GUARDIANES de tus DERECHOS
Personería de Bogotá, D. C.

INFORME

GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección de Tecnologías de la Información y las Comunicaciones – DTIC

Bogotá, Diciembre de 2023

GUARDIANES de tus DERECHOS
Personería de Bogotá, D. C.

TABLA DE CONTENIDO

1. INTRODUCCION

La Personería de Bogotá, D.C., como Entidad de carácter gubernamental enfocada al servicio al ciudadano está intercambiando de forma continua información con entidades públicas y privadas, así como con la ciudadanía en general.

Tomando como referencia, la norma ISO 31000:2018 y el Modelo de Seguridad y Privacidad de la Información – MSPI, se ha establecido la Gestión de Riesgos asociados a la información, se han identificado, analizado y valorado los riesgos y mediante un tratamiento se han establecido controles eficaces para proteger los activos de información, y de TI, de la entidad.

De igual manera el Modelo de Seguridad y Privacidad de la Información – MSPI, de la Política de Gobierno Digital de MINTIC, establece metas, resultados y entregables para las fases de Planificación e Implementación del SGSI.

En este informe se presenta el análisis de los riesgos con vigencia 2023 los cuales fueron identificados durante el año 2022 y su respectiva valoración y el plan de acción para la mitigación de los mismos.

2. OBJETIVO

Documentar el plan estratégico para la mitigación de riesgos basado en la generación de un plan documentado que contenga las acciones a tomar, teniendo en cuenta los resultados y conceptos consolidados en la matriz de riesgos institucional. De igual forma este documento pretende informar de manera clara el estado actual de la entidad frente a los riesgos de seguridad de la información y orientar las acciones adecuadas para la mitigación de los mismos basados en la priorización de actividades para alcanzar los objetivos esperados frente a la planeación estratégica.

3. ALCANCE

Administración y gestión de riesgos de seguridad de la información a nivel de los procesos en la Entidad a partir del Modelo de Seguridad y Privacidad de la Información emitido por MINTIC en la Política de Gobierno Digital y la norma ISO/IEC 27001 vigente aplicable.

4. RESPONSABLES

Dirección de Tecnologías de la Información y las Comunicaciones – DTIC

El Plan de Tratamiento de Riesgos de Seguridad de la Información es responsabilidad de la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, quien dicta lineamientos, metodologías y procedimientos del caso para seguimiento, implementación de controles y acciones para mitigar los riesgos de Seguridad de la Información.

La dirección de TICS es la responsable de implementar el plan de comunicación, sensibilización y capacitación para concientizar a los(as) funcionarios(as) y contratistas y proveedores en el tratamiento de los riesgos de seguridad de la información en la Personería de Bogotá D.C., así como de apoyar los procesos en gestión de riesgos de seguridad de información.

Líderes de los Procesos de la Personería de Bogotá D.C.

Son responsables de identificar los riesgos; establecer las acciones y/o controles para mitigarlos; aprobar los planes de tratamiento de los riesgos identificados; generar los informes de gestión y ejecución; realizar las actualizaciones periódicas de los riesgos de seguridad de la información en sus mapas de riesgos de procesos; y reportar de forma oportuna a la Dirección de Planeación y a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC.

5. DEFINICIONES

- **Activo:** Cualquier elemento que tenga valor para la organización.

- **Análisis del riesgo:** Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.

- **Causa:** Elemento específico que origina el evento.

- **Contexto externo**: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).

- **Controles**: Procesos, políticas y/o actividades que pueden modificar el riesgo.

- **Criterios de riesgos**: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

- **Evaluación del Riesgo**: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

- **Evento:** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.

- **Riesgo:** 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).

- **SGSI:** Sistema de Gestión de Seguridad de la Información.

6. DESARROLLO DEL DOCUMENTO

En este documento se hace una descripción general de la clasificación de los riesgos, para posteriormente hacer un análisis más detallado de los riesgos de cada proceso, donde se enfatizó en la construcción de un mapa de calor que tuvo en cuenta la probabilidad y el impacto, las cuales son dos variables que se consideran de alta importancia para la clasificación y priorización que se deben dar a los controles de los riesgos.

Clasificación de los Riesgos de la matriz general

En los procesos se han identificado 3 clases de Riesgo

- Riesgos Estratégicos
- Riesgos de Gestión
- Riesgos de Seguridad de Información

En este documento se describen los ítems de la matriz de riesgos, específicamente los que tienen que ver con seguridad de la información.

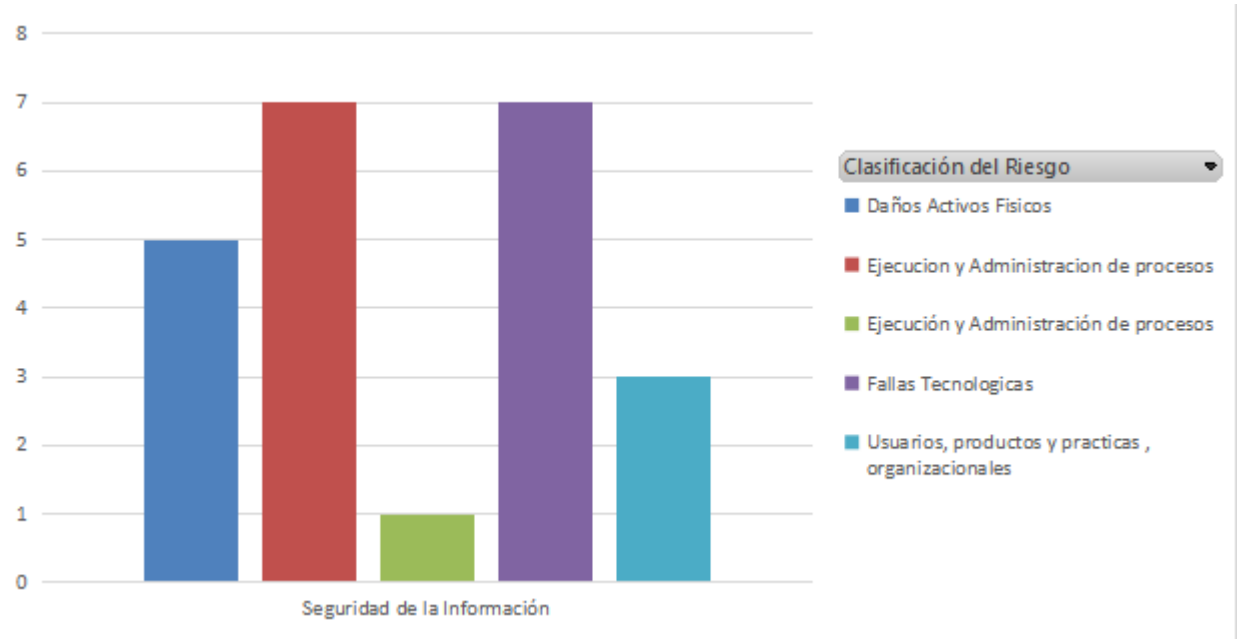
6.1. RIESGOS IDENTIFICADOS EN LOS PROCESOS

En este apartado se presentan los riesgos de seguridad de la información clasificados por tipo y se hace una descripción general de los datos conforme a las cantidades y a su

peso porcentual respecto al total general, teniendo en cuenta la probabilidad inherente de cada uno.

6.1.1. CLASIFICACIÓN DE LOS RIESGOS

En la Gráfica 1 se presenta la cantidad de riesgos de seguridad de la información respecto a la clasificación del riesgo



Gráfica 1

El primer hallazgo que se pretende analizar es la existencia de una distribución casi uniforme respecto a la cantidad de riesgos y su clasificación. La mayoría de ellos se encuentran en los procesos de ejecución y fallas tecnológicas, para su mitigación se debe plantear políticas que establezcan procesos que mitiguen riesgos de fuga de la información o su exposición a agentes potencialmente peligrosos. Las otras clasificaciones que presentan cinco y tres riesgos respectivamente son riesgos ocasionados por daños en activos físicos y a causa de prácticas organizacionales y de usuario. Finalmente se encontró una gran disminución relacionado a los riesgos clasificados como ejecución y administración de procesos. Este es un ítem muy importante ya que el año pasado este era la clasificación que presentaba mayor cantidad de riesgos, lo que muestra que los planes de ejecución para la mitigación y o anulación de riesgos ha tenido un efecto positivo.

Descripción de los Riesgos

De acuerdo con la descripción, se puede observar el Nivel de Riesgo respecto a la probabilidad Inherente de que ocurra. En este sentido, podemos observar en la Gráfica 2 que se ha reducido considerablemente la cantidad de riesgos con probabilidades altas y muy altas de ocurrencia. La mayoría de los riesgos tienen una probabilidad inherente media.

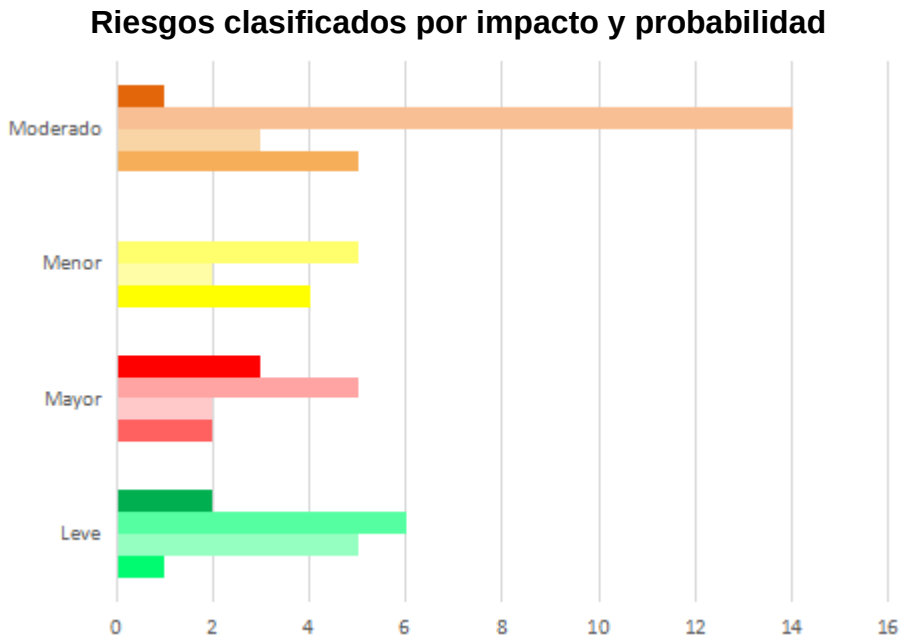
Gráfica 2

Riesgos clasificados por probabilidad e impacto:

Para este análisis de los riesgos se han clasificado el impacto y la probabilidad de que el riesgo se materialice, para el diseño de estas gráficas se ha asignado al impacto una escala de colores, siendo el verde el más leve, el amarillo menor, naranja para moderado y el rojo para los de mayor impacto, por otra parte, la probabilidad de que ocurra se ha representado con la intensidad de cada uno de los colores. De este modo el mapa de calor de riesgos queda definido como se muestra en la siguiente tabla para todos los riesgos de la matriz institucional.

		Probabilidad Inherente			
		Muy alta	Alta	Media	Baja
Impacto Inherente	Mayor	3	2	5	2
	Moderado	1	5	14	3
	Menor	0	4	5	2
	Leve	2	1	6	5

Tabla 1: Mapa de calor de los riesgos



Gráfica 3

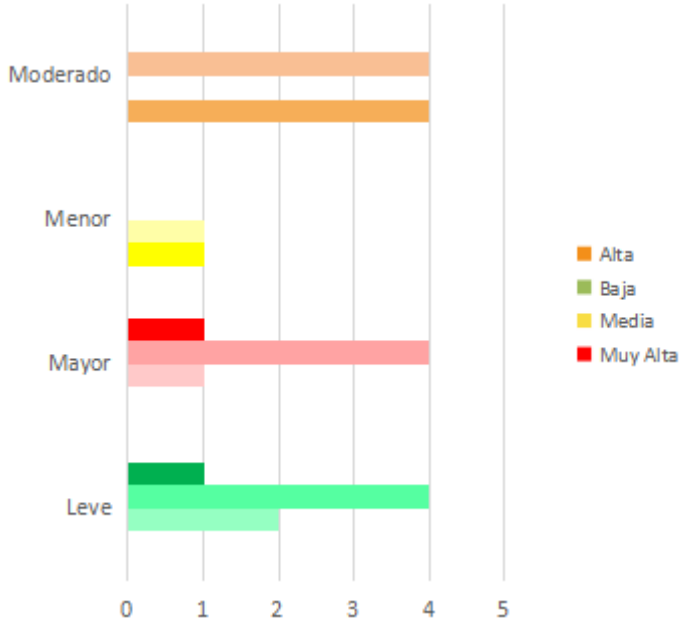
De la Gráfica 3 podemos destacar que tenemos 3 riesgos clasificados en la zona más delicada (Impacto alto con alta probabilidad de que ocurra), estos en particular deben ser tratados con especial atención.

En cuanto a los riesgos de seguridad de la información, se tienen identificados 23 riesgos, los cuales se distribuyen como se muestran en la siguiente tabla:

		Probabilidad Inherente			
		Muy alta	Alta	Media	Baja
Impacto Inherente	Mayor	1	0	4	1
	Moderado	0	4	4	0
	Menor	0	1	0	1
	Leve	1	4	0	2

Tabla 2: Mapa de calor de riesgos de seguridad de la información

Riesgos de seguridad de la información clasificados por impacto y probabilidad



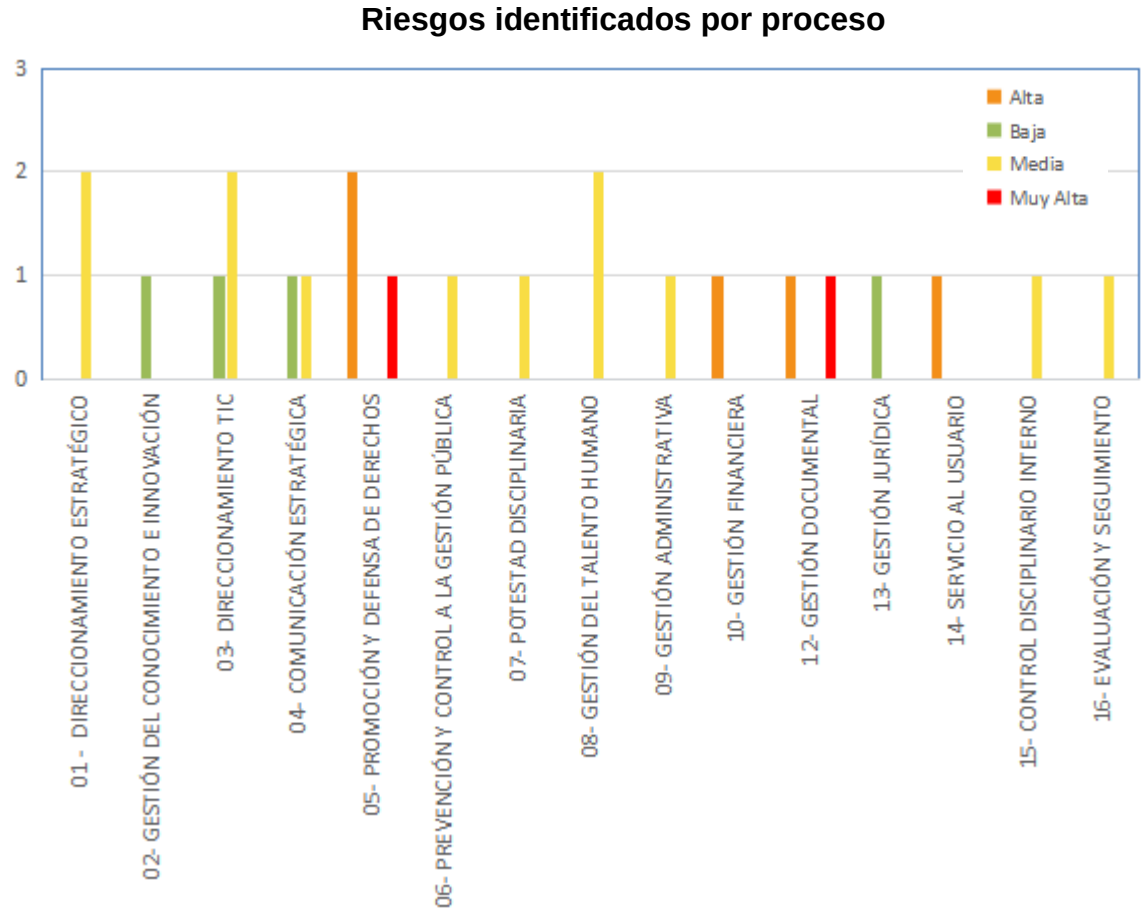
Gráfica 4

En la Gráfica 4 vemos que tan solo hay 1 riesgo clasificado en la zona de mayor riesgo (Impacto alto con alta probabilidad de que ocurra), se debe hacer énfasis en los seguimientos a las acciones de mitigación o tratamiento.

6.2. RIESGOS IDENTIFICADOS POR PROCESOS

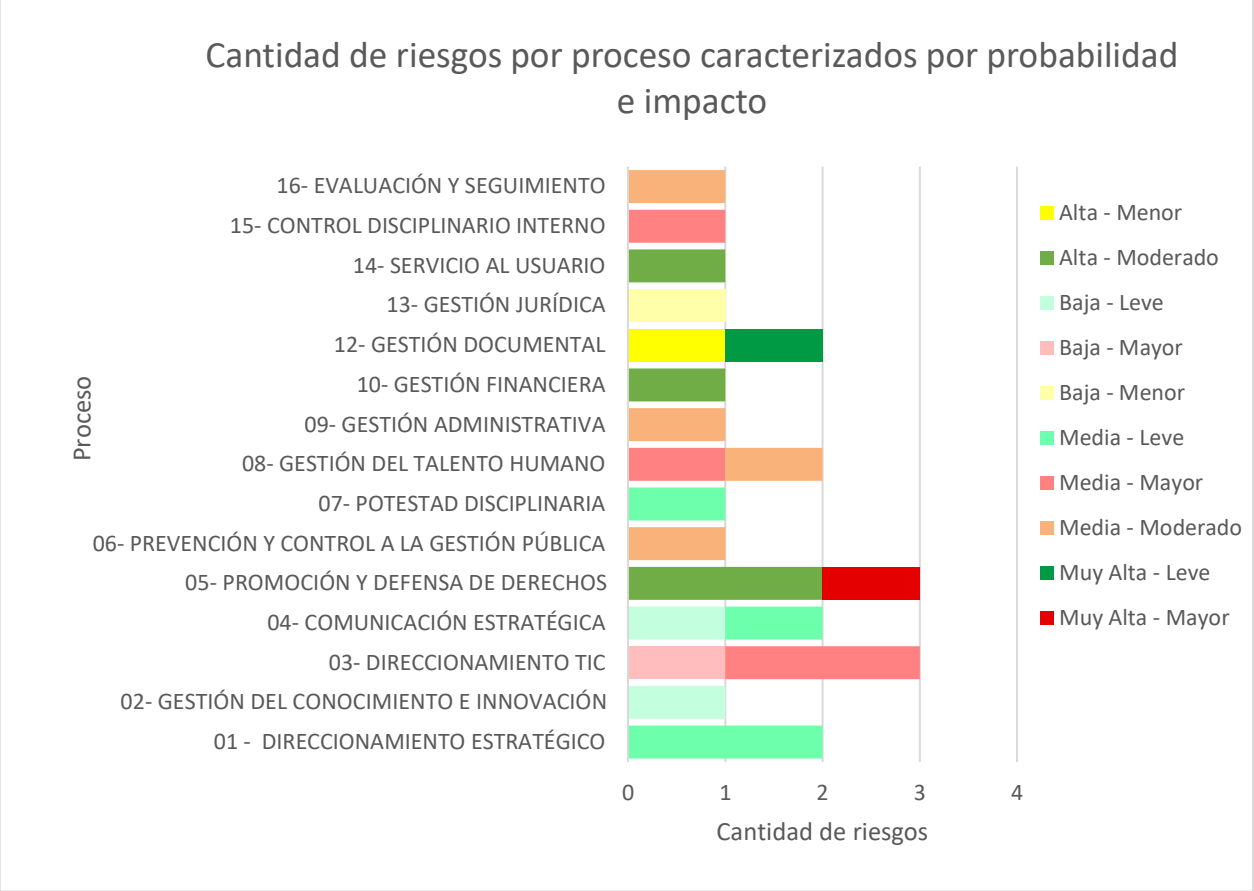
En esta sección del documento abordamos los riesgos desagregados por los diferentes procesos de la entidad, en este sentido se busca enfatizar en aquellos riesgos de mayor impacto y de alta probabilidad de que ocurran, con el objetivo de definir acciones concretas que ayuden a mitigar la materialización de dichos riesgos.

En la Gráfica 5 se representa para cada uno de los procesos el número de riesgos de seguridad de la información clasificados por la probabilidad inherente de que se materialicen.



Gráfica 5

Como podemos observar la Gráfica 5 muestra una distribución de la cantidad de riesgos detectados por cada uno de los procesos, caracterizando la probabilidad inherente y el impacto que tendrían.



Gráfica 6

Por otra parte, la Gráfica 6 muestra la distribución de riesgos de cada proceso teniendo en cuenta el mapa de calor descrito en la sección anterior, construido a partir del impacto y de la probabilidad inherente.

En la siguiente tabla se presentan la cantidad de riesgos de seguridad de la información por probabilidad inherente para cada proceso:

Proceso	Alta	Baja	Media	Muy Alta	Total
01 - DIRECCIONAMIENTO ESTRATÉGICO			2		**2**
02- GESTIÓN DEL CONOCIMIENTO E INNOVACIÓN		1			**1**
03- DIRECCIONAMIENTO TIC		1	2		**3**
04- COMUNICACIÓN ESTRATÉGICA		1	1		**2**
05- PROMOCIÓN Y DEFENSA DE DERECHOS	2			1	**3**
06- PREVENCIÓN Y CONTROL A LA GESTIÓN PÚBLICA			1		**1**
07- POTESTAD DISCIPLINARIA			1		**1**
08- GESTIÓN DEL TALENTO HUMANO			2		**2**
09- GESTIÓN ADMINISTRATIVA			1		**1**
10- GESTIÓN FINANCIERA	1				**1**
12- GESTIÓN DOCUMENTAL	1			1	**2**
13- GESTIÓN JURÍDICA		1			**1**
14- SERVICIO AL USUARIO	1				**1**
15- CONTROL DISCIPLINARIO INTERNO			1		**1**
16- EVALUACIÓN Y SEGUIMIENTO			1		**1**
Total	**5**	**4**	**12**	**2**	**23**

Tabla 3: Cantidad de riesgos de seguridad por probabilidad

En la Tabla 4: se presentan los riesgos de cada proceso clasificados por el impacto que tendrían en caso de llegar a materializarse.

Proceso	Mayor	Moderado	Menor	Leve	Total
01 - DIRECCIONAMIENTO ESTRATÉGICO				2	**2**
02- GESTIÓN DEL CONOCIMIENTO E INNOVACIÓN				1	**1**
03- DIRECCIONAMIENTO TIC	3				**3**
04- COMUNICACIÓN ESTRATÉGICA				2	**2**

Proceso	Mayor	Moderado	Menor	Leve	Total
05- PROMOCIÓN Y DEFENSA DE DERECHOS	1	2			**3**
06- PREVENCIÓN Y CONTROL A LA GESTIÓN PÚBLICA		1			**1**
07- POTESTAD DISCIPLINARIA				1	**1**
08- GESTIÓN DEL TALENTO HUMANO	1	1			**2**
09- GESTIÓN ADMINISTRATIVA		1			**1**
10- GESTIÓN FINANCIERA		1			**1**
12- GESTIÓN DOCUMENTAL			1	1	**2**
13- GESTIÓN JURÍDICA			1		**1**
14- SERVICIO AL USUARIO		1			**1**
15- CONTROL DISCIPLINARIO INTERNO	1				**1**
16- EVALUACIÓN Y SEGUIMIENTO		1			**1**
Total	**6**	**8**	**2**	**7**	**23**

Tabla 4: Cantidad de riesgos de seguridad de la información según el impacto

6.3.1 DIRECCIONAMIENTO ESTRATÉGICO

La descripción del riesgo para cada proceso se describe a continuación, así como las acciones a tomar y el control que se debe llevar a cabo para mitigar la probabilidad de que los riesgos se materialicen. De igual forma se presenta el indicador a medir para cada uno de ellos.

✓ Posibilidad de pérdida de la Integridad y disponibilidad de la Información digital

- Probabilidad de que ocurra: 60%
- Impacto: **Leve**
- Zona de riesgo: Moderado
- Afectaciones: El riesgo afecta la imagen de alguna área de la organización
- **Control:** Realizar un backup documentos recibidos y generados en el proceso, en una carpeta compartida y en el One Drive.
- **Acción a realizar:** Solicitar la gestión de los permisos y acceso a la carpeta de red compartida en red de contratistas y funcionarios cuando se requiera.
- Indicador: Solicitudes permisos y acceso a la carpeta de red realizados.

- ✓ Posibilidad de pérdida de la disponibilidad de la Información Física
  - Probabilidad de que ocurra: 60%
  - Impacto: **Leve**
  - Zona de riesgo: Moderado
  - Afectaciones: El riesgo afecta la imagen de alguna área de la organización
  - **Control:** 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.
  - **Acción a realizar:** Revisión y organización del archivo físico del proceso de acuerdo con los criterios de gestión documental
  - Indicador: Actividades realizadas dentro del proceso

6.3.2 GESTIÓN DEL CONOCIMIENTO E INNOVACIÓN

- ✓ Posibilidad de pérdida reputacional por la afectación de los documentos del proceso en medio digital o electrónico debido a la Gestión inadecuada de los expedientes digitales del proceso.
  - Probabilidad de que ocurra: 40%
  - Impacto: **Menor**
  - Zona de riesgo: Bajo
  - Afectaciones: El riesgo afecta la imagen de alguna área de la organización.
  - **Control:** El funcionario(a) designado(a) por la Dirección de Gestión del Conocimiento e Innovación verifica que se realicen cuatrimestralmente copias de seguridad de los expedientes digitales
  - **Acción a realizar:**
    - Realizar copias de seguridad de los documentos que se encuentran en la carpeta compartida del proceso.
    - Actas de reunión de seguimiento y control a la gestión de la información en los expedientes digitales que se encuentran en la carpeta compartida del proceso.
  - Indicador: Copias de seguridad cuatrimestrales de los documentos que se encuentran en la carpeta compartida del proceso.

6.3.3 DIRECCIONAMIENTO TIC

- ✓ Posibilidad de pérdida económica y reputacional debido a los ataques cibernéticos y/o eventos de seguridad.
  - Probabilidad de que ocurra: 40%
  - Impacto: **Mayor**
  - Zona de riesgo: Alto
  - Afectaciones: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
  - **Control:** Divulgación de TIPS de Seguridad de la Información
  - **Acción a realizar:**
    - Divulgación de tips de Seguridad de la Información.
    - Plan de trabajo de tratamiento de vulnerabilidades de seguridad.
    - Realizar seguimiento al tratamiento de eventos de Seguridad de la Información identificados.
  - Indicadores:
    - Cumplimiento de las actividades definidas.
    - Plan de trabajo de tratamiento de vulnerabilidades de seguridad.
    - Tratamiento de eventos de Seguridad de la Información.

- ✓ Posibilidad de pérdida económico y reputacional por obsolescencia de software, ya que el tiempo de vida se puede acortar sino se mantienen correctamente.
  - Probabilidad de que ocurra: 60%
  - Impacto: **Mayor**
  - Zona de riesgo: Alto
  - Afectaciones: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
  - **Control:** Realizar actividades de tratamiento de vulnerabilidades de seguridad.
  - **Acción a realizar:**
    - Plan de trabajo de tratamiento de vulnerabilidades de seguridad y/o actividades de actualización o mejoras al software.
    - Propuesta de necesidad de adquisición de software.
  - Indicadores:
    - Plan de trabajo de tratamiento de vulnerabilidades de seguridad y/o actividades de actualización o mejoras al software
    - Documento con la propuesta de necesidad de adquisición de software.

- ✓ Posibilidad de pérdida económico y reputacional por obsolescencia de hardware, ya que entran en desuso, por insuficiente desempeño frente a nuevas tecnologías.
  - Probabilidad de que ocurra: 60%
  - Impacto: **Mayor**
  - Zona de riesgo: Alto
  - Afectaciones: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
  - **Control:** Medir el porcentaje de requerimientos atendidos oportunamente.
  - **Acción a realizar:**
    - Medir el nivel de satisfacción de los usuarios frente a los servicios de TI.
    - Documento y/o hojas de vida de actividades de mantenimiento preventivo de hardware.
    - Propuesta de necesidad de adquisición de hardware.
  - Indicadores:
    - Medir el nivel de satisfacción de los usuarios frente a los servicios de TI.
    - Documento y/o hojas de vida de actividades de mantenimiento preventivo de hardware.
    - Documento con la propuesta de necesidad de adquisición de software.

6.3.4 COMUNICACIÓN ESTRATÉGICA

- ✓ Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico y/o digital.
  - Probabilidad de que ocurra: 60%
  - Impacto: **Leve**
  - Zona de riesgo: Moderado
  - Afectaciones: El riesgo afecta la imagen de alguna área de la organización.
  - **Control:** Digitalización de documentos físicos del proceso e información digital almacenada en nubes públicas.
  - **Acción a realizar:**
    - Se solicita a todos los funcionarios y contratistas de la OAC guardar los productos realizados o la información susceptible de ser almacenada en los equipos asignados, servidor carpeta prensa, discos duros extraíbles y correos electrónicos.
    - Solicitar a los directivos y a la Dirección de TIC los equipos tecnológicos necesarios para continuar respaldando la información que se almacena y evitar pérdidas por insuficiencia de memoria.
    - Se tienen carpetas para almacenar la información impresa susceptible de almacenamiento.
  - Indicadores:

- Porcentaje de información o producto susceptible de ser almacenado sin respaldo.

✓ Posibilidad de afectación económica por divulgación no autorizada de la información reservada o sujeta a tratamiento de datos personales.
- Probabilidad de que ocurra: 40%
- Impacto: **Leve**
- Zona de riesgo: Bajo
- Afectaciones: El riesgo afecta la imagen de alguna área de la organización.
- **Control:** Validar con los delegados, o los coordinadores y/o personero(a) los contenidos de los boletines que se dan antes de emitir una comunicación.
- **Acción a realizar:**
  - Se imprimen, diligencian y hacen firmar los formatos 04-FR-02 Autorización de uso de derechos de imagen sobre fotografías y fijaciones audiovisuales (video), propiedad intelectual y habeas data otorgado a la personería de Bogotá para menores de edad y 04-FR-03 Autorización de uso de derechos de imagen sobre fotografías y fijaciones audiovisuales (video), propiedad intelectual y habeas data otorgado a la personería de Bogotá. cuando se produce material susceptible de aprobación por uso de imagen, propiedad intelectual y datos personales.
- Indicadores:
  - Porcentaje de información reservada o sujeta a tratamiento de datos personales no autorizada.

6.3.5 PROMOCIÓN Y DEFENSA DE DERECHOS

✓ Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico.
- Probabilidad de que ocurra: 80%
- Impacto: **Moderado**
- Zona de riesgo: Alto
- Afectaciones: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
- **Control:** Complementar los controles existentes enfocados al adecuado manejo, tratamiento y almacenamiento de los documentos físicos. Propósito: Evitar la pérdida de documentos físicos bajo el manejo de personal autorizado y con el tratamiento archivístico adecuado.
- **Acción a realizar:**
  - Clasificar información documental Critica (Inventario de Activos de Información elaborado por la Dirección de TIC). (40%).

- 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 30%).
- Asignar espacio seguro con acceso restringido a personal no autorizado (En el caso del edifico 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 30%).

- Indicadores:
  - Porcentaje de avance de implementación de las acciones definidas.

✓ Posibilidad de pérdida o daño de los documentos o datos críticos del proceso en medio digital - electrónico.
- Probabilidad de que ocurra: 80%
- Impacto: **Moderado**
- Zona de riesgo: Alto
- Afectaciones: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
- **Control:** Carpetas compartidas según los parámetros exigidos por la Dirección TIC (Carpeta de servidor de archivos o sitio ONE DRIVE institucional). Propósito: Trabajar los documentos digitales por personal autorizado en entornos seguros y sin probabilidad de perdida de información.
- **Acción a realizar:**
  - Clasificar información documental Critica (Inventario de Activos de Información elaborado por la Dirección de TIC). (40%).
  - Almacenar los documentos críticos en medio digital en la estructura de carpetas y subcarpetas definida para cada Personería Delegada o Local. (60%).
- Indicadores:
  - Porcentaje de avance de implementación de las acciones definidas.

✓ Posibilidad de divulgar información con datos críticos o sensibles de la Entidad y usuarios.
- Probabilidad de que ocurra: 100%
- Impacto: **Mayor**
- Zona de riesgo: Alto
- Afectaciones: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.

- **Control:** Complementar los controles existentes enfocados al adecuado tratamiento de la información y datos sensibles de los usuarios. Propósito: Evitar la fuga de información crítica y sensible tanto de la Entidad como de los usuarios.
- **Acción a realizar:**
  - 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.
- Indicadores:
  - Porcentaje de avance de implementación de las acciones definidas.

6.3.6 PREVENCIÓN Y CONTROL A LA GESTIÓN PÚBLICA

✓ Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico.
- Probabilidad de que ocurra: 60%
- Impacto: **Moderado**
- Zona de riesgo: Moderado
- Afectaciones: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
- **Control:** Guardar en el servidor de la Entidad los soportes de las diferentes actividades realizadas.
- **Acción a realizar:**
  - Realizar seguimiento a la Carpeta de servidor de archivos o sitio ONE DRIVE institucional que garantice la custodia y seguridad de la información de los informes y seguimiento generados.
- Indicadores:
  - Documentos guardados en servidor o en el drive.

6.3.7 POTESTAD DISCIPLINARIA

✓ Posibilidad de pérdida de documentación, que hacen parte de la unidad probatoria o CD, DVD y/o USB sin información.
- Probabilidad de que ocurra: 60%
- Impacto: **Leve**
- Zona de riesgo: Moderado
- Afectaciones: El riesgo afecta la imagen de alguna área de la organización.
- **Control:** Se tienen establecido unos parámetros para el control del expediente, en donde se relacionan los folios que conforman el expediente, se relacionan en bases de datos y cada vez que el expediente pasa por cada una de las fases

en sus etapas se debe actualizar los folios cuadernos y CD que lo conforman como unidad documental, de igual manera se imprime planillas para el recibo y/o entrega.

- **Acción a realizar:**
  - N/A.

- Indicadores:
  - N/A

6.3.8 GESTIÓN DEL TALENTO HUMANO

✓ Posibilidad de pérdida económica 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.

- Probabilidad de que ocurra: 60%
- Impacto: **Moderado**
- Zona de riesgo: Moderado.
- Afectaciones: Entre 50 y 100 SMLMV.
- **Control:** 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 con el personal responsable para su custodia.
- **Acción a realizar:**
  - Digitalizar la información crítica del proceso que se encuentre en medio físico y almacenarla en el sitio de ONE DRIVE o servidor institucional, en carpetas con acceso restringido a personal no autorizado.
- Indicadores:
  - Documentos y/o carpetas digitalizadas en One drive o servidor institucional
  - Número de folios insertados en las historias laborales, registrados en la hoja de control
  - Número de expedientes en préstamo, registrados en el formato Control consulta o préstamo de documentos de archivo

- ✓ Posibilidad de pérdida económica y reputacional por ciber ataques realizados por un externo e interno para divulgar y utilizar información con datos personales de los funcionarios porque se exponen públicamente.
  - Probabilidad de que ocurra: 60%
  - Impacto: **Mayor**
  - Zona de riesgo: Alto.
  - Afectaciones: Entre 100 y 500 SMLMV.
  - **Control:** 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 con el personal responsable para su custodia.
  - **Acción a realizar:**
    - Socializar el Compromiso de Confidencialidad y No Divulgación de la Información y sensibilizar sobre el uso adecuado de la información de la entidad y la seguridad informática.
    - Almacenar y cifrar la información digital que contenga datos sensibles o reservados, en carpeta de ONE DRIVE o servidor institucional, con acceso restringido a personal no autorizado.
    - Manejar los datos consignados en las planillas y/o registros conforme a lo dispuesto en la ley de Habeas Data (Ley 1581 de 2012).
  - Indicadores:
    - Compromiso de Confidencialidad y No Divulgación de la Información socializado y firmado
    - Número de folios insertados en las historias laborales, registrados en la hoja de control
    - Número de expedientes en préstamo, registrados en el formato Control consulta o préstamo de documentos de archivo.

6.3.9 GESTIÓN ADMINISTRATIVA

- ✓ Pérdida o daño de la información física del proceso.
  - Probabilidad de que ocurra: 60%
  - Impacto: **Moderado**
  - Zona de riesgo: Moderado.
  - Afectaciones: Entre 50 y 100 SMLMV.
  - **Control:** Digitalización permanente de los documentos producidos desde el proceso de Gestión Administrativa, salvaguardando la información en una carpeta virtual.
  - **Acción a realizar:**

- Realizar 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.
- Realizar una transferencia anual de los documentos físicos de la Subdirección de Gestión Documental y Recursos Físicos del archivo de gestión al archivo central, de acuerdo con la TRD y el cronograma de transferencias.

- Indicadores:
  - No. de seguimientos realizados

6.3.10 GESTIÓN FINANCIERA

✓ Posibilidad de afectación reputacional por reporte del área de control interno debido a perdida, daño, manipulación indebida de los documentos críticos del proceso, pérdida de conocimiento de información contenida en medios físico y digital - electrónico, hardware averiado y/o software desactualizado.

- Probabilidad de que ocurra: 80%
- Impacto: **Menor**
- Zona de riesgo: Moderado.
- Afectaciones: El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores.
- **Control:** Restricción de acceso al archivo de gestión, salvaguardar los documentos digital - electrónicos en la carpeta de red institucional.
- **Acción a realizar:**
  - Mantener la información en sitio seguro (Físico y/o digital), registrando la información digital en carpeta de ONE DRIVE institucional con acceso restringido a personal no autorizado.
  - Verificar que el personal que administra o intervenga en el procesamiento de información documente las actividades realizadas, mediante la elaboración de formatos, guías, instructivos, imágenes, videos, manuales, cuando aplique.

6.3.11 GESTIÓN DOCUMENTAL

- ✓ Posibilidad de pérdida reputacional debido al deterioro, destrucción, extravío o pérdida de la documentación institucional en soporte físico en archivo central.
  - Probabilidad de que ocurra: 80%
  - Impacto: **Moderado**
  - Zona de riesgo: Alto.
  - Afectaciones: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
  - **Control:** Aplicación de instrumentos de control como inventarios documentales y controles de préstamos y consultas.
  - **Acción a realizar:**
    - Verificar mediante el formato control de préstamos y consultas documentales (formato 12-FR-02).

- ✓ 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.
  - Probabilidad de que ocurra: 100%
  - Impacto: **Menor**
  - Zona de riesgo: Alto.
  - Afectaciones: El riesgo afecta la imagen de alguna área de la organización.
  - **Control:** Servicio de vigilancia privada con monitoreo mediante cámaras internas y perimetrales en archivo central y de sensores de movimiento.
  - **Acción a realizar:**
    - Identificar documentos con información confidencial
    - Lineamiento para atención de consulta y préstamos documentales del Archivo Central.

6.3.11 GESTIÓN JURÍDICA

- ✓ Posibilidad de 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.
  - Probabilidad de que ocurra: 40%
  - Impacto: **Menor**
  - Zona de riesgo: Moderado.
  - Afectaciones: El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores.

- **Control:** Se 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).
- **Acción a realizar:**
  - Realizar backup de las carpetas de registro de sanciones en el sitio ONE DRIVE institucional.

6.3.11 SERVICIO AL USUARIO

✓ Posibilidad de Pérdida de información relevante para el proceso.
- Probabilidad de que ocurra: 80%
- Impacto: **Moderado**
- Zona de riesgo: Alto.
- Afectaciones: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
- **Control:** Realiza copia de seguridad de la información contenida en el repositorio office 365 del usuario nsamudio@personeriabogotá.gov.co.
- **Acción a realizar:**
  - Realiza copia de seguridad de los documentos críticos en la carpeta compartida de servidor de la Entidad o en One drive del proceso servicio al usuario.
  - Conceder accesos a los funcionarios (as) y contratistas de la Secretaría General, a través de share point de One Drive del repositorio de office 365.

6.3.12 CONTROL DISCIPLINARIO INTERNO

✓ Posibilidad de ausencia o pérdida de integridad de la información contenida en los expedientes disciplinarios y sus anexos físicos o digitales.
- Probabilidad de que ocurra: 60%
- Impacto: **Mayor**
- Zona de riesgo: Alto.
- Afectaciones: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
- **Control:** Sensibilizar a todo el talento humano que cumple labores en la Oficina de Control Interno Disciplinario, con el fin de evitar la materialización de alguna fuga de información, advirtiendo los riesgos personales y para la entidad y el cumplimiento de las normas técnicas de archivo y gestión documental.

- **Acción a realizar:**
  - Asignar espacio seguro (archivadores o gabeteros) con acceso restringido a personal no autorizado, para resguardar los documentos físicos que sean críticos para el proceso y designar personal responsable para su custodia.
  - Digitalizar la información crítica del proceso que se encuentre en medio físico y almacenarla en el sitio de ONE DRIVE institucional, en carpetas con acceso restringido a personal no autorizado.
  - Implementar Sistema de control de acceso a los espacios donde se resguarden los documentos físicos que sean críticos para el proceso.

6.3.13 EVALUACIÓN Y SEGUIMIENTO

✓ Posibilidad de afectación reputacional debido a la pérdida o daño de la información documentada del Proceso registrada en medio físico y digital.
- Probabilidad de que ocurra: 60%
- Impacto: **Moderado**
- Zona de riesgo: Moderado.
- Afectaciones: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
- **Control:** Almacenar la información en medios físicos y digitales.
- **Acción a realizar:**
  - Designar un responsable de la custodia, manejo y control de los documentos físicos y digitales del Proceso, manteniendo acceso restringido a personal no autorizado.
  - Digitalizar la información del proceso y almacenarla en la Carpeta Compartida de la OCI con acceso restringido a personal no autorizado.
  - Mantener actualizado el formato único de inventario documental FUID

7. FORTALEZAS

➢ Los procesos tienen el compromiso de identificar los riesgos de seguridad y proteger los activos de información.

➢ Existe una mayor comprensión del Sistema de Seguridad de la Información SGSI, lo cual se evidencia en la alineación de los riesgos con los controles permitiendo una mitigación más efectiva.

8. CONCLUSIONES

- Para los procesos que tienen los riesgos de mayor impacto y probabilidad el SGSI debe fortalecer el acompañamiento, para asegurar que las acciones implementadas controlen la causa raíz que origina estos riesgos.

- El Sistema de Gestión de Seguridad de la Información SGSI debe comunicar de forma integral la relación entre los activos de información, riesgos de seguridad y controles, para establecer una valoración y tratamiento que refleje la importancia del activo de información en la Entidad.

9. RECOMENDACIONES

- Aplicar los protocolos para salvaguardar los activos de información de la Entidad, siguiendo los lineamientos, recomendaciones y alertas de seguridad socializados por el Sistema de Seguridad de la Información SGSI.

- Robustecer el seguimiento a la implementación de los controles incluyéndolos dentro de los planes de mejoramiento.