**Contenido**

[1. INTRODUCCIÓN 2](#_Toc40793810)

[2. OBJETIVO 3](#_Toc40793811)

[3. ALCANCE 3](#_Toc40793812)

[4. PRODUCTOS ESPERADOS 4](#_Toc40793813)

[5. TÉRMINOS Y DEFINICIONES 4](#_Toc40793814)

[6. DESARROLLO DEL ALCANCE DE LA ACTIVIDAD PRINCIPAL 7](#_Toc40793815)

[6.1. Revisión y Actualización del SGSI de la Gestión de TIC 8](#_Toc40793816)

[6.1.1. Descripción 8](#_Toc40793817)

[6.1.2. Políticas 8](#_Toc40793818)

[6.1.3. Roles y responsabilidades 9](#_Toc40793819)

[6.1.4. Documentos de Apoyo 10](#_Toc40793820)

[6.2. Seguimiento permanente a la gestión del riesgo, para asegurar su pertinencia, adecuación y eficacia 11](#_Toc40793821)

[6.2.1. Descripción 11](#_Toc40793822)

[6.2.2. Políticas 12](#_Toc40793823)

[6.2.3. Roles y responsabilidades 12](#_Toc40793824)

[6.2.4. Documentos de Apoyo: 13](#_Toc40793825)

[6.3. Seguimiento a la Gestión de Incidentes de Seguridad 13](#_Toc40793826)

[6.3.1. Descripción 13](#_Toc40793827)

[6.3.2. Roles y responsabilidades 13](#_Toc40793828)

[6.3.3. Políticas 14](#_Toc40793829)

[6.3.4. Documentos de Apoyo: 14](#_Toc40793830)

[7. FACTORES DE ÉXITO 14](#_Toc40793831)

[7.1. Factores Claves de éxito 14](#_Toc40793832)

[7.2. Factores Críticos de éxito 14](#_Toc40793833)

[8. ASPECTOS DE INTEGRACIÓN 15](#_Toc40793834)

[8.1. Relación con otras Actividades Principales 15](#_Toc40793835)

[8.2. Relación con otros Procesos del SUG o Externos 15](#_Toc40793836)

[9. HISTORIAL DE CAMBIOS 16](#_Toc40793837)

[10. APROBACIÓN 17](#_Toc40793838)

# INTRODUCCIÓN

La Actividad Principal del Proceso Apo 1.3 Gobierno y Gestión de TIC “**Gobierno de Seguridad Digital y de la Información para la Gestión de TIC**” tiene como foco principal revisar y evaluar de forma permanente el estado del Sistema de Gestión de Seguridad de la Información con el propósito de establecer un marco de actuación en el que se fijen objetivos de seguridad y se establezcan los lineamientos de seguridad al interior de la DT y para la Gestión de TIC.

Lo anterior, acorde con la responsabilidad de la DT en la definición de políticas y mecanismos de seguridad digital de la institución y la contribución que esta Dirección según su competencia, debe hacer al cumplimiento de políticas del Estado relativas a la seguridad digital y de la información comprendidas en las normas, políticas y demás lineamientos que indican a continuación:

* Todas las políticas, procesos, procedimientos y actividades relacionadas con la Seguridad de la Información para la Gestión de TIC, se deben elaborar, gestionar y ejecutar en el marco de lo establecido a nivel normativo y en los lineamientos y políticas estatales tales como
  + Decreto 2482 de 2012 que establece el Modelo Integral de Planeación y Gestión – FURAG.
  + Políticas de Gobierno Digital y Seguridad Digital (que reemplaza la Estrategia de Gobierno en línea, del Decreto 1078 de mayo 26 de 2015 y modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios., define la seguridad de la información como principio de la Política de Gobierno Digital), la cual está definida en el Modelo Integrado de Planeación y Gestión (MIPG), adoptado en la entidad mediante Resolución 0974 del 11 de abril de 2018, donde se crea el Comité Institucional de Gestión y Desempeño del Ministerio de Hacienda.
  + Manual para la Implementación de la Política de Gobierno Digital (Ultima versión, Diciembre de 2018, Versión 6).
  + Ley 1712 o de Transparencia – Decreto 0103 de enero 20 de 2015.
  + Ley 1581 o de Protección de Datos Personales
  + CONPES 3584 de abril 11 de 2016- Política Nacional de Seguridad Digital.
  + Guía para la administración del riesgo y el diseño de controles en entidades públicas-Riesgos de gestión, corrupción y seguridad digital, y en particular su Anexo 4, Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, del DAFP.
  + Recomendaciones y buenas prácticas que se han generado de las Mesas de Trabajo de Infraestructura Crítica, Riesgo Operacional y Ciberdefensa, coordinadas por el CCOCI (Comando Conjunto Cibernético del Ejército Nacional).
* Todas las políticas, procesos, procedimientos y actividades relacionadas con la Seguridad de la Información para la Gestión de TIC tendrán en cuenta como marco de referencia, las mejores prácticas y estándares de la industria, tales como las normas ISO 27001 (Versión vigente) y asociadas, NTC 5254, ISO 31000.

# OBJETIVO

Mantener actualizado el sistema de gestión de seguridad de la información (SGSI), para efectos de garantizar que los riesgos que puedan afectar la información y los activos de información y de seguridad digital que sean administrados y/o gestionados por la Dirección de Tecnología, se gobiernan de manera eficiente y eficaz.

# ALCANCE

El desarrollo de la AP Gobierno de la Seguridad de la Información para la Gestión de TIC cubre los siguientes aspectos.

* Revisión y actualización de las políticas, procesos y procedimientos de seguridad de la información y seguridad digital para la Gestión de TIC.
* Revisión y actualización de los lineamientos y metodologías de gestión de riesgos de seguridad de la información y seguridad digital para la Gestión de TIC, 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.

El Gobierno y la Gestión de la Seguridad de la Información se ajustan al ciclo PHVA (en inglés PDCA), y bajo esta premisa, esta AP se enfoca en las etapas de Planeación y Verificación, mientras que el Hacer y el Actuar están a cargo de las otras AP´s que conforman el proceso Apo.1.3

Cabe anotar, que el alcance de esta AP no cubre la práctica establecida en el SUG referida a la gestión de riesgos del proceso, dado que la gestión de riesgos en esta AP se enfoca en los activos de información y de seguridad digital que administra la DT, bajo el estándar internacional adoptado y las políticas establecidas por el Estado.

# PRODUCTOS ESPERADOS

Aplicación de políticas y lineamientos definidos en este documento en lo relativo a:

* Revisión y actualización de las políticas, procesos y procedimientos de seguridad de la información para la Gestión de TIC.
* Revisión y actualización de los lineamientos y metodologías de gestión de riesgos de seguridad de la información y de seguridad digital para la Gestión de TIC, 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 y de seguridad digital identificados mediante la revisión de eventos, planes de tratamiento y sus resultados.

# ÉRMINOS Y DEFINICIONES

* **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.
* **Activo de Seguridad Digital**; Son elementos tales como aplicaciones de la entidad, servicios Web, redes, información física o digital, Tecnologías de la información (TI), Tecnologías de Operación (TO), que utiliza la organización para su funcionamiento,
* **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): onjunto 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.
* **Dominio**: Corresponde a cada uno de los aspectos que comprende o regula una norma técnica.
* **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.
* **Norma Técnica:** documento escrito, aprobado por un organismo reconocido y accesible al público. Para su elaboración se requiere el consenso de todas las partes interesadas (Fabricantes, administraciones, usuarios y consumidores, centros de investigación y laboratorios, asociaciones y colegios profesionales, agentes sociales, etc…)

Su objetivo es establecer los requisitos que deben cumplir los productos o servicios para asegurar su aptitud para el uso, seguridad, protección del producto, etc.

Su aplicación acostumbra a ser voluntaria, pero puede ser declarada de cumplimiento obligatorio cuando una norma jurídica así lo establezca.

Se identifica por unas siglas (UNE, EN, ISO, IEC, DIN, NT, BS, ASTM, etc.), un número y la fecha de publicación.

**Norma técnica internacional**: Es una norma adoptada por un organismo internacional de normalización, tal como ISO (Internacional Standard Organization), y que debe ser accesible al público.

* **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.
* **eguridad 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). En caso de la DT, el SMGI está definido en la documentación relacionada con la AP Gobierno de la seguridad (documento marco y relacionados)
* **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

# DESARROLLO DEL ALCANCE DE LA ACTIVIDAD PRINCIPAL

# Revisión y Actualización del SGSI de la Gestión de TIC

# Descripción

Consiste en realizar de forma periódica el diagnóstico, del estado del SGSI respecto a los marcos de referencia que se hayan adoptado, a partir del cual se determine el nivel de seguridad y privacidad de la información y de los activos de información que gestiona la DT y se establezcan las acciones requeridas para su actualización, para los dominios aplicables a esta dependencia. La anterior incluye la revisión de los dominios, su estado de desarrollo y madurez, su nivel de aplicabilidad al proceso Apo.1.3 Gobierno y gestión de TIC de la Dirección y las actividades a ser realizadas para cerrar la brecha, así como la posible inclusión de dominios no contemplados.

Como parte del SGSI, se deben incluir los componentes establecidos por las políticas y lineamientos estatales, como el Modelo de Privacidad y Seguridad de la Información.

# Políticas

1. El SGSI de la DT debe ser revisado, como mínimo una vez cada año, con base en las buenas prácticas o estándares ampliamente reconocidos en la materia y de acuerdo con las necesidades de la Dirección y la entidad.
2. La DT debe asegurar que el documento de políticas de seguridad de la información se mantenga vigente y que se adelantan acciones para que el mismo sea conocido y está disponible para consulta de cualquier funcionario, contratista o pasante de la entidad.
3. La Metodología de Gestión de Riesgos de Seguridad debe estar ajustada y alineada con los lineamientos estatales que, para tal fin, establezcan las entidades competentes.
4. Al menos una vez al año deben realizarse actividades de socialización y sensibilización sobre el estado del SGSI y los lineamientos estatales sobre seguridad, dirigidas a los funcionarios y contratistas de la DT, utilizando para tal fin los diferentes esquemas y canales de comunicación existentes, entre ellos, los REPAC y las reuniones de Informe de Gestión de la DT:
5. La revisión y actualización de los activos de información de la DT debe realizarse periódicamente, teniendo como principal criterio, mantener actualizado el inventario de los activos de información que soporten los servicios esenciales y críticos del Ministerio y de acuerdo con las directrices que para tal fin emita el Director de la DT.

# Roles y responsabilidades

Comité de Seguridad Digital y de la Información DT.

Ver **Anexo 1. Reglamento Comité de Seguridad Digital y de la Información DT**.

Director de Tecnología:

* Asegurar que en el diagnóstico, revisión y actualización del SGSI, participen los Subdirectores, funcionarios y contratistas relacionados con el objeto de la AP.
* Gestionar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Dirección

Gestor de Seguridad TIC

* Presentar propuestas para la actualización de los componentes del SGSI de acuerdo con la evolución las normas técnicas aplicables, la evolución de las TIC y las necesidades de la DT.
* Efectuar las actualizaciones del SGSI que se identifiquen y/o requieran, en articulación con las políticas y lineamientos del Estado y con las necesidades de la entidad.
* Orientar y articular la actualización e implementación de las políticas de seguridad de la información dentro de los procesos de la DT.
* Reportar al Comité de Seguridad Digital y de la Información DT. Comité de Seguridad el estado de la seguridad de la información y de la seguridad digital de la DT.
* Proponer y coordinar la estrategia de divulgación y concientización de Seguridad de la Información para todos los funcionarios y terceros que tengan acceso a los activos de información y de seguridad digital de la DT.
* Coordinar pruebas de penetración y análisis de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción, Contingencia y cualquier otro que se requiera) de acuerdo con la disponibilidad de recursos técnicos, humanos y financieros.
* Entregar los informes que sean solicitados en relación con los asuntos de competencia de la AP.
* Proponer y coordinar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la DT a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables. Para la realización de estas se debe tener en cuenta la disponibilidad de recursos técnicos, humanos y financieros.
* Realizar funciones de la Secretaría Técnica del Comité de Seguridad Digital y de la Información DT.
* Revisar la aplicación de la metodología de gestión de riesgos y los procedimientos asociados, para que esté alineada con las directrices estatales que, para tal fin, establezcan las entidades competentes.
* Coordinar la actualización periódica del inventario de los activos de información a cargo de la DT, así como la valoración y gestión de los riesgos asociados a los activos.

Director y Subdirectores DT:

* Identificar las necesidades de actualización del SGSI
* Asegurar que las responsabilidades del área a su cargo en el SGSI de la DT sean conocidas y atendidas, a través de la aplicación de los procedimientos y controles que le correspondan.

Dueño y/o Administrador de Activo de Información

* Gestionar de acuerdo con lo establecido en la norma ISO 27001, los riesgos asociados a los activos de información que le corresponde administrar.

# Documentos de Apoyo

* Apo.1.Man.3.2 Manual de Políticas de Seguridad
* Apo.1.3 Man.3.2.1 Manual de Políticas de Seguridad para Usuario Final
* Apo.1.Man.3.3 Estándar de Seguridad para Aplicativos
* **Anexo 1.** Reglamento Comité de Seguridad Digital y de la Información DT

# Seguimiento permanente a la gestión del riesgo, para asegurar su pertinencia, adecuación y eficacia

# Descripción

Consiste en monitorear y verificar que la gestión de riesgos en la DT y en la Gestión de TIC, se realice según lo establecido desde el SGSI, atiende los cambios en el entorno de los riesgos relacionados con la seguridad de la información, así como los cambios en los componentes de plataforma y aplicaciones de software.

Considerando que la Gestión de Riesgos en la DT comprende riesgos asociados a la seguridad de la información y la seguridad digital, de acuerdo con los lineamientos del Estado, los cuales son de obligatorio cumplimiento, la DT seguirá lo establecido en la Metodología de Gestión de Riesgos del Ministerio de Hacienda, la cual se ajusta a la Guía para la administración del riesgo y el diseño de controles en entidades públicas-Riesgos de gestión, corrupción y seguridad digital, emitida por el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones. La metodología del Ministerio adopta dentro de sus anexos, y en particular, el Anexo 4, Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, como el marco metodológico para realizar la gestión de riesgos de seguridad digital que le compete a la DT.

Por tanto, la DT no actualizará metodologías propias, sino que adoptará las actualizaciones y/o mejoras que se hagan en la Guía del Ministerio, como consecuencia de mejoras o actualizaciones en los lineamientos, que hagan los entes encargados a nivel nacional.

Como complemento a la Guía adoptada, la DT revisará las recomendaciones y buenas prácticas que se generen de las Mesas de Trabajo de Infraestructura Crítica, Riesgo Operacional y Ciberdefensa, coordinadas por el CCOC (Comando Conjunto Cibernético del Ejército Nacional), en especial las contenidas en la Guía para la identificación de Infraestructuras Críticas Cibernéticas nacionales (ICCN) los Planes Nacional de protección y defensa de las ICCN y el de Protección y Defensa de las ICC del sector financiero, con el fin de incorporarlas a los anexos correspondientes de la Guía de gestión de Riesgos del Ministerio.

# Políticas

1. El seguimiento a la matriz de riesgos y a los controles implementados, debe hacerse como mínimo de forma anual, por muestreo, de acuerdo con criticidades y prioridades definidas.

# Roles y responsabilidades

Gestor de Seguridad TIC

* Realizar la revisión de la gestión de riesgos de seguridad a partir de la información registrada en la matriz de riesgos de seguridad.
* Elaborar el informe de resultados y recomendaciones de la revisión de la gestión de riesgos y hacer su presentación al Comité de Seguridad Digital y de la Información DT.
* Identificar ajustes al SGSI derivados en la revisión efectuada y presentarlos ante el Comité de seguridad.
* Brindar apoyo técnico para el análisis de riesgo de seguridad de la información y para la aplicación de la Metodología de Riesgos del Ministerio y sus anexos.
* Verificar que se lleve a cabo la implementación de controles de seguridad en un esquema práctico y dinámico para el manejo seguro de la información, con base en el análisis de riesgos que permita identificar las vulnerabilidades frente a las diferentes amenazas externas e internas.
* Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

Comité de Seguridad Informática DT

Ver **Anexo 1. Reglamento Comité de Seguridad Digital y de la Información DT**

Subdirectores DT

* Efectuar la gestión de riesgos de los activos de información a su cargo.
* Reportar la información requerida para mantener actualizada la matriz de riesgos de seguridad.

# ocumentos de Apoyo:

NA.

# Seguimiento a la Gestión de Incidentes de Seguridad

# Descripción

Consiste en monitorear y verificar que la gestión de incidentes de seguridad se realice de acuerdo con los procedimientos establecidos, y se atiendan de forma oportuna.

# Roles y responsabilidades

Gestor de Seguridad de la Información

* Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes de seguridad informática.
* Orientar el análisis y manejo de incidentes de seguridad.
* Realizar la revisión de la gestión de incidentes de seguridad de la información, a partir de la información registrada en la plataforma utilizada por la DT para tal fin.
* Elaborar el informe de resultados y recomendaciones de la revisión de la gestión de incidentes de seguridad y hacer su presentación al Comité de Seguridad, cuando se requiera.
* Identificar ajustes al SGSI derivados en la revisión efectuada y tramitar su aprobación ante el Comité de Seguridad Digital y de la Información DT.
* Evaluar y coordinar la implementación de controles específicos de seguridad para nuevos servicios.

Comité de Seguridad Digital y de la Información DT:

Ver **Anexo 1. Reglamento Comité de Seguridad Digital y de la Información DT**

Subdirectores DT:

* Efectuar la gestión de los incidentes de seguridad que sean de competencia de la Subdirección a su cargo.

# Políticas

1. La Gestión de Incidentes de Seguridad debe considerar dentro de los niveles de escalamiento, las instancias estatales que pueden apoyar el análisis y atención de incidentes (Por ejemplo: COLCERT, DIJIN, CSIRT de la Policía, CCOC, etc)

# Documentos de Apoyo:

* Procedimiento para Gestión de Incidentes de Seguridad

# FACTORES DE ÉXITO

# Factores Claves de éxito

* Contar con una política de seguridad de la información formalizada para Gestión de TIC, al interior de la DT.
* Apropiación del concepto de seguridad de la información al interior de la DT
* Efectividad de la comunicación y socialización de los temas de seguridad en el MHCP.
* Riesgos de los activos de información gestionados por los responsables de los mismos.
* Incidentes de seguridad visibilizados y gestionados**.**

# Factores Críticos de éxito

* Compromiso de la alta dirección de la DT y la participación por parte de los funcionarios de la DT en la gestión del riesgo.
* Actualización y revisión periódica de las políticas de administración y gestión del riesgo.
* La concienciación, socialización y divulgación continúa de los temas de seguridad.
* Definición oportuna y adecuada de los aspectos técnicos requeridos por los diferentes grupos de la DT.
* Seguimiento adecuado y oportuno a las actividades enmarcadas dentro del SGSI de la DT, que permita la toma de acciones tendientes a facilitar la ejecución efectiva de las actividades de gestión de la seguridad informática.
* Recopilación y aprovechamiento de las lecciones aprendidas en relación con gestión de riesgos e incidentes de seguridad.

# ASPECTOS DE INTEGRACIÓN

# Relación con otras Actividades Principales

| **Desde esta AP** | **Actividad Principal** | **Descripción** | **Mecanismo de Entrega / Recibo** |
| --- | --- | --- | --- |
| Recibe de | Gobierno de Arquitectura Tecnológica | Definición de nuevos componentes o tipos de soluciones que impliquen ajustes en la gestión de riesgos, clasificación de activos de información, incidentes de seguridad y/o vulnerabilidades | Documento descriptivo de componente o servicio de arquitectura |
| Recibe de | Gestión de Servicios TIC | Registros/Evidencias de la gestión de riesgos asociados a los activos de información involucrados en la Gestión de TIC y de incidentes de seguridad. | Informe aplicación de controles y gestión de vulnerabilidades de componentes de plataforma que soportan servicios TIC |

# Relación con otros Procesos del SUG o Externos

| **Proceso** | **Insumo o Salida** | **Descripción** | **Mecanismo de Entrega / Recibo** |
| --- | --- | --- | --- |
| Instancias estatales que pueden apoyar el análisis y atención de incidentes (Por ejemplo: COLCERT, DIJIN, CSIRT de la Policía, CCOC, etc) | Salida | Los incidentes de seguridad que deban ser escalados de acuerdo con las políticas establecidos deben ser comunicados a las instancias Estatales, bien sea para solicitar apoyo o para contribuir a la red de conocimiento sobre este tipo de incidentes | Correo electrónico o redes sociales |
| Instancias estatales como COLCERT, DIJIN, CSIRT de la Policía, CSIRT Gobierno de MinTic, CCOCI, etc) | Insumo | Informes de vulnerabilidades identificados en la plataforma del MHCP  Descripción de posibles ataques a la plataforma del MHCP o de otras entidades | **Correo electrónico, redes sociales o teléfono** |

# 

# HISTORIAL DE CAMBIOS

| **FECHA** | **VERSIÓN** | **DESCRIPCIÓN DEL CAMBIO** | **ASESOR SUG** |
| --- | --- | --- | --- |
| 01–12-2016 | 1 | Creación del documento | Derly Catherine Cifuentes Guerrero |
| 20-05-2020 | 2 | * Se actualiza el documento a la plantilla para manual establecida en el SUG. * Se incorpora el concepto de seguridad digital. * Se ajusta el apartado 4.2, de acuerdo con los lineamientos estatales en seguridad digital. * Se incorpora lo relativo a la relación con instancias estatales de ciberseguridad y ciberdefensa. * Se incorpora el anexo que define las condiciones del Comité de Seguridad Digital y de la información DT. | Liliana Parra Ramirez |

# APROBACIÓN

|  |  |
| --- | --- |
| **ELABORADO POR:** | **Nombre**: Alejandro I. Cruz  **Cargo**: Asesor  **Dependencia**: Despacho Dirección de Tecnología  **Fecha:** 30-08-2019 |
| **REVISADO POR:** | **Nombre**: Alejandro I. Cruz  **Cargo**: Asesor  **Dependencia**: Despacho Dirección de Tecnología  **Fecha:** 30-08-2019 |
| **APROBADO POR:** | **Nombre:** Ricardo Ríos Rosales  **Cargo:** Director de Tecnología  **Dependencia:** Despacho de la Dirección de Tecnología  **Fecha:** 20-05-2020 |

**ANEXO 1. - REGLAMENTO COMITÉ DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN DT**

1. **OBJETIVO DEL COMITÉ**

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.

Lo anterior alineado con los lineamientos que, sobre la materia de seguridad de la información y digital, emitan los entes de gobierno con competencia en el tema.

1. **PARTICIPANTES**

* 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 que en el momento laboren para la entidad

El Comité podrá sesionar con la asistencia del Director y los Asesores de Despacho que manejen los temas de seguridad, quienes son los miembros base del Comité.

1. **PERIODICIDAD**

Trimestral, aunque se pueden citar a Comités Extraordinarios, de acuerdo con temas de interés prioritario.

**NOTA**: Los temas propios del Comité se pueden tratar en los Comités Estratégicos de la Dirección, caso en el cual, el Comité Estratégico, tendrá la connotación de Comité de Seguridad en cuanto a las decisiones que se tomen en materia de Seguridad Digital y de la Información DT.

1. **FUNCIONES**

* Revisar el cumplimiento de las políticas de seguridad de la información y digital, buscando establecer un marco de actuación en el que se fijen objetivos de seguridad y se establezca la orientación general de los lineamientos de seguridad al interior de la Dirección.
* Seguimiento a los proyectos relacionados con seguridad informática, seguridad 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 en la DT
* En general, las que se establezcan dentro del documento de la AP (Actividad Principal) Gobierno de Seguridad de la Información para la Gestión de TIC, y que estén bajo responsabilidad de este Comité.

El comité tiene carácter de asesor, la gestión de la seguridad digital y de la información, será función de cada subdirector y su equipo de trabajo como responsables de los activos.

1. **POLITICAS**

* Cuando el Comité lo considere pertinente se podrá citar a terceros.
* La Secretaria Técnica del Comité estará bajo la responsabilidad del Asesor de Despacho designado para tal fin, y que tenga bajo su cargo los temas y/o proyectos de seguridad.
* Los temas tratados en el Comité son de carácter confidencial, excepto los que expresamente se consideren que pueden ser comunicados a otras personas o funcionarios.