**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 2](#_Toc107516079)

[2. OBJETIVO 2](#_Toc107516080)

[3. ALCANCE 2](#_Toc107516081)

[4. PRODUCTOS ESPERADOS 2](#_Toc107516082)

[5. TÉRMINOS Y DEFINICIONES. 3](#_Toc107516083)

[6. DOCUMENTOS DE REFERENCIA 5](#_Toc107516084)

[7. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI 6](#_Toc107516085)

[8. ESTRATEGIA DE SEGURIDAD DIGITAL 8](#_Toc107516086)

[**8.1.** **Liderazgo de seguridad de la información** 8](#_Toc107516087)

[**8.2.** **Gestión de riesgos** 9](#_Toc107516088)

[**8.3.** **Implementación de controles** 9](#_Toc107516089)

[**8.4.** **Gestión de incidentes** 9](#_Toc107516090)

[**8.5.** **Concientización** 9](#_Toc107516091)

[9. PORTAFOLIO DE PROYECTOS / ACTIVIDADES 9](#_Toc107516092)

[10. CRONOGRAMA DE ACTIVIDADES 10](#_Toc107516096)

[11. ANÁLISIS PRESUPUESTAL 12](#_Toc107516097)

[12. RESPONSABLES 12](#_Toc107516098)

[13. HISTORIAL DE CAMBIOS 14](#_Toc107516099)

[14. APROBACIÓN 14](#_Toc107516100)

**Índice de tablas**

[**Tabla 1. Nivel Madurez del dominio de Seguridad 6**](#_Toc107516101)

[**Tabla 2. Resultados prueba de phishing controlada 7**](#_Toc107516102)

[**Tabla 3. Proyectos de Seguridad de la Información 9**](#_Toc107516103)

[**Tabla 4. Cronograma de Actividades 10**](#_Toc107516104)

[**Tabla 5. Análisis Presupuestal 12**](#_Toc107516105)

# 1. INTRODUCCIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información es un instrumento que soporta el Sistema Integrado de Gestión de Seguridad de la Información, que establece las actividades pertinentes para proteger la información que procesa el Ministerio de Hacienda y Crédito Público por lo cual a continuación se describen dichas actividades enmarcadas en el cumplimiento de los requisitos establecidos en la estrategia de seguridad digital, en el Artículo 5 de la 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”.*

Nota: El Plan Estratégico de Seguridad y Privacidad de la Información incluye lo relacionado con el plan operacional de seguridad y privacidad de la información.

# 2. OBJETIVO

Establecer estrategias a seguir para fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Ministerio de Hacienda y Crédito Público, para reducir los riesgos a los que está expuesta la Entidad hasta niveles aceptables de acuerdo con la Política de Administración del Riesgo de esta.

# 3. ALCANCE

Identificar y priorizar procesos soportados por el Sistema de Gestión de Seguridad de la Información para establecer estrategias a seguir en el marco de su implementación incluyendo la:

* Revisión y actualización de las políticas, procesos y procedimientos de seguridad de la información y seguridad digital para el Ministerio de Hacienda y Crédito Público – MHCP.
* Revisión y actualización de los lineamientos y metodologías de gestión de riesgos de seguridad de la información y seguridad digital, que expida el Gobierno Nacional
* Revisión continua a la gestión del riesgo, para evaluar la pertinencia y aplicación de los controles establecidos para los activos de información identificados mediante la revisión de eventos, planes de tratamiento y sus resultados.

# 4. PRODUCTOS ESPERADOS

* Autodiagnóstico de Seguridad De la información de la Entidad
* Identificación y clasificación de los Activos de Información de la Entidad.
* Identificación, valoración y tratamiento de los Riesgos de Seguridad Digital.
* Gestión de Incidentes de Seguridad de la Información de la Entidad.
* Implementación de Controles de Seguridad de la Información de la Entidad.

# 5. TÉRMINOS Y DEFINICIONES.[[1]](#footnote-1)

* **Activos de información**: Se considera como tal a la infraestructura de hardware y software en los que la información se procesa, se almacena o se transmite, la información que posee un valor y es necesaria para realizar los procesos misionales y de apoyo administrativo de la Entidad, los servicios computacionales y de comunicaciones. Se pueden clasificar de la siguiente manera:
* **Electrónicos**: Bases de datos, archivos, registros de auditoría, información de archivo, aplicaciones, herramientas de desarrollo y utilidades.
* **Físicos**: Documentos impresos, manuscritos y hardware.
* **Servicios**: Servicios computacionales y de comunicaciones.
* **Personas**: Incluyendo sus calificaciones, competencias y experiencia.
* **Intangibles**: Ideas, conocimiento, conversaciones.
* **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
* **Amenaza cibernética**: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).
* **CCOCI**; Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.
* **CERT**: Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).
* **Cibercrímen** (Delito cibernético): conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).
* **Ciberdefensa:** Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).
* **Ciberseguridad**: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).
* **CSIRT**: Por su sigla en inglés: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).
* **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
* **Declaración de aplicabilidad**: (en inglés Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
* **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
* **Gestión** **de Riesgo**: proceso de identificación y evaluación de riesgos y la toma de acciones efectivas para reducirlos a un nivel aceptable. Incluye la valoración de riesgos; análisis costo-beneficio de las acciones y controles de mitigación, y la selección, implementación y valoración de controles de seguridad.
* **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
* **Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).
* **Información**: es todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.
* **Infraestructura crítica cibernética nacional:** Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).
* **Ingeniería social**: consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
* **Integridad**: Propiedad de la información relativa a su exactitud y completitud.
* **Riesgo**: en el marco de la gestión de la seguridad de la información y de acuerdo con la ISO 27001, es la 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.
* **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2015).
* **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).
* **SGSI**: Sigla del Sistema de Gestión de la Seguridad de la Información. (ISMS en inglés, Information Security Management System).
* **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

# 6. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

* 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”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
* 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”.
* Manual de Gobierno Digital – MINTIC.
* Modelo de Seguridad y Privacidad de la Información – MINTIC.

# ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

La medición del estado actual de la implementación del SGSI se realiza de acuerdo con el autodiagnóstico de seguridad y privacidad de la información, la evaluación de FURAG en cuanto a la política de Seguridad Digital y el desarrollo de la cultura de seguridad de la información.

A continuación, se muestra el resultado de la evaluación de madurez del Modelo de Seguridad y Privacidad de la Información – MSPI identificado en el documento de autodiagnóstico, por cada uno de los dominios definidos en dicho modelo

**Tabla 1. Nivel Madurez del dominio de Seguridad**

FUENTE: Tomado de Autodiagnóstico V 2020\_MSPI\_MHCP\_V1

| **NO.** | **DOMINIO** | **CALIFICACIÓN ACTUAL** | **EVALUACIÓN DE EFECTIVIDAD DE CONTROL** |
| --- | --- | --- | --- |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 100 | OPTIMIZADO |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 93 | OPTIMIZADO |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 100 | OPTIMIZADO |
| A.8 | GESTIÓN DE ACTIVOS | 96 | OPTIMIZADO |
| A.9 | CONTROL DE ACCESO | 100 | OPTIMIZADO |
| A.10 | CRIPTOGRAFÍA | 40 | REPETIBLE |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 100 | OPTIMIZADO |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 100 | OPTIMIZADO |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 100 | OPTIMIZADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 93 | OPTIMIZADO |
| A.15 | RELACIONES CON LOS PROVEEDORES | 100 | OPTIMIZADO |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 100 | OPTIMIZADO |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 90 | OPTIMIZADO |
| A.18 | CUMPLIMIENTO | 96.5 | OPTIMIZADO |
| **PROMEDIO EVALUACIÓN DE CONTROLES** | **93** | **OPTIMIZADO** |

De la tabla anterior se puede concluir que actualmente el MHCP se encuentra en un nivel de madurez OPTIMIZADO con un valor promedio de 93 sobre un máximo de 100.

En cuanto a los resultados de la evaluación del FURAG, a continuación, se evidencia el incremento en el cumplimiento del habilitador transversal de seguridad de la información alrededor de la comparativa de los cuatro años donde inicia su medición con un porcentaje de 78,2 para el 2018 y para el 2021 finaliza con una medición de 86,9, mostrando su incremento. Ver ilustración1.



Ilustración 1- Comparativa años Furag

En cuanto al desarrollo de la cultura de seguridad de la información se presentan a continuación las actividades realizadas con el propósito de fortalecer las competencias de los colaboradores de la entidad, en materia de uso seguro de los servicios TIC tanto en el entorno laboral como en el personal.

* Sesiones de sensibilización en temas de seguridad de la información y ciberseguridad
* Encuesta Ciberseguridad Clon para evaluación de capacidades en materia de seguridad
* Ejercicios de ataques simulados y controlados de ingeniería social particularmente de phishing.
* Habilitación del botón de phishing en los correos electrónicos como estrategia de prevención frente a la ocurrencia o materialización de un incidente de seguridad de la información.
* Remisión de tips de seguridad de la información a través de medios cómo correo electrónico, intranet, carteleras entre otros.
* Trabajo en equipo con las entidades del sector para fortalecer las estrategias de contención frente a la posibilidad de ataque informáticos en fechas importantes para el estado donde las entidades gubernamentales pueden ser blancos de ataque.
* Fortalecimiento de los conceptos técnicos de los usuarios frente a la administración de las herramientas de seguridad informática para desarrollar un criterio eficaz.
* Desarrollo de una prueba controlada de phishing de 1.298 funcionarios, contratistas y pasantes, mediante la herramienta knowbe4 del MHCP con los siguientes resultados:

**Tabla 2. Resultados prueba de phishing controlada**

|  |  |  |  |
| --- | --- | --- | --- |
| Acciones realizadas | Febrero 2021 | Junio 2021 | Mayo 2022 |
| Correos Entregados | 976 | 980 | 1291 |
| Correos    Abiertos | 185 | 422 | 267 |
| Correos que presionaron el link | 53 | 239 | 211 |
| Correos que respondieron | 3 | 5 | 3 |
| Correos que abrieron el adjunto | 0 | 12 | 0 |

A partir de los resultados observados en la prueba efectuada, se convoca a una capacitación de refuerzo a quienes abrieron el correo, presionaron el link contenido en el correo o lo respondieron.

# 8. ESTRATEGIA DE SEGURIDAD DIGITAL

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 las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Ilustración 2 - Estrategias de Seguridad de la Información

## **Liderazgo de seguridad de la información**

Certificar que se establezca el 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 de riesgos**

Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

## **Implementación de controles**

Planificar e implementar 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**

Mantener una 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.

## **Concientización**

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.

# 9. PORTAFOLIO DE PROYECTOS / ACTIVIDADES

1.
2.
3.

A continuación, se listan los siguientes proyectos que se esperan sean desarrollados, alineados con el Plan Estratégico de Tecnologías de la entidad.

**Tabla 3. Proyectos de Seguridad de la Información**

| **ID\_ Proyecto** | **ID\_Iniciativa** | **Nombre Proyecto** | **Área líder** |
| --- | --- | --- | --- |
| PRY-16 | IT016 | Diseñar el componente de privacidad relacionado con la seguridad de los datos | Dirección de Tecnología |
| PRY-17 | IT017 | Fortalecer el modelo de seguridad y privacidad de la información | Dirección de Tecnología |
| PRY-18 | IT018 | Contratar el servicio de gestión de eventos, monitoreo y respuesta a incidentes de seguridad | Dirección de Tecnología |

 Fuente: PETI Institucional

# 10. CRONOGRAMA DE ACTIVIDADES

A continuación, se presenta el componente operacional de este plan a desarrollar que incluyen los proyectos de seguridad alineado con lo establecido en el plan estratégico institucional.

**Tabla 4. Cronograma de Actividades**

| **Área Organizativa** | **Nombre de la tarea** | **Descripción**  | **Categoría / Proyecto** | **Política de Gestión y Desempeño** | **Responsable de tarea**  | **Fecha Inicio** | **Fecha Fin** | **Fuente de Financiación**  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Dirección de Tecnología | Liderazgo de seguridad de la información | Fortalecer el modelo de seguridad y privacidad de la información | Implementar el Modelo de Seguridad y Privacidad de la Información | Política Gobierno Digital | Luis Orlando Arenas Ruiz | 01/07/2022 | 30/12/2022 | Fuente de recursos: Funcionamiento 'Fuente de recursos: InversiónProyecto: Implantación estratégica de fortalecimiento y modernización de las TICS en el MHCP |
| Dirección de Tecnología | Gestión de riesgos | Identificar, evaluar, gestionar los riesgos de seguridad digital | Desarrollar el plan de tratamiento de riesgos | Política Gobierno Digital | Luis Orlando Arenas Ruiz | 01/07/2022 | 30/12/2022 | Fuente de recursos: Funcionamiento 'Fuente de recursos: InversiónProyecto: Implantación estratégica de fortalecimiento y modernización de las TICS en el MHCP |
|  |  |  |  |  |  |  |  |  |
| Dirección de Tecnología | Implementación de controles | Diseñar el componente de privacidad relacionado con la seguridad de los datos | Implementar los controles de seguridad de la información | Política Gobierno Digital | Luis Orlando Arenas Ruiz | 01/07/2022 | 30/12/2022 | Fuente de recursos: Funcionamiento 'Fuente de recursos: InversiónProyecto: Implantación estratégica de fortalecimiento y modernización de las TICS en el MHCP |
| Dirección de Tecnología | Gestión de incidentes | Contratar el servicio de gestión de eventos, monitoreo y respuesta a incidentes de seguridad | Desarrollar la gestión de incidentes de seguridad de la información | Política Gobierno Digital | Luis Orlando Arenas Ruiz | 01/07/2022 | 30/12/2022 | Fuente de recursos: Funcionamiento 'Fuente de recursos: InversiónProyecto: Implantación estratégica de fortalecimiento y modernización de las TICS en el MHCP |
| Dirección de Tecnología | Concientización | Programar y desarrollar, conjuntamente con la Subdirección de Recursos Humanos, jornadas de sensibilización y capacitación de los funcionarios y contratistas de la entidad, sobre seguridad de la información y riesgos informáticos | Desarrollar Jornadas de Sensibilización y capacitación sobre seguridad de la información | Política Gobierno Digital | Luis Orlando Arenas Ruiz | 01/07/2022 | 30/12/2022 | Fuente de recursos: Funcionamiento 'Fuente de recursos: InversiónProyecto: Implantación estratégica de fortalecimiento y modernización de las TICS en el MHCP |

# 11. ANÁLISIS PRESUPUESTAL

Con base en los proyectos definidos para el PETI, se estima el presupuesto aproximado para los proyectos establecidos y los cuales fueron presentados en el Comité Institucional de Gestión y Desempeño para su aprobación.

**Tabla 5. Análisis Presupuestal**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID\_ Proyecto** | **ID\_Iniciativa** | **Nombre Proyecto** | **Área líder** | **Tiempo estimado total** | **Costo estimado inversión** |
| PRY-16 | IT016 | Diseñar el componente de privacidad relacionado con la seguridad de los datos | Dirección de Tecnología | 39 Meses | $5.718.909.426,08 |
| PRY-17 | IT017 | Fortalecer el modelo de seguridad y privacidad de la información | Dirección de Tecnología | 10 Meses | $1.422.604.649,48 |
| PRY-18 | IT018 | Contratar el servicio de gestión de eventos, monitoreo y respuesta a incidentes de seguridad | Dirección de Tecnología | 10 Meses | $2.873.776.140,03 |

# 12. RESPONSABLES

**Comité interno Institucional de Gestión y Desempeño**

* Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
	+ Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas
	+ necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.
	+ Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información

a los procesos de la entidad.

* + Aprobar acciones y mejores prácticas que en la implementación del MSPI.
	+ Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
* Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

**Comité interno de Seguridad y privacidad de la información y Seguridad digital (Conformado por: Director de Tecnología, Subdirector de Ingeniería de Software o su delegado, Subdirector de Administración de Recursos Tecnológicos o su delegado, Asesores del Despacho de la Dirección de Tecnología encargados del manejo de temas de seguridad, Consultores de Seguridad).**

* Definir los lineamientos y políticas de seguridad informática a ser aplicadas como parte del desarrollo de las funciones establecidas en el artículo 25 del Decreto 4712 de 2008, que son:
	+ Definir el modelo en seguridad informática y el plan de acción para su implantación.
	+ Diseñar, probar y hacer seguimiento a los mecanismos de seguridad en tecnología.
	+ Definir, divulgar, mantener actualizadas y hacer seguimiento a la aplicación de las políticas, estándares, metodologías y procedimientos en materia tecnológica para el Ministerio de Hacienda y Crédito Público.
* Seguimiento a los proyectos relacionados con seguridad informática, seguridad y privacidad de la información y seguridad digital.
* Revisar y validar la implementación de medidas y controles de seguridad que permitan, en un esquema práctico y dinámico, identificar las vulnerabilidades y riesgos frente a las diferentes amenazas externas e internas y mitigarlas.
* Revisar y acordar metodologías y procesos específicos relativos a la seguridad informática, de la información y digital, que se puedan aplicar para el Ministerio de Hacienda y Crédito Público – MHCP.
* Sesionar de forma mensual.

# 13. HISTORIAL DE CAMBIOS

| **FECHA** | **VERSIÓN** | **DESCRIPCIÓN DEL CAMBIO** | **ASESOR SUG** |
| --- | --- | --- | --- |
| 28/06/2022 | 1 | Creación del documento | Giovanny Montenegro |

# 14. APROBACIÓN

|  |  |
| --- | --- |
| **ELABORADO POR:**  | **Nombre:** Luis Orlando Arenas Ruiz - Isis Gomez Peralta**Cargo:** Asesor-1020-6 - Contratista**Fecha:** 24/06/2022 |
| **REVISADO POR:** | **Nombre:** Ricardo Fernelix Rios Rosales**Cargo:** Director de Tecnologia**Fecha:** 29/06/2022 |
| **APROBADO POR:** | **Nombre:** Comité Institucional de Gestión y Desempeño**Cargo:**  Comité Institucional de Gestión y Desempeño**Fecha:** 01/07/2022 |

1. Términos y Definiciones SGCN [↑](#footnote-ref-1)