Imagen que contiene interior, hombre, tabla, cuarto

Descripción generada automáticamente

**Plan de Seguridad y Privacidad de la Información**

Versión 1

29 de enero 2025

**Versión 2 - Julio de 2024**

**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc188899263)

[3. ALCANCE 5](#_Toc188899264)

[4. NORMATIVIDAD 5](#_Toc188899265)

[5. ESTADO ACTUAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6](#_Toc188899266)

[6. ESTRATEGIA DE SEGURIDAD 8](#_Toc188899267)

[a. Liderazgo 9](#_Toc188899268)

[b. Gestión del Riesgo 9](#_Toc188899269)

[c. Controles 9](#_Toc188899270)

[d. Gestión de incidentes 9](#_Toc188899271)

[e. Sensibilización 9](#_Toc188899272)

[7. PROYECTOS Y ACTIVIDADES 10](#_Toc188899273)

[8. PLAN DE ACCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 10](#_Toc188899274)

[9. RESPONSABLES 15](#_Toc188899275)

[10. PRESUPUESTO 15](#_Toc188899276)

# 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

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

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.

1. **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.

# 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.

# 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”.

# 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 27001:2022 se muestra a continuación:

Ilustración 1: Estado del MSPI del MHCP, medición diciembre 2024. Fuente: Dirección de Tecnología del MHCP

# 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.

## 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.

## 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.

## 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.

## 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.

## 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.

# PROYECTOS Y ACTIVIDADES

|  |  |  |
| --- | --- | --- |
| Proyecto | Actividad | Meta o indicador |
| Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información | Mejora continua de todos los elementos que articulan el MSPI dentro de la entidad. | MSPI actualizado |

# 

# 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  GESTIÓN DE ACTIVOS. | | | | |  |
| 1.1 | Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación | 1 Feb 2025 | 30 Sep 2025 | Gestión de Tecnología y Seguridad de la Información  Gestión de Tecnología y Seguridad de la Información | Formato Instrumentos de  identificación de activos de información actualizado |
| 1.2 | Socializar la metodología de activos de información | 1 Jul 2025 | 31 Jul 2025 | Actas de reuniones |
| 1.3 | Consolidar el inventario de activos de Información. | 1 Nov 2025 | 30 Nov 2025 | Matrices de activos de información en la página de la entidad y en datos abiertos |
| 1.4 | Publicar el consolidado de activos de información en SMGI | 1 Dic 2025 | 10 Dic 2025 | Envío de memorando |
| 1.5 | Envío del consolidado de activos de información a la OAPES, para el respectivo reporte del índice de información clasificada y reservada | 15 Dic 2025 | 16 Dic 2025 | Envío de correo electrónico |
| 1.6 | Publicación del Registro Activos de Información en la sección de transparencia y en el portal de datos abiertos de la entidad o a aquel que lo sustituya. | 22 Dic 2025 | 23 Dic 2025 | Página web de la entidad. |
| 2. Riesgos de Seguridad y Privacidad de la Información  ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES. | | | | |  |
| 2.1 | Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación | 1 Mar del 2025 | 1 Jul 2025 | Gestión de Tecnología y Seguridad de la Información  Gestión de Tecnología y Seguridad de la Información | Mapa de riesgos de los procesos. |
| 2.2 | Sensibilización | 1 Mar del 2025 | 1 Jul 2025 | Mapa de riesgos de los procesos. |
| 2.3 | Aceptación de Riesgos Identificados | 1 Ago del 2025 | 31 Ago 2025 | Memorando de aceptación |
| 2.4 | Seguimiento Fase de Tratamiento | 1 Nov del 2025 | 31 Nov 2025 | Actas de seguimiento |
| 3. Gestión de Incidentes de Seguridad y Privacidad de la Información  INCIDENTES DE SEGURIDAD | | | | | |
| 3.1 | Socializar el procedimiento a los colaboradores de la Entidad. | 1 Feb 2025 | 30 Mar 2025 | Gestión de Tecnología y Seguridad de la Información  Gestión de Tecnología y Seguridad de la Información | Correo electrónico |
| 3.2 | sensibilizar sobre la caracterización de incidentes de seguridad a los agentes del Centro de Servicio Tecnológico | 1 Feb 2025 | 20 Dic 2025 | Correo electrónico |
| 3.3 | Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido. | 1 Feb 2025 | 31 Dic 2025 | Reporte e incidentes |
| 3.4 | Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI | 1 Feb 2025 | 31 Dic 2025 | Plan de remediciones |
| 4. Requisitos Legales de Seguridad y Privacidad  CUMPLIMIENTO DE LOS REQUISITOS LEGALES | | | | | |
| 4.1 | Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información. | 1 Abr 2025 | 20 May 2025 | Gestión de Tecnología y Seguridad de la Información | Instrumento de autodiagnóstico actualizado |
| 4.2 | Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente. | 1 Feb 2025 | 31 Dic 2025 | Revisión y actualización de los lineamientos de Seguridad y Privacidad de la Información de la entidad. |
| 5. Acciones de mejora del Sistema de Gestión de Seguridad de la Información  MEJORA | | | | | |
| 5.1 | Avances Acciones  Correctivas y  Acciones de Mejora del Sistema de  Gestión de Seguridad de la Información | Febrero 1 del 2025 | Diciembre 20 del 2025 | Gestión de Tecnología y Seguridad de la Información | Sistema de Gestión de Seguridad de la Información con sus mejoras |
| 6. Auditorías al Sistema de Gestión de Seguridad de la Información  AUDITORÍA INTERNA | | | | | |
| 6.1 | Participar en las  Auditorías al Sistema de Gestión de  Seguridad de la Información | 1 Feb 2025 | 20 Dic 2025 | Gestión de Tecnología y Seguridad de la Información | Informe de auditoría. |
| 7. Enfoque Sectorial  ENTIDADES DEL SECTOR HACIENDA | | | | | |
| 7.1 | Realizar mesa sectorial de seguridad y privacidad de la información y seguridad digital y | 1 May 2025 | 20 Dic 2025 | Gestión de Tecnología y Seguridad de la Información | Correos electrónicos |
| 7.2 | Realizar seguimiento a la implementación del MSPÏ y ICC en las entidades adscritas al sector | 1 Jun 2025 | 20 Dic 2025 | Gestión de Tecnología y Seguridad de la Información | Correos electrónicos |
| 8. Indicadores del Sistema de Gestión de Seguridad de la Información  SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN | | | | | |
| 8.1 | Revisión y actualización de los indicadores de Seguridad y Privacidad de la Información | 1 Jun 2025 | 20 Dic 2025 | Gestión 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.

# RESPONSABLES

El Oficial de Seguridad y Privacidad de la Información es el responsable 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.

# PRESUPUESTO

Para la vigencia 2025 se asignó el siguiente presupuesto para el proceso Gestión de Tecnología y Seguridad de la Información.

| Ítem | Iniciativa | Inversión 2025 |
| --- | --- | --- |
| 1 | Contratar los servicios de un Centro de Operaciones de Seguridad (SOC) para el monitoreo, alertamiento y gestión de la seguridad de la información de la plataforma tecnológica del Ministerio de Hacienda y Crédito Público | $2.221.269.420 |
| 2 | Adquirir la suscripción, actualización y el soporte técnico de la herramienta de administración y gestión de componentes de información y datos (gobernabilidad de datos) VARONIS del Ministerio de Hacienda y Crédito Público | $ 644.774.989 |
| 3 | Prestar servicios profesionales a la Dirección de Tecnología en la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con la política de Gobierno Digital y Seguridad Digital, así como validar y verificar los planes de mitigación y remediación de riesgos y la implementación de controles tecnológicos. | $ 110.000.00 |
|  | Total | $ 2.976.044.409 |

|  |  |
| --- | --- |
| **ELABORADO POR:** | **Nombre:** Francisco José Ariza Pastor  **Cargo:** Contratista  **Fecha:** 27-01-2025 |
| **REVISADO POR:** | **Nombre:** Marly Esther De Moya Amaris  **Cargo:** Profesional Especializado  **Fecha:** 27-01-2025 |
| **VALIDADO POR:** | **Nombre:** Ricardo Fernelix Ríos Rosales  **Cargo:** Director de Tecnología  **Fecha:** 28-01-2025 |

Aprobado mediante Comité Institucional de Control Interno del 29 de enero 2025.

Imagen que contiene interior, tabla, cuarto, hombre

Descripción generada automáticamente

**Ministerio de Hacienda y Crédito Público**

Dirección: Carrera 8 No. 6C–38, Bogotá D.C., Colombia

Conmutador: (+57) 601 3 81 17 00

Línea Gratuita: (+57) 01 8000 910071

Correo institucional: [relacionciudadano@minhacienda.gov.co](mailto:relacionciudadano@minhacienda.gov.co)