PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ministerio de Hacienda y Crédito Público

Aprobación 29 y 31 de enero 2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión (MIPG), como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

De otra parte, el manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones, establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Así mismo, la Política de Gobierno Digital contempla dentro de su estructura como uno de sus habilitadores el denominado ***Seguridad y Privacidad de la Información*** como se muestra a continuación

Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información (en adelante MSPI). No obstante, la política de seguridad y privacidad de la entidad se encuentra amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular al principio de Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del estado, y de los servicios que prestan al ciudadano.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de Seguridad y Privacidad de la Información al interior del Ministerio de Hacienda y Crédito Público.

2. OBJETIVO

Establecer medidas, actividades y lecciones aprendidas que permitan fortalecer la mejora continua del Modelo de Seguridad y Privacidad de la Información, desde el enfoque de protección de los activos de información, respecto a confidencialidad, integridad y disponibilidad, que soportan la prestación de servicios digitales del Ministerio de Hacienda y Crédito Público, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios y demás partes interesadas.

3. ALCANCE

El presente documento aplica a todo el modelo de operación por procesos del Ministerio de Hacienda y Crédito Público dando cumplimiento a lo establecido en el Decreto 612 de 2018, a la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información alineado con la NTC/IEC ISO 27001, así como la estrategia de Seguridad Digital del Estado colombiano.

4. NORMATIVIDAD

- Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).
- 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 utilicen 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".
- 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".

- Decisión Andina 351 de 2015 "Régimen común sobre derecho de autor y derechos conexos".
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.
- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.
- Decreto 767 del 2022, "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 de Tecnologías de la Información y las Comunicaciones"
- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2018.
- Norma Técnica Colombiana ISO27001:2013.
- Norma Técnica Colombiana ISO31000:2013.
- Decreto 338 del 2022, "por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital".

5. ESTADO ACTUAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 se muestra a continuación:

Ilustración 1: Estado del MSPI del MHCP, medición diciembre 2023. Fuente: Dirección de Tecnología del MHCP

6. ESTRATEGIA DE SEGURIDAD

El Ministerio de Hacienda define, implementa, evalúa y mejora las estrategias de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, con base en el Modelo de Seguridad y Privacidad de la Información -MSPI, así como en la política de riesgos de la entidad donde se incluye lo referente a seguridad de la información y lo establecido en el procedimiento de gestión de incidentes de seguridad de la información. Dado lo anterior el Ministerio de Hacienda define cinco (5) ejes, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

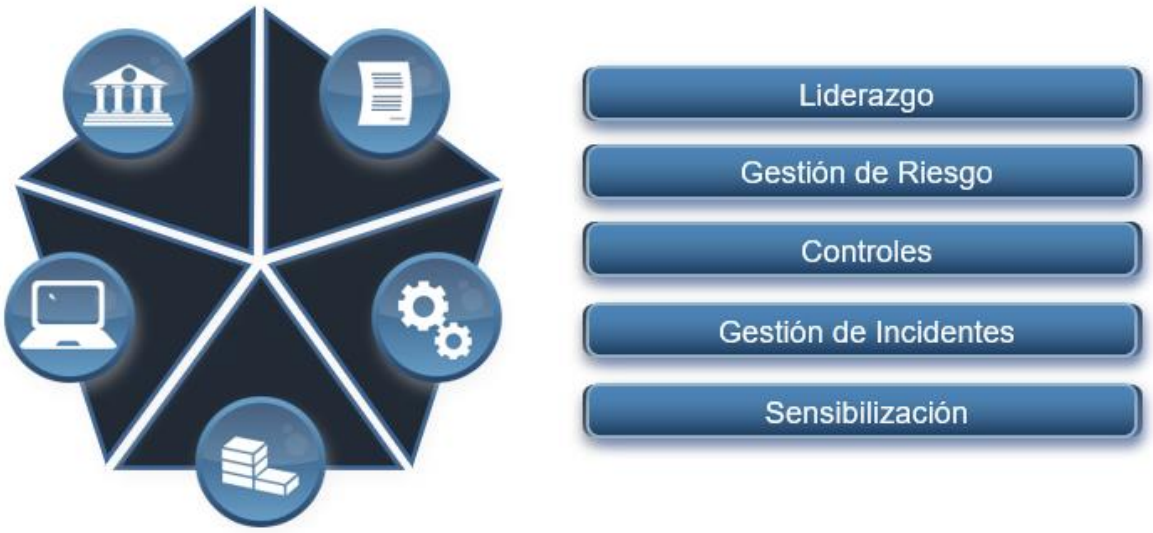

Ilustración 2: Estrategia de Seguridad y Privacidad de la Información del MHCP.

a. Liderazgo

En el primer eje se establecen la acciones a ejecutar para el correcto funcionamiento del Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos

que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

b. Gestión del Riesgo

En esta etapa se gestionan los riesgos de seguridad de la información a través de la identificación y valoración que se defina buscando prevenir y mitigar los efectos no deseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

c. Controles

Se ejecutan las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.

d. Gestión de incidentes

En este eje se realiza la administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

e. Sensibilización

En esta última etapa se busca fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

7. PROYECTOS Y ACTIVIDADES

Proyecto	Actividad	Meta o indicador
Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información	Actualización de la política de seguridad de la entidad.	Política actualizada

8. PLAN DE ACCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1. Activos de información Dominio 8. GESTIÓN DE ACTIVOS.					
1.1	Actualización formato instrumentos de identificación de activos de información	Marzo 1 del 2024	Julio 31 del 2024	Gestión de Tecnología y Seguridad de la Información	Formato Instrumentos de identificación de activos de información actualizado
1.2	Actualización de Activos de información	Agosto 1 del 2024	Noviembre 30 del 2024		Matrices de activos de información actualizado
1.3	Publicación Instrumentos de activos de información del MHCP	Diciembre 1 del 2024	Diciembre 20 del 2024		Consolidado Matrices de activos de información en la página de la entidad y en datos abiertos

1.4	Generación de instrumentos de información pública ley 1712	Diciembre 1 del 2024	Diciembre 20 del 2024		Instrumentos de gestión de información púbica
2. Riesgos de Seguridad y Privacidad de la Información 6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES.					
2.1	Actualización del Plan de Gestión de Riesgos de Seguridad y Privacidad de la información	Marzo 1 del 2024	Abril 31 del 2024	Gestión de Tecnología y Seguridad de la Información	Plan de Gestión de Riesgos de Seguridad y Privacidad de la información actualizado
2.2	Ejecución del Plan de Gestión de Riesgos de Seguridad y Privacidad de la información.	Marzo 1 del 2024	Diciembre 20 del 2024		Plan de Gestión de Riesgos de Seguridad y Privacidad de la información ejecutado
3. Plan de Sensibilización en Seguridad y Privacidad de la Información 7.2.2 SENSABILIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGUR. DE LA INFORMAC.					
3.1	Actualización del Plan de Concienciación en Seguridad y Privacidad de la información	Febrero 1 del 2024	Marzo 30 del 2024	Gestión de Tecnología y Seguridad de la Información Grupo de Talento Humano / Grupo de Comunicaciones	Documento Plan de Concienciación en Seguridad y Privacidad actualizada
3.2	Ejecución del Plan de Concienciación en Seguridad y Privacidad de la información.	Marzo 1 del 2024	Diciembre 20 del 2024		Informe de ejecución Plan de Concienciación en Seguridad y Privacidad
4. Requisitos Legales de Seguridad y Privacidad 18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES.					

4.1	Revisión de Requisitos Legales de Seguridad y Privacidad	Abril 1 del 2024	Diciembre 20 del 2024	Gestión de Tecnología y Seguridad de la Información	Propuesta para el Normograma con normatividad actualizada
5. Acciones de mejora del Sistema de Gestión de Seguridad de la Información 10. MEJORA					
5.1	Avances Acciones Correctivas y Acciones de Mejora del Sistema de Gestión de Seguridad de la Información	Febrero 1 del 2024	Diciembre 20 del 2024	Gestión de Tecnología y Seguridad de la Información	Sistema de Gestión de Seguridad de la Información con sus mejoras
6. Dominios de la Norma ISO 27001:2022 Toda la norma					
6.1	Revisión de Manual y Políticas de Seguridad del Sistema de Gestión de Seguridad de la Información.	Febrero 1 del 2024	Marzo 31 del 2024	Gestión de Tecnología y Seguridad de la Información	Documento Manual y Políticas de Seguridad de la Información revisado y/o actualizado.
6.2	Revisión y/o actualización de los controles del modelo de seguridad de la información	Mayo 1 del 2024	Diciembre 20 del 2024		Instrumento de medición y seguimiento de controles del modelo
7. Auditorías al Sistema de Gestión de Seguridad de la Información 9.2 AUDITORÍA INTERNA					
7.1	Participar en las Auditorías al Sistema de Gestión de	Febrero 1 del 2024	Diciembre 20 del 2024	Gestión de Tecnología y Seguridad de la Información	Actas de participación de las auditorias

	Seguridad de la Información				
	8. Gestión de Incidentes de Seguridad de la Información 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.				
8.1	Atención de Incidentes de Seguridad de la Información	Febrero 1 - 2024	Diciembre 20 – 2024	Gestión de Tecnología y Seguridad de la Información	Documentos de evidencias
8.2	Realizar seguimiento a los informes de eventos y vulnerabilidades emitidos por el SOC contratado por la entidad	Febrero 1 – 2024	Diciembre 20 – 2024	Gestión de Tecnología y Seguridad de la Información	Documentos de seguimiento de los eventos y vulnerabilidades
	9. Indicadores del Sistema de Gestión de Seguridad de la Información 9.1 SEGUIMIENTO. MEDICIÓN. ANÁLISIS Y EVALUACIÓN				
9.1	Revisión y actualización de los indicadores de Seguridad y Privacidad de la Información	Junio 1 del 2024	Diciembre 20 del 2024	Grupo de Transformación Digital, Gestion de Tecnología y Seguridad de la Información	Documento de Indicadores actualizados

- Acciones por implementar que van orientadas al mantenimiento del MSPI.
- Acciones por implementar que van orientadas a la mejora del MSPI.

9. RESPONSABLES

Los responsables de liderar la Política de Seguridad Digital adelantaran las actividades concernientes con el propósito de aportar al fortalecimiento del modelo de seguridad y privacidad de la información, sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.