e incluye las orientaciones para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información, el cual debe ser aplicado sobre todos los procesos de la E.S.E. Hospital Santa Isabel y de cumplimiento por parte de todos los colaboradores con relación contractual.

# RESPONSABLE

La Alta Dirección apoyará la implementación del MSPI con el liderazgo de Gestión de la información, como eje trasversal de la entidad, la sub Mesa de Gobierno Digital para la implementación de la dimensión de arquitectura organizacional y seguridad de información, en lo que respecta a los sistemas de información y la seguridad de los mismos, definiendo para tal fin, las siguientes funciones:

1. Aprobar los lineamientos, metodologías relacionada con la seguridad de información y gobierno digital.
2. Coordinar la implementación de los modelos de gobierno digital y de seguridad de la información.
3. Revisar el avance en la implementación de los modelos de gobierno digital y de seguridad de información.
4. Aprobar lineamientos, metodologías y prácticas al interior de la unidad para la implementación de las estrategias demarcadas en los modelos descritos.
5. Diseñar las estrategias para la apropiación de los modelos de gobierno digital y de seguridad de la información.
6. Diseñar y estructurar la Arquitectura empresarial de la E.S.E.
7. Evaluar y Aprobar las nuevas tecnologías en pro del desarrollo de las funciones de la E.S.E.

En este sentido, la sub Mesa Gobierno Digital está integrado por:

* 1. Jefe de la Oficina de Gestión de la Información, líder.
  2. Jefe de la Oficina de Gestión de Control Interno
  3. Líder de Oficina de Comunicaciones
  4. Líder del archivo administrativo
  5. Responsable de la infraestructura de la E.S.E.
  6. Representante de la Oficina de Gestión Jurídica

De la misma manera y entendiendo que el modelo de seguridad de la información no es un sistema aislado, todos los funcionarios, contratistas, estudiantes y demás partes que conforman a la E.S.E. son parte activa del desarrollo e implementación del MSPI, teniendo claridad que son ellos, los propietarios de los activos de información y el frente más vulnerable del eslabón de la seguridad de la información, por ende, es el más atacado por las amenazas.

# PARTES INTERESADAS

La E.S.E. Hospital Santa isabel reconoce como sus grupos de interés a:

|  |  |
| --- | --- |
| **PARTE INTERESADA** | **DESCRIPCIÓN** |
| Usuarios directos | Todos los usuarios con vinculo de:   * Carrera administrativa/ personal de planta permanente * Libre nombramiento y remoción en planta permanente * Personal de planta temporal * Contratista |
| Usuarios Indirectos | La ciudadanía. |
| Entidades publicas | Autoridades del sector y entes del Estado. |
| Terceros relacionados | Gremios del ecosistema, estudiantes en práctica, proveedores |
| Entidades externas | Entidades homologas de otros países y los organismos internacionales de referencia. |

# MARCO LEGAL

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la E.S.E., en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

**Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

**Decreto 1008 de 2018:** Por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título

9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

**CONPES 3854 de 2016:** Política Nacional de Seguridad Digital

**CONPES 3854 de 2016 objetivo general:** “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.

**Manual para la Implementación de la Política de Gobierno Digital:** Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2)

Versión 7, abril de 2019

**Modelo de Seguridad y privacidad de la información – MSPI:** Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales

**NTC / ISO 27001:2013:** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

**NTC / ISO 27002:2013:** Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

**Decreto 2573 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

**Decreto 2609 de 2012:** Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

**Decreto 2693 de 2012:** Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.

**Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

**Ley 1581 de 2012 g) Principio de seguridad:** “La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.”

**Ley 1581 de 2012, Artículo 17, ítem d:** “Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”

**Ley 1712 de 2014, “principio de transparencia”:** “Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.”

**Ley 1712 de 2014, artículo 7:** “Disponibilidad de la información” “En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.”

**Ley 1712 de 2014 -Título III:** “Excepciones acceso a la información” “Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.”

**Decreto 1413 de 2017, artículo 2.2.17.6.6:** “Seguridad de la información.” “Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.”

**Decreto 1413 de 2007, artículo 2.2.17.6.1:** “Responsable y encargado del tratamiento”: “Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen.”

**Decreto 1413 de 2007, artículo 2.2.17.6.3:** “Responsabilidad demostrada”: “Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.”

**Decreto 1413 de 2007, artículo 2.2.17.6.5:** “Privacidad por diseño y por defecto”: “Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy lmpact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador”

**Decreto 1413 de 2017, artículo 2.2.17.5.10:** “Derechos de los usuarios de los servicios ciudadanos digitales”: “1. Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador. 2. Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales. 3. Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre. 4. Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales. 5. Elegir y cambiar libremente el operador de servicios ciudadanos digitales 6. Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.

**Decreto 1413 de 2017, artículo 2.2.17.2.1.1:** “Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad: Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicas cuando lo requieran.”

**Decreto 612 de 2018, artículo 1:** “Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web.”

**Ley 1448 de 2011, Artículo 29:** “…Las autoridades garantizarán la confidencialidad de la información suministrada por las víctimas…” “Brindar información veraz y completa a las autoridades encargadas de hacer el registro y el seguimiento de su situación o la de su hogar, por lo menos una vez al año, salvo que existan razones justificadas que impidan suministrar esta información. Las autoridades garantizarán la confidencialidad de la información suministrada por las víctimas y de manera excepcional podrá ser conocida por las distintas entidades que conforman el Sistema Nacional de Atención y Reparación de las Víctimas para lo cual suscribirán un acuerdo de confidencialidad respecto del uso y manejo de la información.

**Ley 1437 de 2011, Capítulo IV:** “utilización de medios electrónicos en el procedimiento administrativo”. “Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”

# 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 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 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).

**Modelo de Seguridad y Privacidad de la Información (MSPI):** El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

**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.

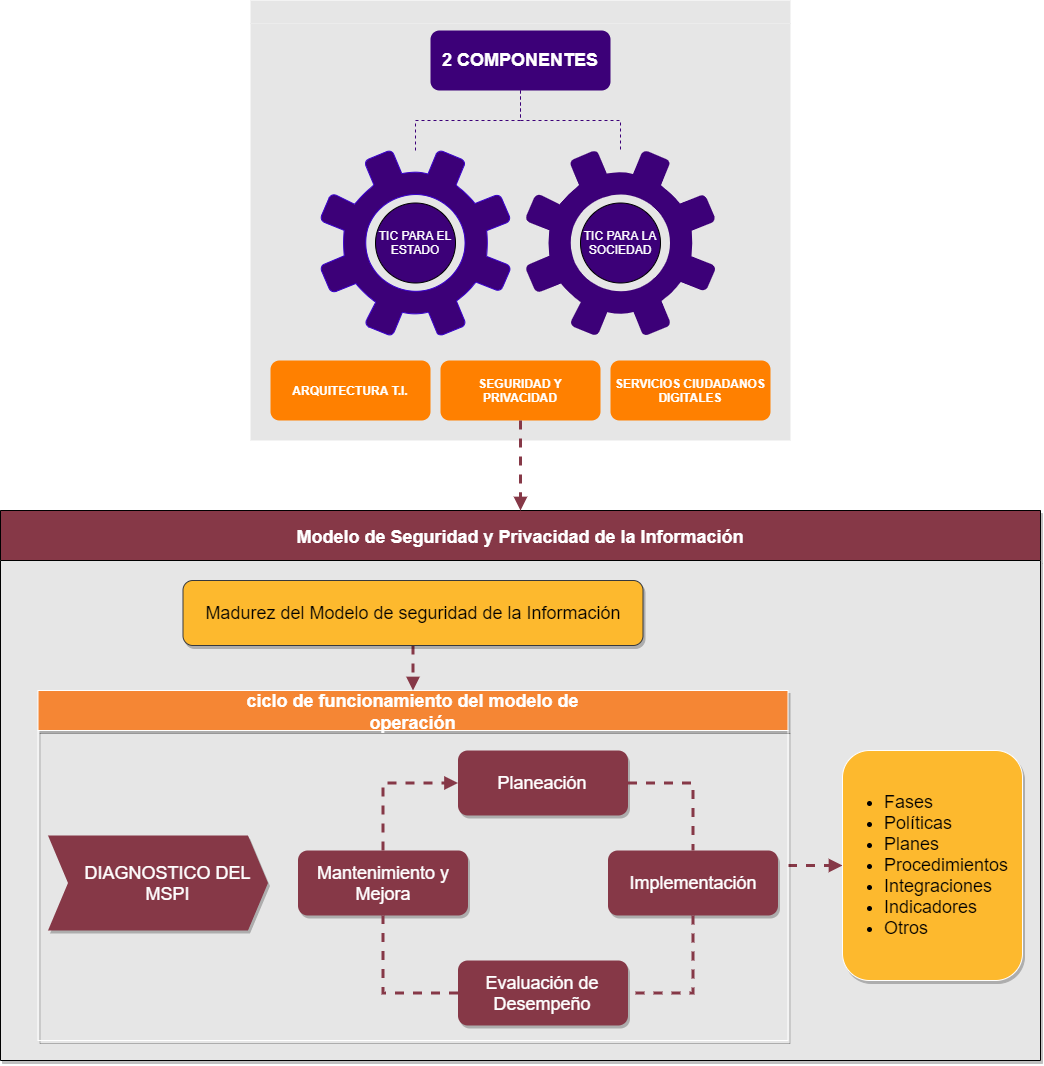
**DAFP:** El Departamento Administrativo de la Función Pública (DAFP) es la entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional.

# MODELO SE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION MSPI

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

La siguiente figura muestra el modelo de seguridad y privacidad de la información desde una mirada de 360°, mostrando cada uno de sus componentes, entradas y salidas. el modelo se basa en uno de los tres habilitadores transversales de la estrategia de gobierno digital del MINTIC.



# CICLO DE OPERACIÓN DEL MSPI

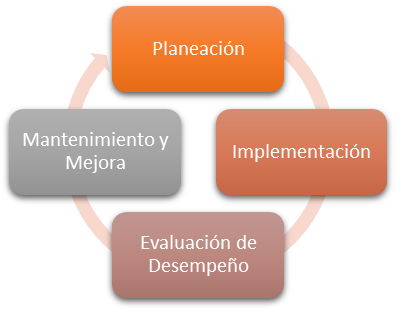
La E.S.E adopta y aplica el modelo de seguridad y privacidad de la información contemplando un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. El presente Modelo contempla 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

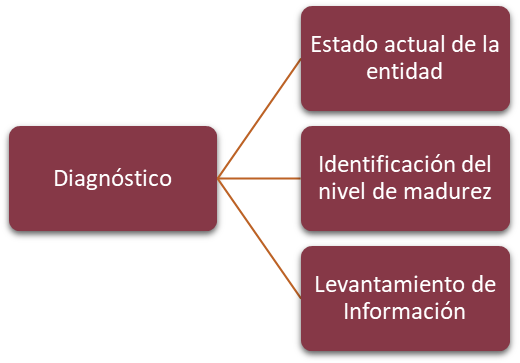
El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables

A continuación, se describe el ciclo de operación del MSPI en el cual se contemplan cinco (5) fases que lo comprenden. Estas, contienen 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.



# FASE PREVIA DE DIAGNOSTICO DEL MSPI

Esta fase permite por medio del uso de herramientas de diagnóstico, actividades de reconocimiento y valoración de controles de seguridad de la información, identificar cual es el estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este de diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad de la información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.



Fuente: Documento Modelo de Seguridad y Privacidad de la Información Estrategia de Gobierno en Línea

|  |  |  |  |
| --- | --- | --- | --- |
| **Diagnostico** | | | |
| **Metas** | **Actividades** | **Instrumentos** | **Resultados** |
| Determinar el estado actual de la gestión de  seguridad y privacidad de la información al  interior de la Entidad | Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. | Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013.  Instrumento de Evaluación MSPI de MINTIC. | Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC. |
| Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad. | Valoración del nivel de estratificación de la entidad frente a la seguridad de la información con base en el método planteado en el documento ‘ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES’ del  modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0. |  | Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo ‘MODELO DE MADUREZ’ del  documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea. |
| Definir el mapa de Ruta de las actividades orientadas a la planificación e implementación del modelo de  seguridad y privacidad de la información acorde con el informe de diagnóstico. | Registro de las fases, actividades, recursos y tiempos necesarios para la planeación e implementación del modelo de seguridad y privacidad de la información. | Mapa de ruta y Cronograma de actividades | Mapa de ruta y Cronograma de actividades |

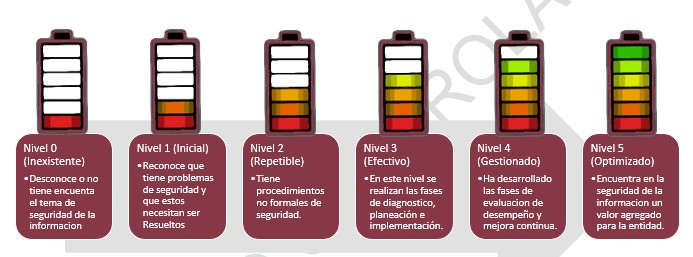
# Estado actual

La entidad se encuentra en un proceso de transformación digital, donde se evalúan la implementación de nuevas políticas de Seguridad de la información, aplicación de criterios de protección de datos, ajustes a los procedimientos de seguridad, entre otros. Se avanza cada vez más en la identificación de toda la información de la Entidad, de manera que a través del análisis de riesgo y el etiquetado de la información se logre clasificar y aplicar controles de Ciberseguridad.

Al interior de la entidad se cuenta con un sistema de Gestión de Calidad, el cual contempla el sistema de gestión de seguridad de la información (SGSI), este sistema no está implementado en su totalidad y no se usa activamente, lo cual afecta la gestión de riesgos de seguridad; es por ello que se está en proceso de implementación, iniciando con todo el levantamiento de información necesaria para iniciar su ciclo de operación.

# Nivel de Madurez

Definir el alcance del MSPI permitirá a la E.S.E. establecer los límites sobre los cuales se implementará la seguridad y privacidad de la información, por lo tanto, se deben tener claros los procesos misionales, estratégicos, de apoyo y de evaluación de la Entidad y toda la infraestructura que los soporte. Acorde a la vigencia actual, el avance general en el ciclo PHVA, de acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, la E.S.E. se encuentra en un estado **Efectivo**. A continuación, se detalla cómo fue la clasificación de este:



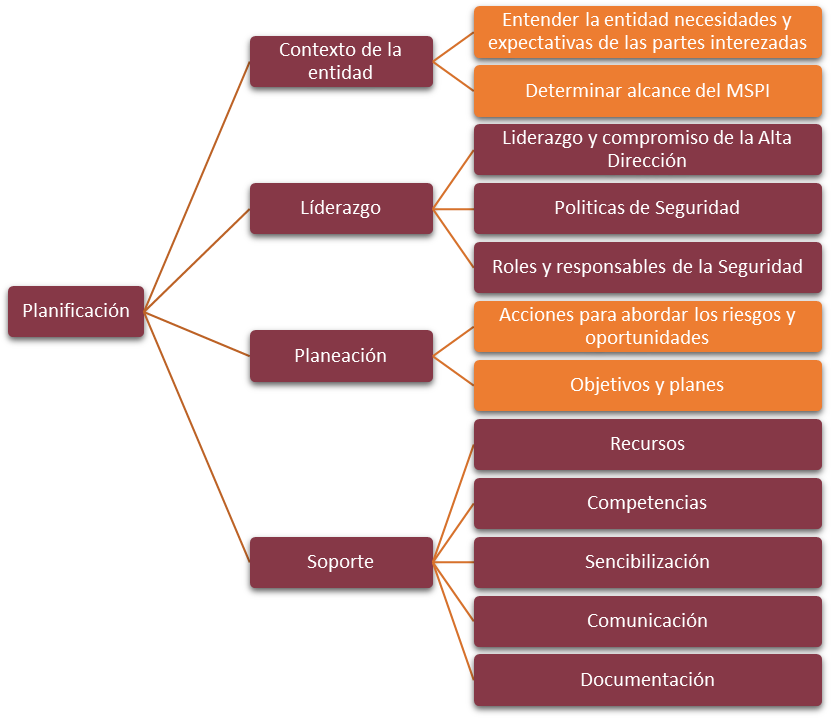
|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **DOMINIO** | **EVALUACIÓN DE EFECTIVIDAD**  **DE CONTROL** | **OBJETIVO 2022** |
| A.5 | Políticas de seguridad de la información | Efectivo | Optimizado |
| A.6 | Organización de la seguridad de la información | Repetible | Efectivo |
| A.7 | Seguridad de los recursos humanos | Efectivo | Efectivo |
| A.8 | Gestión de activos | Gestionado | Gestionado |
| A.9 | Control de acceso | Efectivo | Efectivo |
| A.10 | Criptografía | Inicial | Efectivo |
| A.11 | Seguridad física y del entorno | Efectivo | Efectivo |
| A.12 | Seguridad de las operaciones | Efectivo | Efectivo |
| A.13 | Seguridad de las comunicaciones | Repetible | Efectivo |
| A.14 | Adquisición, desarrollo y mantenimiento de sistemas | Repetible | Efectivo |
| A.15 | Relaciones con los proveedores | Efectivo | Gestionado |
| A.16 | Gestión de incidentes de seguridad de la información | Efectivo | Optimizado |
| A.17 | Aspectos de seguridad de la información de la gestión de la continuidad del negocio | Efectivo | Gestionado |
| A.18 | Cumplimiento | Efectivo | Efectivo |
| **PROMEDIO EVALUACIÓN DE CONTROLES** | | Efectivo | Gestionado |

El estado de madurez **Efectivo, en el cual se encuentra la Entidad,** indica que se cuentan con políticas de seguridad y un manual aprobado por las directivas, con controles para el aseguramiento de la información, los cuales se irán ajustando de acuerdo a la planeación que se realice.



# FASE DE PLANIFICACIÓN

En esta fase se elaborará el Plan de Seguridad y Privacidad de la Información a partir de los resultados generados en la fase de diagnóstico y garantizando su alineación con la planeación estratégica de la E.S.E.



|  |  |  |  |
| --- | --- | --- | --- |
| Planificación | | | |
| Metas | Resultados | Instrumentos | |
| MSPI | MRAE |
| Política de Seguridad y Privacidad de la Información | Documento con la política de seguridad de la información | Guía No 2 – Política General MSPI | * LI.ES.02 * LI.ES.06 * LI.ES.07 * LI.ES.08 * LI.ES.09 * LI.ES.10 * LI.GO.01 * LI.GO.04 |
| Incorporación de nuevas políticas de seguridad y privacidad de la información | Manual con las políticas de seguridad y procedimiento en el tratamiento de los datos | Guía no 2 - Política General MSPI |
| Procedimientos de seguridad de la información. | Documento de Gestión de la Información | Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información | * LI.GO.07 * LI.GO.08 * LI.GO.09 * LI.GO.10 * LI.INF.01 * LI.INF.02 * LI.INF.09 * LI.INF.10 * LI.INF.11 |
| Roles y responsabilidades de seguridad y privacidad de la información. | Documento de Gestión de la Información | Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información. |
|  |  |  | * LI.INF.14 * LI.SIS.22 * LI.SIS.23 * LI.SIS.01 * LI.ST.05 * LI.ST.06 * LI.ST.09 * LI.ST.10 * LI.ST.12 * LI.ST.13 * LI.ST.14 * LI.UA.01 |
|  |  |  | * LI.UA.02 * LI.UA.03 * LI.UA.04 * LI.UA.05 * LI.UA.06 |
|  |  |  |
| Integración del MSPI con el Sistema de Gestión documental | Integración del MSPI, con el sistema de gestión documental de la entidad. | Guía No 6 - Gestión Documental |  |
| Identificación, Valoración y tratamiento de riesgo. | Mapa de Riesgos de la ESE. | Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad |
| Plan de Comunicaciones. | Documento con el plan de comunicación, sensibilización y capacitación para la entidad. | Guía No 14 - Plan de comunicación, sensibilización y capacitación |

# PRESENTACIÓN DE LA ENTIDAD

## **Misión**

La E.S.E. Hospital Santa Isabel del Municipio de San Pedro de los Milagros, ofrece servicios de salud de primer nivel de complejidad y especialidades clínicas en forma intramural y extramural con equidad e igualdad para toda la comunidad local y de la región del norte cercano de Antioquia; brindando calidad, seguridad, humanización y trabajo en equipo, orientado a la promoción de la salud, prevención de la enfermedad y fomento de los estilos de vida saludable, aplicando el uso de las tecnologías adecuadas y desarrollando la innovación social; que contribuyan con el mejoramiento de la calidad de vida de sus gentes, socialmente responsable y amigable con el medio ambiente; en alianza estratégica con nuestros usuarios y clientes, que permita su sostenibilidad social y financiera.

## **Visión**

La E.S.E. Hospital Santa Isabel del Municipio de San Pedro de los Milagros, al año 2025, tendrá un modelo de atención en salud enfocado en Atención Primaria en Salud, con fortaleza en Promoción y Prevención, prestando sus servicios de forma humanizada y segura a sus usuarios, comprometidos con el mejoramiento continuo de sus procesos, con un talento humano idóneo en capacitación permanente y tecnología de adecuada, aumentando la oferta institucional de servicios de salud, permitiendo la sostenibilidad social y financiera de la empresa.

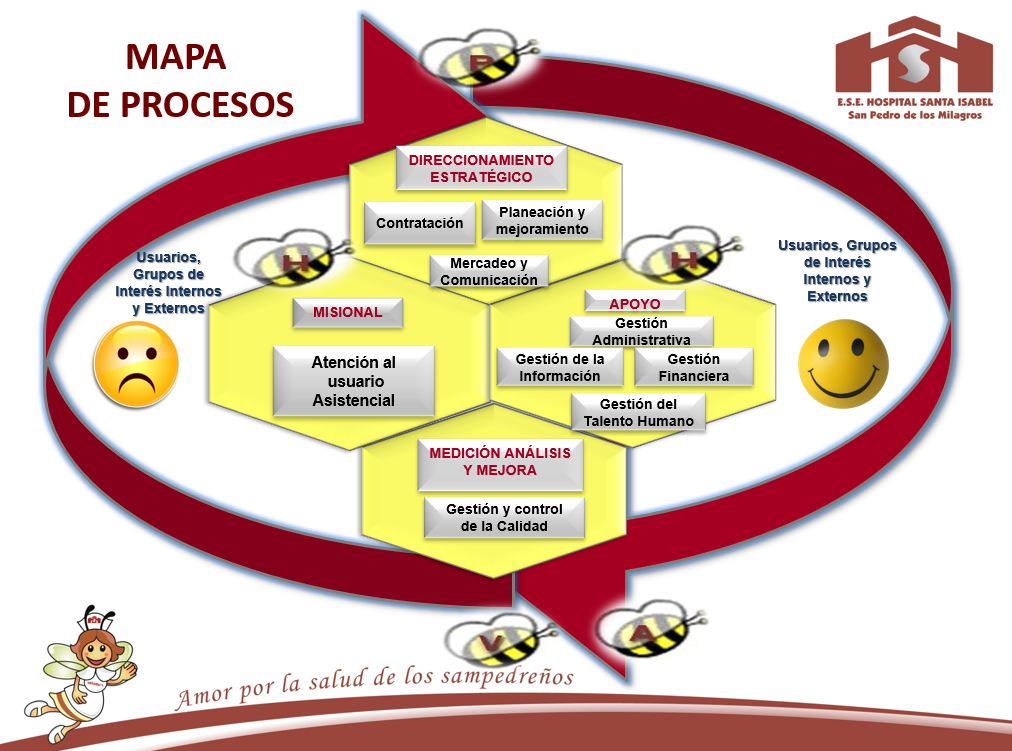
## **Valores corporativos**

* Responsabilidad: Cumplir a cabalidad las tareas, usando adecuadamente los recursos y los bienes públicos para el trabajo, minimizando el impacto negativo en el medio ambiente y las personas.
* Compromiso: Empoderarse de la labor con sentido de pertenencia, asumiendo los retos y garantizando el cumplimiento de las metas organizacionales.
* Equidad: Encaminar esfuerzos por entregar servicios acorde a las necesidades de los usuarios y sus colaboradores.
* Igualdad: Brindar la misma calidad en la prestación de los servicios.
* Respeto: Garantizar derechos de los usuarios y colaboradores, aceptar las diferencias culturales, religiosas, sociales, políticas y económicas, sin que esto sea causal de discriminación.
* Honestidad: Actuar con transparencia, sin ocultar información que sea de interés para los colaboradores y los usuarios y asumiendo las consecuencias de sus actos.
* Confianza: Actuar de manera acorde a las circunstancias generando seguridad en las personas receptoras de nuestros actos.
* Vocación de Servicio: Actuar de manera solidaria y desinteresada, sin requerir retribuciones.
* Lealtad: Es la promesa por el cumplimiento de los pactos o acuerdos que se hacen entre las personas y con el manejo de la imagen institucional .

## **Organigrama**



## **Mapa de Procesos**



# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Hospital establece una política general y otras políticas específicas desde Gestión de la Información, en cumplimiento con el MSPI y teniendo en cuenta los siguientes criterios:

**Creación de políticas:** En la E.S.E. Hospital Santa Isabellas políticas deben ser creadas por el área encargada de la seguridad y privacidad de la información y respaldadas por la Alta Dirección de la entidad con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas.

**Aprobación de políticas:** En la E.S.E. Hospital Santa Isabel, las políticas relacionadas con la seguridad y privacidad de la información deben ser aprobadas por la Alta Dirección con base en las recomendaciones del área encargada de la seguridad y privacidad de la información.

**Actualización de políticas:** Las políticas de seguridad y privacidad de la información se deben revisar periódicamente, al igual la normatividad que a esta se refiera con el fin de realizar los ajustes pertinentes. Cualquier requerimiento de modificación, cambio o actualización de las políticas de seguridad y privacidad de la información, debe ser dirigida a la Alta Dirección con base en las recomendaciones del área encargada.

**Reglas de escritura de las políticas:** Las políticas estarán escritas en forma sencilla y específica, el enunciado bien redactado y estará definido en un lenguaje técnico y explícito para los usuarios.

**Nivel de cumplimiento de la política:** Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento del 100% de la política. El incumplimiento de la política de seguridad y privacidad de la información y seguridad digital, traerá consigo, las consecuencias legales que apliquen a la normatividad de la E.S.E, incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a la Seguridad y privacidad de la información y seguridad digital.

# MANUAL DE POLÍTICAS

La E.S.E. Hospital en conformidad con los avances en la Implementación del Modelo de Seguridad y Privacidad de la Información, publicara y divulgara las siguientes políticas desarrolladas para la estructuración del MSPI.

# General:

* + - * Política de Seguridad y Privacidad de la Información y Seguridad Digital
      * Políticas Gestión de Riesgos
      * Política de protección de datos
      * Política de gestión de tecnología
      * Política de confidencialidad y privacidad

# Especificas:

* + - * Política de Gestión de Activos
      * Política de Control de Acceso
      * Política de Gestión de Incidentes de Seguridad de la Información
      * Política de Seguridad de las Operaciones
      * Política de respaldo de información

# PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Para La E.S.E. Hospital Santa Isabel, los procedimientos, lineamientos e instructivos u/o guías, constituyen una base importante para la preservación de la seguridad y privacidad de la información. Se han diseñado procedimientos, lineamientos e instructivos, que cubren las políticas de seguridad y privacidad de la información para los cuales han tenido en cuenta las 21 guías definidas en los lineamientos de MINTIC a través del Modelo de Seguridad y Privacidad de la Información.

# ROLES Y RESPONSABILIDADES

Con el fin de lograr el cumplimiento de la política de Seguridad y Privacidad de la Información y Seguridad Digital, y el MSPI, individualizara los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a los sistemas.

Para la asignación de los responsables, la E.S.E. analizará las funciones de cada rol comparándolas con el personal de la entidad, es necesario que las responsabilidades asignadas en el desarrollo del de la política de Seguridad y Privacidad de la Información y Seguridad Digital y el MSPI, para cada perfil, sean incorporadas a los manuales de funciones de acuerdo con el cargo que desempeñan.

A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implantación y seguimiento de la política de Seguridad y Privacidad de la Información y Seguridad Digital y el MSPI.

|  |  |  |
| --- | --- | --- |
| **Recurso Humano** | **Rol** | **Responsabilidades** |
| Gerente de la E.S.E. Hospital Santa Isabel | Alta Dirección | Apoyo implementación  MSPI en Gestión Estratégica |
| Sub Mesa de Gobierno Digital | Toma de decisiones | Toma de decisiones frente a la seguridad de la Información |
| Líder de la Oficina de Gestión de la Información | Responsable MSPI | Liderazgo y responsabilidad del MSPI Gestión estratégica y táctica |
| Dueño del Riesgo | Gestión de Riesgos de seguridad de la Información | Gestión riesgos de seguridad de la información del proceso |
| Partes Interesadas | Cumplimiento MSPI | Dar estricto cumplimiento a lo estipulado en el MSPI. |
| Proveedores | Cumplimiento MSPI | Dar estricto cumplimiento a lo estipulado en el MSPI. |
| Gestión integral de la Calidad y Planeación | Apoyo operativo de las actividades requeridas del MSPI | Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces. |
| Grupo de Infraestructura Tecnológica | Gestión de la transición y migración IPv4 a IPv6 Ejecución de actividades del MSPI | Llevar a cabo la implementación del protocolo IPv6 en la entidad. Orquestación de las partes interesadas. Cumplimento del aseguramiento de IPv6 Gestión de riesgos tecnológicos de IPv6.  Ejecución de actividades del MSPI |

# Gerencia de la E.S.E. Hospital Santa Isabel

Como muestra de su compromiso la alta dirección, se compromete en la gestión y apoyo a la implementación del MSPI y aprueba los siguientes:

* Aprobar los objetivos de seguridad de la información, los cuales estarán alineados con los objetivos estratégicos de la E.S.E.
* Aprobar anualmente o cuando se requiera la Política de Seguridad y Privacidad de la Información y seguridad digital de la E.S.E. y el modelo del MSPI.
* Velar por que los requisitos del MSPI, se encuentran integrados en todos los procesos críticos de la entidad.
* Proporcionar los recursos necesarios para la implementación y desarrollo de las actividades del MSPI.
* Velar por la ejecución y desarrollo de las actividades del MSPI.
* Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos para la entidad.
* Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad.

# Líder de la Oficina de Gestión de la Información

Se recomienda a la E.S.E., acorde al Decreto 1499 de 2017 emitido por el DAFP, designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección.

Así mismo, debe pertenecer e informar a la sub Mesa de Gobierno Digital, todo lo referente al MSPI, siendo oportuno con su asistencia y buscando siempre el mejoramiento continuo de cualquier necesidad de mejora respecto a la seguridad y privacidad de la información de la E.S.E.

El líder de la Oficina de Gestión de la Información, tendrá la responsabilidad de liderar a la sub Mesa de Gobierno Digital y desarrollará las siguientes funciones (además de las determinadas en el Acuerdo No. 006 del 23 de octubre de 2008):

* Emitir conceptos referentes a riesgos y seguridad de la información de la entidad, para la toma de decisiones por parte de la sub Mesa de Gobierno Digital.
* Coordinar la implementación, despliegue y sostenibilidad del MSPI.
* Mantener una comunicación clara, oportuna, completa y permanente con los integrantes de la sub Mesa de Gobierno Digital.
* Definir las herramientas, metodologías y lineamientos necesarios para la implementación del MSPI.
* Realizar seguimiento a los objetivos planteados frente al MSPI, para detectar desviaciones y tomar las acciones correctivas necesarias.
* Verificar el cumplimiento de la implementación de los objetivos y tareas asignadas a la sub Mesa de Gobierno Digital.
* Verificar que se incluyan los temas asociados al MSPI, dentro del (PIC) plan de capacitaciones de la entidad.
* Asegurar que se definan e implementen actividades de sensibilización y concientización frente a la seguridad de la información a la Alta Dirección y demás partes interesadas.
* Emitir conceptos y asesoría sobre los temas de seguridad de la información al Comité de integrado de gestión y desempeño para la toma de decisiones.
* Capacitar a los funcionarios de la Entidad sobre las maneras de proteger la información.

# Sub Mesa de Gobierno Digital

La Sub Mesa de Gobierno Digital, apoyará y tomará decisiones frente al proceso de definición, implementación, operación, seguimiento, revisión, mantenimiento y mejora del MSPI, a través de un equipo de trabajo conformado y con funciones determinadas en la Resolución No. 3156 de 26 de septiembre de 2018.

# Responsable de los riesgos de seguridad de la información

Todos los funcionarios de la E.S.E. serán responsables de la identificación, evaluación y control de los riesgos de seguridad de la información y seguridad digital. No obstante, se debe asignar un responsable de la actualización y verificación de los activos de información, de los riesgos de seguridad y privacidad de la información de cada proceso. Las principales responsabilidades de este rol incluyen:

* Identificar, registrar y actualizar los activos de información de su dependencia o proceso de responsabilidad.
* Realizar la clasificación y valorización de los activos de información en compañía con el responsable de la administración de estos.
* Realizar la revisión como mínimo anualmente de los activos de información para garantizar que corresponde a los requisitos legales, normativos, contractuales y de la entidad.
* Realizar la gestión requerida para que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información de su proceso.
* Determinar los privilegios de acceso y criterios de respaldo para los activos de información bajo su propiedad.
* Revisar y asegurar que los privilegios de acceso a los activos de información de los cuales es responsable sean los adecuados.
* Aprobar la divulgación de información que este bajo su proceso.
* Comunicar violaciones de seguridad o incidentes sobre los activos de información de su proceso.
* Velar porque la información que le ha sido confiada sea protegida durante todo su ciclo de vida (creación, almacenamiento, distribución, transporte y destrucción segura) de modificaciones y usos no autorizados.

# Responsabilidades de las partes interesadas

Las partes interesadas en sus funciones y roles dentro de la E.S.E. Hospital Santa Isabel, tienen autorización y acceso a la información y/o activos provenientes del responsables o líderes de los procesos, dentro de las cuales se incluyen:

* Cumplir con todas aquellas responsabilidades que han sido definidas en las políticas de seguridad y privacidad de la información y seguridad digital de la E.S.E.
* Proteger la información que la entidad le ha suministrado para la ejecución de sus labores.
* Firmar un acuerdo de confidencialidad y/o no divulgación antes de iniciar formalmente sus labores dentro de la entidad.
* Realizar un entendimiento de las políticas, procedimientos, manuales y otros referentes en materia del MSPI de la entidad.
* Usar los activos de información de la entidad y los recursos de manera segura y adecuada para desempeñar sus funciones laborales.

# Responsabilidades de proveedores

Es responsabilidad de todos los proveedores, que tengan acceso a la información de la E.S.E., cumplir con todas las políticas y procedimientos definidos frente a la protección de la información, las cuales le han sido suministrados para la labor designada y así mismo usar de manera segura los activos de información que le fueran asignados. Los proveedores deben estar autorizados por el responsable o líder del proceso, quien será el gestor del control y vigilancia del uso adecuado de los activos de información. Los proveedores deben aceptar por escrito los términos y condiciones de uso de los activos de información, así como el cumplimiento estricto de las políticas de seguridad de la información y protección de datos de la E.S.E. Hospital Santa Isabel antes de su acceso a los mismos.

# Gestión integral de la Calidad y Planeación

* Guiar a la Alta dirección de la E.S.E. ante incidentes de seguridad mediante los planes de respuesta de incidentes.
* Coordinar la realización del análisis de riesgos de seguridad de la información.
* Realizar seguimiento a la elaboración y desarrollo del Plan de Seguridad de la Información.
* Gestionar junto con el área de Gestión de la información, la referenciación de mejores prácticas frente a la seguridad de la información.
* Velar y promover la actualización de las políticas de seguridad de la información.

# Grupo de Infraestructura Tecnológica

* Activar la opción de cifrado a los equipos de cómputo para los casos que lo ameriten, imposibilitando la copia o extracción de datos si no se conoce el método de desbloqueo.
* Aplicar la opción de borrado de información en los equipos de cómputo institucionales que deban ser prestados, utilizando herramientas tecnológicas que imposibiliten la recuperación de esta y restaurando los valores de fábrica, para evitar divulgación no autorizada de información en caso de pérdida o hurto.
* Realizar las copias de seguridad de la información contenida en las unidades de red de los servidores asignadas a cada usuario.
* El Grupo de Infraestructura Tecnológica creará, modificará, bloqueará o eliminará las cuentas de usuarios sobre las unidades de red, los recursos tecnológicos y los sistemas de información de la entidad, acorde con el procedimiento establecido y según solicitud por escrito de las partes interesadas.
* Realizar los cambios necesarios a los roles y perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos de acuerdo a solicitud escrita de las partes interesadas.
* Gestionar los incidentes de seguridad de la información.
* Evaluar y autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica y los sistemas de información de la entidad.
* Velar por que la implementación de los cambios de tipo infraestructura y en los sistemas de información se lleve a cabo sin generar mayores contratiempos en la operatividad de los procesos para el cumplimiento de la misión institucional.
* El líder o quien haga sus veces del Grupo de Infraestructura Tecnológica debe asegurarse de que todos los funcionarios y/o servidores públicos, contratistas, como también los proveedores que cumplen una función en la gestión de la continuidad de la operación de TI, estén familiarizados con las políticas de seguridad y privacidad de la información y seguridad digital de la E.S.E.

# INTEGRACIÓN DEL MSPI CON EL SISTEMA DE GESTIÓN DOCUMENTAL*.*

La E.S.E. cuenta con varios repositorios oficiales de documentación, como son: la página web, el correo electrónico, el sistema de información CNT, carpetas compartidas y archivo físico en cada proceso de la entidad. Estos repositorios deben cumplir con las siguientes características que permitirán asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información:

* Acceso continúo a la información a través del sistema de Información Mercurio, donde se encuentra protegida en formato de lectura PDF o formato de imagen.
* Transmisión de información entre el usuario y el servidor a través de protocolos seguros, que permite garantizar la confidencialidad de la información
* Desde los sistemas de información de la E.S.E, se otorgan los permisos de acceso y/o modificación de la información de acuerdo a cada perfil.
* Los permisos de acceso los debe ser aprobados previamente por la Oficina de Gestión de la Información para el caso del MSPI.
* Algunos documentos del MSPI serán clasificados como confidenciales (reservados o clasificados), los cuales no se podrán tener acceso para el público en general, únicamente se tendrá acceso al personal autorizado y se hará desde las instalaciones de la E.S.E.
* Etiquetado de los activos de información según la confidencialidad, disponibilidad y criticidad de la información.

En el caso de los documentos derivados de actividades realizadas, en la E.S.E., se establecen los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y la disposición de los registros que le permitan la recuperación de la información y la preservación de la memoria institucional de la entidad de acuerdo a lo estipulado en las tablas de retención documental (TRD).

# GESTIÓN DE RIESGOS

La E.S.E. ha documentado, establecido y publicado el manual y plan para la administración del riesgo de la E.S.E en el cual se documenta el proceso para el tratamiento de los riesgos derivados de la Seguridad de la Información.

Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se emplearán los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos en la guía del DAFP.

# PLAN DE COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN

La E.S.E. Hospital Santa Isabel ha establecido la articulación del plan de comunicación, sensibilización y capacitación con la Guía Metodológica para la - implementación del Plan Nacional de Formación y Capacitación (PNFC): Profesionalización y Desarrollo de los Servidores Públicos del DAFP 2019.

Se realizará una integración con el Plan Institucional de Capacitación (PIC), donde se incorporan los objetivos en materia de seguridad y privacidad de la información y seguridad digital, consiguiendo el apoyo de la alta dirección y del proceso de Talento Humano, realizando así la inclusión en los programas de entrenamiento en puesto de trabajo y educación para el trabajo y desarrollo humano, todo lo referente en materia del MSPI, promoviendo así estrategias para crear, incentivar y mantener una cultura organizacional mediante la generación de competencias y hábitos de protección de la información en todos los niveles de la Entidad.

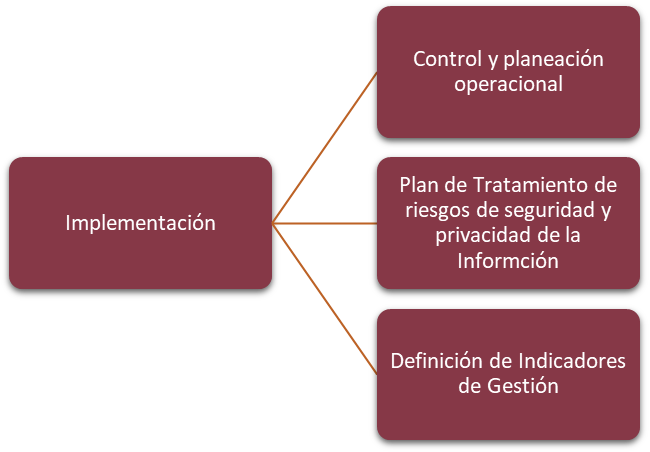
# PLAN DE TRANSICIÓN DE IPV4 A IPV6

Para llevar a cabo el proceso de transición de IPv4 a IPv6, se cumplirá con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar según los plazos establecidos en la Resolución 2710 del 2017 para la implementación del protocolo IPv6 en Colombia.

El Decreto 1008 de 2018, establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC. Dentro de la política se detalla el Habilitador de Arquitectura, el cual contiene todas las temáticas y productos que deberán desarrollar las entidades en el marco del fortalecimiento de las capacidades internas de gestión de las tecnologías, así mismo el Marco de Referencia de Arquitectura Empresarial V 2.0 es uno de los pilares de este habilitador.

Es así como el “Plan General de Transición para la Adopción de IPv6” se encuentra alineado con lo definido en dicho marco, sus guías y plantillas y funge como uno de los artefactos o productos definidos para mejorar la prestación de los servicios de tecnologías de la información de la E.S.E. en el marco del cumplimiento de la política de Gobierno Digital.

# FASE DE IMPLEMENTACIÓN



El contenido de la figura fue tomado de la Norma ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI

|  |  |  |  |
| --- | --- | --- | --- |
| Evaluación del Desempeño | | | |
| Metas | Resultados | Instrumentos | |
| MSPI | MRAE |
| Planificación y Control Operacional | Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. | Documento con el plan de tratamiento de riesgos.  Documento con la declaración de aplicabilidad. | * LI.ES.09 * LI.ES.10 * LI.GO.04 * LI.GO.09 |
| Implementación del plan de tratamiento de riesgos. | Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. | Documento con la declaración de aplicabilidad.  Documento con el plan de tratamiento de riesgos. | * LI.GO.10 * LI.GO.14 * LI.GO.15 * LI.INF.09 |
| Indicadores De Gestión. | Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. | Guía No 9 - Indicadores de Gestión SI. | * LI.INF.10 * LI.INF.11 * LI.INF.14 * LI.INF.15 |
|  |  |  | * LI.SIS.22 |
|  |  |  | * LI.SIS.23 |
|  |  |  | * LI.ST.05 * LI.ST.06 * LI.ST.09 * LI.ST.10 * LI.ST.12 |
| Plan de Transición de IPv4 a IPv6 | Implementación de las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6. | * LI.ST.13 * LI.UA.01 |

# PLANIFICACIÓN Y CONTROL OPERACIONAL

La E.S.E. Hospital Santa Isabel realizará la planificación, implementación y control a los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información, garantizando que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

Con el compromiso de la alta dirección se realizará ajustes, inicialmente en el manual de procesos y procedimientos (MMC015), buscando la inclusión de la contribución y asesoramiento de toda el área de Gestión de la Información en materia de seguridad, privacidad de la información y aplicación del esquema de gobierno de los componentes de información.

Se documentará la información necesaria que contribuya a evidenciar que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevar un control de cambios como lo describe el Manual de Formas y Formatos (MMC006), que permitirá tomar acciones para mitigar efectos adversos cuando sea necesario.

# IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

La E.S.E. Hospital Santa Isabel ha documentado, establecido y publicado el manual y plan para la administración del riesgo de la E.S.E (IGE002), en el que se documenta el proceso para el tratamiento de los riesgos derivados de la Seguridad de la Información y seguridad digital.

El análisis y evaluación de riesgos inicia desde la caracterización de los activos de información de acuerdo a su criticidad, desde allí se realizará el análisis pertinente y la formulación de los controles.

# INDICADORES DE GESTIÓN

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se unificará al esquema de seguimiento y medición al cumplimiento establecido en la E.S.E. por medio del CMI; en este se incluirán indicadores de aspectos del MSPI que permitan contextualizar una toma de decisiones de manera oportuna.

Se incluirán indicadores de:

* Efectividad en los controles.
* Eficiencia del MSPI al interior de la entidad.
* Conocimiento de seguridad al interior de la entidad.

|  |  |  |
| --- | --- | --- |
| **Nombre del Indicador** | Proporción de avance en la ejecución del MSPI (Modelo de Seguridad y Privacidad de la Información) | |
| **ASPECTOS GENERALES** | | |
| **Justificación** | Conocer el cumplimiento de las actividades implementadas respecto al modelo de seguridad y privacidad de la información | |
| **Atributo o Característica** | Efectividad | |
| **Niveles de Desagregación** | No aplica | |
| **DEFINICIÓN PERACIONAL** | | |
| **Numerador** | Porcentaje ejecutado del plan de trabajo en el periodo | |
| **Denominador** | Porcentaje esperado de avance del plan de trabajo en el periodo | |
| **Unidad de Medición** | Relación porcentual | |
| **Tipo operación aritmética** | Proporción | |
| **Factor** | 100 | |
| **Fórmula de Calculo** | Porcentaje ejecutado del plan de trabajo en el periodo | |
| Porcentaje esperado de avance del plan de trabajo en el periodo | |
|  | **Numerador** | **Denominador** |
| **Fuente de los datos** | MSPI | Diagnostico MSPI |
| **Criterios de inclusión y exclusión** | No aplica | No aplica |
| **Responsable de la Generación de los Datos** | Gestión de la Información | Gestión de la Información |

|  |  |  |  |
| --- | --- | --- | --- |
| **Responsable del Análisis del indicador** | | Gestión de la Información | |
| **Periodicidad recomendada (no**  **obligatoria) de generación de la información** | | Semestral | |
| **METAS** | | | |
| **Desempeño Superior** | | 100% | |
| **Desempeño Bajo** | | 68% | |
| **Direccionalidad del indicador** | | Ascendente | |
|  | | | |
| **Nombre del Indicador** | Porcentaje de nivel de madurez de los controles de seguridad planeados para la vigencia | | |
| **ASPECTOS GENERALES** | | | |
| **Justificación** | Preservar y avanzar en el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información. | | |
| **Atributo o Característica** | Efectividad | | |
| **Niveles de Desagregación** | No aplica | | |
| **DEFINICIÓN PERACIONAL** | | | |
| **Numerador** | Número de Controles con nivel mayor o igual a Efectivo | | |
| **Denominador** | Número total de Controles que se evalúan en el nivel de madurez del MSPI | | |
| **Unidad de Medición** | Relación porcentual | | |
| **Tipo operación aritmética** | Proporción | | |
| **Factor** | 100 | | |
| **Fórmula de Calculo** | Número de Controles Implementados y con nivel mayor o igual a Efectivo | | |
| Número total de Controles que se evalúan en el nivel de madurez del MSPI | | |
|  | **Numerador** | | **Denominador** |
| **Fuente de los datos** | Instrumento de identificación de la línea base de seguridad | | Instrumento de identificación de la línea base de seguridad |
| **Criterios de inclusión y exclusión** | Controles Implementados y con nivel mayor o igual a Efectivo | | No aplica |
| **Responsable de la Generación de los Datos** | Gestión de la Información | | Gestión de la Información |
| **Responsable del Análisis del indicador** | Gestión de la Información | | |
| **Periodicidad recomendada (no** | Semestral | | |



|  |  |
| --- | --- |
| **obligatoria) de generación de la información** |  |
| **METAS** | |
| **Desempeño Superior** | 45% |
| **Desempeño Bajo** | 10% |
| **Direccionalidad del indicador** | Ascendente |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre del Indicador** | | Porcentaje de cumplimiento del Plan de auditorías de seguridad de la información. | | | |
| **ASPECTOS GENERALES** | | | | | |
| **Justificación** | | Velar por el cumplimiento del plan de auditorías de seguridad y privacidad de la información las cuales afectan la planeación requerida en el desarrollo de las actividades del MSPI. | | | |
| **Atributo o Característica** | | Eficacia | | | |
| **Niveles de Desagregación** | | No aplica | | | |
| **DEFINICIÓN PERACIONAL** | | | | | |
| **Numerador** | | Número de auditorías del plan desarrolladas en el periodo evaluado | | | |
| **Denominador** | | Número total de auditorías planeadas en el periodo evaluado | | | |
| **Unidad de Medición** | | Relación porcentual | | | |
| **Tipo operación aritmética** | | Proporción | | | |
| **Factor** | | 100 | | | |
| **Fórmula de Calculo** | | Número de auditorías del plan desarrolladas en el periodo evaluado | | | |
| Número total de auditorías planeadas en el periodo evaluado | | | |
|  | | **Numerador** | **Denominador** | | |
| **Fuente de los datos** | | Plan de Auditorias | Plan de Auditorias | | |
| **Criterios de inclusión y exclusión** | | Número de auditorías del plan desarrolladas en el  periodo evaluado |  | | |
| **Responsable de la Generación de los Datos** | | Gestión de la Información | Gestión de la Información | | |
| **Responsable del Análisis del indicador** | | Gestión de la Información | | | |
| **Periodicidad recomendada (no obligatoria) de generación de la**  **información** | | Semestral | | | |
| **METAS** | | | | | |
| **Desempeño Superior** | | 100% | | | |
| **Desempeño Bajo** | | 70% | | | |
|  | 42 de 48 | Edición: 2 | | MIF013 |  |



|  |  |
| --- | --- |
| **Direccionalidad del indicador** | Ascendente |

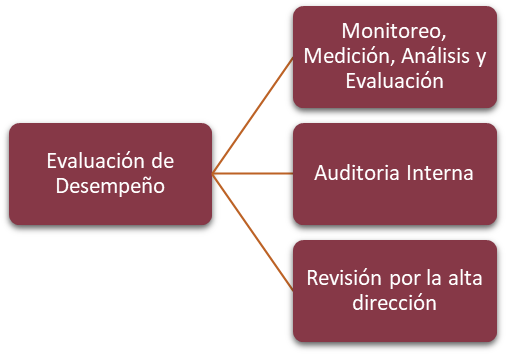
|  |  |  |
| --- | --- | --- |
| **Nombre del Indicador** | Porcentaje de colaboradores que obtuvieron entre 8 y 10 en la  evaluación de conocimiento de las Políticas de Seguridad y Privacidad de la información y Seguridad Digital. | |
| **ASPECTOS GENERALES** | | |
| **Justificación** | Identificar el nivel de cultura de los colaboradores de la Entidad | |
| **Atributo o Característica** | Gestión del conocimiento | |
| **Niveles de Desagregación** | No aplica | |
| **DEFINICIÓN PERACIONAL** | | |
| **Numerador** | Número de colaboradores que obtuvieron entre 8 y 10 en la evaluación de conocimiento de las Políticas de Seguridad y Privacidad de la información y Seguridad Digital. | |
| **Denominador** | Número total de colaboradores que realizaron la capacitación | |
| **Unidad de Medición** | Relación porcentual | |
| **Tipo operación aritmética** | Proporción | |
| **Factor** | 100 | |
| **Fórmula de Calculo** | Número de colaboradores que obtuvieron entre 8 y 10 en la evaluación de conocimiento de las Políticas de Seguridad y Privacidad de la información y Seguridad Digital. | |
| Número total de colaboradores que realizaron la capacitación | |
|  | **Numerador** | **Denominador** |
| **Fuente de los datos** | Informe de Capacitaciones | Informe de Capacitaciones |
| **Criterios de inclusión y exclusión** | Colaboradores con puntaje entre 8 y 10 en el primer  intento | No aplica |
| **Responsable de la Generación de los Datos** | Plataforma de capacitaciones | Plataforma de capacitaciones |
| **Responsable del Análisis del indicador** | Gestión de la Información | |
| **Periodicidad recomendada (no**  **obligatoria) de generación de la información** | Anual | |
| **METAS** | | |
| **Desempeño Superior** | 87% | |
| **Desempeño Bajo** | 60% | |
| **Direccionalidad del indicador** | Ascendente | |

|  |  |  |
| --- | --- | --- |
| 43 de 48 | Edición: 2 | MIF013 |

# PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se elaborará el documento detallado con el Plan de Transición e Implementación del Protocolo IPv6 en la Entidad. Las guías de apoyo para esta labor son “Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6”.

# FASE DE EVALUACIÓN DE DESEMPEÑO



Fuente: Documento Modelo de Seguridad y Privacidad de la Información Estrategia de Gobierno en Línea

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Evaluación del Desempeño | | | | | | | |
| Metas | | Resultados | | Instrumentos | | | |
| MSPI | | MRAE | |
| Plan de revisión y seguimiento, a la implementación del MSPI. | | Documento actualizado con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. | | Guía No 16 – Evaluación del desempeño. | | * LI.ES.12 * LI.ES.13 * LI.GO.03 * LI.GO.11 * LI.GO.12 * LI.INF.09 * LI.INF.11 * LI.INF.13 * LI.INF.14 * LI.INF.15 * LI.SIS.23 * LI.ST.05 | |
| 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. | | Guía No 15 – Guía de Auditoría. | |
|  | 44 de 48 | | Edición: 2 | | MIF013 | |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | * LI.ST.06 * LI.ST.08 * LI.ST.15 * LI.UA.07 * LI.UA.08 |

La E.S.E., evaluará el desempeño y la eficacia del MSPI contra las políticas, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la sub mesa de gobierno digital y a la alta dirección para su revisión y toma de decisiones.

* + 1. **PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DEL MSPI**

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

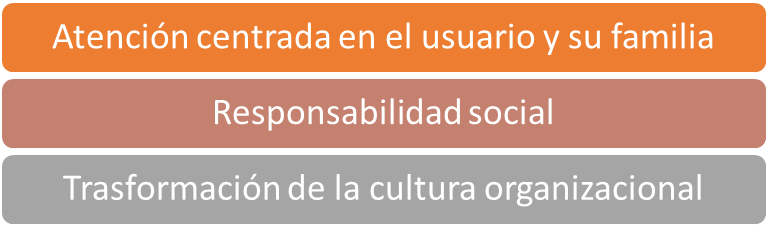
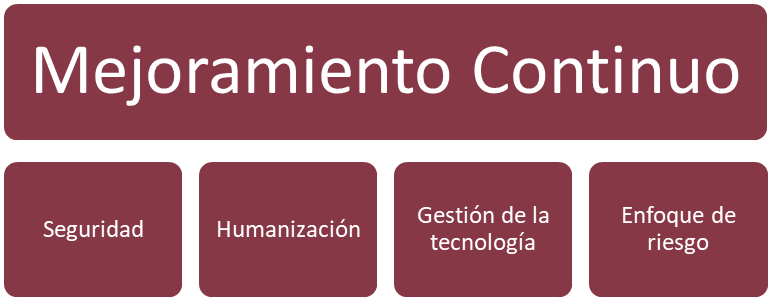
En esta acción se llevará a cabo las siguientes actividades:

* 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 riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
* Seguimiento a la programación y ejecución de las actividades de auditorías 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 E.S.E.
* Revisión de los resultados de los indicadores de gestión del MSPI.
* Revisiones de acciones o planes de mejora.

# PLAN DE EJECUCIÓN DE AUDITORIAS

En esta etapa se adopta el Manual de Auditoría (MMC002), de la E.S.E., donde se define el programa general de auditoría, teniendo como entrada el PAMEC institucional, en el cual, a partir de la ruta crítica, identifica los estándares y procesos priorizados para la vigencia; frente a los cuales se implementan las auditorías que integran el programa general de auditorías de la vigencia.

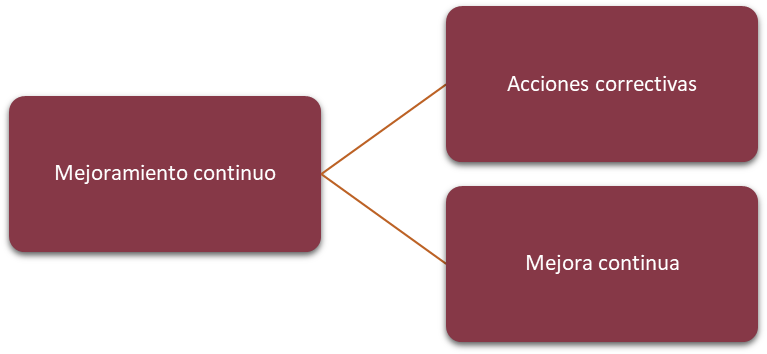
El Programa General de Auditorías de la E.S.E. adopta los pilares del Sistema Único de Acreditación, teniendo en cuenta que es esté, el eje central del PAMEC institucional.



A partir de la priorización de estándares y procesos del PAMEC, se define para el programa de auditorías de la vigencia los siguientes:

* + - * Procesos a auditar.
      * Frecuencia de las auditorías.
      * Alcance de las auditorías.
      * Criterios que se van a auditar y que se tendrán en cuenta para la construcción de las Listas de chequeo de las auditorías.

# FASE DE MEJORA CONTINUA



|  |  |  |  |
| --- | --- | --- | --- |
| Mejora continua | | | |
| Metas | Resultados | Instrumentos | |
| MSPI | MRAE |
| Plan de mejora continua | Documento con el plan de mejoramiento.  Documento con el plan de comunicación de resultados. | Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17  – Mejora Continua | * LI.GO.03 * LI.GO.12 * LI.GO.13 * LI.INF.14 * LI.INF.15 * LI.ST.15 * LI.UA.9 * LI.UA.10 |

La E.S.E. con la visión de mantener y mejorar los aspectos de seguridad de la información, adoptará el modelo de mejoramiento continuo (UMC003) desarrollado en la E.S.E., en este se tomarán en cuenta los resultados de la fase 4 “Evaluación de desempeño” la cual está basada en los resultados de las actividades de seguimiento y medición (indicadores). Los resultados obtenidos en el plan de mejoramiento continuo, se presentarán a la Sub Mesa de Gobierno Digital anualmente, también desde esta se evaluarán las capacitaciones que serán incluidas en el PIC (Plan Institucional de Capacitaciones) de la E.S.E.

Por lo tanto, la E.S.E.:

* Implementará las mejoras identificadas en el MSPI
* Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.
* Implementará acciones de mejora basadas en las lecciones aprendidas.

# BIBLIOGRAFIA

* [Decreto 2573 de 2014 Por el cual se establecen los lineamientos](https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf) [generales de la Estrategia de Gobierno en línea](https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf)
* Norma técnica colombiana NTC-ISO /IEC 27005
* [Modelo de Seguridad y Privacidad de la Información (MSPI)](https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf)

[Guías para la construcción del Modelo de Seguridad y Privacidad de la](https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/) [Información (MSPI)](https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/)