MINISTERIO DE TRANSPORTE

UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 1.0

Fecha: Enero 31 -2023

Tabla de contenido

1. Introducción

La información que es elaborada y generada por los procesos de la UPIT es un activo de alto valor que, como otros bienes de la organización, necesita ser protegida de forma apropiada. A medida que los procesos de la Entidad se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con reglas de alto nivel que permitan el control y administración efectiva de los datos, así como la protección de una amplia gama de amenazas. Lo anterior, permite asegurar la continuidad de los procesos institucionales y la entrega de productos y servicios a los ciudadanos.

El presente plan pretende facilitar la comprensión del proceso de adopción de la seguridad y privacidad de la información en la UPIT, de tal forma que permita controlar los riesgos de seguridad digital y proteja la privacidad de la información y los datos, de los procesos y las personas vinculadas con dicha información.

2. Objetivos

El principal objetivo del presente plan es definir las actividades de adopción y mantenimiento de seguridad y privacidad de la información en la UPIT para:

- Dar cumplimiento regulatorio a lo expedido por el Ministerio de Tecnologías de la información y las Comunicaciones (MinTIC) así como el cumplimiento de los requisitos legales y regulatorios pertinentes.
- Promover los comportamientos de seguridad responsables dentro de la UPIT.
- Proteger la información y la organización.
- Evaluar las amenazas actuales y futuras de la información.
- Promover la mejora continua.
- Ofrecer mayor calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad.
- Establecer la base para que la UPIT pueda adoptar y certificar a largo plazo un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001.

3. Alcance

El alcance del presente plan comprende la definición de las actividades que deben llevarse a cabo dentro de la UPIT para adoptar la seguridad digital dentro del marco de la política de gobierno digital y el Modelo de Seguridad y Privacidad de la Información, así como definir las fechas propuestas para cumplir con dichas actividades durante las vigencias de 2023, 2024 y 2025.

Es importante aclarar que la UPIT iniciará el desarrollo de la estrategia que le permita adoptar el MSPI, la cual tiene como propósito adicional, definir, establecer, implementar, operar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en el estándar ISO/IEC 27001, en miras a lograr una certificación internacional a largo plazo. Por lo tanto, la Entidad podrá referirse a la adopción del MSPI o de un SGSI según su progreso.

4. Marco normativo

A continuación, se listan los documentos, resoluciones o normativas que se utilizan de base para la construcción del presente plan.

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

- **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 usen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- **Ley 1581 de 2012:** "Por la cual se dictan disposiciones generales para la protección de datos personales". Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

- **Norma ISO/IEC 27001:2013:** Sistemas de Gestión de Seguridad de la Información.

- **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". Reglamentada parcialmente por el Decreto Nacional 103 de 2015.

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

- **Decreto 1078 del 26 de 2015:** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- **Documento CONPES 3995 de 2020:** "Política Nacional de confianza y Seguridad Digital".

- **Directiva Presidencial 03 de marzo de 2021**: Por medio de la cual se establecen los "Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de datos."

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

- **Resolución 1519 de 2022 (MinTIC):** "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**"**

5. Definiciones

A continuación, se listan los términos que podrían usarse dentro del documento con su respectiva definición.

- **Activo de información:** Todo aquello que tiene valor para la entidad, por lo tanto, debe protegerse. De acuerdo con la norma ISO/IEC 27001, los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

- **Confidencialidad:** Que la información solo sea accedida por las personas autorizadas para ello.

- **Amenaza:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Seguridad informática:** Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.

6. Actividades para la adopción de seguridad y privacidad de la información

Si bien la UPIT debe adoptar la seguridad digital en todos sus procesos, el presente plan se enfoca en la adopción progresiva del Modelo de Seguridad y Privacidad de la Información (MSPI) a través de diferentes actividades que se implementarán a corto, mediano y largo plazo. Para llevar a cabo lo anterior, la UPIT toma como referencia el Documento Maestro del Modelo de Seguridad y Privacidad de la Información[1] (en adelante MSPI), el cual brinda los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

De acuerdo con lo anterior, el Plan de Seguridad y Privacidad de la Información contempla el desarrollo de las fases que se presentan a continuación:

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf.

Ilustración 1. Fases de la implementación del MSPI

Fuente: Tomado del Documento Maestro del MSPI

6.1. Fase 1. Diagnóstico (En el ciclo PHVA: Planear)

Como actividad fundamental, la UPIT desarrollará en primera medida un diagnóstico (Análisis GAP) que le permitirá identificar el estado actual en materia de seguridad de la información y adopción del MSPI. Esto le permite a la Entidad determinar los aspectos con mayor debilidad y las actividades a desarrollar para mitigar la brecha. Por lo anterior, es necesario que el diagnóstico se realice antes de iniciar la fase de Planificación. Una vez se cuente con el diagnóstico se podrán identificar detalladamente los recursos necesarios, costos, tiempos de implementación, entregables, hitos, que implica y demanda el establecimiento, la operación y la mejora continua del MSPI.

Para llevar a cabo el diagnóstico, la Entidad utilizará como instrumento el documento "Instrumento de Evaluación MSPI" dispuesto por MinTIC en su página web[2].

[2] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

6.2. Fase 2. Planificación (En el ciclo PHVA: Planear)

Posterior a la ejecución del Diagnóstico, la UPIT procederá a desarrollar la fase de Planificación, la cual tiene como objetivo determinar las necesidades y objetivos de seguridad y privacidad de la información, teniendo en cuenta el mapa de procesos, el tamaño de la Entidad y en general el contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo esta la parte más importante del ciclo.

Para llevar a cabo esta fase, la UPIT trabajará en los siguientes aspectos:

a) **Contexto:** Identificar el contexto de la Entidad de tal forma que se comprenda y entienda la misión de la Entidad, su contexto y su entorno. De igual forma, en esta actividad se contempla la identificación de necesidades y expectativas de las partes interesadas y la definición del Alcance del MSPI.

b) **Liderazgo:** Determinar las funciones de seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo. De igual forma, dentro de esta actividad se contempla la actualización de la política de Seguridad y privacidad de la Información (que se definió inicialmente en la resolución 045 del 24 de marzo del 2022 expedida por la UPIT, así los roles y responsabilidades para la adopción del MSPI.

c) **Planeación**: Dentro de esta actividad se contempla llevar a cabo la identificación de activos de información e infraestructura crítica, la valoración de los riesgos de seguridad de la información y su respectivo plan tratamiento.

d) **Soporte:** Para lograr el desarrollo de las actividades de adopción del MSPI, la UPIT contempla dentro de esta actividad determinar y proporcionar los recursos necesarios para su respectiva adopción. De igual forma, en esta actividad se contempla la definición de un plan de capacitación y sensibilización que permita a la Entidad contar con el conocimiento y formación necesario para la adopción del MSPI.

6.3. Fase 3. Operación (En el ciclo PHVA: Hacer)

Una vez se haya desarrollado la fase de planificación, la Entidad se dispondrá a realizar la implementación de los respectivos controles de seguridad que permitan la mitigación de los riesgos que se hayan identificado previamente. Para lograr el objetivo de esta fase, la UPIT realizará la planificación e implementación del plan de tratamiento de riesgos de seguridad de la información que se haya construido en la Fase de Planificación. Es decir, en la fase de operación se implementan los planes y controles para lograr los objetivos del MSPI. Dentro de las actividades de esta fase se contempla:

a) Implementar el Plan de Control y planeación Operacional.
b) Implementar el plan de Tratamiento de Riesgos de Seguridad y privacidad de la información.
c) Definir los indicadores de gestión del MSPI.

6.4. Fase 4. Evaluación de desempeño (En el ciclo PHVA: Verificar)

Una vez se haya terminado la fase de operación (implementación) se lleva a cabo la fase de Evaluación de desempeño, la cual permite a la UPIT evaluar la efectividad de las acciones tomadas a través de los indicadores definidos, de tal forma que incluya la correcta interacción entre el MSPI, MIPG y los requerimientos normativos. Dentro de esta fase se contemplan las siguientes actividades:

a) **Seguimiento, medición, análisis y evaluación.** En esta actividad la UPIT garantizará que se conozca de manera permanente la gestión que se ha realizado para la adopción del MSPI, así como sus logros y metas. Esto requiere que se determinen los recursos para el monitoreo, el desempeño, los resultados y la aceptación formal por parte de la Entidad. Esta actividad permite generar los resultados de los indicadores, así como los informes producto de la evaluación de desempeño.

b) **Auditoría Interna.** La UPIT realizará auditorías Internas al MSPI (o SGSI) de tal forma que permita identificar las debilidades y los controles a mejorar, así como el cumplimiento del MSPI.

c) **Revisión por la dirección.** En esta actividad la UPIT realizará el reporte respectivo de la información resultante de las evaluaciones de desempeño del MSPI, requerimientos de aprobación de documentos, incidentes, comportamientos y demás aspectos relevantes para que la dirección se encuentre al tanto y le permita determinar su conveniencia, adecuación y eficacia.

6.5. Fase 5. Mejoramiento Continuo (En el ciclo PHVA: Actuar)

Como última fase del ciclo se lleva a cabo la fase de mejoramiento continuo, en la cual se establecen los procedimientos necesarios para identificar desviaciones en las reglas definidas por el MSPI, así como las acciones necesarias para su solución y no repetición. Es decir, se consolidan los resultados de la fase de evaluación de desempeño y se diseña el plan de mejoramiento continuo para tomar oportunamente las acciones que permitan a la Entidad mitigar las debilidades que fueron identificadas. Como resultado de esta fase se debe generar el "Plan anual de mejora del MSPI" o los planes de mejoramiento respectivos según lo indiquen los procedimientos internos de la Entidad.

7. Plan de seguridad y privacidad de la información

A continuación, se presenta el plan de seguridad y privacidad de la información. Dentro de este plan se incluyen las actividades generales mencionadas dentro del presente documento y las fechas para su ejecución. No obstante, la información detallada para llevar a cabo cada una de las fases se encuentra dentro del documento "Anexo 1. Mapa de ruta de Seguridad y privacidad de la Información."

Es importante aclarar que dependiendo de la madurez de la Entidad frente a la adopción de MIPG, así como sistemas de gestión de calidad, seguridad y salud en el trabajo, entre otros, existirán actividades de seguridad y privacidad de la información que no se realizan desde cero, sino que se integrarán con las ya definidas, documentadas o socializadas dentro de la Entidad. Esto permita a la UPIT ahorrar costos y tiempo en la adopción del MSPI.

De igual forma, para la implementación del MSPI se seguirán las guías[3] y la documentación respectiva[4] dispuesta por el MinTIC, en materia de Seguridad de la Información, para las entidades del gobierno colombiano.

Tabla 1. Plan general de seguridad y privacidad de la Información.

Actividades	2023		2024		2025	
	S1	S2	S1	S2	S1	S2
Fase 1. Diagnóstico						
Diagnóstico del MSPI						
Fase 2. Planificación						
Identificación del contexto						
Definición del alcance del MSPI						
Establecimiento del liderazgo						
Planeación						
Soporte y recursos						
Toma de conciencia- sensibilización						
Fase 3. Operación						
Implementación de planes y controles.						
Fase 4. Evaluación de desempeño						
Seguimiento, medición, análisis y evaluación.						
Auditoría Interna						
Revisión por la dirección						
Fase 5. Mejoramiento continuo						
Plan de mejoramiento						

Fuente: Propia

8. Anexos

Anexo 1. Mapa de ruta de Seguridad y privacidad de la Información. (Dado que este anexo es de manejo interno de la UPIT, no será objeto de publicación en la página web de la Entidad.)

[3] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[4] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

9. Control de cambios

Fecha	Descripción del cambio o modificación	Versión generada
31/01/2023	Documento inicial	1.0