SECRETARÍA DISTRITAL DE PLANEACIÓN

A-LE-373 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SDP

Responsables:

Comité Institucional de Gestión y Desempeño
Dirección de Tecnologías de la Información y las Comunicaciones
Actualización presentada y aprobada en sesión del Comité Institucional de Gestión y Desempeño de la SDP realizada el 26 de julio de 2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Con el fin de brindar herramientas para proteger a las entidades públicas de sufrir incidentes de seguridad digital que cada vez son más frecuentes y que podrían llegar a afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, como entidad encargada de establecer los lineamientos para la implementación de la Política de seguridad Digital y la Política de Gobierno Digital en las entidades públicas, elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y definió los lineamientos para su implementación.

La Alta Dirección de la Secretaría Distrital de Planeación - SDP, en su claro compromiso frente a los temas relacionados con la Seguridad de la Información, forma parte del Comité Institucional de Gestión y Desempeño, instancia encargada de aprobar el Modelo de Seguridad y Privacidad de la Información – MSPI y asegurar su articulación con el Modelo Integrado de Planeación y Gestión. En este sentido, la SDP, expidió las Resoluciones No. 1923 de 2022 “Por la cual se dictan otras disposiciones relacionadas con el Sistema de Gestión SG-MIPG de la Secretaría Distrital de Planeación y se deroga la Resolución 0998 de 2021” y la Resolución No. 1771 de 2018 “por la cual se establecen los responsables de la Política de Gobierno Digital”; así mismo, aprobó la Política de Seguridad de la Información A-LE-429 y la Declaración de Aplicabilidad del SGSI en la SDP (A-LE-334), de acuerdo con los controles del Anexo A, de la norma internacional ISO/IEC 27001, versión 2013 entre otros instrumentos que hacen parte la implementación del MSPI y que conforman el Sistema de Gestión de Seguridad de la Información SGSI.

El desarrollo del Modelo de Seguridad y Privacidad de la Información – MSPI, en la SDP, se basa en la aplicación de la metodología del ciclo PHVA (Planear, Hacer, Verificar y Actuar) y el cumplimiento de los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento definidos por MINTIC; el modelo consta de cinco (5) fases **Diagnóstico, Planificación, Operación, Evaluación de desempeño y**

Mejoramiento Continuo. las cuales se describen en el presente documento.1

2. ALCANCE

El Modelo de Seguridad y Privacidad de la Información – MSPI aplica a todos los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de la Secretaría Distrital de Planeación, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

3. OBJETIVO GENERAL

Proporcionar en la Secretaría Distrital de Planeación los mecanismos, lineamientos e instrumentos que permitan adoptar, implementar y apropiar el Modelo de Seguridad y Privacidad de la Información - MSPI de conformidad con las directrices dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC y la Alta Consejería Distrital de TIC

4. OBJETIVOS ESPECÍFICOS

- Desarrollar e implementar la estrategia de seguridad digital en la Secretaría Distrital de Planeación.

- Establecer procedimientos de seguridad que permitan a la Secretaría Distrital de Planeación apropiar el habilitador de seguridad en la política de Gobierno Digital.

- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de la Secretaría Distrital de Planeación.

1 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.
- Contribuir al desarrollo y ejecución del Plan Estratégico de la Secretaría Distrital de Planeación y el Plan Estratégico de Tecnologías de la Información y de las Comunicaciones a través del Plan de Seguridad y Privacidad de la Información.

5. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Modelo de Seguridad y Privacidad de la Información – MSPI, es el instrumento que soporta el habilitador transversal de la Seguridad de la Información de la Secretaría Distrital de Planeación - SDP, y de acuerdo con el Manual de Gobierno Digital, busca “que la SDP implemente los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos”.

El ciclo de operación definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC para el Modelo, define para la Implementación del MSPI cuatro etapas: PLANIFICACIÓN, OPERACIÓN, EVALUACIÓN DEL DESEMPEÑO Y MEJORA CONTINUA.

Figura 1. *Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información*
Fuente: *"Modelo de Seguridad y Privacidad de la Información"* - Anexo 1 de la Resolución 500 de 2021 de MINTIC

A continuación, se describen las fases del modelo que dan cumplimiento a las directrices del Gobierno Nacional (Resolución 500 de 2021 de 2021, Anexo 1 Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones dispuesto por MINTIC) y Gobierno Territorial (Alta Consejería Distrital de TIC).

6. FASE DE DIAGNÓSTICO

En cumplimiento de la Política de Gobierno Digital, la Política de Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información, La Secretaría Distrital de Planeación, en esta fase debe establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifican de forma específica los controles implementados y faltantes y de esta manera contar con insumos para la fase de planificación.

El diagnóstico se realiza antes de iniciar la fase de planificación, y luego se actualiza posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño, será incluido como un insumo en la fase de mejoramiento continuo.

Lineamiento:

Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la entidad respecto a la Seguridad y privacidad de la Información.

Propósito:

Identificar el nivel de madurez de seguridad y privacidad de la información en el que se encuentra la entidad, como punto de partida para la implementación del MSPI.

5.1 DIAGNÓSTICO	
Entradas	**Salidas**
• Para la identificación del estado de implementación del MSPI, se utiliza la herramienta de autodiagnóstico del MSPI. • Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.	• Documento con el resultado de la aplicación de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en la Entidad, y sus acciones de mejora.

7. FASE 1: PLANIFICACION

Para el desarrollo de esta fase se utilizan los resultados de la fase anterior para proceder a elaborar el Plan de Seguridad y Privacidad de la Información, con el objetivo de realizar la planeación del tiempo, recursos y presupuesto de las actividades que se van a desarrollar relacionadas con el MSPI.

Los documentos que se deben generar en esta fase son:

- Alcance MSPI
- Acto administrativo con las funciones de seguridad y privacidad de la información.
- Política de seguridad y privacidad de la información.
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
- Procedimiento de inventario y clasificación de la Información e infraestructura crítica
- Metodología de inventario y clasificación de la información e infraestructura crítica
- Procedimiento de gestión de riesgos de seguridad de la información
- Plan de tratamiento de riesgos de seguridad de la información
- Declaración de aplicabilidad
- Manual de políticas de Seguridad de la Información
- Plan de capacitación y sensibilización en seguridad de la información.

7.1. Contexto

7.1.1. Comprensión de la organización y de su contexto

Lineamiento:

Determinar los elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la entidad.

Propósito:

Conocer en detalle las características de la entidad y su entorno con el fin de implementar el Modelo de Seguridad y Privacidad de la Información adaptado a las condiciones específicas de cada entidad.

FASE 1 PLANIFICACIÓN 7.1.1 Comprensión de la organización y de su contexto	
Entradas	Salidas

FASE 1 PLANIFICACIÓN 7.1.1 Comprensión de la organización y de su contexto	
• Para establecer el contexto de la Entidad debe tener en cuenta los aspectos relacionados en el Manual Operativo MIPG. • Modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	Documentos obligatorios: Contexto de la entidad
• Plan Estratégico de la Entidad	

7.1.2. Necesidades y expectativas de los interesados

Lineamiento:

Se deben determinar las partes interesadas internas o externas y personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información de la entidad o que puedan verse afectados en caso de que estas se vean comprometidas. Adicionalmente se deberán determinar las necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información. Las partes interesadas deberán incluir los requisitos legales, reglamentarios y contractuales.

Propósito:

Conocer las expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información, para asegurar que el modelo garantizará su cumplimiento.

FASE 1 PLANIFICACIÓN 7.1.2 Necesidades y expectativas de los interesados	
Entradas	**Salidas**
• Comprensión de la organización y de su contexto (Numeral 7.1.1). • Política de Planeación institucional (Numeral 7.1.1). Comprensión de la organización y de su contexto). • Plan Nacional de Desarrollo. • Política de Gobierno Digital. • Entrevistas con los líderes de procesos de la Entidad. • Listado de entidades de orden nacional o territorial que se relacionan directamente el cumplimiento misional de la Entidad.	Documentos obligatorios: Partes interesadas. (Política de Planeación Institucional).

FASE 1 PLANIFICACIÓN 7.1.2 Necesidades y expectativas de los interesados	
• Listado de proveedores de la Entidad. • Listado de operadores de la Entidad. • Normatividad que le aplique a la Entidad de acuerdo con funcionalidad respectivamente.	

7.1.3. Definición del alcance del MSPI

Lineamiento:

Determinar los límites y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad. Determinar a qué procesos y recursos tecnológicos se realizará la implementación del MSPI.

Propósito:

Identificar qué información (generada o utilizada en los procesos de la entidad) será protegida mediante la adopción del MSPI.

FASE 1 PLANIFICACIÓN 7.1.3 Definición del alcance del MSPI	
Entradas	**Salidas**
• 7.1.1 Comprensión de la organización y de su contexto. • 7.1.2 Necesidades y expectativas de los interesados. • Modelo de procesos, modelo organizacional, modelo de servicios y catálogo de servicios tecnológicos; siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Presupuesto disponible para implementar el MSPI. • Listado de las sedes físicas donde opera la Entidad.	• Alcance del MSPI (Este alcance puede estar integrado al Manual del Sistema de Gestión, o en el documento del Modelo de Planeación y Gestión).

7.2. Liderazgo

7.2.1. Liderazgo y Compromiso

Lineamiento:

La Entidad debe incluir como parte de las funciones del Comité Institucional de Gestión y Desempeño o quien haga sus veces, las relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo, con el propósito de facilitar la implementación, de modo que permita dar cumplimento entre otras, a las siguientes acciones:

- Establecer y aprobar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Asegurar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Apropiar el conocimiento en la entidad en temas relacionados con el MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo, etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos una vez por año).

Propósito:

Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.

FASE 1 PLANIFICACIÓN 7.2.1 Liderazgo y Compromiso	
Entradas	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • 7.1.2 Necesidades y expectativas de los interesados.	• Evidencia en el acto administrativo que soporta la conformación del Comité Institucional de Gestión y Desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

7.2.2. Política de seguridad y privacidad de la información

Lineamiento:

Se debe establecer en la política de seguridad y privacidad de la información, en la que se debe tener en cuenta lo siguiente:

- Misión de la entidad
- Normatividad vigente la cual se debe contar para el funcionamiento de la entidad
- Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua una vez el MSPI sea adoptado
- Estar alineada con el contexto de la entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.
- Se deben asignar los roles y responsabilidades que se identifiquen.
- Actualizar el acto administrativo de constitución del Comité Institucional de Gestión y Desempeño, incluyendo temas de seguridad de la información y seguridad digital.
- Ser comunicada al interior de la entidad y a los interesados que aplique.
- La política establece la base respecto al comportamiento de personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad.

Propósito:

Orientar y apoyar por parte de la alta dirección de la entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente.

FASE 1 PLANIFICACIÓN 7.2.2 Política de seguridad y privacidad de la información	
Entradas	Salidas

FASE 1 PLANIFICACIÓN 7.2.2 Política de seguridad y privacidad de la información	
• Comprensión de la organización y de su contexto. • Necesidades y expectativas de los interesados. • Definición del alcance del MSPI. • Requerimientos normativos.	• Acto administrativo con la adopción de la Política de seguridad y privacidad de la información.

7.2.3. Roles y responsabilidades

Lineamiento:

Articular con las áreas o dependencias de la entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el Comité Institucional de Gestión y Desempeño, para que sean aprobados y comunicados dentro de la entidad. Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; si el cargo no existe en la entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica de la Entidad, de igual manera la persona designada deberá ser incluida como miembro del Comité Institucional de Gestión y Desempeño y en el Comité de Control Interno con voz, pero sin voto.

Propósito:

Hay que asegurar que los funcionarios de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

FASE 1 PLANIFICACION 7.2.3 Roles y responsabilidades	
Entradas	**Salidas**
• 7.1.3 Definición del alcance del MSPI • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.	Roles y responsabilidades

7.3. Planificación

7.3.1. Identificación de activos de información e infraestructura critica

Lineamiento:

La entidad debe definir y aplicar un proceso de identificación y clasificación de la información, que permita:

- Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
- Clasificar los activos de información de acuerdo a los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.
- Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.

Propósito:

Estructurar una metodología que permita identificar y clasificar los activos de información

PLANIFICACIÓN 7.3.1 Identificación de activos de información e infraestructura crítica	
Entradas	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Guía para la Gestión y Clasificación de Activos de Información.	• Procedimiento de inventario y clasificación de la información.2 • Documento metodológico de inventario y clasificación de la información.

7.3.2. Valoración de los riesgos de seguridad de la información

Lineamiento:

La entidad debe definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita:

- Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI.
- Identificar los responsables de la gestión de riesgos. dueños de los riesgos.
- Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
- Determinar el apetito de riesgos definido por la entidad
- Establecer criterios de aceptación de los riesgos.
- Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance.
- Determinar los niveles de riesgo.
- Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral.

2 Anexo 1. Guía para la Gestión y Clasificación de Activos de Información

- Priorización de los riesgos analizados para su tratamiento.

Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables.

Propósito:

Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.

FASE 1: PLANIFICACIÓN 7.3.2 Valoración de los riesgos de seguridad de la información	
Entradas	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • 7.2.2 Política de seguridad y privacidad de la información. • Directorio de servicios de componentes de información, de acuerdo con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Inventario de activos de información de la Entidad usando: o Guía - Gestión inventario, clasificación de activos e infraestructura critica • Proceso de valoración de riesgos de la seguridad de la información definido por medio de: o Lineamientos para la Gestión del Riesgo de Seguridad Digital en entidades Públicas - Guía riesgos vigente.	• Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno.

7.3.3. Plan de tratamiento de los riesgos de seguridad de la información

Lineamiento:

- La entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:
- Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.

- Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.
- Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad. Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional de Gestión y Desempeño, o quien haga sus veces.

Propósito:

- Estructurar una metodología que permita definir las acciones que debe seguir la entidad para poder gestionar los riesgos de seguridad y privacidad de la información.

FASE 1: PLANIFICACIÓN 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información	
Entradas	**Salidas**
• Inventario de activos de información de la Entidad. • 7.3.2 Valoración de los riesgos de seguridad de la información	• A-LE-515 Plan de tratamiento de riesgos de seguridad de la información, aprobado por el Comité Institucional de Gestión y Desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). • A-LE-334 Declaración de aplicabilidad, aceptada y aprobadas en el Comité Institucional de Gestión y Desempeño.

7.4. Soporte

7.4.1. Recursos

Lineamiento:

- La entidad debe determinar y proporcionar los recursos necesarios para adoptar el MSPI, teniendo en cuenta que es un proceso transversal de la entidad, se requiere que se disponga de los recursos humanos, técnicos, financieros y en general

cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI.

Propósito:

Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.

FASE 1: PLANIFICACIÓN 7.4.1 Recursos	
Entradas	**Salidas**
• 7.1 Contexto. • 7.1.3 Definición del alcance del MSPI. • 7.2.2 Política de seguridad y privacidad de la información. • 7.2.3 Roles y responsabilidades. • 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.	• Incluir dentro de los proyectos de inversión de la Entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido.

7.4.2. Competencia, toma de conciencia y comunicación

Lineamiento:

La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para:

- Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
- Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.
- Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.
- Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado,

cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

Propósito:

Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos sus funcionarios estén al tanto de la política de seguridad y privacidad, cuál es su rol en el cumplimiento del MSPI, beneficios y consecuencias de no poner en práctica las reglas definidas en el modelo (desde el punto de vista de seguridad y privacidad de la información).

FASE 1: PLANIFICACIÓN 7.4.2 Competencia, toma de conciencia y comunicación	
Entradas	**Salidas**
• 7.1.3 Definición del alcance del MSPI. • 7.2.3 Roles y responsabilidades. • Manual de funciones de la Entidad. • Plan de capacitación Institucional.	• Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones – PIC. • Plan de comunicaciones del modelo de seguridad y privacidad de la información.

8. Fase 2: Operación

Una vez culminada las actividades del MSPI de la fase de 7.3 Planificación, se llevará acabo la implementación de los controles, con el fin de dar cumplimiento a los requisitos del MSPI. Los documentos que se deben generar en esta fase son:

- Plan de implementación de controles de seguridad y privacidad de la información
- Evidencia de la implementación de los controles de seguridad y privacidad de la información.

8.1. Planificación e implementación

Lineamiento:

La entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional de gestión y desempeño.

Propósito:

Implementar los planes y controles para lograr los objetivos del MSPI

FASE 2: OPERACIÓN 8.1 Planificación e implementación	
Entradas	**Salidas**
• 7.3.2 Valoración de los riesgos de seguridad de la información. • Plan de 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.	• Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.

9. Fase 3: Evaluación de desempeño

Una vez culminadas las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

9.1. Seguimiento, medición, análisis y evaluación

Lineamiento:

Es importante que las entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer

los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el Comité Institucional de Gestión y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

Propósito:

Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.1 Seguimiento, medición, análisis y evaluación	
Entradas	**Salidas**
• Documento con los resultados de la valoración de los riesgos. • Documento con los resultados del tratamiento de riesgos de seguridad de la información. • Resultado de la implementación de los controles.	• Hoja de vida de indicadores3, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018. • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.

9.2. Auditoría Interna

Lineamiento:

Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.

Propósito:

Realizar seguimiento a la implementación del MSPI

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.2 Auditoría Interna	
Entradas	**Salidas**
• Todos los documentos producto de las salidas de las fases anteriores del MSPI. • El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías.	• Resultados de las auditorías internas. • No conformidades de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el

3 Para la definición de los indicadores utilizar como modelo la Guía - Indicadores Gestión de Seguridad de la Información

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.2 Auditoría Interna	
• Informes y compromisos adquiridos en los comités institucionales de gestión y desempeño. • El informe de los incidentes de seguridad y privacidad de la información reportada y la solución de estos. • Informe sobre los cambios PESTEL (legales, procesos, reglamentarios, regulatorios, tecnológicos, ambientales, o aquellos en el marco del contexto de la organización) en la Entidad. • Indicadores definidos y aprobados para la evaluación del MSPI.	Comité de Coordinación de Control Interno.

9.3. Revisión por la dirección

Lineamiento:

Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.

Propósito:

Revisar el MSPI de la entidad, por parte de la alta dirección (comité de gestión institucional), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

FASE 3: EVALUACIÓN Y DESEMPEÑO 9.3 Revisión por la Dirección	
Entradas	**Salidas**
• Todos los documentos del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la Entidad.	• Revisión a la implementación. • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.

10. fase 4: Mejoramiento continuo

Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

10.1. Mejora

Lineamiento:

Es importante que las entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.

Propósito:

Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

FASE 4: MEJORAMIENTO CONTINUO 10.1 Mejora	
Entradas	**Salidas**
• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. • Resultados de auditorías y revisiones independientes al MSPI.	• Plan anual de mejora del MSPI

11. ADOPCIÓN DEL PROTOCOLO IPv6

En el presente capitulo se relacionan las fases para el proceso de transición del protocolo IPv4 a IPv6 que, aunque no hace parte de la última versión de Modelo de Seguridad y Privacidad de la Información, en atención a la recomendación de la Oficina de Control Interno de la SDP, se incluye este ítem en el cual se describen las etapas de análisis, planeación y la implementación del protocolo IPv6.

Figura 2. *Fases del proceso de transición del protocolo IPv4 al IPv6*

11.1. FASE DE PLANEACIÓN

En esta fase, se debe definir el plan y la estrategia de transición de IPv4 a IPv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

En la Tabla Siguiente, se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia.

PLANEACIÓN			
Metas	**Resultados**	**Instrumentos**	
		MSPI	MAE
Plan y estrategia de transición de IPv4 a IPv6.	Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones	Guía No 20 – Transición IPv4 a IPv6. Guía No 19 – Aseguramiento	

PLANEACIÓN			
Metas	Resultados	Instrumentos	
		MSPI	MAE
	para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones. Documento que define la estrategia para la implementación y aseguramiento del protocolo IPv6 en concordancia con la política de seguridad de las entidades.	del protocolo IPv6. Circular 002 de 2011 del MinTIC.	

11.2. FASE DE IMPLEMENTACIÓN

En esta fase se realizan actividades tales como habilitación del direccionamiento de IPv6, montaje, ejecución y corrección de configuraciones para pruebas piloto, activar las políticas de seguridad de IPv6, validar la funcionalidad de los servicios y aplicaciones de las entidades, entre otras.

En la siguiente tabla se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia.

Implementación		
Metas	Resultados	Instrumentos

		MSPI	MRAE
Implementación del plan y estrategia de transición de IPv4 a IPv6.	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.	Guía No 20 – Transición IPv4 a IPv6. Guía No 19 – Aseguramiento del protocolo IPv6. Circular 002 de 2011 del MinTIC.	

11.3. FASE – PRUEBAS DE FUNCIONALIDAD

En esta fase se hacen pruebas de funcionalidad y/o monitoreo de IPv6, en sistemas de información, de almacenamiento, de comunicaciones y servicios; frente a las políticas de seguridad perimetral, de servidores de cómputo, equipos de comunicaciones, de almacenamiento, entre otros. Tener en cuenta que se debe elaborar un inventario final de servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento de IPv6.

En la siguiente tabla se describen las metas, entregables e instrumentos que pueden ser utilizados para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia.

Pruebas de Funcionalidad			
Metas	**Resultados**	**Instrumentos**	
		MSPI	MRAE
Plan de pruebas de Funcionalidad de IPv4 a IPv6.	Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación. Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación.	Guía No 20 – Transición IPv4 a IPv6. Guía No 19 – Aseguramiento del protocolo IPv6.	

	Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.		

12. DEFINICIÓN DE INDICADORES MSPI

Tabla 2. Indicadores de Gestión Seguridad de la Información

PRODUCTO	NOMBRE DEL INDICADOR	OBJETIVO DEL INDICADOR	FÓRMULA	TIPO	UNIDAD DE MEDIDA	META PERIODO
ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	Nivel de Compromiso de la Alta Dirección	Hacer seguimiento, al compromiso sobre el sistema seguridad de la información, por parte de la alta dirección	# de revisiones realizadas por la alta dirección al año / # revisiones programadas para el año	Eficacia	Porcentaje	100%
CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN	Activos de Información de la SDP revisados y actualizados	Revisar y actualizar los activos de información de la SDP por proceso	# de procesos con activos de información (RAI) revisados y actualizados en la vigencia/# de procesos de la SDP	Eficacia	Porcentaje	95%
PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN	Nivel de Ejecución del Plan de Capacitación y Sensibilización en Seguridad de la Información de la SDP	Hacer seguimiento a la ejecución del Plan Capacitación y Sensibilización en Seguridad de la Información de la SDP	# de estrategias desarrolladas al año que cumplen con la meta de ejecución >=90% / # de estrategias programadas para desarrollar al año siguiendo lo establecido en el plan de capacitación y sensibilización	Eficacia	Porcentaje	90%
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP	Porcentaje de políticas de Seguridad de la Información	Mide el porcentaje de actualización o creación de	# de políticas de Seguridad de la Información	Eficacia	Porcentaje	90%

Tabla 2. Indicadores de Gestión Seguridad de la Información						
PRODUCTO	**NOMBRE DEL INDICADOR**	**OBJETIVO DEL INDICADOR**	**FÓRMULA**	**TIPO**	**UNIDAD DE MEDIDA**	**META PERIODO**
	actualizadas o definidas en la vigencia	políticas de seguridad de la información definidas en la vigencia	actualizadas o creadas en la vigencia / # de políticas de seguridad de la información planeadas para actualización o creación en la vigencia			
EJECUCIÓN DEL MSPI EN LA SDP	Nivel de Madurez de las fases del MSPI	Controlar el avance de las Fases del MSPI en términos de Madurez	# de actividades desarrolladas durante la vigencia en el Plan de Acción del MSPI / # de actividades definidas para desarrollar en la vigencia en el Plan de Acción del MSPI	Eficacia	Porcentaje	90%
GESTIÓN DE INCIDENCIAS DE SEGURIDAD	Porcentaje de atención a las incidencias de seguridad realizadas por los usuarios de la SDP	Medir el porcentaje de incidencias de Seguridad de la Información atendidas en la vigencia	(# de incidencias de seguridad atendidas en la vigencia /# de incidencias de seguridad recibidas en la vigencia) *100	Eficacia	Porcentaje	92%

13. ANEXOS DE CONSULTA

Hacen parte del presente documento los anexos definidos en el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones de febrero de 20214:

- Controles y objetivos de control

4 Resolución 500 de 2021 de MinTIC. Anexo 1 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

- Guía - Roles y responsabilidades
- Guía - Gestión inventario clasificación de activos e infraestructura critica
- Guía para la gestión de riesgos de seguridad de la información (DAFP)
- Guía - Indicadores Gestión de Seguridad de la Información

14. NORMATIVIDAD

Conforme a lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas5, que aplican a la Secretaría Distrital de Planeación:

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- 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 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de

5 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- 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 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño
- Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

15. GLOSARIO

El Modelo incluye la siguiente terminología para su comprensión6:

6 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso 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 ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001).

- **Activos de Información y recursos:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

- **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 27001).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27001).

- **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 27001).

- **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:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- **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 este documento 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)

- **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 27001).

- **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 27001) y según Norma NTC-ISO 22301 del 20 de noviembre de 2019, Seguridad y resiliencia. Sistema de gestión de continuidad del negocio. Requisitos se define en el numeral 3.4 como: Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad del negocio.

- **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 27001).

- **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 27001).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001).

- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- **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 27001).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001).

- **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.

16. DERECHOS DE AUTOR

El contenido de este documento incluye textos sugeridos en los lineamientos, guías, documentos maestros publicados por MinTIC en el Modelo de Seguridad y Privacidad de la Información.

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/#:~:text=El%20Modelo%20de%20Seguridad%20y%20Privacidad%20de%20la,la%20implementaci%C3%B3n%20de%20la%20Pol%C3%ADtica%20de%20Gobierno%20Digital.

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno Digital.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

HISTORIAL DE CAMBIOS		
VERSIÓN	**FECHA**	**RAZÓN DEL CAMBIO**
1	12/mar./2024	Se inicia en versión 1 por cambio de software, las anteriores versiones se pueden consultar en SIPA.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Marisol Rubiano Casas **Cargo:** Contratista - AGATA **Fecha:** 12/mar./2024	**Nombre:** Martin Ricardo Linares Puentes **Cargo:** Profesional Especializado **Fecha:** 12/mar./2024	**Nombre:** Nicolas Sanchez Barrera **Cargo:** Director **Fecha:** 12/mar./2024