Personería de Bogotá, D. C.

# INFORME

## GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
## VIGENCIA 2024

**Dirección de Tecnologías de la Información y las Comunicaciones – DTIC**

**Bogotá, Febrero de 2025**

# TABLA DE CONTENIDO

# LISTA DE TABLAS

# LISTA DE GRAFICOS

## IDENTIFICACIÓN DEL INFORME

| Fecha | Periodo del informe |
|---|---|
| Febrero de 2025 | Enero a diciembre de 2024 |

## 1. INTRODUCCIÓN

La Personería de Bogotá, D.C., en cumplimiento de sus funciones, implementa acciones y estrategias para garantizar la seguridad de la información como uno de sus activos más importantes para el cumplimiento de sus objetivos estratégicos. Para esto, se establecen acciones enmarcadas en la normatividad legal vigente como el Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital(…)",* el Modelo de Seguridad de Privacidad de la Información MSPI de MINTIC, la Resolución interna 250 de 2023 mediante la cual establece la adopción, implementación y sostenibilidad de los Sistemas de Gestión de la entidad, entre ellos el Sistema de Gestión de Seguridad de la Información SGSI, y la Resolución interna 242 de 2023 "Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información SGSI- bajo la NTC-ISO 27001", norma que establece los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información con un enfoque basado en la gestión de riesgos, que para el caso de la Personería de Bogotá, D.C., cuenta con una metodología descrita en la "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04" aplicable a todos los procesos de la entidad y la cual incluye la gestión de los riesgos de seguridad de la información alineada con la "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS" y el ANEXO TÉCNICO 4 "MODELO NACIONAL DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS" del Departamento Administrativo de la Función Pública DAFP.

La gestión de riesgos de seguridad de la información se realiza mediante la aplicación de la metodología de riesgos de la Personería de Bogotá, D.C., para lo cual los 16 procesos de la entidad han identificado y valorado los riesgos, evaluado los controles existentes y planeado las acciones de tratamiento correspondientes para prevenir la posible materialización de dichos riesgos.

El seguimiento de los riesgos de seguridad de la información se realiza de forma cuatrimestral de acuerdo a lo establecido en la guía para la administración del riesgo de la entidad, y se encuentra publicado en la ruta MIPG/Gestión de Riesgos de la intranet corporativa, el cual puede ser verificado en el link Intranet Personería de Bogotá D.C. - Gestión de Riesgos (personeriabogota.gov.co).

La Dirección de Tecnologías de la Información y las Comunicaciones, como responsable del Sistema de Gestión de Seguridad de la Información SGSI, y en cumplimiento de los requisitos de la NTC-ISO/IEC 27001:2022, realiza el seguimiento a la gestión realizada por los procesos respecto del análisis, evaluación y tratamiento de los riesgos de

seguridad de la información y presenta los resultados de la efectividad de los controles y las correspondientes recomendaciones de mejora.

## 2. ALCANCE

Este informe presenta el estado y los resultados de la gestión de riesgos de seguridad de la información realizada por los procesos de la Personería de Bogotá, D.C. durante la vigencia 2024, de acuerdo a lo establecido en la Guía para la Administración del Riesgo código 01-GU-04, y los requisitos de la NTC-ISO/IEC 27001:2022, la "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS" y el ANEXO TÉCNICO 4 "MODELO NACIONAL DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS" del Departamento Administrativo de la Función Pública DAFP.

## 3. OBJETIVO

Presentar los resultados de la análisis a la gestión de los riesgos de seguridad de la información de la Personería de Bogotá, D.C. durante la vigencia 2024, verificando la pertinencia y eficacia de los controles existentes y de las acciones de tratamientos programadas para los riesgos ubicados en una zona de riesgos residual "ALTA" o "EXTREMA", desde el punto de vista de seguridad de la información y tomando como referencia la GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO CÓDIGO 01-GU-04 de la Personería, los requisitos de la NTC-ISO/IEC 27001:2022, la "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS" y el ANEXO TÉCNICO 4 "MODELO NACIONAL DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS" del Departamento Administrativo de la Función Pública DAFP.

## 4. METODOLOGÍA

Para la realización del presente informe, se toma como insumo principal el documento con el mapa de riesgos institucional publicado en la página web y/o portal de intranet, y se solicitó información adicional a los diferentes procesos como responsables de la gestión de riesgos incluidos los de seguridad de la información:

- Solicitud información a los procesos sobre la materialización e identificación de nuevos de riesgos de seguridad de la información.
- Análisis de la información presentada por la Oficina de Control Interno, en los informes de seguimiento cuatrimestral al mapa de riesgos de gestión de la Personería.
- Análisis de la información correspondiente a los riesgos de seguridad de la información para cada uno de los procesos de la entidad, consolidados en el mapa de riesgos institucional.

## 5. ANÁLISIS DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

### 5.1. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La gestión de riesgos de seguridad de la información inicia con la identificación, clasificación y valoración de 458 activos de información que permite establecer cuáles son las fuentes de información que tienen valor para la entidad y que por su criticidad deber ser protegidos mediante una adecuada gestión del riesgo y la implementación de controles y planes de acción para mitigarlos.

| CRITICIDAD DE ACTIVOS | |
|---|---|
| CRITICO | 97 |
| MODERADO | 214 |
| BAJO | 147 |
| **TOTAL** | **458** |

Tabla 1. Total de activos de información por criticidad
Tomado de: Inventario de activos de información


Gráfico 1. Total de activos de información por criticidad
Tomado de: Inventario de activos de información


Gráfico 2. Total de activos de información por proceso
Tomado de: Inventario de activos de información

| # | PROCESO | CRITICO | MODERADO | BAJO | TOTAL ACTIVOS |
|---|---|---|---|---|---|
| 1 | Direccionamiento Estratégico | 0 | 25 | 11 | 36 |
| 2 | Gestión del Conocimiento e Innovación | 0 | 4 | 17 | 21 |
| 3 | Direccionamiento TIC | 39 | 22 | 10 | 71 |
| 4 | Comunicación Estratégica | 3 | 8 | 2 | 13 |
| 5 | Promoción y Defensa de Derechos | 10 | 49 | 41 | 100 |
| 6 | Prevención y Control a la Función Pública | 0 | 14 | 1 | 15 |
| 7 | Potestad Disciplinaria | 8 | 8 | 3 | 19 |
| 8 | Gestión del Talento Humano | 12 | 9 | 3 | 24 |
| 9 | Gestión Administrativa | 4 | 12 | 7 | 23 |
| 10 | Gestión Financiera | 1 | 39 | 31 | 71 |
| 11 | Gestión Contractual | 0 | 3 | 1 | 4 |
| 12 | Gestión Documental | 5 | 7 | 15 | 27 |
| 13 | Gestión Jurídica | 8 | 3 | 2 | 13 |
| 14 | Servicio al Usuario | 1 | 4 | 0 | 5 |
| 15 | Control Interno Disciplinario | 6 | 1 | 0 | 7 |
| 16 | Evaluación y Seguimiento | 0 | 6 | 3 | 9 |
| | **TOTAL** | **97** | **214** | **147** | **458** |

Tabla 2. Criticidad de los activos de información por proceso
Tomado de: Inventario de activos de información

Los procesos han realizado la identificación de sus activos de información y se encuentran actualizado con fecha al mes de septiembre de 2024, encontrando una cifra significativa de 97 activos de información con un valor "**CRÍTICO"** que deberían ser objeto de especial atención en la gestión de riesgos de seguridad de la información.

## 5.2. IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION

| RIESGOS IDENTIFICADOS | |
|---|---|
| **ZONA DE RIESGO RESIDUAL** | **CANTIDAD** |
| EXTREMO | 3 |
| ALTO | 5 |
| MODERADO | 7 |
| BAJO | 7 |
| **TOTAL** | **22** |

Tabla 3. Total de riesgos de seguridad de la información por zona residual
Tomado de: Mapa de riesgos institucional

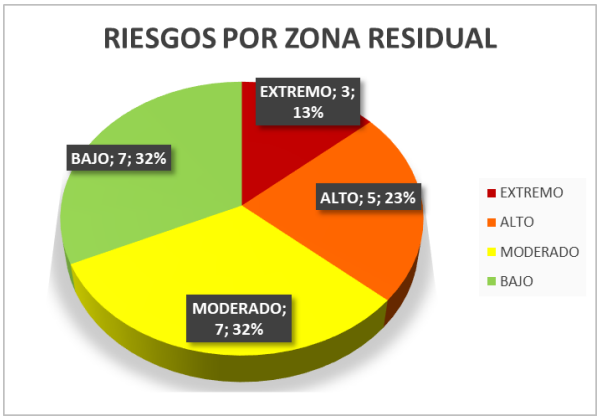


Gráfico 3. Porcentaje de riesgos de seguridad de la información por zona residual
Tomado de: Mapa de riesgos institucional


Gráfico 4. Comparación riesgos de seguridad Vs Activos de información
Tomado de: Mapa de riesgos institucional – Inventario de activos de información

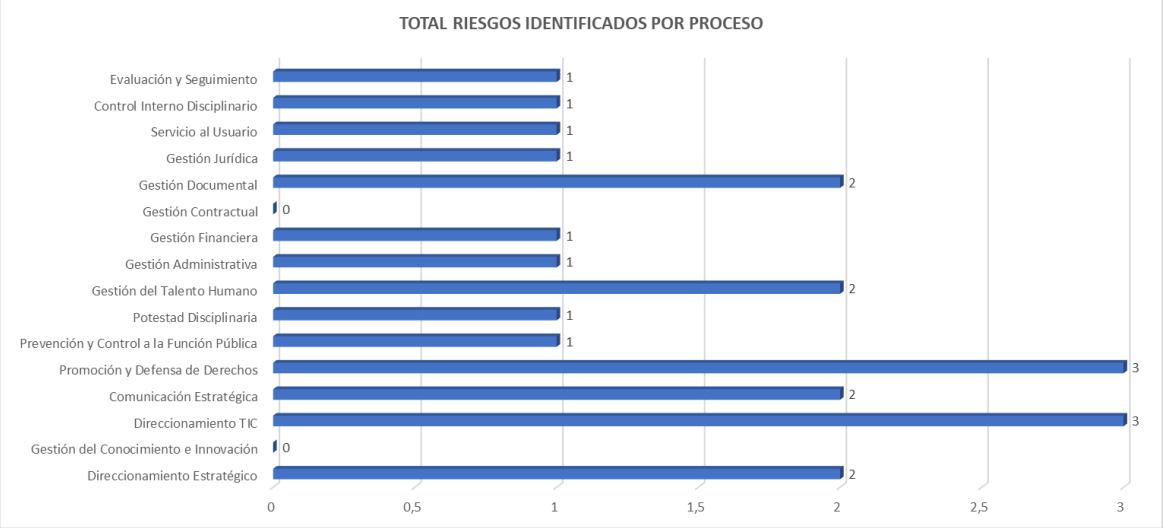


Gráfico 5. Total de riesgos de seguridad de la información por proceso
Tomado de: Mapa de riesgos institucional

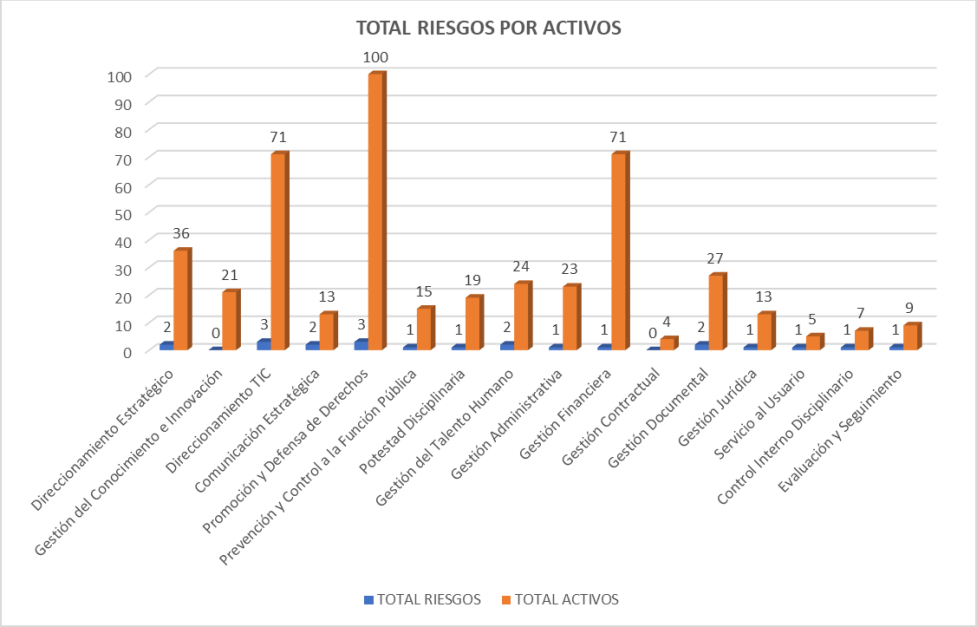


Gráfico 6. Comparación riesgos de seguridad Vs Activos de información por proceso
Tomado de: Mapa de riesgos institucional – Inventario de activos de información

Al analizar la cantidad de riesgos identificados y evaluados por los 16 procesos, se nota una tendencia de evaluación entre 1 y 3 riesgos de seguridad de la información como máximo, y solamente dos (2) procesos identificaron tres (3) riesgos, lo que representa un número de riesgos valorados relativamente bajo (22 en total) frente a la cantidad de activos de información identificados (458 en total) de los cuales noventa y siete (97) fueron valorados como críticos. Los procesos Gestión del conocimiento e innovación y Gestión contractual no identificaron riesgos de seguridad de la información.

## 5.3. VALORACIÓN Y EFECTIVIDAD DE LOS CONTROLES EXISTENTES PARA LOS RIESGOS DE SEGURIDAD DE LA INFORMACION

| | | | ZONA DE RIESGO INHERENTE | | | | | ZONA DE RIESGO RESIDUAL | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| # | PROCESO | TOTAL RIESGOS | EXTREMO | ALTO | MODERADO | BAJO | CONTROLES | EXTREMO | ALTO | MODERADO | BAJO |
| 1 | Direccionamiento Estratégico | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 |
| 2 | Gestión del Conocimiento e Innovación | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | Direccionamiento TIC | 3 | 0 | 3 | 0 | 0 | 6 | 0 | 3 | 0 | 0 |
| 4 | Comunicación Estratégica | 2 | 0 | 0 | 1 | 1 | 6 | 0 | 0 | 0 | 2 |
| 5 | Promoción y Defensa de Derechos | 3 | 3 | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 0 |
| 6 | Prevención y Control a la Función Pública | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 7 | Potestad Disciplinaria | 1 | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | 0 |
| 8 | Gestión del Talento Humano | 2 | 0 | 1 | 1 | 0 | 6 | 0 | 1 | 1 | 0 |
| 9 | Gestión Administrativa | 1 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | 1 | 0 |
| 10 | Gestión Financiera | 1 | 0 | 1 | 0 | 0 | 3 | 0 | 0 | 1 | 0 |
| 11 | Gestión Contractual | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | Gestión Documental | 2 | 0 | 1 | 1 | 0 | 6 | 0 | 0 | 0 | 2 |
| 13 | Gestión Jurídica | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 14 | Servicio al Usuario | 1 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | 1 | 0 |
| 15 | Control Interno Disciplinario | 1 | 0 | 1 | 0 | 0 | 2 | 0 | 1 | 0 | 0 |
| 16 | Evaluación y Seguimiento | 1 | 0 | 0 | 1 | 0 | 3 | 0 | 0 | 1 | 0 |
| | **TOTAL** | **22** | **3** | **8** | **10** | **1** | **45** | **3** | **5** | **7** | **7** |

Tabla 4. Valoración riesgos de seguridad de la información por proceso
Tomado de: Mapa de riesgos institucional

## IDENTIFICACION DE LOS RIESGOS POR IMPACTO INHERENTE

| | | IMPACTO | | | | | |
|---|---|---|---|---|---|---|---|
| PROBABILIDAD | Muy Alta 100% | 1 | | | | | Extremo |
| | Alta 80% | | | 2 | 2 | 3 | Alto |
| | Media 60% | 2 | 2 | 5 | 3 | | Moderado |
| | Baja 40% | 1 | 1 | | | | Bajo |
| | Muy Baja 20% | | | | | | |
| | | Leve 20% | Menor 40% | Moderado 60% | Mayor 80% | Catastrófico 100% | |

Tabla 5. Identificación de riesgos de seguridad de la información por impacto inherente
Tomado de: Mapa de riesgos institucional

## IDENTIFICACION DE LOS RIESGOS POR IMPACTO RESIDUAL

| PROBABILIDAD | IMPACTO | | | | | |
|---|---|---|---|---|---|---|
| Muy Alta 100% | | | | | | Extremo |
| Alta 80% | | | | | | Alto |
| Media 60% | | | | | | Moderado |
| Baja 40% | | | | | 3 | Bajo |
| Muy Baja 20% | 4 | 3 | 7 | 5 | | |
| | Leve 20% | Menor 40% | Moderado 60% | Mayor 80% | Catastrófico 100% | |

Tabla 6. Identificación de riesgos de seguridad de la información por impacto residual
Tomado de: Mapa de riesgos institucional

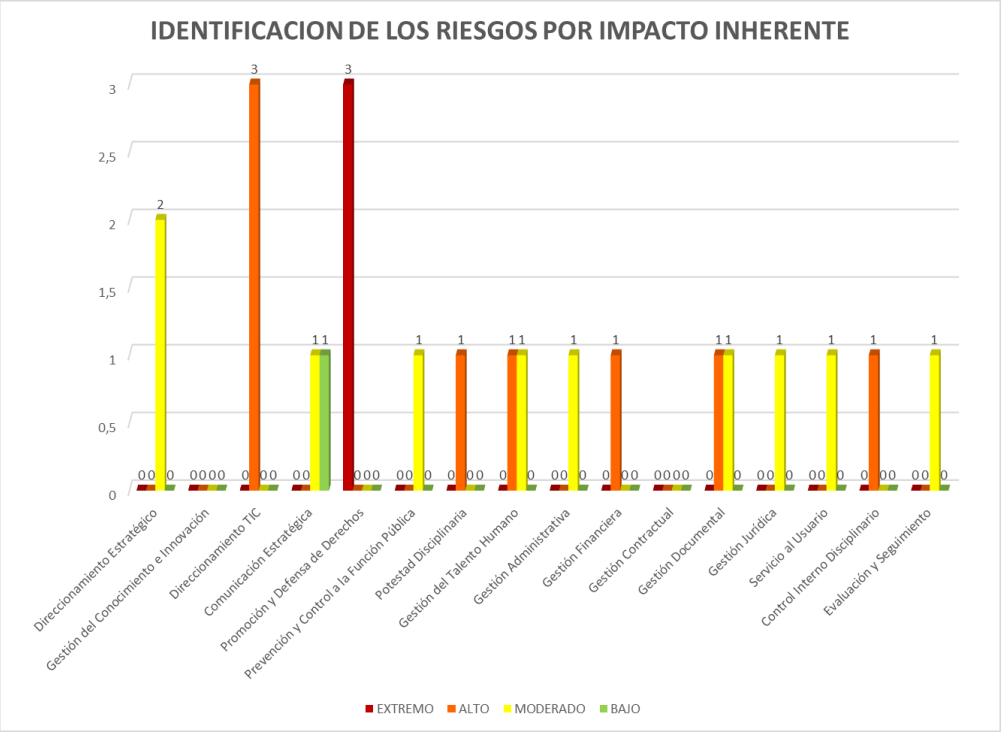


Gráfico 7. Identificación de riesgos de seguridad de la información por impacto inherente
Tomado de: Mapa de riesgos institucional

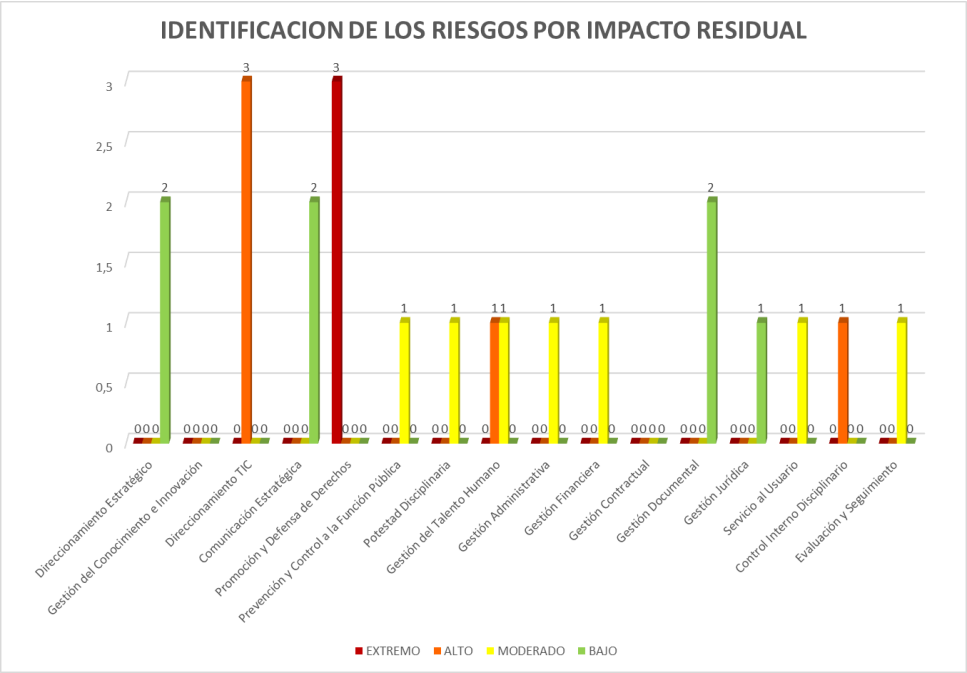


Gráfico 8. Identificación de riesgos de seguridad de la información por impacto residual
Tomado de: Mapa de riesgos institucional

En análisis realizado, se evidencia que una vez valorados los controles existentes de riesgos de seguridad de la información, para ocho (8) de los catorce (14) procesos que identificaron riesgos de seguridad de la información, (Direccionamiento TIC, Promoción y defensa de derechos, Prevención y control a la función pública, Gestión del Talento Humano, Gestión administrativa, Servicio al usuario, Control interno disciplinario y Evaluación y seguimiento), la valoración del riesgo residual se mantiene igual a la valoración del riesgo inherente, lo que puede indicar:

- Los controles de seguridad existentes son ineficaces o insuficientes, no tienen un impacto significativo en la reducción del riesgo o no son lo suficientemente robustos para mitigar el riesgo adecuadamente.

- Falta implementar o identificar medidas efectivas de mitigación o no se están ejecutando las acciones suficientes para reducir el riesgo de manera efectiva.

- Los controles implementados no son los adecuados para controlar efectivamente el riesgo de acuerdo con su naturaleza, o el riesgo inherente podría estar siendo mal evaluado.

## 5.4. PLANES DE ACCION PARA EL TRATAMIENTO DE RIESGOS

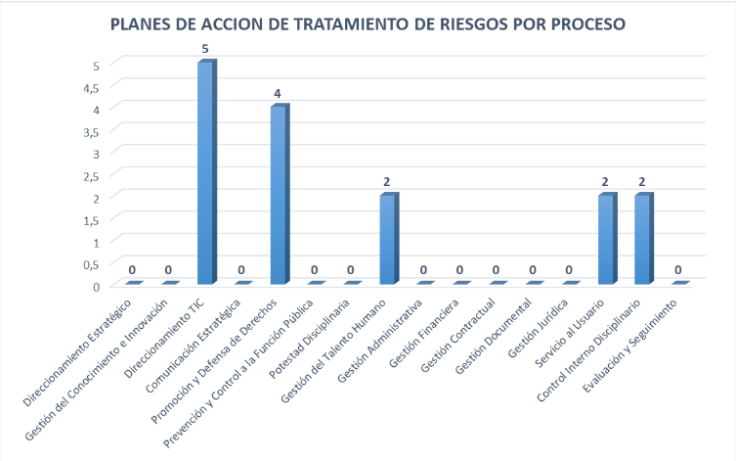


Gráfico 9. Planes de acción de riesgos por procesos
Tomado de: Mapa de riesgos institucional

Para la vigencia 2024, se encuentran identificados un total de 22 riesgos de seguridad de la información los cuales cuentan con 24 controles existentes y 15 acciones de tratamiento de riesgos para 5 procesos que presentan riesgos en zona de impacto residual alto o extremo, a los cuales se les ha realizado el seguimiento cuatrimestral de acuerdo con lo establecido en la guía para la administración del riesgo de la entidad y que se puede consultar en el portal de la intranet institucional en el link Personería de Bogotá - Vigencia 2024 (personeriabogota.gov.co).

## 5.5. EFECTIVIDAD DE LOS CONTROLES Y PLANES DE ACCIÓN PARA EL TRATAMIENTO DE RIESGOS

Para determinar la efectividad de los controles, la Dirección de Tecnologías de la Información y las Comunicaciones, solicitó a los 16 procesos de la entidad, informar si durante la vigencia 2024 se materializaron riesgos de seguridad de la información y si se habían identificado nuevos riesgos de seguridad de la información, obteniendo los siguientes resultados:

| # | PROCESO | TOTAL RIESGOS | PLAN DE ACCIÓN | RIESGOS MATERIALIZADOS | ¿HA IDENTIFICADO NUEVOS RIESGOS? |
|---|---|---|---|---|---|
| 1 | Direccionamiento Estratégico | 2 | 0 | 0 | 0 |
| 2 | Gestión del Conocimiento e Innovación | 0 | 0 | 0 | 0 |
| 3 | Direccionamiento TIC | 3 | 6 | 0 | 0 |
| 4 | Comunicación Estratégica | 2 | 0 | 0 | 0 |
| 5 | Promoción y Defensa de Derechos | 3 | 4 | 0 | 0 |
| 6 | Prevención y Control a la Función Pública | 1 | 0 | 0 | 0 |
| 7 | Potestad Disciplinaria | 1 | 0 | 0 | 1 |
| 8 | Gestión del Talento Humano | 2 | 2 | 0 | 0 |
| 9 | Gestión Administrativa | 1 | 0 | No reporta | No reporta |

| # | PROCESO | TOTAL RIESGOS | PLAN DE ACCIÓN | RIESGOS MATERIALIZADOS | ¿HA IDENTIFICADO NUEVOS RIESGOS? |
|---|---|---|---|---|---|
| 10 | Gestión Financiera | 1 | 0 | 0 | 0 |
| 11 | Gestión Contractual | 0 | 0 | 0 | 0 |
| 12 | Gestión Documental | 2 | 0 | 0 | 0 |
| 13 | Gestión Jurídica | 1 | 0 | 0 | 1 |
| 14 | Servicio al Usuario | 1 | 2 | 0 | 0 |
| 15 | Control Interno Disciplinario | 1 | 2 | 0 | 0 |
| 16 | Evaluación y Seguimiento | 1 | 0 | 0 | 0 |
| | **TOTAL** | **22** | **15** | **0** | **2** |

Tabla 7. Reporte de riesgos materializados por proceso
Tomado de: Mapa de riesgos institucional


Gráfico 10. Efectividad de controles
Tomado de: Mapa de riesgos institucional

De acuerdo con el reporte recibido, 15 de los 16 procesos informan que no se han materializado riesgos de seguridad de la información, el proceso Gestión Administrativa no reportó la información solicitada. Tomando como referencia los 15 procesos que suministraron información, de los 22 riesgos identificados se cuenta con 24 controles existentes y 15 acciones para tratamiento del riesgo residual, presentando una eficacia del 100% al no haberse materializado ningún riesgo de seguridad de la información; de igual manera, los procesos 7. Potestad Disciplinaria y 13. Gestión Jurídica manifiestan haber identificado nuevos riesgos de seguridad de la información los cuales deberían incluirse en el mapa de riesgos institucional para su correspondiente evaluación y tratamiento.

## 6. ANALISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN POR PROCESO

De acuerdo a la información recopilad del mapa de riesgos institucional, el siguiente es el análisis realizado a cada uno de los riesgos de seguridad de la información evaluados por los 16 procesos de la Personería de Bogotá, D.C.

## 01. Direccionamiento estratégico

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 2. Posibilidad de afectación y reputacional por pérdida de la Integridad y disponibilidad de la Información digital, debido a los ataques en los sistemas de información, fallas tecnológicas en infraestructura no administrada por la Entidad. | 1.El profesional de la Dirección de planeación realiza un Backup de los documentos creados, actualizados e eliminados en el aplicativo del Sistema de gestión de la calidad en una carpeta compartida de la Dirección de Planeación (Ubicada en el servidor Planeacion\\172.28.4.36)<br><br>2. El profesional de la Dirección de Planeación realiza un Backup de los informes y documentos recibidos en la Dirección de Planeación en el OneDrive y en la carpeta compartida de la Dirección de Planeación (ubicada en el servidor Planeación//172.28.4.36). | BAJO | N/A | Se observa la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 2 | 3. Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico | 1. El gestor documental administra el archivo de gestión del proceso en procura de su organización y en cumplimiento de lo dispuesto en el Manual de Gestión Documental y directrices existentes al respecto en la Entidad | BAJO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 02. Gestión del conocimiento e innovación

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | No identificado | No identificado | N/A | N/A | El proceso no identificó riesgos de seguridad de la información. Para las futuras vigencias, se recomienda incluir en la gestión de los riesgos del proceso, los riesgos de seguridad de la información teniendo en cuenta sus |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| | | | | | principios, (Integridad, disponibilidad y/o confidencialidad) y la criticidad de sus activos de información. |

## 03. Direccionamiento TIC

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 4. Posibilidad de pérdida económica y reputacional por ataques cibernéticos que afecten la red de datos, sistemas de información, bases de datos y/o configuración de algún activo de información. | 1. El equipo Monitoreo CRI (Centro de Reacción Inmediata) realiza monitoreo de aplicaciones<br><br>2. Los equipos de Gestión de Capacidades e Infraestructura adquisición e implementación Centro de Operaciones de Seguridad - SOC alineado al Plan Estratégico de Tecnologías yel Plan Anual de Adquisiciones<br><br>3. El equipo de Gestión de Seguridad realiza monitoreo y seguimiento eventos e incidentes de seguridad Conforme al procedimiento de gestión de incidentes de seguridad de la información | ALTO | 1. Reporte herramienta de monitoreo. (33%)<br><br>2. Contrato de adquisición y soporte de la implementación del SOC. 33%)<br><br>3. Seguimiento a eventos e incidentes de Seguridad de la Información identificado. (33%) | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 2 | 5. Posibilidad de pérdida económica y reputacional por vulnerabilidades resultado de la obsolescencia en el hardware y/o software que afecten la disponibilidad, integridad y confidencialidad de la información. | 1.El equipo de Gobierno y Estrategia de TI, Gestión de Infraestructura y Aplicaciones construye el documento de renovación de tecnologías con ALTO el inventario del hardware y software del parque computacional | ALTO | 1. Documento de renovación de tecnologías (100%) | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 3 | 6.Posibilidad de pérdida económica y reputacional por perdida o inaccesibilidad a la información de la entidad, que afecte la continuidad del negocio | 1. El equipo Monitoreo CRI (Centro de Reacción Inmediata) realiza monitoreo a las bases de datos.<br><br>2.El equipo Gestión de Infraestructura realiza las copias de respaldo de los sistemas de información ubicados en la nube Oracle y Datacenter físico y virtual | ALTO | 1. Reporte herramienta de monitoreo. (50%)<br><br>2. Reporte copias de respaldo. (50%) | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 04. Comunicación estratégica

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de pérdida reputacional por daño o pérdida de los documentos críticos del proceso en medio físico y/o digital. | 1. Cada uno de los funcionarios o contratistas guarda y respalda los insumos y productos realizados Proporcionar la información a una carpeta compartida para el respaldo de la OAC.<br><br>2. El referente de archivo solicita y organiza los documentos controlados y los insumos o productos que se deban archivar Según la relevancia y validez temporal de la información<br><br>3. La jefe OAC solicita una copia de los insumos y productos realizados tanto a contratistas como a funcionarios realiza un Backup organizado con la información para evitar pérdida ante la rotación del personal | BAJO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 2 | 4. Posibilidad de afectación económica y reputacional por divulgación no autorizada de la información reservada o sujeta a tratamiento de datos personales. | 1. Ejes de periodismo y audiovisuales hace el diligenciamiento y firman los formatos de uso de imagen y datos personales o guardan la evidencia en video de la autorización por parte de la persona involucrada.<br><br>2. El referente de archivo recopila y guarda en archivo los formatos diligenciados y firmados con las autorizaciones pertinentes. De ser necesario guardar un respaldo digital.<br><br>3. La jefe OAC Solicita a los funcionarios y contratistas el uso de los formatos de autorización de datos o imagen | BAJO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 05. Promoción y defensa de derechos

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 6. Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico | 1. Los referentes de gestión de cada dependencia realizan de manera anual el inventario de activos de la información que producen para tomar las acciones pertinentes que eviten la pérdida o daño de la documentación física. | EXTREMO | 1. Designar personal de planta autorizado por dependencia para la custodia de los documentos físicos (base de datos con nombres, cedula, cargo, etc.). (Una sola actividad en el año equivalente al 50%).<br><br>2. Asignar espacio seguro con acceso restringido a personal no autorizado (En el caso del edificio CAC, el archivo se encuentra en estantería en los pasillos donde transitan los usuarios, por tanto, se deben asegurar los estantes con llaves en custodia del personal autorizado). (Una sola actividad en el año equivalente al 50%)." | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 2 | 7. Posibilidad de pérdida o daño de los documentos o datos críticos del proceso en medio digital – electrónico | 1. Los referentes de gestión de cada dependencia realizan de manera anual el inventario de activos de la información que producen para tomar las acciones pertinentes que eviten la pérdida o daño de la documentación digital. | EXTREMO | 1. Almacenar los documentos críticos en medio digital en la estructura de carpetas y subcarpetas definida para cada Personería Delegada o Local. (Una sola actividad en el año equivalente al 100%). | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 3 | 8. Posibilidad de divulgar información con datos críticos o sensibles de la Entidad y usuarios. | 1. Los referentes de gestión de cada dependencia realizan de manera anual el inventario de activos de la información que producen para tomar las acciones pertinentes que eviten la divulgación de información reservada o clasificada | EXTREMO | 1. Sensibilizar a los funcionarios y contratistas del proceso de Promoción y Defensa de Derechos en el manejo adecuado de la información de la Entidad, normatividad vigente, tipos de datos, entre otros temas. (Una sola actividad en el año equivalente al 100%). | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 06. Prevención y control a la función pública

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 2. Posibilidad de afectación reputacional por no contar con los soportes de las actividades realizadas en el proceso debido a la pérdida o daño de los documentos críticos. | 1. El equipo de trabajo del proceso de prevención y control a la función pública Guardar en el servidor de la Entidad los soportes de las diferentes actividades realizadas. | MODERADO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 07. Potestad disciplinaria

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de afectación reputacional por la pérdida de documentación, que hacen parte de la unidad probatoria o CD,DVD y/o USB sin información, generando mora en el impulso procesal debido a la falta de cuidado y control sobre las piezas documentales que conforman el expediente disciplinario | 1. Secretaria Común - abogados PQ y comunicaciones y notificaciones verificar el contenido de cada uno de los expedientes junto con su correcta hoja de control de la foliación, cada vez que el expediente cambie de custodio registrar en documento o sistema los folios y contenido recibido<br><br>2. Abogados y Secretarios de despacho verificar el contenido de cada uno de los expedientes junto con su correcta hoja de control de la foliación, cada vez que el expediente cambie de custodio registrar en documento o sistema los folios y contenido recibido. | MODERADO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 08. Gestión del talento humano

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 7. Posibilidad de afectación Económica (o presupuestal) y Reputacional por pérdida o daño de la información física del proceso debido a desastres naturales o industriales, robo, extravío, actos de vandalismo o terrorismo y daño del papel físico. | 1. El equipo de funcionarios(as) de las Subdirecciones de Gestión y Desarrollo del Talento Humano, garantizan el acceso restringido a personal no autorizado al espacio seguro destinado para resguardar los documentos físicos de la historia laboral y archivo de seguimiento a enfermedades laborales, permitiendo solamente el acceso al personal responsable para su custodia.<br><br>2. El equipo de funcionarios(as) de las Subdirecciones de Gestión y Desarrollo del Talento Humano, controla el ingreso de todo documento que deba ser incorporado a la historia laboralo al archivo de seguimiento a enfermedades laborales, mediante el diligenciamiento y registro del formato Hoja de Control.<br><br>3. El(la) funcionario(a) designado(a) por el Subdirector(a) de Gestión o de desarrollo del Talento Humano respectivamente, deberá realizar el control de las consultas o préstamos de los expedientes o documentos de historias laborales o archivo de seguimiento a enfermedades laborales, realizando el registro correspondiente en el formato de control de consulta y/o préstamo de documentos de archivo. | MODERADO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 2 | 8. Posibilidad de afectación Económica (o presupuestal) y Reputacional por ciberataques por un externo o interno para divulgar y utilizar información con datos personales de los(as) funcionarios(as) debido a que se exponen documentos públicamente con información personal y confidencial de los(as) funcionarios(as) | 1. El equipo de funcionarios(as) de las Subdirecciones de Gestión y Desarrollo del Talento Humano, garantizan el acceso restringido a personal no autorizado al espacio seguro destinado para resguardar los documentos físicos de la historia laboral y archivo de seguimiento a enfermedades laborales, permitiendo solamente el acceso al personal responsable para su custodia.<br><br>2. El equipo de funcionarios(as) de la Dirección de Talento Humano y Subdirección de Desarrollo del Talento Humano, al momento de la vinculación de un nuevo(a) funcionario, entregan el formato Compromiso de Confidencialidad y No Divulgación de la Información como parte de los documentos para posesión, o cuando se requiera acceso a los documentos de archivo de seguimiento a Medicina Laboral, solicitándole que sea leído el documento y sea debidamente firmado.<br><br>3. El(la) funcionario(a) designado(a) por el Subdirector(a) de Gestión o de desarrollo del Talento Humano respectivamente, deberá realizar el control de las consultas o préstamos de los expedientes o documentos de historias laborales o archivo de seguimiento a enfermedades laborales, realizando el registro correspondiente en el formato de control de consulta y/o préstamo de documentos de archivo. | ALTO | 1. Solicitar apoyo de la Dirección DTIC y/o del responsable de la custodia de la información vulnerada, con el fin de que se corrija o eliminen las razones que originaron la vulnerabilidad de la información. (50%)<br><br>2. Se debe interponer la denuncia penal ante la Fiscalía General de la Nación y/o remitir el caso a la Oficina de Control Interno Disciplinario para que se adelante la investigación correspondiente. (50%). | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 09. Gestión administrativa

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de afectación económica por pérdida o daño de la información física del proceso, debido a los desastres naturales o industriales. | 1. La Subdirección de Gestión Documental y Recursos Físico realiza un autocontrol trimestral de la carpeta compartida verificando que los documentos que se producen en la Subdirección con ocasión del proceso de Gestión Administrativa a fin de garantizar que se salvaguarde la información de los servicios prestados.<br><br>2. La Subdirección de Gestión Documental y Recursos Físicos realiza una transferencia de documentos del archivo de gestión al archivo central. | MODERADO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 10. Gestión financiera

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de afectación reputacional por sanción de organismo de control o la oficina de control interno debido a pérdida, daño, manipulación indebida de los documentos críticos del proceso, pérdida de conocimiento de la información contenida en medios físico y digital - electrónico, hardware averiado y/o software desactualizado. | 1. Profesional de la Subdirección de Gestión Financiera restringe el acceso al archivo de gestión, salvaguardar los documentos digital - electrónicos en la carpeta de red institucional.<br><br>2. Subdirector de Gestión Financiera genera lineamientos para la entrega de la información a cargo de los funcionarios, verificando que esta se encuentre consignada en la carpeta compartida del área.<br><br>3. Subdirector de Gestión Financiera genera revisión y reporte cuatrimestral por parte de cada funcionario sobre el estado del Hardware y del Software asignado para su labor. | MODERADO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 11. Gestión contractual

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | No identificado | No identificado | N/A | N/A | El proceso no identificó riesgos de seguridad de la información. Para las futuras vigencias, se recomienda incluir en la gestión de los riesgos del proceso, los riesgos de seguridad de la información teniendo en cuenta sus principios, (Integridad, disponibilidad y/o confidencialidad) y la criticidad de sus activos de información. |

## 12. Gestión documental

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 1. Posibilidad de pérdida reputacional debido al deterioro, destrucción, extravío o pérdida de la documentación institucional en soporte físico en archivo central | 1. Contratista responsable de la custodia del archivo central Aplicación de instrumentos de control como inventarios documentales y controles de préstamos y consultas Formato de control de préstamos y consultas de documentos (12-FR-02). Registrar las consultas documentales para su control y conocimiento de los documentos consultados y las dependencias interesadas.<br><br>2. Servicio de vigilancia provisto por el contratista responsable de la custodia del archivo central de la Personería de Bogotá. Servicio de vigilancia privada con monitoreo por cámaras internas y perimetrales y de sensores de movimiento en archivo central, junto con la instalación de estantería para conservación de archivos y monitoreo de condiciones ambientales mediante equipos instalados en archivo central. Evitar acciones delictivas que afecten los documentos custodiados en el archivo central, así como el acceso a las áreas de depósito a personas no autorizadas.<br><br>3. Contratista responsable de la custodia del archivo central suministra el documento solicitado en préstamo mediante copia digitalizada del mismo, para evitar su retiro del lugar donde se conserva. Disminuir el retiro de documentos del archivo central, con ocasión de su consulta | BAJO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 2 | 3. Posibilidad de pérdida reputacional debido a la divulgación no autorizada de los documentos reservados o sujetos a tratamiento de datos personales bajo custodia del archivo central | 1. Servicio de vigilancia provisto por el contratista responsable de la custodia del archivo central de la Personería de Bogotá. Servicio de vigilancia privada con monitoreo mediante cámaras internas y perimetrales en archivo central y de sensores de movimiento evita acciones delictivas que afecten los documentos custodiados en el archivo central, así como el acceso a las áreas de depósito a personas no autorizadas.<br><br>2. Servicio de vigilancia provisto por el contratista responsable de la custodia del archivo central de la Personería de Bogotá. Restricción de acceso al archivo a personas no autorizadas. Evitar el acceso a las áreas de custodia del archivo central de personal que ponga en riesgo la documentación, así como evitar el retiro de documentos sin registro en los controles de préstamo y consulta.<br><br>3. Contratista responsable de la custodia del archivo central controla la consulta de documentos, mediante Formato de control, préstamo y consulta de documentos 12-FR-02. Registrar las consultas documentales para su control y conocimiento de los documentos consultados y las dependencias interesadas. | BAJO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 13. Gestión Jurídica

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de afectación reputacional por pérdida de información de documentos que sirven de insumo para el registro de sanciones disciplinarias, con datos críticos o sensibles de la Entidad y ciudadanos, debido a la inexistencia de Backup de las carpetas de registro | 1. Profesional de la OAJ realiza copia de carpetas de registro de sanciones en drive institucional (el Backup corresponde a un documento de apoyo que no se sujeta a las normas de gestión documental) | BAJO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 14. Servicio al usuario

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 2. Posibilidad de afectación económica por pérdida de información relevante para el proceso debido a la falta de herramientas o estrategias tecnológicas para el control seguro de documentos digitales. | 1. Profesional Especializado de la Secretaría General Realiza copia de seguridad de la información contenida en el repositorio office 365 del usuario nsamudio@personeriabogotá.gov.co a través de Microsoft office, correo nsamudio@personeriabogota.gov.co, OneDrive, carpeta PERSONERIA, subcarpeta EVIDENCIAS, subcarpeta MIPG.<br><br>2. Profesional Especializado de la Secretaría General Implementar prácticas solidas de gestión de acceso a consulta de la información a través de Microsoft office, correo nsamudio@personeriabogota.gov.co, OneDrive, carpeta PERSONERIA, subcarpeta EVIDENCIAS, subcarpeta MIPG. | MODERADO | 1. Realizar copia de seguridad de los documentos críticos en la carpeta compartida de servidor de la entidad o en OneDrive del proceso servicio al usuario.<br><br>2. Conceder accesos a los funcionarios (as) y contratistas responsables del proceso Servicio al Usuario de la Secretaría General, a través de SharePoint de OneDrive del repositorio de office 365. | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 15. Control disciplinario interno

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de pérdida de integridad de la información y/o documentación contenida en los expedientes disciplinarios y sus anexos físicos o digitales. | 1. Todos(as) los(as) funcionarios(as) de la dependencia participan en acciones de sensibilización en gestión documental y mejores prácticas en Seguridad de la Información<br><br>2. Todos(as) los(as) funcionarios(as) de la dependencia controlan el acceso de personal externo a las instalaciones de la Oficina de Control Interno Disciplinario | ALTO | 1. Efectuar un control de los expedientes mediante el inventario documental actualizado. 50%<br><br>2. Controlar el flujo de expedientes para consulta y digitalización. 50% | Se observa la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 16. Evaluación y seguimiento

| # | Descripción del riesgo | Controles existentes | Zona de riesgo residual | Acciones de tratamiento | Observaciones DTIC |
|---|---|---|---|---|---|
| 1 | 3. Posibilidad de afectación reputacional debido a la pérdida o daño de la información documentada del Proceso registrada en medio físico y digital. | 1. Jefe Oficina de Control Interno y Equipo OCI. Designar un responsable de la custodia, manejo y control de los documentos físicos y digitales del Proceso, manteniendo acceso restringido a personal no autorizado.<br><br>2. Digitalizar la información del proceso y almacenarla en la Carpeta Compartida de la OCI con acceso restringido a personal no autorizado.<br><br>3. Mantener actualizado el formato único de inventario documental FUID Almacenar la información en medios físicos y digitales | MODERADO | N/A | Se recomienda redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).<br><br>Para determinar la causa raíz (¿Por qué?) se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo. (Consultar listado de vulnerabilidades y amenazas del ANEXO 4-DAFP).<br><br>Los controles de los riesgos de seguridad de la información se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. |

## 7. RECOMENDACIONES GENERALES

Reportar oportunamente la información solicitada por el proceso Direccionamiento TIC, respecto de la materialización de riesgos de seguridad de la información e identificación de nuevos riesgos, brindando la información suficiente y oportuna con el fin de facilitar el análisis de la efectividad de controles.

Incluir para futuras vigencias, los nuevos riesgos de seguridad de la información identificados por los procesos de la entidad.

Dado el alcance del SGSI, los activos de información identificados, las amenazas y vulnerabilidades existentes y los potenciales impactos negativos que representaría la pérdida de confidencialidad, disponibilidad o integridad de la información para la entidad, se recomienda que para la vigencia 2025 se realice la gestión de los riesgos de seguridad de la información para la totalidad de los procesos de la Personería de Bogotá, D.C.

Redactar la identificación del riesgo respecto a los principios de seguridad de la información (Integridad, disponibilidad y/o confidencialidad).

Para determinar la causa raíz (¿Por qué?) de los riesgos de seguridad de la información, se recomienda analizar y tomar como referencia las amenazas y vulnerabilidades que pueden hacer daño a los activos de información y producir la materialización del riesgo, de acuerdo al listado de vulnerabilidades y amenazas del ANEXO TÉCNICO 4 “MODELO NACIONAL DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS” del DAFP.

Los controles de los riesgos de seguridad de la información y las acciones de tratamiento se deberían identificar teniendo en cuenta los controles del ANEXO A de la NTC-ISO/IEC 27001:2022, como insumo base para mitigar los riesgos, sin embargo, el proceso podrá implementar nuevos controles que no estén incluidos en el ANEXO A, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

**EDGAR ALFONSO RAMÍREZ HERNÁNDEZ**
Director de Tecnologías de la Información y las Comunicaciones

Elaboró: Darley Ocampo García- Dirección de Tecnologías de la Información y las Comunicaciones DTIC
Revisó: Edgar Alfonso Ramírez Hernández- Dirección de Tecnologías de la Información y las Comunicaciones DTIC
Aprobó: Edgar Alfonso Ramírez Hernández- Dirección de Tecnologías de la Información y las Comunicaciones DTIC