TABLA DE CONTENIDO

INTRODUCCIÓN

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

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

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 riesgos.

La RAP, reconoce la importancia y ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones dado que en la gestión de los procesos estratégicos, misionales y de apoyo, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa para la entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de Gestión y Seguridad de la Información, siguiendo los lineamientos del MSPI de la Estrategia de Gobierno Digital, a su vez reglamentado a través del Decreto 1008 de 2018, Decreto 1078 de 2015 y el Decreto 2573 de 2014 y el CONPES 3854 de 2016, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno Digital.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, el SGSI de la RAP adoptará una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

Así mismo, el SGSI de la RAP definirá políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoría y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

Lo anterior se complementa con los programas de formación y transferencia de conocimiento en seguridad de la información y las campañas de sensibilización que se liderarán al interior de la entidad. Así pues, la entidad expone a través de este manual el modelo del SGSI adoptado por la entidad de acuerdo con el ciclo PHVA (planear, hacer, verificar y actuar), con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada.

Dicho plan establecerá el contexto, las políticas, los objetivos, el alcance, los procedimientos, las metodologías, los roles, las responsabilidades y las autoridades del SGSI; de acuerdo con los requisitos legales, los contractuales y los normativos, que le aplican a la entidad, en el marco de seguridad de la información. Para tal fin, la entidad ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2015, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2018 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como ISO 27002:2022, ISO 27005:2018, el modelo nacional de riesgos de seguridad digital y las guías definidas por el MinTIC para la implementación del MSPI; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

1. OBJETIVO

Asegurar la adopción integral del Modelo se Seguridad y Privacidad de la Información (MSPI) bajo un enfoque de mejora continua.

OBJETIVOS ESPECÍFICOS

- ✓ Establecer un cronograma basado en el ciclo de mejora continua para la adopción integral del Modelo de Seguridad y Privacidad de la Información.
- ✓ Establecer medidas de implementación y de verificación de los controles previstos en el Modelo de Seguridad y Privacidad de la Información con base en los riesgos identificados de seguridad de la información en la entidad.
- ✓ Comunicar e implementar la estrategia de seguridad de la información.
- ✓ Incrementar el nivel de madurez en la gestión de la seguridad de la información.

2. ALCANCE

El plan está previsto para el alcance del Sistema de Gestión de Seguridad de la Información de la Región Administrativa y de Planificación - RAP EJE CAFETERO, el cual proveerá las herramientas de control en general a la gestión segura de la información en la totalidad de los procesos de la Entidad.

3. MARCO NORMATIVO

- **Constitución Política.** Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.

- **Ley 527 de 1999.** "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"

- **Ley 594 de 2000.** "Ley General de Archivo"

- **Ley 962 de 2005.** "Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas"

- **Ley 1150 de 2007.** "Seguridad de la información electrónica en contratación en línea"

- **Ley 1266 de 2008**. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países

- **Ley 1273 de 2009.** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.

- **Ley 1341 de 2009.** "Tecnologías de la Información y aplicación de seguridad".

- **Ley 1437 de 2011.** "Procedimiento Administrativo y aplicación de criterios de seguridad".

- **Ley 1480 de 2011.** "Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas".

- **Ley 1581 de 2012.** "Por la cual se dictan disposiciones generales para la Protección de Datos Personales".

- **Decreto Ley 019 de 2012.** "Racionalización de trámites a través de medios electrónicos. Criterio de seguridad".

- **Ley 1621 de 2013.** "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones".

- **Ley 1712 de 2014.** "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

- **Decreto 1727 de 2009.** "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información".

- **Decreto 2952 de 2010.** "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".

- **Decreto 2364 de 2012.** "Firma electrónica".

- **Decreto 2609 de 2012**. "Expediente electrónico"

- **Decreto 2693 de 2012**. "Gobierno electrónico"

- **Decreto 1377 de 2013.** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

- **Decreto 1510 de 2013.** "Contratación pública electrónica"

- **Decreto 886 de 2014.** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"

- **Decreto 1083 de 2015.** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".

- **Decreto 1078 de 2015.** Por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de Información y las Comunicaciones.

- **Decreto 1008 de 2018.** "Por el 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 Tecnologías de la Información y las Comunicaciones"

- **Decreto 1413 de 2017.** "Por la cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2018, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- **Decreto 415 de 2016.** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2011 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.

- **CONPES 3975 de 2019.** Política Nacional para la Transformación Digital e Inteligencia Artificial.

- **Resolución 1519 de 2020.** "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".

4. GLOSARIO

- **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 esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

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

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

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

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior. (ArCert).

- **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).

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000).

- **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).

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000).

- **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).

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000).

- **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.

- **No repudio:** El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. También se puede definir como el servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (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.

- **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 Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original. (ArCert).

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

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

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

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

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

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

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

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

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

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

5. PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

El 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 seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno Digital, 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.
La Entidad, buscando desarrollar el Modelo de Seguridad y Privacidad de la Información (MSPI) ha establecido una estrategia integral de aseguramiento de la información de forma tal que su adopción se está realizando de forma integrada con el Sistema de Gestión de Seguridad de la Información, considerando que la norma ISO/IEC 27001:2022 es base de ambos sistemas y que las guías técnicas desarrolladas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, se basan en dicha norma y consideran el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia Gobierno Digital: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

A nivel metodológico, se ha seguido la estructura riesgo - control, de forma tal que las actividades iniciales están orientadas a conocer los riesgos de seguridad de la información (Guía 7 - Gestión de Riesgos) alineado al Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD), para ello es necesario comenzar con la identificación de los activos (Guía 5 – Guía para la Gestión y Clasificación de Activos de Información) y las posteriores a tratarlo (Guía 8 - Controles de Seguridad de la Información) así como a asegurar la mejora continua en el proceso de gestión del riesgo y de seguridad de la información (Guía 9 - Indicadores Gestión de Seguridad de la Información, Guía 15 – Auditoria, Guía 16 - Evaluación de Desempeño, y Guía 17 - Mejora continua).

Las demás guías, dada su naturaleza de control, una vez alineadas con el Anexo A de la norma ISO/IEC 27001 son aplicadas conforme a los resultados del análisis de riesgos: Guía 2 - Política General MSPI, Guía 1 - Metodología de pruebas de efectividad, Guía 6 - Gestión Documental, Guía 4 - Roles y responsabilidades, Guía 3 - Procedimiento de Seguridad de la Información, Guía 12 - Seguridad en la Nube, Guía 21 - Gestión de Incidentes, Guía 13 - Evidencia Digital, Guía 10 - Continuidad de Negocio, Guía 11 - Análisis de Impacto de Negocio.

Este apartado del documento busca proveer a las Entidades del Estado en general, y a la RAP en particular, un conjunto de lineamientos de seguridad de la información para que la alta dirección conozca los requisitos y etapas para la implementación del Modelo de Seguridad y Privacidad de la Información, abordando aspectos que cubren la preparación de la entidad, la definición de las brechas, la alineación y la implementación del Sistema de Gestión de Seguridad de la Información, SGSI, como modelo sostenible:

ACCIONES	RESULTADOS	HERRAMIENTA	DURACIÓN
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad Identificar el nivel de madurez de seguridad y privacidad de la información	Diagnóstico de la Entidad en seguridad y privacidad de la información	Instructivo de Evaluación	1 MES
Desarrollo de las políticas Comunicación de la política Monitoreo	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	1 MES
Inventario de activos Clasificación y etiquetado de activos de la información Gestión de los activos de información (Propiedad, uso, devolución, manejo de activos)	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información.	Guía No 5 - Gestión Clasificación de Activos	1 MES
Contextualización Modelado de amenazas Evaluación de Vulnerabilidades	Documento identificando vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Guía No 1 - Metodología de Pruebas de Efectividad	MES Y MEDIO
Identificación de Riesgos Análisis de riesgos Evaluación del riesgo Valoración de controles para el tratamiento del riesgo	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	Guía No 7 - Gestión de Riesgos. Guía No 8 - Controles de Seguridad de la Información	MES Y MEDIO
Políticas de administración del riesgo	Documentos revisados y aprobados por la alta Dirección.	Guía 12- Seguridad en la Nube Guía 18 – Lineamientos terminales de áreas financieras de entidades públicas	

Análisis de Impacto del Negocio	Documento de impacto del negocio con los procesos críticos, prioridades de sistemas y aplicaciones, listado de tiempos	Guía No 10 - Continuidad de Negocio Guía No 11 - Análisis de Impacto de Negocio	1 MES
Ajuste y/o creación de procedimientos de la entidad en lo relacionado a seguridad de la información Integración del MSPI con el Sistema de Gestión documental Definición de roles y responsabilidades	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional. Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información Guía No 6 - Gestión Documental Guía No 4 - Roles y responsabilidad es de seguridad y privacidad de la información.	1 MES
Diseño del programa de sensibilización y capacitación Implementación del programa	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	15 DIAS
Indicadores De Gestión SGSI Planeación de la auditoría Revisión y Seguimiento del MSPI	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 9 - Indicadores de Gestión SI. Guía No 15 – Guía de Auditoría.	1 MES
Plan de mejoramiento	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. Documento con el plan de mejoramiento	Guía No 16 – Evaluación del desempeño. Guía No 17 – Mejora Continua	
Detección, evaluación y análisis de incidentes	Documento para la gestión de incidentes	Guía No 21 - Gestión de Incidentes	15 DIAS

6. DESCRIPCIÓN DETALLADA DEL CICLO DE OPERACIÓN

La implementación de políticas, lineamientos y buenas prácticas que buscan proteger la información como activo valioso, es el objetivo del conjunto de estándares tenidos en cuenta en el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden.

En este sentido, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta la Entidad y a efectos de asegurar la continuidad de negocio y minimizar los daños, se desarrollan una serie de pasos de aplicación propuestos por MINTIC.

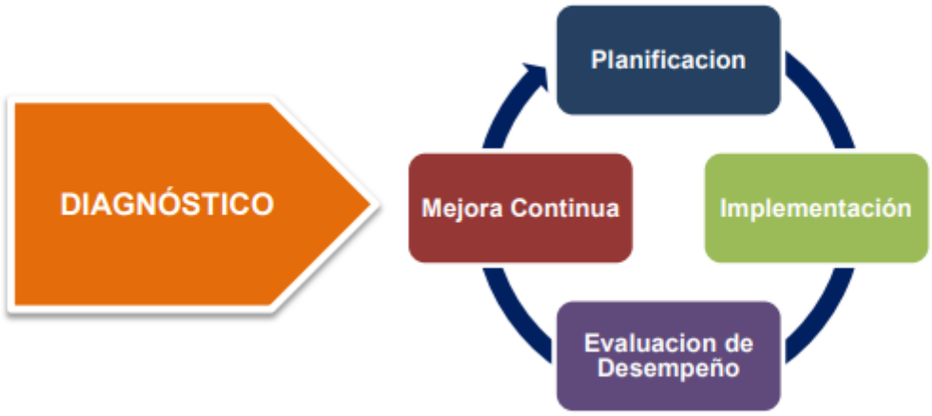

Ilustración – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

6.1. FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

Con el fin de identificar el estado actual y el nivel de madurez de seguridad y privacidad de la información en la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, que de ahora en adelante se denominará MSPI, el cual hace parte integral de la Estrategia de Gobierno digital, la RAP ejecuta una lista de actividades.

Ilustración – Etapas previas a la implementación

La herramienta principal implementada es el instrumento recomendado por MinTIC:

- Autoevaluación del Modelo de Seguridad de la Información: Este brinda un punto de partida a las entidades al realizar un diagnóstico de los requisitos del MSPI que se han desarrollado, de acuerdo con el nivel madurez y los dominios de la norma ISO 27001:2022.

Se recolectó la información con la ayuda de la guía de autoevaluación y se envía al Ministerio TIC para su análisis y posterior retroalimentación a la Entidad.

El resultado de la aplicación del instrumento de autoevaluación servirá como base para determinar el nivel de madurez de seguridad y privacidad de la información en la entidad y establecer la brecha con los objetivos a alcanzar.

Una vez Ministerio TIC remita a la Entidad el resultado del diagnóstico inicial y se haya determinado el nivel de madurez, se procede al desarrollo de la fase de Planificación. Los entregables asociados a las metas en la fase de etapas previas a la implementación deben ser revisados y aprobados por la alta Dirección.
En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

Tabla - Metas, Resultados e Instrumentos de la fase etapas previas a la implementación:

Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

6.2. FASE DE PLANIFICACIÓN

Esta fase tiene la finalidad de generar un plan de seguridad y privacidad alineado con el propósito misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

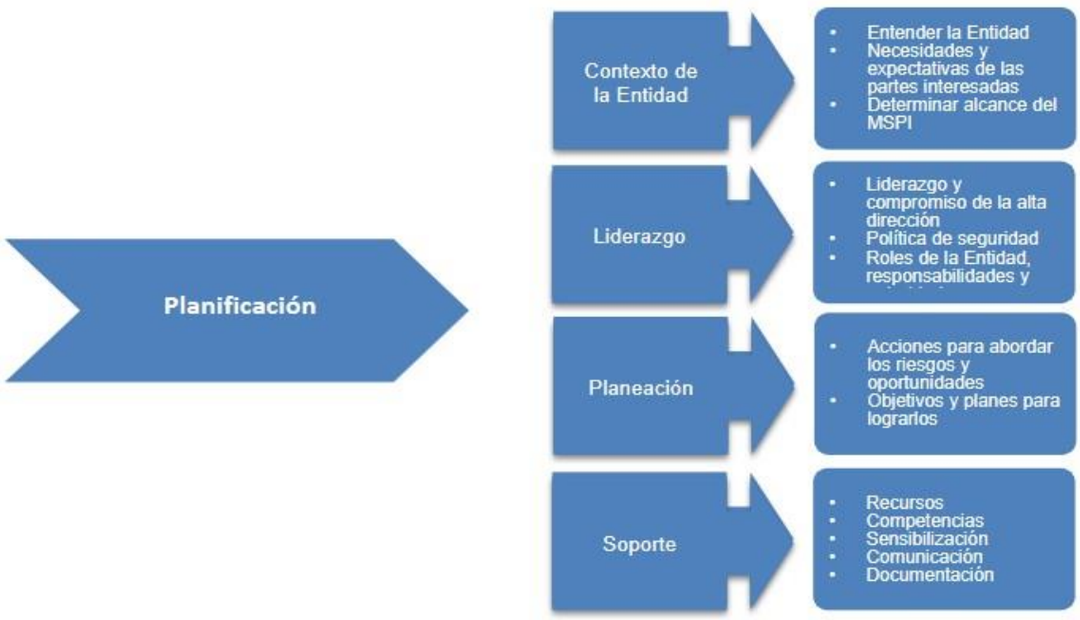

Ilustración - Fase de planificación

En la fase de Planificación del MSPI se pretende alcanzar las siguientes metas:

Planificación			
Metas	**Resultados**	**INSTRUMENTOS MSPI**	**MRAE**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 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 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
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestion Documental	
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Guía No 7 - Gestion 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	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	

Tabla - Metas, Resultados e Instrumentos de la Fase de Planificación

Los resultados asociados a las metas en la Fase de Planificación deben ser revisados y aprobados por la alta Dirección.

6.3.FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad llevar a cabo la implementación de las actividades planificadas en la fase de planificación del MSPI, teniendo en cuenta los aspectos más relevantes en los procesos de implementación del MSPI.

Ilustración - Fase de implementación

Tomando como base en los resultados obtenidos en las fases de previas a la implementación y planificación del Modelo de Operación de Seguridad y Privacidad de la Información (MSPI), y de acuerdo con la identificación de las necesidades de la Entidad, se elabora el plan de Implementación y se ejecuta el plan de tratamiento de riesgos del MSPI.

Implementación			
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 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 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
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.	
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.	
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	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

Tabla Metas, Resultados e Instrumentos de la Fase de Implementación

6.4.FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base en los resultados que arroja los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.

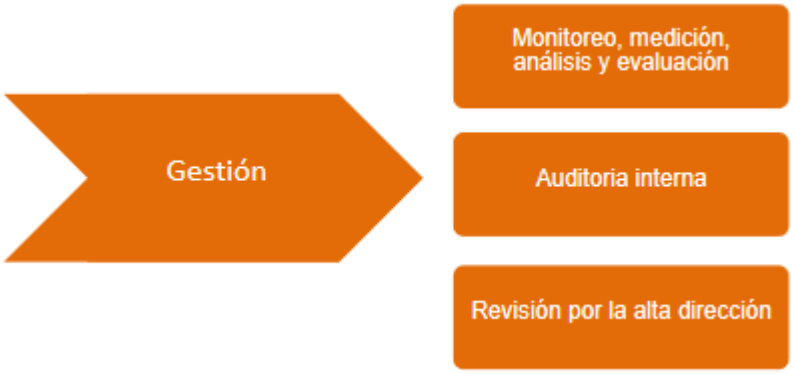

Ilustración - Fase de Evaluación de desempeño

Para definir el plan de seguimiento, evaluación y análisis del MSPI, se requiere dar respuesta a los siguientes interrogantes:

1. ¿Qué actividades dentro del MSPI deben ser monitoreadas y evaluadas?
2. ¿Qué acciones son necesarias para ese seguimiento y evaluación?
3. ¿Quién es el responsable de las acciones de seguimiento y evaluación?
4. ¿Cuándo se planifican las acciones de seguimiento y evaluación (oportunidad y periodicidad)?
5. ¿Qué metodología se está usando para hacer seguimiento y evaluación del MSPI?
6. ¿Qué recursos (financieros, humanos, técnicos, entre otros) se requieren para la ejecución del plan de seguimiento?

Evaluación del Desempeño			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	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 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
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.	

Tabla - Evaluación de desempeño

6.5. FASE DE MEJORA CONTINUA

Esta fase le permitirá a la Entidad, consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.

Ilustración - Fase de mejoramiento continúo

En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

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

Tabla 4 - Fase de mejoramiento continuo

7. DOCUMENTOS DE REFERENCIA

Ministerio de Tecnologías de Información, Modelo de Seguridad de la Información, disponible en https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de- Seguridad/

Ministerio de Tecnologías de Información, Modelo de Gestión de Riesgos de Seguridad digital