Personería de Bogotá, D. C.

INFORME

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN VIGENCIA 2025

Dirección de Tecnologías de la Información y las Comunicaciones – DTIC

Bogotá, febrero de 2026

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE GRAFICOS

IDENTIFICACIÓN DEL INFORME

Fecha	Periodo del informe
Febrero de 2026	Enero a diciembre de 2025

1. INTRODUCCIÓN

La Personería de Bogotá, D. C., en cumplimiento de sus funciones y objetivos estratégicos, implementa acciones y estrategias orientadas a garantizar la seguridad de la información como uno de sus activos más importantes para el desarrollo de su misión institucional. En este marco, la Entidad adopta y aplica lineamientos establecidos en la normatividad legal vigente, tales como el Decreto 1008 de 2018, *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital"*, el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones, así como la Resolución Interna 180 de 2025, mediante la cual se adopta, implementa y asegura la sostenibilidad de los Sistemas de Gestión de la Entidad, entre ellos el Sistema de Gestión de Seguridad de la Información - SGSI.

Adicionalmente, mediante la Resolución Interna 242 de 2023 se adopta el Sistema de Gestión de Seguridad de la Información bajo la NTC-ISO/IEC 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. Para el caso de la Personería de Bogotá, D. C., este enfoque se desarrolla a través de la metodología definida en la Guía para la Administración del Riesgo Código 01-GU-04, aplicable a todos los procesos de la Entidad, la cual establece directrices para la administración de los riesgos estratégicos, de gestión, **de seguridad de la información**, de corrupción y demás riesgos institucionales.

En este contexto, 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 adelantada por los procesos institucionales respecto del análisis, evaluación y tratamiento de los riesgos de seguridad de la información, y presenta los resultados relacionados con la efectividad de los controles implementados, así como las correspondientes recomendaciones de mejora.

2. ALCANCE

El presente informe de gestión de riesgos de seguridad de la información tiene como alcance la identificación, análisis, evaluación y seguimiento de los riesgos que afectan los activos de información de la Personería de Bogotá D. C., en todos sus procesos, como parte de la Dimensión 7 – Control Interno del MIPG, en concordancia con el Modelo Estándar de Control Interno - MECI y el Sistema de Gestión de Seguridad de la

Información – SGSI (ISO 27001), apoyando la política de Seguridad Digital y el esquema de líneas de defensa institucional.

3. OBJETIVO

Presentar los resultados del análisis a la gestión de los riesgos de seguridad de la información de la Personería de Bogotá, D. C., durante la vigencia 2025, como parte de la Dimensión 7 – Control Interno del Modelo Integrado de Planeación y Gestión (MIPG), verificando la pertinencia y eficacia de los controles existentes y de las acciones de tratamiento programadas, con el fin de apoyar la evaluación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

4. METODOLOGÍA

La metodología empleada para el desarrollo del presente informe se fundamenta en un enfoque sistemático y articulado de gestión del riesgo, orientado a garantizar la adecuada identificación, análisis, evaluación y seguimiento de los riesgos de seguridad de la información. Para tal efecto, el análisis se desarrolla tomando como referencia la Guía para la Administración del Riesgo Código 01-GU-04 de la Personería de Bogotá, D. C., los requisitos establecidos en la NTC-ISO/IEC 27001:2022, y la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública – DAFP, asegurando su alineación con el Sistema de Control Interno y el enfoque de mejora continua adoptado por la Entidad.

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

5.1. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El proceso de gestión de riesgos inicia con la identificación, clasificación y valoración de quinientos sesenta y cinco (565) activos de información, lo que permite establecer las fuentes de información que generan valor para la entidad y que, debido a su criticidad, deben ser protegidas mediante una adecuada gestión del riesgo y la implementación de controles y planes de tratamiento orientados a mitigarlos.

CRITICIDAD DE ACTIVOS	
CRITICO	115
MODERADO	309
BAJO	141
TOTAL	565

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

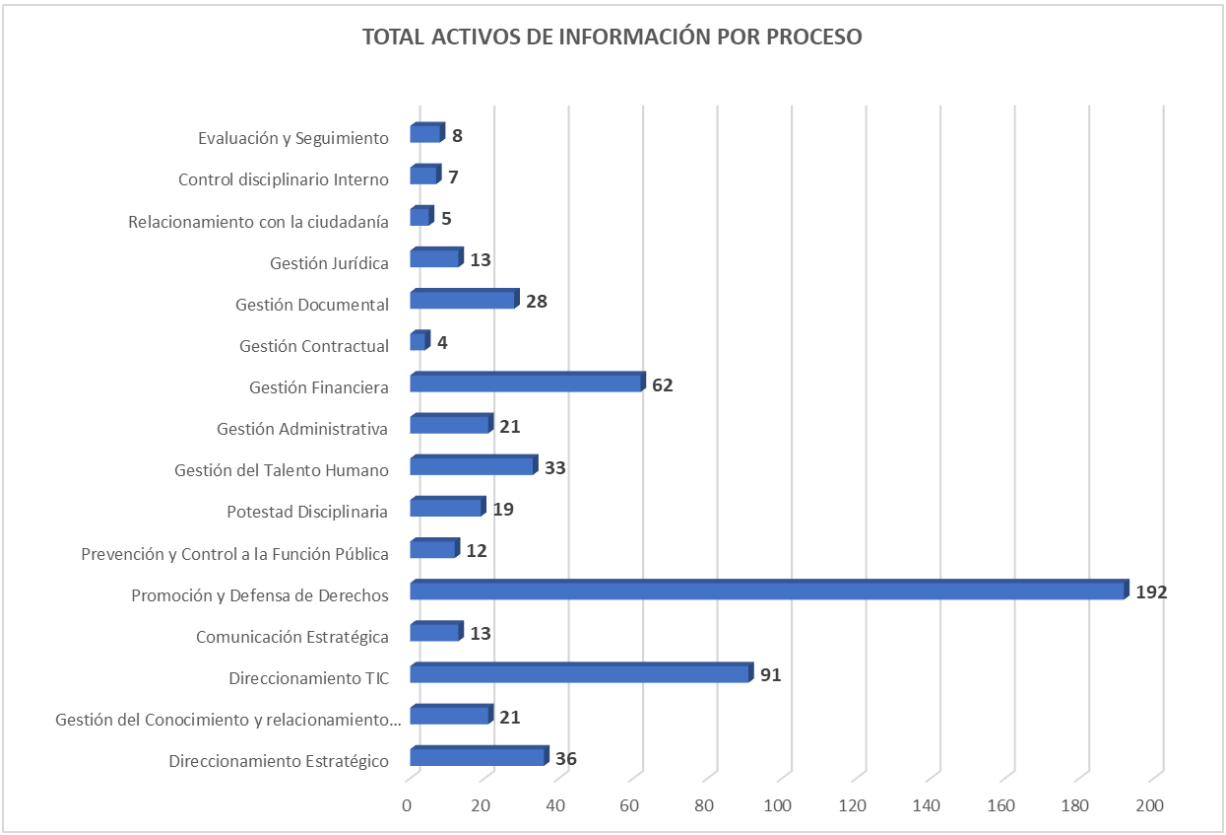

Gráfico 2. Total de activos de información por proceso
Tomado de: Inventario de activos de información

#	PROCESO	CRITICO	MODERADO	BAJO	TOTAL ACTIVOS
1	Direccionamiento Estratégico	0	25	11	36
2	Gestión del Conocimiento y relacionamiento institucional	0	2	19	21
3	Direccionamiento TIC	58	28	5	91
4	Comunicación Estratégica	5	6	2	13
5	Promoción y Defensa de Derechos	4	144	44	192
6	Prevención y Control a la Función Pública	3	9	0	12
7	Potestad Disciplinaria	8	8	3	19
8	Gestión del Talento Humano	11	19	3	33
9	Gestión Administrativa	6	9	6	21
10	Gestión Financiera	1	35	26	62
11	Gestión Contractual	0	3	1	4
12	Gestión Documental	5	6	17	28
13	Gestión Jurídica	7	4	2	13
14	Relacionamiento con la ciudadanía	1	4	0	5
15	Control disciplinario Interno	6	1	0	7
16	Evaluación y Seguimiento	0	6	2	8
	TOTAL	**115**	**309**	**141**	**565**

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 actualizados con fecha al mes de diciembre de 2025, encontrando una cifra significativa de 115 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	2
ALTO	2
MODERADO	9
BAJO	12
TOTAL	**25**

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

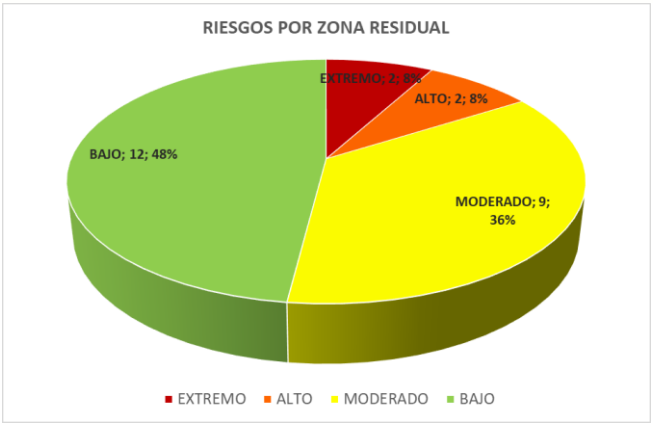

Gráfico 3. Porcentaje de riesgos de seguridad de la información por zona residual
Tomado de: Mapa de riesgos institucional

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

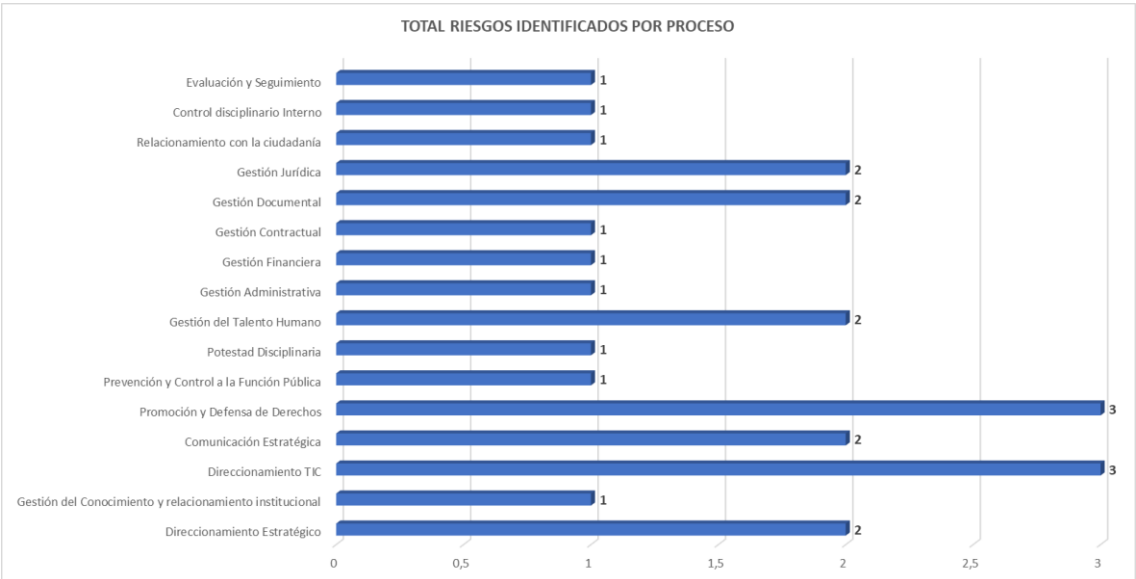

Gráfico 5. Total de riesgos de seguridad de la información por proceso
Tomado de: Mapa de riesgos institucional

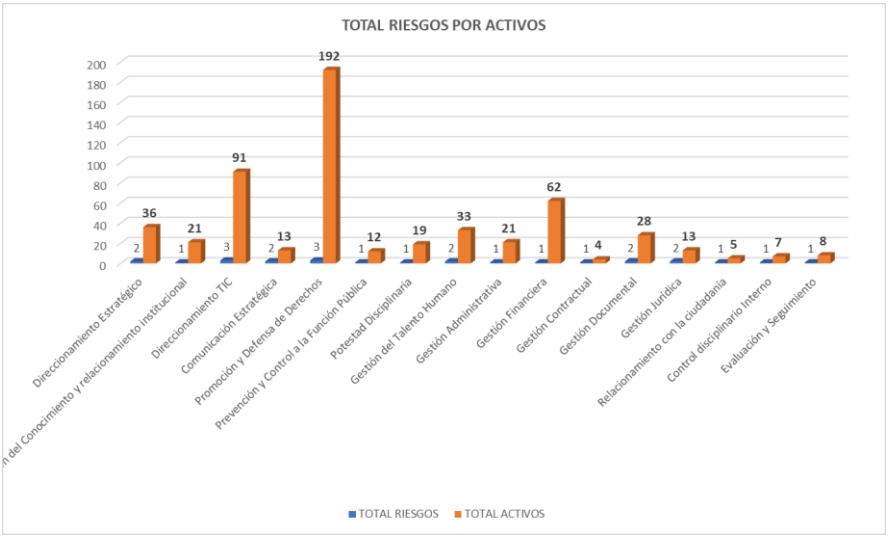

Gráfico 6. Comparación riesgos de seguridad Vs Activos de información por proceso
Tomado de: Mapa de riesgos institucional – Inventario de activos de información

Se observa que, en los 16 procesos evaluados, la identificación y valoración de riesgos de seguridad de la información presenta una tendencia baja, con un rango entre uno (1) y tres (3) riesgos por proceso, y únicamente dos (2) procesos registran tres (3) riesgos valorados. En total, se identificaron y evaluaron veinticinco (25) riesgos, cifra que resulta limitada frente al número de activos de información inventariados (565 activos), de los cuales ciento quince (115) fueron clasificados como críticos. Este comportamiento sugiere una posible subestimación del panorama real de riesgos del SGSI.

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	3	0	0	0	2
2	Gestión del Conocimiento y relacionamiento institucional	1	0	0	1	0	1	0	0	0	1
3	Direccionamiento TIC	3	0	3	0	0	9	0	0	1	2
4	Comunicación Estratégica	2	0	0	1	1	6	0	0	0	2
5	Promoción y Defensa de Derechos	3	2	1	0	0	5	2	0	1	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	7	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	1	0	0	1	0	2	0	0	0	1
12	Gestión Documental	2	0	1	1	0	6	0	0	0	2
13	Gestión Jurídica	2	0	0	2	0	2	0	0	0	2
14	Relacionamiento con la ciudadanía	1	0	0	1	0	3	0	0	1	0
15	Control disciplinario Interno	1	0	1	0	0	3	0	1	0	0
16	Evaluación y Seguimiento	1	0	0	1	0	4	0	0	1	0
	TOTAL	25	2	9	13	1	59	2	2	9	12

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

IDENTIFICACION DE LOS RIESGOS POR IMPACTO INHERENTE

IDENTIFICACIÓN DE LOS RIESGOS POR IMPACTO INHERENTE						
		IMPACTO				
PROBABILIDAD	Muy Alta 100%	1			3		Extremo
	Alta 80%		1	3		2	Alto
	Media 60%	2	3	5	2		Moderado
	Baja 40%	2		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

		IMPACTO					
PROBABILIDAD	Muy Alta 100%						Extremo
	Alta 80%						Alto
	Media 60%						Moderado
	Baja 40%			1		2	Bajo
	Muy Baja 20%	5	6	9	2		
		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

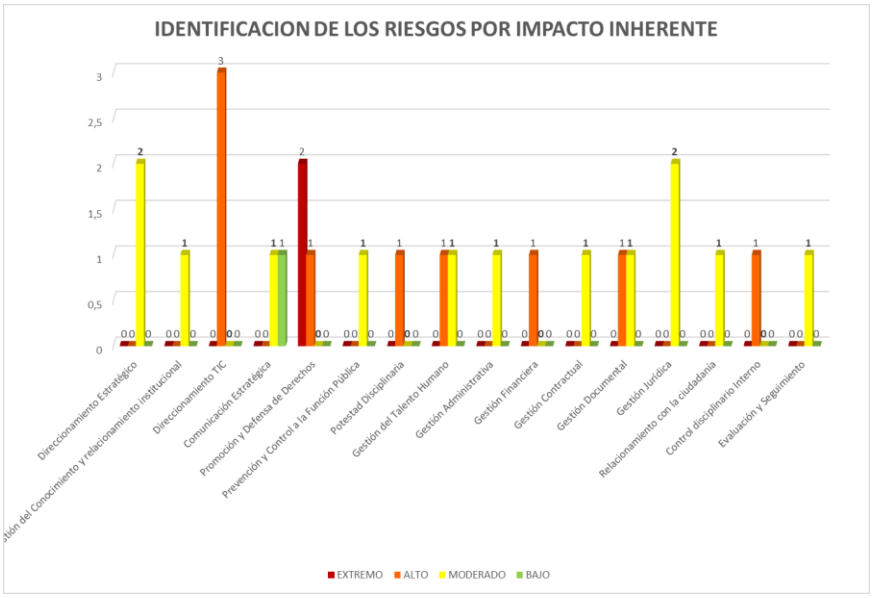

Gráfico 7. Impacto inherente por procesos
Tomado de: Mapa de riesgos institucional

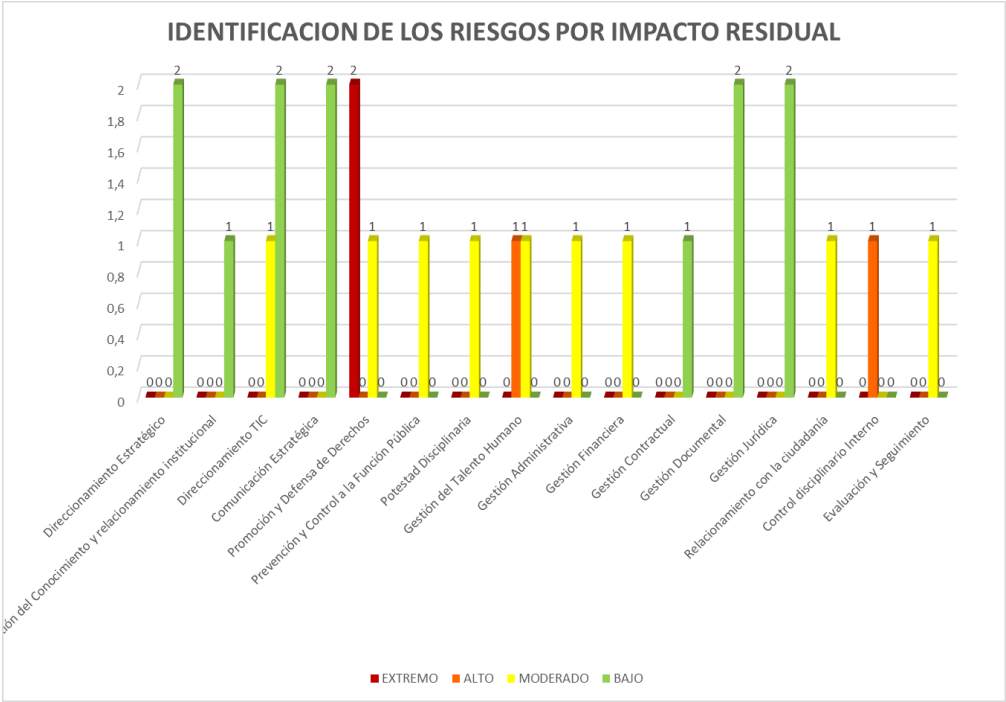

Gráfico 8. Impacto residual por procesos
Tomado de: Mapa de riesgos institucional

En análisis realizado, se evidencia que una vez valorados los controles existentes de riesgos de seguridad de la información, la valoración del riesgo residual se mantiene igual a la valoración del riesgo inherente para siete (7) de los dieciséis (16) procesos institucionales, (Promoción y defensa de derechos, Prevención y control a la función pública, Gestión del Talento Humano, Gestión administrativa, Relacionamiento con la Ciudadanía, Control disciplinario interno y Evaluación y seguimiento), 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.

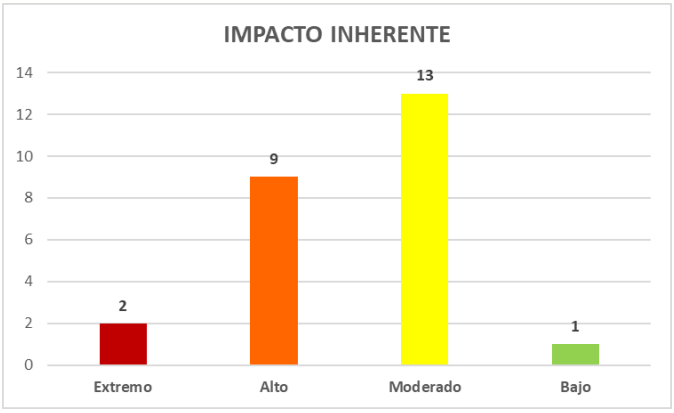

Gráfico 9. Identificación de riesgos de seguridad de la información por impacto inherente
Tomado de: Mapa de riesgos institucional

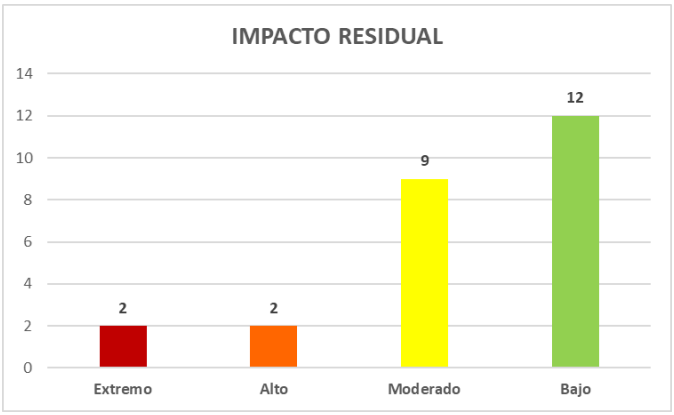

Gráfico 10. Identificación de riesgos de seguridad de la información por impacto residual
Tomado de: Mapa de riesgos institucional

En el análisis general de la evaluación de los riesgos de seguridad de la información se evidencia que el número de riesgos ubicados en las zonas de riesgo residual extremo y moderado se mantiene estable. Asimismo, se observa una disminución significativa en los riesgos clasificados en la zona de riesgo alto, lo cual se traduce en un aumento de riesgos en la zona de riesgo residual bajo.

El comportamiento descrito indica una mejoría en la gestión del riesgo de seguridad de la información.

Estabilidad en riesgos extremos y moderados: Sugiere la necesidad de revisar si los controles implementados para estos riesgos están siendo realmente eficaces o si requieren acciones adicionales para reducirlos.

Disminución de riesgos altos: Esta reducción es un resultado positivo y evidencia que las acciones de mitigación aplicadas han sido efectivas. Los controles implementados

han logrado reducir la probabilidad o el impacto de estos riesgos, llevándolos a niveles más manejables.

Aumento de riesgos en la zona residual baja: Que más riesgos migren a esta categoría demuestra un fortalecimiento del proceso de gestión del riesgo. Significa que después de aplicar controles, los riesgos remanentes son más bajos y aceptables para la entidad.

Estos resultados reflejan un avance favorable en la madurez del Sistema de Gestión de Seguridad de la Información (SGSI), especialmente en la efectividad de los controles implementados. No obstante, se recomienda mantener el monitoreo continuo y revisar especialmente aquellos riesgos que permanecen en niveles extremos y moderados para asegurar su adecuada mitigación.

5.4. PLANES DE ACCION PARA EL TRATAMIENTO DE RIESGOS

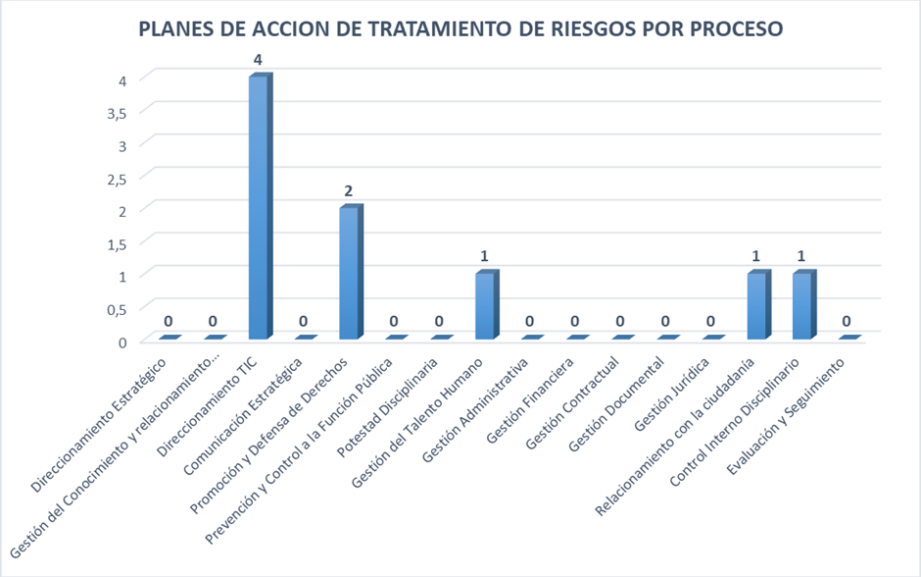

Gráfico 11. Planes de acción de riesgos por procesos
Tomado de: Mapa de riesgos institucional

Para la vigencia 2025, se encuentran identificados un total de 25 riesgos de seguridad de la información los cuales cuentan con un total de 59 controles implementados y 9 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.

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

#	PROCESO	TOTAL RIESGOS	PLAN DE ACCIÓN	RIESGOS MATERIALIZADOS	¿HA IDENTIFICADO NUEVOS RIESGOS?
1	Direccionamiento Estratégico	2	0	0	0
2	Gestión del Conocimiento y relacionamiento institucional	1	0	0	0
3	Direccionamiento TIC	3	4	2	0
4	Comunicación Estratégica	2	0	0	0
5	Promoción y Defensa de Derechos	3	2	0	0
6	Prevención y Control a la Función Pública	1	0	0	0
7	Potestad Disciplinaria	1	0	0	0
8	Gestión del Talento Humano	2	1	0	0
9	Gestión Administrativa	1	0	0	0
10	Gestión Financiera	1	0	0	0
11	Gestión Contractual	1	0	0	0
12	Gestión Documental	2	0	0	0
13	Gestión Jurídica	2	0	0	0
14	Relacionamiento con la ciudadanía	1	1	0	0
15	Control Disciplinario Interno	1	1	0	0
16	Direccionamiento Estratégico	1	0	0	0
	TOTAL	**25**	**9**	**2**	**0**

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

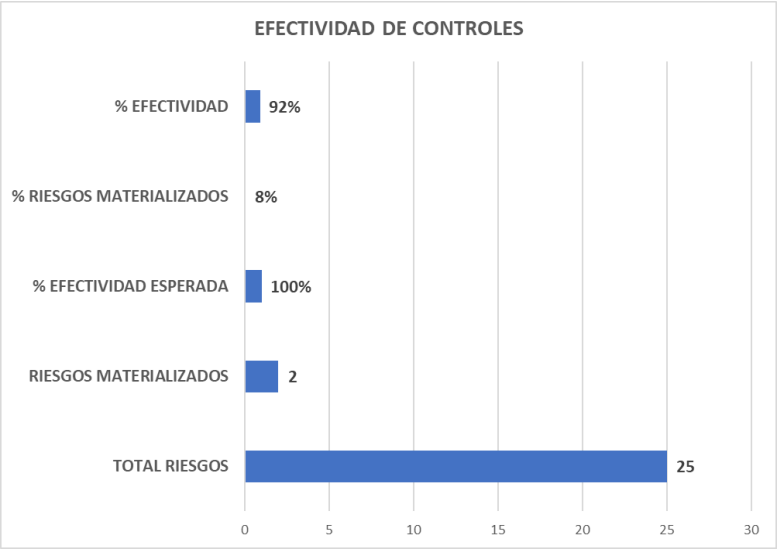

Gráfico 12. Efectividad de controles
Tomado de: Mapa de riesgos institucional

De los dieciséis (16) procesos evaluados, se reportó la materialización de dos (2) riesgos de seguridad de la información durante el periodo analizado. Respecto de los veinticinco

(25) riesgos identificados, se encuentran documentados cincuenta y nueve (59) controles implementados y nueve (9) acciones de tratamiento orientadas a mitigar el riesgo residual. Con base en esta gestión, se observa un nivel de eficacia del 92%, al presentarse únicamente dos riesgos materializados, los cuales fueron reportados por el proceso 03 – Dirección TIC a la Dirección de Planeación.

En relación con estos eventos, se definieron e implementaron acciones de tratamiento adicionales, de acuerdo con el procedimiento institucional vigente para la gestión de riesgos de seguridad de la información.

6. ANALISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y COMPARACIÓN DE CONTROLES IMPLEMENTADOS POR PROCESO

Con base en la información recopilada a partir del mapa de riesgos institucional, se presenta el análisis de los riesgos de seguridad de la información identificados y evaluados en los dieciséis (16) procesos de la Personería de Bogotá, D. C., con el fin de verificar su adecuada formulación y gestión.

Para cada proceso, se realizó el análisis a nivel de identificación, redacción y alineación de los riesgos de seguridad de la información, de conformidad con los lineamientos establecidos en la Guía para la Administración del Riesgo Código 01-GU-04 y en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública - DAFP.

Adicionalmente, se efectuó la comparación entre los controles existentes y las acciones definidas para el tratamiento de los riesgos de seguridad de la información, con fecha de corte a diciembre de 2025, frente a los controles establecidos en el Anexo A de la NTC-ISO/IEC 27001:2022. Como resultado de este ejercicio, se identificaron las brechas existentes y se formularon recomendaciones de mejora, orientadas al fortalecimiento del Sistema de Gestión de Seguridad de la Información – SGSI.

01.Direccionamiento estratégico					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	Posibilidad de afectación 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.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	N/A	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (integridad y disponibilidad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad.

01.Direccionamiento estratégico					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de la Información digital por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología del DAFP, se evidenció que la identificación de los riesgos de seguridad de la información no incorpora las amenazas y vulnerabilidades definidas en la guía, lo que constituye una brecha metodológica que afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información. Se evidencia que la redacción de los controles implementados incluye información sensible y específica, como la dirección IP del servidor, pese a tratarse de un documento de carácter público. Esta situación demuestra una brecha de seguridad, al exponerse detalles operativos innecesarios que pueden ser utilizados por terceros para actividades de reconocimiento, ingeniería social o ataques dirigidos, incrementando el riesgo de compromiso de la seguridad de la información institucional.
2	Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	N/A	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (disponibilidad e integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos

01.Direccionamiento estratégico					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. El control implementado se relaciona con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control A.5.10 – Uso aceptable de la información y otros activos asociados, por estar relacionado con el manejo adecuado de la información.

Observaciones y/o recomendaciones

Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos.

Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001.

Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.

Ajustar la redacción de los controles implementados, eliminando la referencia a información sensible, teniendo en cuenta que se trata de un documento de carácter público. La actividad debe describirse de manera general y funcional, enfocándose en el proceso y no configuraciones particulares, con el fin de evitar la exposición de información sensible, reducir el riesgo de ataques de ingeniería social, phishing dirigido y reconocimiento por parte de terceros.

02-Gestión del Conocimiento e Innovación					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	Posibilidad de afectación reputacional debido al incumplimiento en las metas del proceso e insatisfacción de los grupos de valor por debilidades en el almacenamiento de los documentos producidos por los funcionarios y colaboradores de la Dirección de Gestión del Conocimiento e Innovación	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	N/A	El riesgo formulado no permite identificar si se refiere a pérdida de confidencialidad, integridad o disponibilidad, ni relaciona claramente (Impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. El control implementado por el proceso corresponde a los controles aplicables según el ANEXO A de la NTC-ISO/IEC 27001, correspondiendo al control A.5.10 – Uso aceptable de la información y otros activos asociados, por estar relacionado con el manejo adecuado de la información.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda, incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001 Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

03-Direccionamiento TIC					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	Posibilidad de pérdida económica y reputacional por	**Campo anonimizado.** los controles detallados asociados a cada riesgo han	Moderado	**Campo anonimizado.**	La redacción del riesgo permite identificar de manera clara la afectación en los

03-Direccionamiento TIC					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
	sanciones de entidades reguladoras, publicaciones en medios de comunicación y/o afectación de las funciones de la entidad, debido al deterioro o modificación no autorizada de la información institucional almacenada, procesada o transmitida a través de equipos, redes de datos y/o sistemas de información de la infraestructura tecnológica de la Personería de Bogotá, D.C.	sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.		los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	principios de la información, al hacer referencia al deterioro o modificación no autorizada de la información (Pérdida de integridad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: "Posibilidad de **[impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Las vulnerabilidades identificadas para el riesgo se encuentran alineadas con lo establecido en la "Guía para la Administración del Riesgo" Código 01-GU-04 y con el Anexo 4 de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP; no obstante, se identifica una brecha en la aplicación integral de la metodología, dado que para la determinación de la causa inmediata no se está considerando de manera explícita la lista de amenazas definida en la citada guía, lo cual afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos metodológicos establecidos. Los controles implementados por el proceso corresponden a los controles aplicables al

03-Direccionamiento TIC					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					riesgo según el ANEXO A de la NTC-ISO/IEC 27001.
2	Posibilidad de pérdida económica y/o reputacional por sanciones de entidades reguladoras, publicaciones en medios de comunicación y/o afectación de las funciones de la entidad, debido a la pérdida de disponibilidad de los equipos y/o sistemas de información que almacenan, procesan o transmiten información institucional ubicados en la nube de AZURE y ORACLE o en máquinas físicas o virtuales ONPREMISE (Datacenter sede principal)	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la "pérdida de disponibilidad", facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04, sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Las vulnerabilidades identificadas para el riesgo se encuentran alineadas con lo establecido en la "Guía para la Administración del Riesgo" Código 01-GU-04 y con el Anexo 4 de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP; no obstante, se identifica una brecha en la aplicación integral de la metodología, dado que para la determinación de la causa inmediata no se está considerando de manera explícita la lista de amenazas definida en la citada guía, lo cual afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos metodológicos establecidos.

03-Direccionamiento TIC					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					Los controles implementados por el proceso corresponden a los controles aplicables al riesgo según el ANEXO A de la NTC-ISO/IEC 27001.
3	Posibilidad de pérdida económica y reputacional por sanciones de entidades reguladoras, publicaciones en medios de comunicación y/o afectación de las funciones de la entidad, debido a la divulgación no autorizada de información institucional sensible, almacenada, procesada o transmitida a través de equipos, redes de datos y/o sistemas de información de la infraestructura tecnológica de la Personería de Bogotá, D.C	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia explícita a la divulgación no autorizada (Pérdida de confidencialidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. Sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad)., se recomienda mejorarlo con la estructura: "Posibilidad de **[impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]**", con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Las vulnerabilidades identificadas para el riesgo se encuentran alineadas con lo establecido en la "Guía para la Administración del Riesgo" Código 01-GU-04 y con el Anexo 4 de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP; no obstante, se identifica una brecha en la aplicación integral de la metodología, dado que para la determinación de la causa inmediata no se está considerando de manera explícita la lista de amenazas

03-Direccionamiento TIC					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					definida en la citada guía, lo cual afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos metodológicos establecidos. Los controles implementados por el proceso corresponden a los controles aplicables al riesgo según el ANEXO A de la NTC-ISO/IEC 27001; y se evidencian que dichos controles están dirigidos a la remediación o mitigación de las vulnerabilidades identificadas para este riesgo.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda, incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001					

04-Comunicación estratégica					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	Posibilidad de pérdida reputacional por daño o pérdida de los documentos críticos del proceso en medio físico y/o digital	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Integridad y disponibilidad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04.

04-Comunicación estratégica					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
					Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información, 5.10 Uso aceptable de la información y otros activos asociados y 8.13 Copia de seguridad de la información respectivamente.
2	Posibilidad de afectación económica y reputacional por divulgación no autorizada de la información reservada o sujeta a tratamiento de datos personales.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia explícita a la divulgación no autorizada (Pérdida de confidencialidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos.

04-Comunicación estratégica					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 5.34 Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés), 8.13 Copia de seguridad de la información y 5.34 Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)

Observaciones y/o recomendaciones

Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos.

Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001.

Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.

05-Promoción y Defensa de Derechos					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	Posibilidad de pérdida o daño de los documentos críticos del proceso en medio físico	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Extremo	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e Integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por**

05-Promoción y Defensa de Derechos					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					[Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]", con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso y las acciones de tratamiento planeadas corresponden a los aplicables al riesgo según el ANEXO A de la NTC-ISO/IEC 27001 de 2022. 5.9 Inventario de información y otros activos asociados, 5.18 Derechos de acceso y 7.3 Asegurar oficinas, habitaciones e instalaciones, respectivamente.
2	Posibilidad de pérdida o daño de los documentos o datos críticos del proceso en medio digital - electrónico	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Extremo	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e Integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad.

05-Promoción y Defensa de Derechos					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
					El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso y las acciones de tratamiento planeadas corresponden a los aplicables al riesgo según el ANEXO A de la NTC-ISO/IEC 27001 de 2022. 5.9 Inventario de información y otros activos asociados y 5.10 Uso aceptable de la información y otros activos asociados, respectivamente.
3	Posibilidad de divulgar información con datos críticos o sensibles de la Entidad y usuarios.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que	Moderado	NO APLICA	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la divulgación de información (Pérdida de confidencialidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo,

05-Promoción y Defensa de Derechos					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
		pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.			el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 5.9 Inventario de información y otros activos asociados
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

06-Prevención y Control a la Función Pública					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	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.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Moderado	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e Integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. El control implementado por el proceso corresponde a los aplicables al riesgo según el ANEXO A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control				

07-Potestad Disciplinaria					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	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.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Moderado	NO APLICA	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la pérdida de información (Pérdida de disponibilidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología del DAFP, se evidenció que la identificación de los riesgos de seguridad de la información no incorpora en el campo [Causa Inmediata] las amenazas definidas en la guía, lo que constituye una brecha metodológica que afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 5.10 Uso aceptable de la información y otros activos asociados.

Observaciones y/o recomendaciones

Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos.

Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001.

Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.

08-Gestión del Talento Humano					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	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.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Moderado	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, de conformidad con la metodología del DAFP, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Seguido de esto, se recomienda reformular el riesgo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 7.3 Asegurar oficinas, habitaciones e instalaciones y 5.10 Uso aceptable de la información y otros activos asociados, respectivamente.
2	Posibilidad de afectación Económica (o presupuestal) y Reputacional por ciberataques por un externo o interno para divulgar y	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda	Alto	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados	La redacción del riesgo permite identificar la afectación en los principios de la información, al hacer referencia a la divulgación de información (Pérdida de confidencialidad), sin embargo, se recomienda redactar los riesgos en términos de afectación a los principios de seguridad de la información

08-Gestión del Talento Humano					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
	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)	ser utilizada para afectar la seguridad de los activos de información de la entidad.		en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	(Confidencialidad, Integridad o Disponibilidad), según corresponda, mejorándolo con la estructura**: "Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. La(s) amenaza(s) y vulnerabilidad(es) identificada(s) para el riesgo está(n) relacionada(s) con lo establecido en la GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Código: 01-GU-04 y el Anexo 4 del DAFP. Los controles implementados por el proceso y las acciones de tratamiento planificadas se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 7.3 Asegurar oficinas, habitaciones e instalaciones, 6.6 Acuerdos de confidencialidad o no divulgación y 5.10 Uso aceptable de la información y otros activos asociados, 8.8 Gestión de vulnerabilidades técnicas y 5.26 Respuesta a incidentes de seguridad de la información, respectivamente.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

09-Gestión Administrativa					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	Posibilidad de afectación económica por pérdida o daño de la información física del proceso, debido a los desastres naturales o industriales.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los	Moderado	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la

09-Gestión Administrativa					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
		activos de información de la entidad.			pérdida de disponibilidad y a la afectación de la integridad de la información analizada, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 5.10 Uso aceptable de la información y otros activos asociados y 5.14 Transferencia de información respectivamente.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

10-Gestión Financiera					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	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, perdida de conocimiento de la información contenida en medios físico y digital - electrónico, por la falta de custodia o almacenamiento adecuados.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Moderado	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 6.3 Conciencia de seguridad de la información, educación y formación, 5.15 Control de acceso y 7.3 Asegurar oficinas, habitaciones e instalaciones, respectivamente.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos.					

10-Gestión Financiera					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

11-Gestión Contractual					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	Posibilidad de afectación económica y reputacional, debido a la perdida de la información contractual publicada en las plataformas contractuales del estado colombiano SECOP II y TIENDA VIRTUAL DEL ESTADO COLOMBIANO.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la pérdida de la información (Pérdida de disponibilidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. Sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 5.10 Uso aceptable de la información y otros activos asociados
Observaciones y/o recomendaciones					

11-Gestión Contractual					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

12-Gestión Documental					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	Posibilidad de pérdida reputacional debido al deterioro, destrucción, extravío o pérdida de la documentación institucional en soporte físico en archivo central	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Integridad y disponibilidad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta

12-Gestión Documental					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 5.10 Uso aceptable de la información y otros activos asociados, 7.4 Monitoreo de la seguridad física y 5.10 Uso aceptable de la información y otros activos asociados, respectivamente.
2	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	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la divulgación no autorizada de los documentos (Pérdida de confidencialidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura**: "Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 7.4 Monitoreo de la seguridad

12-Gestión Documental					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					física, 7.3 Asegurar oficinas, habitaciones e instalaciones y 5.10 Uso aceptable de la información y otros activos asociados, respectivamente.

Observaciones y/o recomendaciones

Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos.

Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001.

Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.

13-Gestión Jurídica					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	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	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	Aunque el tipo de riesgo presenta error en su identificación (Pérdida de confidencialidad), su redacción permite determinar de manera clara la afectación en los principios de la información, al hacer referencia a la pérdida de información (Pérdida de disponibilidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. Sin embargo, se recomienda mejorar la redacción con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Las vulnerabilidades identificadas para el riesgo se encuentran alineadas con lo establecido en la "Guía para la Administración del Riesgo" Código 01-GU-04 y con el Anexo 4 de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP; no obstante, se identifica una brecha en la aplicación integral de la metodología, dado que para la determinación de la **causa inmediata** no se está considerando de manera explícita la lista de amenazas definida en la citada guía, lo cual afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos metodológicos establecidos.

13-Gestión Jurídica					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
					El control implementado por el proceso se relaciona con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información.
2	Posibilidad de afectación reputacional por pérdida de información de la base de datos de acciones de tutela	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Bajo	NO APLICA	Aunque el tipo de riesgo presenta error en su identificación (Pérdida de confidencialidad), la redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la pérdida de información (Pérdida de disponibilidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Las vulnerabilidades identificadas para el riesgo se encuentran alineadas con lo establecido en la "Guía para la Administración del Riesgo" Código 01-GU-04 y con el Anexo 4 de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP; no obstante, se identifica una brecha en la aplicación integral de la metodología, dado que para la determinación de la **causa inmediata** no se está considerando de manera explícita la lista de amenazas definida en la citada guía, lo cual afecta la trazabilidad y alineación del análisis de riesgos con los lineamientos metodológicos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor					

13-Gestión Jurídica					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

14-Servicio al Usuario					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	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.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Moderado	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia a la pérdida de información (Pérdida de disponibilidad), facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del

14-Servicio al Usuario					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
					análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso y las acciones de tratamiento planificadas se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información, 8.3 Restricción de acceso a la información, 8.13 Copia de seguridad de la información y 5.18 Derechos de acceso, respectivamente. Se evidencia que la redacción de los controles existentes incluye información **sensible y específica,** como la identificación de un usuario institucional, direcciones de correo electrónico y la estructura detallada de almacenamiento en la plataforma tecnológica, pese a tratarse de un documento de carácter público. Esta situación demuestra una brecha de seguridad, al exponerse detalles operativos innecesarios que pueden ser utilizados por terceros para actividades de reconocimiento, ingeniería social o ataques dirigidos, incrementando el riesgo de compromiso de la seguridad de la información institucional.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control. Ajustar la descripción de los controles existentes, eliminando la referencia a usuarios específicos, direcciones de correo electrónico, rutas de almacenamiento y estructuras internas de los repositorios tecnológicos, teniendo en cuenta que se trata de un documento de carácter público. La actividad debe describirse de manera general y funcional, enfocándose en el proceso y no en personas o configuraciones particulares, con el fin de evitar la exposición de información sensible, reducir el riesgo de ataques de ingeniería social, phishing dirigido y reconocimiento por parte de terceros.				

15-Control Disciplinario Interno					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
1	Posibilidad de pérdida de integridad de la información y/o documentación contenida en los expedientes disciplinarios y sus anexos físicos o digitales.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Alto	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	La redacción del riesgo permite identificar de manera clara la afectación en los principios de la información, al hacer referencia explícita a la Pérdida de integridad de la información, facilitando su identificación, análisis y alineación con los lineamientos de la NTC-ISO/IEC 27001:2022 y la GUIA PARA LA ADMINISTRACIÓN DEL RIESGO 01-GU-04. Sin embargo, el riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda mejorarlo con la estructura: **"Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]"**, con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados y las acciones de tratamiento planificadas por el proceso, se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo al control 8.13 Copia de seguridad de la información, 7.2 entrada física y 6.3 Conciencia de seguridad de la información, educación y formación, respectivamente.

15-Control Disciplinario Interno					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.					

16-Evaluación y Seguimiento					
#	Descripción del riesgo	Controles existentes	Riesgo residual	Acciones de tratamiento	Análisis de brechas
1	Posibilidad de afectación reputacional debido a la pérdida o daño de la información documentada del Proceso registrada en medio físico y digital.	**Campo anonimizado.** los controles detallados asociados a cada riesgo han sido anonimizados en esta versión pública del informe, con el fin de evitar la divulgación de información que pueda ser utilizada para afectar la seguridad de los activos de información de la entidad.	Moderado	NO APLICA	En la formulación del riesgo se evidencia la combinación de dos atributos de seguridad de la información (Disponibilidad e integridad), lo cual dificulta la correcta identificación y definición de controles específicos para mitigar o prevenir el riesgo. Se recomienda desagregar el riesgo en eventos independientes, diferenciando claramente los escenarios asociados a la pérdida de disponibilidad y a la afectación de la integridad de la información analizada, con el fin de facilitar un análisis preciso en la valoración del riesgo y la definición de controles y tratamientos adecuados para cada atributo de seguridad. El riesgo formulado no relaciona claramente (impacto + causa inmediata + causa raíz) para el caso de seguridad de la información (Impacto + Amenaza + vulnerabilidad). Se recomienda reformularlo con la estructura: "**Posibilidad de [impacto] debido a la pérdida de [Principio de seguridad afectado] de [Activo de información en riesgo] por [Causa inmediata o amenaza] debido a [Causa raíz o vulnerabilidad]",** con el fin de facilitar su identificación, análisis y alineación con los lineamientos establecidos en la Guía para la Administración del Riesgo 01-GU-04. Conforme a la metodología establecida por el DAFP, se evidenció que en la identificación de los riesgos de seguridad de la información no se están considerando de manera adecuada las amenazas y vulnerabilidades definidas en la guía, o bien se presentan de forma indistinta, incorporando amenazas en el campo de vulnerabilidades y viceversa. Esta situación constituye una brecha

16-Evaluación y Seguimiento					
#	**Descripción del riesgo**	**Controles existentes**	**Riesgo residual**	**Acciones de tratamiento**	**Análisis de brechas**
					metodológica que afecta la correcta trazabilidad, consistencia y alineación del análisis de riesgos con los lineamientos establecidos. Los controles implementados por el proceso se relacionan con los controles aplicables según el Anexo A de la NTC-ISO/IEC 27001, correspondiendo a 5.18 Derechos de acceso, 8.3 Restricción de acceso a la información, 8.13 Copia de seguridad de la información y 5.10 Uso aceptable de la información y otros activos asociados, respectivamente.
Observaciones y/o recomendaciones					
Fortalecer el proceso de identificación de riesgos de seguridad de la información, incorporando las amenazas y vulnerabilidades definidas en la guía metodológica del DAFP, con el fin de garantizar la alineación metodológica en el análisis de riesgos. Redactar los riesgos en términos de afectación a los principios de seguridad de la información (Confidencialidad, Integridad o Disponibilidad), según corresponda e incluyendo la relación (impacto + causa inmediata + causa raíz) con el fin de dar una mejor claridad y precisión, describiendo el riesgo de forma concreta e indicando que aspecto específico de la información se ve amenazado, facilitando la identificación de los controles adecuados y el cumplimiento de los requisitos de la NTC-ISO/IEC 27001. Como buena práctica, se recomienda iniciar la descripción de los controles de los riesgos de seguridad de la información, con el número y descripción del control correspondiente al ANEXO A de la NTC-ISO/IEC 27001, seguido a continuación de la descripción de las actividades realizadas por el proceso para la ejecución del control.				

ADRIANA DEL PILAR GUERRA MARTÍNEZ
Directora de Tecnologías de la Información y las Comunicaciones (E)

Elaboró: Darley Ocampo García- Dirección de Tecnologías de la Información y las Comunicaciones DTIC
Revisó: Adriana Del Pilar Guerra Martínez- Dirección de Tecnologías de la Información y las Comunicaciones DTIC
Aprobó: Adriana Del Pilar Guerra Martínez- Dirección de Tecnologías de la Información y las Comunicaciones DTIC