## Control de cambios

| Versión | Fecha | Descripción de la modificación |
|---|---|---|
| **01** | **27 de septiembre de 2023** | Creación del procedimiento que establece la metodología a utilizarse para la Gestión de Riesgos de Seguridad de la Información y sus respectivos lineamientos, en cumplimiento de la Estrategia de Gobierno Digital y Seguridad Digital para la Secretaría Distrital de Gobierno. |

| Método de Elaboración | Revisa | Aprueba |
|---|---|---|
| El documento se elabora por parte de Doris Páez y Carlos Andrés Ortegón de la Dirección de Tecnologías e Información, con el acompañamiento metodológico de la Oficina Asesora de Planeación. | **Orlando Benavides Santacruz**<br>Director de Tecnologías e Información<br><br>**Yamile Espinosa Galindo**<br>Profesional OAP – Analista del proceso | **Gabriel Felipe Angarita Serrano**<br>Jefe Oficina Asesora de Planeación<br>Líder del macroproceso Planeación Estratégica<br><br>Caso Hola No. **345789** |

# 1. INFORMACIÓN GENERAL

## Objetivo del Procedimiento

Establecer la metodología para realizar la gestión integral de los riesgos de Seguridad de la Información que afectan la funcionalidad de la Secretaría Distrital de Gobierno, a través de su identificación, análisis, valoración, definición de estrategias para gestionar integralmente los riesgos, su monitoreo y revisión periódica, en el marco del Modelo Integrado de Planeación y Gestión- MIPG y del Modelo de Seguridad y Privacidad de la Información MSPI y de acuerdo con el Manual de Gestión del Riesgo (PLE-PIN-M001) de la Secretaria Distrital de Gobierno, bajo las mejores prácticas en materia de Seguridad de la Información con el fin de preservar la disponibilidad, confidencialidad e integridad de la información.

## Alcance

Aplica en todos los procesos de la Secretaría Distrital de Gobierno, tanto en el nivel central y como en las Alcaldías Locales, con un enfoque hacia el entorno digital, basándose en los activos de información identificados, catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad de la información, dentro de un ambiente y contexto normal de operación.

Este procedimiento inicia con la identificación de los riesgos de seguridad de la información y termina con la aprobación del plan de tratamiento de riesgos.

## Responsable

Director(a) de Tecnologías e Información.

## Políticas de operación

Para el buen desarrollo de las actividades propuestas en el procedimiento se requiere cumplir con las siguientes condiciones:

1) La Dirección de Tecnologías e Información, a través del equipo de Seguridad de la Información, es la responsable de realizar el acompañamiento en el levantamiento y actualización de los riesgos de Seguridad de la información a Nivel Central y de Alcaldías Locales de la Secretaría Distrital de Gobierno, validando la correcta aplicación de los lineamientos establecidos en este procedimiento. Se deja como evidencia las listas de asistencia del aplicativo TEAMS o Evidencia de Reunión (si es presencial) y la grabación de las mesas de trabajo a que haya lugar.
2) Es responsabilidad de cada una de las dependencias y/o alcaldías locales informar a la Dirección de Tecnologías e Información – equipo de Seguridad de la Información de cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información que se presenten.
3) Es responsabilidad de la Dirección de Tecnologías e Información - equipo de Seguridad de la Información, identificar los Riesgos de Seguridad de la información para la Secretaría Distrital de Gobierno que causen la pérdida de alguno de los tres pilares fundamentales de la Seguridad de la información (confidencialidad, integridad y disponibilidad).

4) Marco de Referencia: Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital GD, la Secretaría Distrital de Gobierno está en la implementación del Plan de Seguridad y Privacidad de la información basado en el Modelo de Seguridad y Privacidad de la Información MSPI en donde es parte fundamental la identificación, valoración y clasificación de los activos de información, a partir de los cuales se genera la identificación y valoración de riesgos de seguridad.

5) Establecimiento del contexto externo: Para determinar el contexto externo vigente en la Secretaría Distrital de Gobierno se debe diligenciar el formato PLE-PIN-F042 Matriz de riesgos de seguridad de la información – hoja Contexto, para ello se debe considerar, los siguientes factores relacionados con el entorno digital:

- Clientes: Aproximadamente se presta servicio a 7.200.000 de ciudadanos de Bogotá D.C. a través del entorno digital por medio de páginas web.
- Proveedores de servicios: algunos de ellos son ETB, Enel, Fortinet, Sumimas, Comercializadora ElectroHomero, Adsum, entre otros.
- Empresas con las que se relacionan especialmente por la misión de la entidad: Alcaldía Mayor de Bogotá, Secretaría General, Alta Consejería TIC, Secretaría de Seguridad y Convivencia, Secretaría de la Mujer, Policía Nacional, Secretaría de Hacienda, Compensar, entre otras.
- Normativas o aspectos jurídicos o normativos que apliquen directa o indirectamente a la entidad.
- Otros aspectos como circunstancia actual de la administración, si se presenta alguna situación especial como Ley de garantías u otros.

Adicionalmente, el contexto interno debe considerar factores que impactan directamente a: la estructura organizacional actual, aplicativos vigentes, reglamentación interna, cantidad de funcionarios y/o contratistas, mapa de procesos vigente. La Secretaría Distrital de Gobierno cuenta con el siguiente organigrama https://www.gobiernobogota.gov.co/content/estructura-organizacional-secretaria-distrital-gobierno

En este contexto se debe considerar que:

- Los sistemas de información o servicios se dividen en:
  - Misionales (JACD, comparendo ambiental, Si Actua, Side, Arco, Sello Seguro, Certificados residencia, Pirpas)
  - Estratégicos (Sigob)
  - De apoyo (Hola, MErcurio, Orfeo, Mimec, Sipse, Siap, Si capital)
  - De servicios (desprendibles de pago, Consulta inventario, certificaciones contractuales)
- La reglamentación interna se encuentra publicada en la página de la entidad.
- La entidad cuenta con aproximadamente 6700 empleados entre funcionarios de planta y contratistas.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones se visualiza en el siguiente mapa de procesos: http://gaia.gobiernobogota.gov.co/content/sistema-integrado-de-gesti%C3%B3n-sdg

6) Política para la identificación de los riesgos inherentes de seguridad digital: Para identificar los riesgos de seguridad de la información, se deben tener en cuenta los siguientes criterios:

- Afectación a la confidencialidad
- Afectación a la integridad
- Afectación a la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso teniendo en cuenta lo establecido en el formato GDI-TIC-F032 *Identificación, valoración y clasificación de activos de información,* el cual se genera a partir de la aplicación del procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información.

Esta etapa se trabajará conjuntamente entre las dependencias y la DTI para analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. El listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados se encuentra descrito en el formato PLE-PIN-F042 *Matriz mapa de riesgos de seguridad de la información*, en las hojas denominadas Amenazas y Vulnerabilidades, respectivamente.

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la Secretaria Distrital de Gobierno debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el proceso responsable de los riesgos, es decir, "que proceso quien tiene que rendir cuentas sobre ellos o quien tiene la autoridad para gestionar el riesgo", toda esta información se registra formato PLE-PIN-F042 *Matriz mapa de riesgos de seguridad de la información.*

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- Lluvia de ideas: Mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Debe existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias (si la reunión es presencial, lo cual se registra en el formato GDI-GPD-F029 Evidencia de reunión).
- Juicio de expertos: A través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración.

7) Política para la valoración de los riesgos: Las diferentes dependencias y localidades de la Secretaría Distrital de Gobierno realizarán la valoración del riesgo para lo cual deben diligenciar el formato PLE-PIN-F042 *Matriz mapa de riesgos de seguridad de la información*, el cual internamente manejará las siguientes valoraciones:

| PROBABILIDAD | VALOR |
|---|---|
| Rara Vez | <=1 |
| Improbable | 2 |
| Posible | 3 |
| Probable | 4 |
| Casi seguro | 5 |

| IMPACTO | VALOR |
|---|---|
| Insignificante | <=1 |
| Menor | 2 |
| Moderado | 3 |
| Mayor | 4 |
| Catastrófico | 5 |

| TOTAL DE LA SOLIDEZ INDIVIDUAL | |
|---|---|
| Fuerte | 100 |
| Moderado | 50 |
| Débil | 0 |

| SOLIDEZ CONJUNTO DE CONTROLES | |
|---|---|
| Fuerte | 100 |
| Moderado | 50<x<=99 |
| Débil | <=50 |

8) Política para el tratamiento de los riesgos de seguridad digital: Una vez se han identificado y evaluado los riesgos, se debe definir el tratamiento para cada uno de ellos, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional. El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, se puede tener en cuenta las opciones para tratar el riesgo como son las siguientes:

- Evitar
- Aceptar
- Transferir
- Mitigar

**NOTA:** Si la Secretaria Distrital de Gobierno decide mitigar o tratar el riesgo mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA del Anexo A de la norma ISO/IEC 27001:2013, como un insumo base para mitigar los riesgos de seguridad de la información. Sin embargo, la entidad puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo en mención, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

9) Política para el monitoreo y revisión de los riesgos de seguridad de la información: La Secretaría Distrital de Gobierno a través de las tres líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar monitoreo de los riesgos y controles tecnológicos, será responsabilidad de cada una de las dependencias y alcaldías locales con el acompañamiento de la Dirección de Tecnologías e Información - equipo de Seguridad de la Información.
- La Dirección de Tecnologías e Información - equipo de Seguridad de la Información de manera conjunta con las dependencias y alcaldías locales efectúa la evaluación del plan de acción y realizan nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad, por lo menos una vez al año.
- Las dependencias y alcaldías locales deben verificar que los controles estén diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- La Dirección de Tecnologías e Información - equipo de Seguridad de la Información debe suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles. Nota: una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó

de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

10) Política para el mejoramiento continuo de la gestión del riesgo de seguridad de la Información: La Secretaría Distrital de Gobierno debe garantizar la mejora continua de la gestión de riesgos de seguridad de la información, por lo tanto, cuando existan hallazgos, falencias o incidentes de seguridad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos.

    Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse. Es importante tener en cuenta y aplicar los lineamientos establecidos en el GCN-M002 *Manual para la gestión de planes de mejoramiento* para la formulación de los planes de mejora, a partir de los siguientes criterios:

    - Las dependencias y alcaldías locales deben revisar y evaluar los hallazgos por riesgos de seguridad de la información encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas, así como las debilidades encontradas como resultado de la gestión del riesgo.
    - Las dependencias y alcaldías locales deben establecer las posibles causas y consecuencias del hallazgo, e igualmente determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
    - Las dependencias y alcaldías locales deben emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad o de los servicios que presta al ciudadano. Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.
    - Una vez las matrices de riesgos de cada una de las dependencias y/o localidades sean aprobadas por el respectivo jefe o alcalde, estás serán guardadas en el sitio dispuesto por la Dirección de Tecnologías e Información - equipo de Seguridad de la Información y no serán publicadas por la información sensible que ellas pueden contener. Así mismo, se realizará un consolidado que será presentado al Comité Institucional de Gestión y Desempeño al menos una vez al año. La trazabilidad de las matrices de riesgos de seguridad de la información se registrará en el cuadro de control de cambios del formato PLE-PIN-F042 *Matriz mapa de riesgos de seguridad de la información*.

## Glosario

• Activo digital: En el contexto de seguridad digital de la información son elementos tales como aplicaciones de la organización, servicios web, redes hardware, información física o digital recurso humano entre otros que utiliza la organización para funcionar en el entorno digital.

• Administración de riesgos: Conjunto de elementos de control que, al interrelacionarse, le permiten a la SDG evaluar aquellos eventos negativos, tanto internos como externos que puedan afectar o impedir el logro de los objetivos institucionales.

• Amenazas: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

• Análisis del riesgo: Establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente) y posterior a la definición de controles para prevenir la ocurrencia del riesgo (análisis del riesgo residual).

• Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

• Asumir el riesgo: Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

• Auditoría Interna de Gestión: Son todas las actividades y procesos sistemáticos, independientes y documentados para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de la auditoría.

• Calificación del riesgo: Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

• Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

• Compartir o transferir el riesgo: Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

• Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos entidades o proceso no autorizados.

• Consecuencia: Son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, los grupos de valor y demás partes interesadas.

• Control: Medida que permite reducir o mitigar un riesgo / acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

• Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

• Evaluación del riesgo: resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo.

• Evitar el riesgo: opción de manejo donde se deben determinar acciones para continuar disminuyendo tanto probabilidad como el impacto, mediante el fortalecimiento de controles, optimización de procesos y el diseño de nuevos controles.

• Gestión del riesgo: Actividad adelantada por la alta dirección de la SDG y demás personal para proporcionar a la administración un aseguramiento razonable para el logro de los objetivos.

• Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

• Integridad: Propiedad de exactitud y completitud.

• Materialización del riesgo: ocurrencia del riesgo identificado.

• Matriz de Riesgos: Resultado de la aplicación de las fases de identificación, análisis, evaluación y tratamiento, en cada proceso en el formato establecido para tal fin.

• Monitorear: Observar, analizar, verificar y evaluar los riesgos identificados, determinando el adecuado desarrollo de cada una de las etapas de administración y el nivel de cumplimiento y efectividad de los controles y acciones definidas.

• Opciones de manejo: Posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

• Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

• Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

• Riesgo de Seguridad de la Información: 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. (ISO/IEC 27000).

• Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital, puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

• Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

• Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

• Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles.

• Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## Siglas

- GD: Gobierno digital
- MIPG: Modelo Integrado de Planeación y Gestión
- OAP: Oficina Asesora de Planeación
- SDG: Secretaría Distrital de Gobierno
- MSPI: Modelo de Seguridad y Privacidad de la Información
- DTI: Dirección e Tecnologías e Información

## Salidas generadas del procedimiento:

| Salida o Resultado | Descripción de la Salida o Resultado | Destinatario |
|---|---|---|
| Riesgos de seguridad de la información | Son los riesgos que establecen 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. | Todos los procesos de la Entidad |

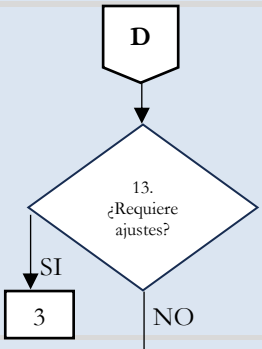
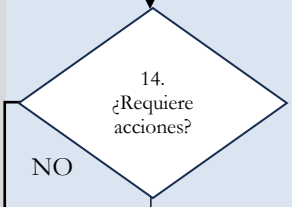
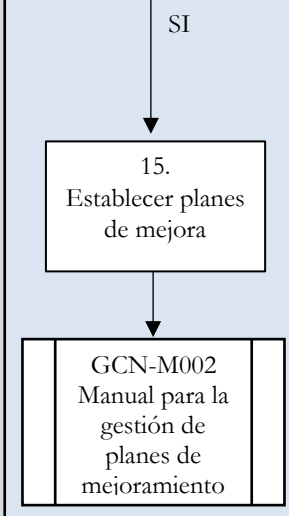
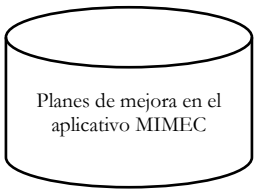
## 2. DESCRIPCIÓN ACTIVIDADES DEL PROCEDIMIENTO

| ACTIVIDAD | RESPONSABLE | DESCRIPCIÓN DE LA ACTIVIDAD | REGISTRO |
|---|---|---|---|
| INICIO | | Inicio del procedimiento | N/A |
| 1. Convocar a los responsables | Director de Tecnologías e Información - Equipo de seguridad de la Información DTI | Se realiza la convocatoria a las diferentes dependencias y/o alcaldías locales con el fin de establecer quienes participaran en el proceso de gestión de riesgos de seguridad de la información. Con la información remitida por los jefes de las dependencias y los alcaldes locales se convoca la capacitación correspondiente. Como evidencia se conservan los correos electrónicos | Correo electrónico |
| 2. Realizar capacitación | Equipo de seguridad de la Información DTI | Se realiza la capacitación (presencial y/o virtual) a las alcaldías locales y/o dependencias del Nivel Central sobre la metodología de gestión de riesgos de seguridad de la información y el formato PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información. La capacitación debe incluir como mínimo los siguientes temas:<br>• Definición del contexto interno, externo y de los procesos de la entidad.<br>• Definición de la política de administración de riesgo.<br>• Designación de roles y responsabilidades.<br>• Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.<br>• Identificación de activos.<br>• Identificación de riesgos.<br>• Valoración de riesgos.<br>• Definición del tratamiento de los riesgos<br><br>En dicha capacitación se solicita a las alcaldías locales y/o dependencias del Nivel Central diligenciar el formato PLE-PIN-F042. | Listado de asistencia – aplicativo Teams.<br><br>GDI-GPD-F029 Evidencia de reunión |
| A | | | |

| ACTIVIDAD | RESPONSABLE | DESCRIPCIÓN DE LA ACTIVIDAD | REGISTRO |
|---|---|---|---|
| 13 / A<br>3. Establecer el contexto interno y externo | Equipo de seguridad de la Información DTI - Área, dependencia - grupo encargado del manejo de la información | Se realiza la identificación del contexto interno y externo de la entidad, profundizando en lo relacionado con seguridad digital. Este contexto se diligencia en el formato PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información – hoja Contexto. Ver Política de Operación No. 5. | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información |
| 4. Identificar los riesgos de seguridad de la información | Área, dependencia - grupo encargado del manejo de la información. | Se realiza a partir de mesas de trabajo conjuntamente con los profesionales de la Dirección de Tecnologías de Información, teniendo en cuenta el contexto, objetivo y alcance de los procesos. Esta identificación se registra en el formato PLE-PIN-F042, para lo cual es necesario que se cuente previamente con el formato GDI-TIC-F032 Identificación, valoración y clasificación de activos de información, debidamente diligenciado y aprobado por el jefe de dependencia o Alcalde Local, según lo establecido por el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información. Ver Política de Operación No. 6. | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información<br>Listado de asistencia – aplicativo Teams |
| 5. Realizar el análisis de los riesgos de seguridad de la información | Área, dependencia - grupo encargado del manejo de la información. | Se establecen cuales son las amenazas, vulnerabilidades y consecuencias asociadas a cada grupo de activos. Se debe tener en cuenta la información contenida en el formato PLE-PIN-F042 que presenta una guía sobre las posibles amenazas y vulnerabilidades de acuerdo con cada tipo de activo y riesgo. | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información<br>Listado de asistencia – aplicativo Teams |
| 6. Valorar los riesgos de seguridad de la información<br>B | Área, dependencia - grupo encargado del manejo de la información. | Se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia e impacto. Se debe seleccionar de acuerdo con las tipologías definidas en el formato PLE-PIN-F042. Ver Política de Operación No. 7. | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información |

| ACTIVIDAD | RESPONSABLE | DESCRIPCIÓN DE LA ACTIVIDAD | REGISTRO |
|---|---|---|---|
| B<br>↓<br>7. Identificar y evaluar controles asociados a los riesgos de seguridad de la información | Área, dependencia - grupo encargado del manejo de la información. | De acuerdo con la metodología una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios. Para esto se deben determinar los controles asociados a cada riesgo, teniendo en cuenta la guía de controles que se presenta en el formato PLE-PIN-F042 -hoja Controles, como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho formato. Igualmente, se pueden incluir otros posibles controles que se manejen para evitar la materialización de los riesgos.<br><br>Se evalúan los controles respondiendo las preguntas asociadas en el formato, lo que presenta de manera automática la valoración del riesgo residual.<br><br>Esta actividad se realiza en mesa de trabajo conjunta con la Dirección de Tecnologías e Información. | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información |
| ↓<br>8. Establecer plan de tratamiento de riesgos de seguridad de la información<br>↓<br>C | Área, dependencia - grupo encargado del manejo de la información. | De acuerdo con la valoración del riesgo, de manera conjunta se establecen estrategias o controles adicionales basados en la norma ISO 27001 tendientes a minimizar o mitigar la ocurrencia del riesgo y el periodo en el cual se realizará el respectivo monitoreo. Ver Política de Operación No. 8. | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información |

| ACTIVIDAD | RESPONSABLE | DESCRIPCIÓN DE LA ACTIVIDAD | REGISTRO |
|---|---|---|---|
| C<br>9. ✓ Revisar y aprobar la matriz mapa de riesgos de seguridad de la información | Jefe de cada dependencia o Alcalde(sa) Local | Revisa y aprueba la matriz mapa de riesgos de seguridad de la información, teniendo en cuenta el objetivo, el contexto y los controles del proceso. Como registro del control queda el correo electrónico de aprobación y/o formato firmado por el responsable. | Correo electrónico<br>PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información |
| 10. ¿Se aprueba?<br>NO<br>3 | N/A | ¿Se aprueba la matriz mapa de riesgos de seguridad de la información?<br><br>Si, continúa con la actividad 11.<br>No, se devuelve a la actividad 3. | N/A |
| SI<br>11. Ejecutar el plan de tratamiento de riesgos de seguridad de la información | Área, dependencia - grupo encargado del manejo de la información. | Cada dependencia o localidad como Primera Línea de Defensa debe ejecutar o poner en práctica los controles indicados en el Plan de tratamiento, de lo cual se debe dejar la respectiva evidencia de su aplicación.<br><br>Nota: La Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos. | Evidencias plan de tratamiento |
| 12. ✓ Realizar el monitoreo y revisión de los riesgos de seguridad de la información<br>D | Equipo de seguridad de la Información DTI - Área, dependencia - grupo encargado del manejo de la información | ✓ El monitoreo se realiza mediante mesa de trabajo para evaluar si se llegó a materializar el riesgo, si se dio aviso de ello, qué fue afectado y demás elementos relacionados. Así mismo, se valida si los controles o estrategias planteadas fueron efectivas o se deben modificar. El monitoreo se realiza en el primer trimestre de cada año, evaluando la gestión de los riesgos de la vigencia anterior. De todo ello, se aporta la respectiva evidencia.<br><br>Se debe supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (Primer Línea de Defensa y la Dirección de Tecnologías de la Información -DTI) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado. Cuando se materialice el riesgo se | PLE-PIN-F042 Matriz mapa de riesgos de seguridad de la información<br>Listado de asistencia – aplicativo Teams.<br>Registro de monitoreo |

| ACTIVIDAD | RESPONSABLE | DESCRIPCIÓN DE LA ACTIVIDAD | REGISTRO |
|---|---|---|---|
| | | deben formular el correspondiente plan de mejoramiento. Ver Política de Operación No. 9. | |
|  | N/A | ¿Se requiere ajustar la matriz de riesgos de seguridad de la información?<br><br>SI, continúa con la actividad 3.<br>NO, continúa con la actividad 14. | N/A |
|  | N/A | ¿Se requiere acciones de mejora?<br><br>SI, continúa con la actividad 15.<br>NO, continúa con la actividad 16. | N/A |
|  | Área, dependencia - grupo encargado del manejo de la información. | Cada dependencia o localidad, dependiendo del seguimiento y monitoreo realizado a los riesgos de seguridad de la información, en caso de hallazgos o falencias, elaborará el respectivo plan de mejora tendiente a minimizar la materialización del riesgo identificado, de acuerdo con lo dispuesto en el GCN-M002 Manual para la gestión de planes de mejoramiento. Ver Política de Operación No. 10. |  |
|  | N/A | Fin del procedimiento | N/A |

## 3. DOCUMENTOS RELACIONADOS

### 3.1 Documentos internos

| Código | Documento |
|---|---|
| PLE-PIN-M001 | Manual de Gestión del Riesgo |
| GCN-M002 | Manual para la gestión de planes de mejoramiento |
| GDI-TIC-P004 | Identificación y Valoración de Activos de información |
| GDI-TIC-F032 | Formato identificación, valoración y clasificación de activos de información |
| PLE-PIN-F042 | Matriz de riesgos de seguridad de la información |

### 3.2 Normatividad vigente

| Norma | Año | Epígrafe | Artículo(s) |
|---|---|---|---|
| Ley 1712 | 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. | Toda la Norma |
| Ley 1581 | 2012 | Disposiciones generales para la protección de datos personales | Toda la Norma |

### 3.3. Documentos externos

| Nombre | Fecha de Publicación o Versión | Entidad que lo Remite | Medio de Consulta |
|---|---|---|---|
| Política Gobierno Digital | | MINTIC | https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/ |
| Manual Gobierno en Línea | 2018 | MINTIC | https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf |
| Modelo Seguridad y Privacidad de la Información | 2016 | MINTIC | https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf |

| Nombre | Fecha de Publicación o Versión | Entidad que lo Remite | Medio de Consulta |
|---|---|---|---|
| ISO 27005 | 2018 | | https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/ |
| Lineamientos para la Administración de Riesgos (Numeral 10.3) | | MINTIC | https://www.mintic.gov.co/portal/715/articles-135827_manual_lienamientos_administracion_riesgos_v9.pdf |
| Guía NO. 7 guía de Gestión de Riesgos | 2016 | MINTIC | https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf |
| Guía para la administración del riesgo y el diseño de controles en entidades públicas | 2011 | DAFP | https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba |
| Anexo 4 Lineamientos para la seguridad digital en entidades públicas | 2018 | DAFP | https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b?version=1.0&t=1533315341876 |
| Modelo Nacional de gestión de Riesgo de la Seguridad de la Información en Entidades Públicas | 2021 | DAFP | https://www.funcionpublica.gov.co/web/mipg/documentos/-/document_library/tfVWGgioFma4/view_file/40592207 |