Fecha de Emisión del Informe	Día	26	Mes	10	Año	2026

Número de Informe:	1/2
Nombre:	Informe de seguimiento al control de los riesgos relacionados con el manejo de información clasificada o reservada y mantenimiento de los controles.
Objetivo:	Realizar el seguimiento y evaluación a los riesgos de seguridad de la información, teniendo en cuenta la identificación y valoración de los riesgos, relacionados con la información reservada y clasificada con su gestión de los controles asociados.
Alcance:	Se inicia con la solicitud y recopilación de la información y concluye con el informe de evaluación al cumplimiento de controles de los riesgos de seguridad de la información.
Periodicidad:	El informe se debe realizar dos (2) veces en el año, con cortes a 30 de septiembre y a 31 de diciembre. El actual informe corresponde al primer corte de enero a septiembre de 2026.

1. MARCO JURÍDICO.

El marco normativo está relacionado con los requisitos usados como referencia al presente informe al seguimiento a los riesgos que están asociados a la seguridad de la información reservada y clasificada:

- **Ley 87 de 1993** "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"

- **Decreto 1499 de 2017** "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"

- **Ley 1712 de 2014 "**Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" como se indica en los siguientes artículos:

  ARTICULO 6 *Definiciones.*

  > d) "*Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley"*

  ARTÍCULO 19. Información exceptuada por daño a los intereses públicos.

  > *"Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias,*

siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional":

a) La defensa y seguridad nacional; (Ver Art. 2.1.1.4.2.1. Decreto 1081 de 2015)

b) La seguridad pública; (Ver Art. 2.1.1.4.2.1. Decreto 1081 de 2015)

c) Las relaciones internacionales; (Ver Art. 2.1.1.4.2.1. Decreto 1081 de 2015)

d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso; (Ver Sentencia C-951 de 2014)

e) El debido proceso y la igualdad de las partes en los procesos judiciales;

f) La administración efectiva de la justicia;

g) Los derechos de la infancia y la adolescencia;

h) La estabilidad macroeconómica y financiera del país; (Ver Art. 2.1.1.4.2.2. Decreto 1081 de 2015)

i) La salud pública.

- **Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 7**

Marco normativo del modelo integrado de planeación y gestión MIPG

1ª. Dimensión: Talento Humano

1.7 Política de Integridad

La Política de Integridad del Modelo Integrado de Planeación y Gestión (MIPG) tiene como propósito fortalecer de manera articulada, preventiva y sostenible la cultura de integridad en el servicio público, mediante la apropiación de principios, valores y comportamientos éticos orientados al interés general, la transparencia, la responsabilidad y la prevención de la corrupción. Su implementación contempla la adopción y apropiación del Código de Integridad del Servicio Público Colombiano, basado en los valores de honestidad, respeto, compromiso, diligencia y justicia; la identificación, prevención y gestión de conflictos de interés; la incorporación de acciones, metas e indicadores de integridad en los instrumentos de planeación institucional, especialmente en el Programa de Transparencia y Ética Pública (PTEP); el fortalecimiento de la gestión de riesgos para la integridad pública; y el desarrollo de actividades de sensibilización, seguimiento, evaluación y mejora continua. Asimismo, requiere articulación con las políticas de Gestión Estratégica del Talento Humano,

Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción, Participación Ciudadana y Control Interno.

3ª. Dimensión: Relación Estado - Ciudadanías

3.10 Política Gobierno Digital

La Política de Gobierno Digital, tiene como propósito impulsar la transformación digital de las entidades públicas mediante el uso y aprovechamiento de las tecnologías de la información y las comunicaciones (TIC), con el fin de fortalecer la relación Estado-ciudadanía, mejorar la prestación de servicios y generar confianza institucional. Su implementación comprende la gobernanza digital, la innovación pública digital, los habilitadores de arquitectura, seguridad y privacidad de la información, servicios ciudadanos digitales y cultura y apropiación, así como líneas de acción orientadas al desarrollo de servicios y procesos inteligentes, la toma de decisiones basada en datos y la consolidación de un Estado abierto. Igualmente, contempla iniciativas de transformación digital y estrategias de ciudades y territorios inteligentes, de acuerdo con las capacidades institucionales y los lineamientos aplicables. Desde la perspectiva de control interno, resulta necesario verificar la articulación de la política con la planeación institucional, la ejecución y seguimiento de los proyectos de transformación digital, la implementación de los habilitadores y las acciones desarrolladas para garantizar servicios digitales accesibles, confiables y seguros, así como la existencia de evidencias que permitan evaluar los resultados obtenidos, la optimización de los procesos y la generación de valor público.

4.9 Política de Seguridad Digital

La Política de Seguridad Digital, se orienta a fortalecer la protección de la información y de los activos institucionales en el entorno digital, mediante la gestión de riesgos de seguridad digital y la implementación de medidas que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información, así como a garantizar la continuidad y el funcionamiento seguro de los servicios institucionales.

Para su implementación, el Manual establece un modelo de gobernanza de seguridad digital, la gestión de riesgos, la identificación y protección de infraestructuras críticas cibernéticas y servicios esenciales, la orientación para la gestión de incidentes y el fortalecimiento de la cultura de seguridad digital. Estos componentes deben desarrollarse de manera progresiva, medible y articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI), el ciclo de mejora continua PHVA y los estándares internacionales, principalmente NIST CSF 2.0 e ISO/IEC 27001:2022. Desde la perspectiva de Control Interno, se debe verificar la identificación y tratamiento de los riesgos, la implementación y eficacia de los controles de seguridad, la capacidad de respuesta y recuperación ante incidentes, la protección de los activos de información y la existencia de evidencias que permitan evaluar el avance y la madurez de la gestión de seguridad digital, considerando los criterios diferenciales y las capacidades institucionales.

6ª. Dimensión: Seguimiento, evaluación y control integral

6.7 Política de Control Interno

La Política de Control Interno, tiene como propósito fortalecer la capacidad institucional para asegurar el cumplimiento de los objetivos, la adecuada gestión de los recursos públicos y la prevención de riesgos que puedan afectar el desempeño de la entidad, mediante la implementación del Modelo Estándar de Control Interno (MECI), articulado con la gestión institucional y la mejora continua.

Su aplicación se fundamenta en los cinco componentes del MECI: ambiente de control, evaluación del riesgo, actividades de control, información y comunicación, y actividades de monitoreo. Estos componentes deben operar de manera articulada para identificar y gestionar riesgos, establecer controles, generar información confiable y evaluar periódicamente la efectividad del sistema. La política establece que el control interno es responsabilidad de todos los servidores públicos, de acuerdo con sus funciones y responsabilidades, y no se limita a las actividades de la Oficina de Control Interno. En consecuencia, desde la perspectiva de auditoría, se debe verificar el diseño y funcionamiento de los controles, la gestión de riesgos, el seguimiento a los planes de mejoramiento, la oportunidad de las acciones correctivas y la generación de evidencias que permitan determinar si los controles contribuyen al cumplimiento de los objetivos institucionales, la transparencia, el uso eficiente de los recursos y la mejora continua.

2. ALINEACIÓN CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓIN – MIPG.

El informe de seguimiento a los controles asociados a los riesgos de seguridad de la información definidos por la Entidad se encuentra alineado con la 1ª. Dimensión: Talento Humano, 3ª. Dimensión: Relación Estado – Ciudadanías, 6ª. Dimensión: Seguimiento, evaluación y control integral, del Modelo Integrado de Planeación y Gestión – MIPG.

3. PROPÓSITO DEL INFORME.

El informe de seguimiento tiene como propósito presentar los resultados del análisis, la evaluación y el seguimiento a los controles establecidos en la matriz de riesgos de seguridad de la información, relacionados con la información clasificada y reservada, con corte al 30 de septiembre de 2026. Para ello, se verifica el cumplimiento de las actividades a cargo de los procesos y/o Direcciones Territoriales de la Unidad para la Atención y Reparación Integral a las Víctimas, tomando como referencia los entregables y las evidencias reportadas en la matriz de riesgos institucional.

El informe está dirigido a la Dirección General, a los integrantes del Comité Institucional de Control Interno y a las dependencias interesadas de la Entidad. Asimismo, constituye un insumo para los organismos de control y la ciudadanía en general, en el marco del ejercicio

del control social, de acuerdo con las condiciones de acceso y reserva de la información aplicables.

El principal aporte de este informe consiste en proporcionar información sobre la gestión realizada por los responsables de ejecutar las acciones definidas como controles para los riesgos identificados en cada proceso. Los resultados permiten a la Alta Dirección conocer el estado de implementación de dichos controles, identificar posibles brechas y adoptar decisiones oportunas y pertinentes para fortalecer la protección, custodia y tratamiento adecuado de la información y los datos institucionales de la UARIV.

4. CONTEXTO DEL INFORME.

Teniendo en cuenta la criticidad de los riesgos de seguridad de la información asociados a los activos de información clasificados y reservados, cuyo compromiso puede afectar la confidencialidad, integridad y disponibilidad de la información sensible de la Unidad, resulta necesario fortalecer los mecanismos de control orientados a prevenir accesos no autorizados, divulgación indebida, alteración, pérdida o afectación de dicha información. En consecuencia, los procesos responsables deben identificar oportunidades de mejora y adoptar las medidas necesarias para robustecer los controles existentes, en concordancia con la matriz de riesgos institucional y las disposiciones normativas aplicables en materia de protección de la información.

La gestión de estos riesgos debe desarrollarse de manera continua y dinámica, mediante el monitoreo permanente, el seguimiento sistemático a la ejecución de los controles y la implementación oportuna de ajustes cuando se identifiquen desviaciones o debilidades. Esta labor requiere el compromiso de los líderes de proceso y de los responsables de los controles, con el propósito de fortalecer la protección de la información clasificada y reservada, reducir la probabilidad de materialización de los riesgos y mitigar sus posibles efectos sobre la seguridad de la información y la continuidad de la operación institucional.

En este contexto, la Oficina de Control Interno, en ejercicio de sus funciones, analizó la información reportada por los procesos responsables sobre la ejecución de los controles asociados a los riesgos de seguridad de la información, con especial atención a la gestión adelantada por la Oficina de Tecnologías de la Información. El análisis consideró los riesgos relacionados con activos de información clasificados y reservados y sus respectivos niveles de severidad, con el fin de identificar posibles debilidades en la ejecución de los controles y formular oportunidades de mejora que contribuyan al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

5. RESULTADOS DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS.

La Oficina de Control Interno mediante correo electrónico del día 02 de septiembre solicito al líder del proceso de la Oficina de Tecnologías de la Informacion, el informe gestionado al análisis y seguimiento que se ha realizado a los riesgos relacionados con el manejo de la información con corte a septiembre del 2025, donde se indique cuáles han sido los resultados

a la ejecución de sus controles y planes de cada uno de los riesgos asociados a la seguridad de la información teniendo en cuenta su pertenencia.

Al anterior requerimiento se recibió respuesta por parte de la Oficina de Tecnologías de la Información el día 18 de septiembre a las 18:53 en donde se indica:

En atención a su solicitud, la Oficina de Tecnologías de la Información (OTI) informa que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026, aprobado por el Comité Institucional de Gestión y Desempeño, establece una periodicidad cuatrimestral para el seguimiento, así:

Periodo	Seguimiento
Enero a Abril	Mayo
Mayo a Agosto	Septiembre
Septiembre a Diciembre	Diciembre

Fuente: https://www.unidadvictimas.gov.co/wp-content/uploads/2026/01/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-de-la-Informacion-2026.pdf

En consecuencia, a la fecha (18 de septiembre de 2026) se realizó el primer seguimiento en mayo de 2026, correspondiente al periodo enero a abril. El segundo seguimiento, correspondiente al periodo mayo a agosto, se encuentra en ejecución, con recolección de información durante septiembre; por lo tanto, se estima que sus resultados y evidencias estarán disponibles en octubre de 2026. El tercer seguimiento (septiembre a diciembre) se realizará en diciembre.

Con este alcance, se remiten los resultados del primer seguimiento:

Se adjunta el informe "Primer Informe Seguimiento Riesgos SGSI - Procesos - Ene-Abr-2026.pdf", que documenta los resultados de la ejecución y seguimiento de los controles establecidos para mitigar los riesgos de cada proceso, así como el avance y cumplimiento de las acciones o planes de tratamiento definidos.

Los soportes y evidencias están disponibles, en modalidad de solo lectura, en el siguiente enlace: Seguimiento Procesos

Seguimiento a nivel de Direcciones Territoriales

Se adjunta el informe "Primer Informe Seguimiento Riesgos SGSI - DT - Ene-Abr-2026.pdf", que documenta los resultados de la ejecución y seguimiento de los controles establecidos para mitigar el riesgo identificado para las Direcciones Territoriales, así como el avance y cumplimiento de las acciones o planes de tratamiento.

Los soportes y evidencias están disponibles, en modalidad de solo lectura, en el siguiente enlace: Seguimiento DTs

Finalmente, se designa como enlace de la OTI al Ingeniero Joaquín Rojas Palomino, líder del equipo de Seguridad de la Información, para atender las inquietudes, aclaraciones o requerimientos adicionales que surjan durante las actividades de verificación y seguimiento de la Oficina de Control Interno.

La Oficina de Control Interno solicitó información adicional mediante correo electrónico enviado el día 15 de octubre a las 11:18 am de la siguiente manera:

Ingeniera Rosybel buenos días, de acuerdo con sus indicaciones en la respuesta a la solicitud de información realizada, solicitamos de su valiosa colaboración en cuanto a que nos puedan enviar el segundo seguimiento correspondiente al periodo mayo a agosto realizado por la OTI de los riesgos de seguridad de la Información, esto con el fin de complementar la información que realizara la Oficina de Control Interno en su seguimiento respectivo.

Del anterior requerimiento se recibió respuesta por parte de la Oficina de Tecnologías de la Información el día 16 de octubre a las 17:06 pm de la siguiente manera:

En atención a su solicitud, se remiten los resultados del segundo seguimiento:

1. ***Seguimiento a nivel de procesos de la Entidad (Nivel Nacional)***

   Se adjunta el informe "Segundo Informe Seguimiento Riesgos SGSI - Procesos - May-Ago-2026.pdf". Los soportes y evidencias están disponibles, en modalidad de solo lectura, en el siguiente enlace: Seguimiento Procesos

2. ***Seguimiento a nivel de Direcciones Territoriales***

   Se adjunta el informe "Segundo Informe Seguimiento Riesgos SGSI - DT - May-Ago-2026.pdf". Los soportes y evidencias están disponibles, en modalidad de solo lectura, en el siguiente enlace: Seguimiento DTs

5.1 Antecedentes

En la Matriz de riesgos implementada por la Entidad se han definido riesgos que están asociados a la información clasificada y reservada, los cuales conforme a su pertenencia y clasificación tienen unos niveles de severidad, alto, o moderado, lo cual indica la necesidad de evaluar de forma específica delimitando su pertenencia, seguimiento, control, y calificación de cumplimiento en cada uno de los procesos como se indica a continuación:

No. del Riesgo	Proceso /Dirección Territorial/Dueño del Riesgo	Tipología el Riesgo	Redacción del Riesgo	Nivel de Severidad	No. de Controles	No. de Planes de Acción
9	Control Interno Disciplinario	Seguridad Información/Digital	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Moderado	1	1
34	Gestión para la asistencia	Seguridad Información/Digital	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad e integridad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada y el uso adecuado	Moderado	1	1

No. del Riesgo	Proceso /Dirección Territorial/Dueño del Riesgo	Tipología el Riesgo	Redacción del Riesgo	Nivel de Severidad	No. de Controles	No. de Planes de Acción
			de la información			
38	Gestión Contractual	Seguridad Información/Digital	Posibilidad de pérdida económica y reputacional por pérdida a la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Alto	1	1
72	Gestión de la Información	Seguridad Información/Digital	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad,	Alto	1	1

No. del Riesgo	Proceso /Dirección Territorial/Dueño del Riesgo	Tipología el Riesgo	Redacción del Riesgo	Nivel de Severidad	No. de Controles	No. de Planes de Acción
			debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.			
93	Gestión Jurídica	Seguridad Información/Digital	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	Alto	1	1

No. del Riesgo	Proceso /Dirección Territorial/Dueño del Riesgo	Tipología el Riesgo	Redacción del Riesgo	Nivel de Severidad	No. de Controles	No. de Planes de Acción
97	Participación y visibilización	Seguridad Información/Digital	Posibilidad de pérdida económica y reputacional por perdida de disponibilidad, integridad y confidencialidad de la información, debido a la omisión, ausencia o insuficiencia de seguimiento a los controles, lineamientos y procedimientos del proceso de Participación y visibilización, para la protección y acceso controlado a la información clasificada y/o reservada.	Alto	1	1

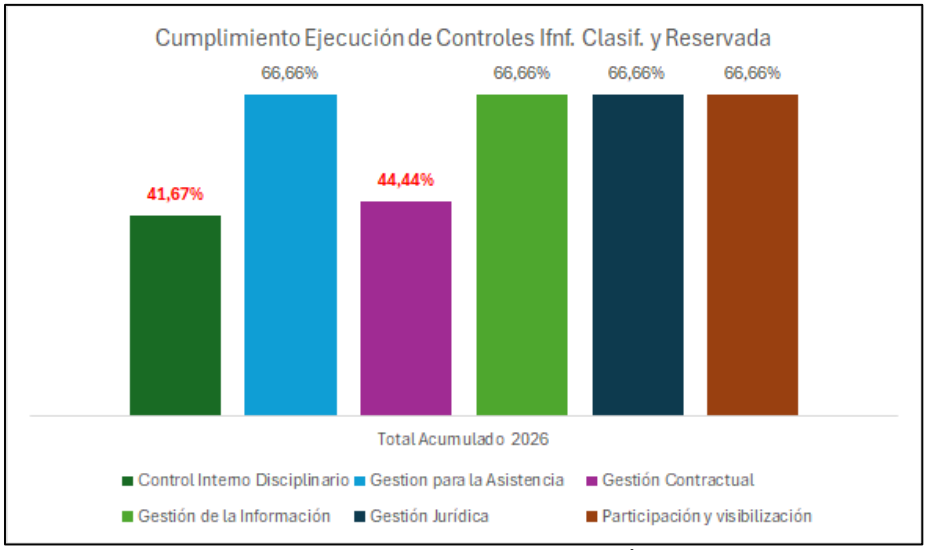
Fuente: Tabla No. 1 – Datos tomados de la Matriz de riegos de la Entidad

5.2 Análisis de la Informacion Oficina de Control Interno

Cumplimiento de ejecución de controles y planes de acción por proceso – riesgos asociados a la información clasificada y reservada

Proceso	Sigla del Proceso	Riesgos		Controles				Resultado Seguimientos 2026				
		Total Riesgos Proceso	Clasificados y Reservados	Número de Controles Proceso	Clasificados y Reservados	Número de Planes	Clasificados y Reservados	% Seguimiento Ene - Abril 33,33%	% Seguimiento May - Agosto. 33,33%	% Seguimiento Septi.- Dic. 33,33%	Total Acumulado 2026	Desviación
Control Interno Disciplinario	CID	2	1	2	1	1	1	25,00%	16,67%	0,00%	41,67%	-24,99%
Gestion para la Asistencia	GPA	1	1	1	1	1	1	33,33%	33,33%	0,00%	66,66%	0%
Gestión Contractual	GC	2	1	4	1	2	1	33,33%	11,11%	0,00%	44,44%	-22,22%
Gestión de la Información	GI	10	1	30	1	12	1	33,33%	33,33%	0,00%	66,66%	0%
Gestión Jurídica	GJ	2	1	4	2	2	1	33,33%	33,33%	0,00%	66,66%	0%
Participación y visibilización	PV	1	1	3	1	1	1	33,33%	33,33%	0,00%	66,66%	0%
Totales		**18**	**6**	**44**	**7**	**19**	**6**	**32%**	**27%**	**0%**	**58,79%**	**-7,87%**

Fuente OTI: Tabla No. 2 – Evaluación OCI



Fuente OTI: Grafica No. 1 – Evaluación OCI

De acuerdo con el seguimiento realizado a los riesgos y controles de los procesos evaluados para la vigencia 2026, se evidencia un avance acumulado del 58,79%, frente al 66,66% esperado, lo que representa una desviación negativa de 7,87% puntos porcentuales.

Los mayores rezagos se presentan en los procesos de Control Interno Disciplinario, con un avance del 41,67% y una desviación del -24,99%, y Gestión Contractual, con un avance del 44,44% y una desviación del -22,22%. Así mismo, se identifican 18 riesgos, de los cuales 6 corresponden a información clasificada y reservada, asociados a 44 controles y 19 planes registrados. Es importante precisar que el seguimiento correspondiente al periodo septiembre-diciembre aún no se ha realizado, por lo que el avance reportado del 0% para este periodo no constituye, por sí mismo, evidencia de incumplimiento.

No obstante, las desviaciones acumuladas en los periodos anteriores no pueden ser revertidas mediante el indicador actual, dado que su metodología de medición no contempla la formulación de planes de acción que permitan compensar los resultados negativos ya registrados. En este sentido, resulta fundamental que, durante el último seguimiento de la vigencia, se revisen las acciones que se vienen ejecutando, se identifiquen oportunidades de

mejora y se adopten las medidas necesarias para fortalecer el cumplimiento de las actividades programadas y así evitar la acumulación de nuevas desviaciones en pro de mejorar el resultado final del indicador con especial atención a los controles asociados a la protección de la información clasificada y reservada.

Seguimientos Definidos

Conforme a los dispuesto por la Oficina Asesora de Planeación, se debe realizar seguimiento de manera trimestral por parte de la Oficina de Tecnologías de la Información en donde se valida el cumplimiento de los controles y planes definidos por los lideres de los procesos en la matriz de riesgos de seguridad de la información, en donde están incluidos del de información clasificada y reservada, estos seguimientos están programados de la siguiente manera:

No. Seguimiento	Fecha de Corte	Calificación Evaluación	Acumulado
1	Enero - Abril	Entre 0% y 33,33%	Resultados seguimiento No. 1
2	Mayo - Agosto	Entre 0% y 33,33%	Resultado seguimiento No.1 + Resultado seguimiento No. 2
3	Septiembre - Diciembre	Entre 0% y 33,33%	Resultado Nos. 1 y 2 + resultado seguimiento No. 3

Fuente OTI: Tabla No. 3 – Programación de Seguimientos

6. ANÁLISIS DEL COMPORTAMIENTO HISTORICO.

Comparativo 2023 al 2026

Proceso	Sigla del Proceso	Calificación			
		2023	2024	2025	2026 Acumulado Septiembre
Comunicación Estratégica	CE	0%	67%	0%	N/A
Control Interno Disciplinario	CID	95%	67%	83%	41,67%
Direccionamiento Estratégico	DE	100%	81%	100%	50,00%
Evaluación Independiente	EI	100%	100%	100%	66,66%
Gestión Administrativa	GA	100%	36%	100%	66,66%
Gestión Contractual	GC	95%	63%	100%	44,44%
Gestión de la Información	GI	100%	100%	100%	66,66%
Gestión Documental	GD	83%	93%	100%	66,66%
Gestión Financiera	GF	67%	75%	100%	33,33%
Gestión Jurídica	GJ	83%	86%	100%	66,66%
Gestión para la asistencia	GPA	100%	83%	100%	66,66%
Gestión Talento Humano	GTH	100%	92%	100%	66,66%
Gestión Interinstitucional	INT	100%	89%	100%	58,33%
Participación y visibilización	PV	83%	57%	100%	66,66%
Prevención Urgente y Atención en la Inmediatez	PUAI	83%	79%	100%	33,33%
Registro y Valoración	RV	100%	78%	100%	66,66%
Relación con el Ciudadano	RC	83%	94%	100%	66,66%
Reparación Integral	RI	95%	83%	100%	58,33%
Totales		**87%**	**79%**	**99%**	**58%**

El análisis comparativo de las calificaciones de cumplimiento de los controles por proceso evidencia variaciones importantes entre las vigencias 2023, 2024 y 2025, así como un resultado acumulado a septiembre de 2026 que requiere atención por parte de los responsables de los procesos.

En términos globales, la calificación pasó del 87% en 2023 al 79% en 2024, se incrementó al 99% en 2025 y registra un 58% acumulado a septiembre de 2026. Este último resultado debe interpretarse considerando que aún está pendiente el seguimiento del último periodo de la vigencia; por tanto, no corresponde a una calificación definitiva anual. No obstante, a la fecha se registra una desviación de 8,66 puntos porcentuales sobre la totalidad de los riesgos de seguridad de la información que han sido implementados en la Entidad y definidos para la gestión de la vigencia 2026, lo que evidencia la necesidad de fortalecer las acciones de seguimiento y verificar las causas de los resultados inferiores a los obtenidos en vigencias anteriores.

El comportamiento de las calificaciones evidencia que, pese a los resultados favorables alcanzados en 2025, cuando la evaluación global llegó al 99%, en el acumulado de septiembre de 2026 se presenta una disminución al 58% de una meta del 66,66%.

Las variaciones más relevantes se observan en Gestión Financiera, Prevención Urgente y Atención en la Inmediatez, Gestión Contractual, Control Interno Disciplinario y Direccionamiento Estratégico.

Sin embargo, debe tenerse en cuenta que la calificación de 2026 es parcial y está pendiente el último seguimiento de la vigencia, por lo que los resultados actuales no constituyen una evaluación definitiva anual. A la fecha, se registra una desviación de 8,66 puntos porcentuales, situación que hace necesario revisar las causas de los resultados obtenidos, verificar las evidencias de cumplimiento y fortalecer las acciones que se encuentran en ejecución. En particular, se recomienda priorizar los procesos con calificaciones más bajas y asegurar que el seguimiento final permita establecer si las disminuciones obedecen al carácter acumulado de la medición o a debilidades reales en la ejecución y efectividad de los controles.

7. ENFOQUE BASADO EN RIESGOS.

Para este seguimiento durante los primeros seguimientos de la vigencia 2026 debe orientarse a priorizar los procesos y controles que presentan mayores niveles de exposición, considerando la cantidad de riesgos identificados, la existencia de información clasificada y reservada, la cobertura de los controles y los resultados de ejecución reportados.

De acuerdo con la información analizada, se identifican 18 riesgos, de los cuales 6 están asociados a información clasificada y reservada, así como 44 controles y 19 planes registrados. En este contexto, se debe dar prioridad a Control Interno Disciplinario, que presenta un avance acumulado del 41,67% y una desviación del -25%, y a Gestión Contractual, con un avance del 44,44% y una desviación del -22%, debido a sus rezagos en el seguimiento. Asimismo, Gestión de la Información requiere atención especial, dado que

concentra 10 de los 18 riesgos identificados y 30 de los 44 controles registrados, lo que representa una mayor concentración de responsabilidades de control.

La priorización debe complementarse con la verificación de los controles asociados a información clasificada y reservada en todos los procesos, evaluando no solo su ejecución, sino también su efectividad para prevenir accesos no autorizados, divulgación indebida, alteración o pérdida de información. Teniendo en cuenta que el seguimiento de septiembre a diciembre aún está pendiente, se recomienda orientar la última evaluación a verificar las acciones en curso, identificar las causas de las desviaciones y fortalecer los controles prioritarios, con el fin de reducir la exposición a los riesgos y evitar nuevos resultados desfavorables al cierre de la vigencia.

En cuanto a riesgos emergentes se identifica la pérdida de efectividad del control interno, la exposición de información clasificada y reservada, la concentración de riesgos en el proceso de Gestión de la Información y la detección tardía de debilidades en los controles implementados. Estas situaciones podrían incrementar la probabilidad de accesos no autorizados, divulgación indebida, alteración o pérdida de información sensible, así como limitar la capacidad institucional para detectar oportunamente desviaciones y adoptar medidas correctivas.

Adicionalmente, la persistencia de resultados desfavorables en procesos como Control Interno Disciplinario y Gestión Contractual, que registran avances acumulados del 41,67% y 44,44%, respectivamente, junto con desviaciones del -25% y -22%, evidencia la necesidad de fortalecer el seguimiento y revisar las acciones en ejecución. En este contexto, existe el riesgo de que las desviaciones se mantengan al cierre de la vigencia y afecten el cumplimiento de los objetivos institucionales y la efectividad de los controles. Estas situaciones deben validarse mediante la revisión de evidencias y la evaluación de los controles considerando que el seguimiento de septiembre a diciembre aún está pendiente de realizarse.

8. CONCLUSIONES DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS

El seguimiento efectuado a los riesgos asociados al manejo de información clasificada y reservada evidencia la necesidad de fortalecer la ejecución y efectividad de los controles establecidos para prevenir accesos no autorizados, divulgación indebida, alteración, pérdida o afectación de la disponibilidad de información sensible de la Entidad.

Si bien el informe registra un avance acumulado del 58,79% frente al 66,66% esperado, con una brecha de 7,87 puntos porcentuales, este resultado refleja el nivel de cumplimiento reportado de las actividades de control y tratamiento, pero no demuestra, por sí solo, que los riesgos estén siendo mitigados eficazmente ni que la información clasificada y reservada se encuentre suficientemente protegida.

La validación debe centrarse en establecer la correspondencia entre cada riesgo identificado, el control implementado, la actividad ejecutada y la evidencia aportada, verificando su pertinencia, suficiencia, integridad, trazabilidad y oportunidad. En particular, se requiere determinar si los controles operan de manera efectiva, si se aplican sobre los activos de

información clasificados o reservados y si sus resultados permiten reducir la probabilidad de materialización del riesgo o su impacto. La existencia de registros, reportes o actividades ejecutadas no constituye, por sí misma, evidencia concluyente de la eficacia del control.

Se identifica la necesidad de priorizar el seguimiento de los riesgos y controles relacionados con los procesos que presentan menores niveles de avance, especialmente Control Interno Disciplinario y Gestión Contractual, así como de Gestión de la Información, por su concentración de riesgos y controles. Esta priorización debe orientarse a establecer posibles debilidades en la protección de la información clasificada y reservada, particularmente frente a escenarios de acceso, consulta, modificación, transferencia, divulgación o eliminación no autorizados.

9. CONCEPTO DE CONTROL INTERNO.

La Oficina de Control Interno, con fundamento en los resultados del seguimiento a los riesgos asociados al manejo de información clasificada y reservada, considera necesario evaluar la eficacia y efectividad operativa de los controles implementados para proteger la confidencialidad, integridad y disponibilidad de esta información.

El informe identifica seis riesgos asociados a dicha categoría, de un total de 18 riesgos evaluados, y registra 44 controles y 19 planes de tratamiento. Asimismo, evidencia rezagos en los procesos de Control Interno Disciplinario y Gestión Contractual, cuyos avances reportados corresponden al 41,67% y 44,44%, respectivamente, así como la de evaluar la concentración significativa de riesgos y controles en el proceso de Gestión de la Información, con 10 riesgos y 30 controles registrados.

Estos resultados hacen necesario verificar la suficiencia del diseño de los controles, su ejecución y trazabilidad, las evidencias que soportan su cumplimiento y su contribución efectiva a la reducción del riesgo residual, con especial atención a los escenarios de acceso, consulta, modificación, divulgación, transferencia o pérdida no autorizados de información clasificada y reservada.

Esta evaluación debe enmarcarse en las disposiciones de la Ley 1581 de 2012, en particular los principios de seguridad y confidencialidad y el deber de implementar medidas técnicas, humanas y administrativas para proteger los datos personales; la Ley 1712 de 2014, en lo relacionado con la protección de la información pública clasificada y reservada y las restricciones legales de acceso; y la Ley 87 de 1993, respecto de la responsabilidad de establecer, mantener y evaluar el Sistema de Control Interno.

De igual manera, corresponde verificar la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI) y de las disposiciones expedidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que resulten aplicables a la Entidad, así como también tener en cuenta la Resolución 500 de 2021, su modificación mediante la Resolución 2277 de 2025 y la Resolución 746 de 2022, en lo que permanezca vigente y sea pertinente.

En este contexto, la Oficina de Control Interno recomienda que los seguimientos efectuados por el proceso responsable no deben limitarse a medir el porcentaje de ejecución de las actividades programadas, sino establecer, mediante evidencia suficiente, pertinente, íntegra y verificable, si los controles operan conforme a su propósito, si responden a la criticidad de la información protegida y si reducen la probabilidad de materialización de los riesgos y sus posibles impactos.

Por lo tanto, se requiere priorizar la revisión de los controles asociados a la información clasificada y reservada, determinar las causas de los rezagos identificados y fortalecer las acciones de tratamiento y monitoreo, de manera que la Entidad pueda demostrar la protección efectiva de esta información y la mejora continua de su gestión de seguridad y privacidad.

APROBÓ



JEFE OFICINA DE CONTROL INTERNO

Elaborado:
Basco Ricaurte Guerra
Contratista Oficina de Control Interno

Anexo 1 Control de cambios

Versión	Fecha de Cambio	Descripción de la modificación
1	04/08/2014	Creación del formato.
2	09/03/2015	Al revisar el formato se evidencia que la casilla fecha de informe está repetida.
3	02/08/2017	Se modifica formato y se adiciona firma aprobación del jefe Oficina de Control Interno.
4	30/04/2020	Se actualiza formato, se ajusta la distribución del texto en filas y columnas, las fuentes y fecha de la tabla control de cambios.
5	28/10/2022	Se actualiza el formato en pie de página con los logos de certificación asociados al sistema de gestión de calidad ISO 9001:2015, ambiental ISO 14001:2015, seguridad y

		salud en el trabajo ISO 45001:2018 seguridad de la información ISO 27001:2013.
6	19/07/2024	Se actualiza el formato es su estructura de contenido, de acuerdo con los requerimientos de la Oficina de Control Interno.