Fecha de Emisión del Informe	Día	24	Mes	02	Año	2026

Número de Informe:	2/2
Nombre:	Informe de seguimiento al control de los riesgos de seguridad de la Información de la UARIV
Objetivo:	Realizar el seguimiento y evaluación a los riesgos de seguridad de la información, teniendo en cuenta la identificación y valoración de los riesgos, así como el diseño de controles y su gestión.
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 junio y a 31 de diciembre de la vigencia. El actual informe corresponde al segundo corte de julio a diciembre de 2025.

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 6

Marco normativo del modelo integrado de planeación y gestión

1ª. Dimensión: Talento Humano

1.3 Política de Integridad

la apropiación de los valores del servicio público.

fortalecer e integrar mecanismos, instrumentos administrativos y orientaciones que garanticen la idoneidad en la prestación del servicio

3ª. Dimensión: Gestión con valores para resultados

3.3.4 Política Gobierno Digital

La Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública.

3.4.2 Política de Seguridad Digital

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

7ª. Dimensión: Control Interno

7.1 Alcance de esta Dimensión

Control Interno

Lineamientos generales para la implementación

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

Este informe de seguimiento a la controles de los riesgos definidos por la Entidad, en cuanto a seguridad de la información esta alineado con las dimensiones 3° de gestión con valores para el resultado y 7° de control interno y contribuye a las directrices de la Política de Gestión y Desempeño Institucional, específicamente la política de Fortalecimiento organizacional y simplificación de procesos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG adoptado por Unidad para las Victimas).

3. PROPÓSITO DEL INFORME.

El presente informe de seguimiento tiene como propósito presentar el resultado del análisis, evaluación y seguimiento a los controles implementados en la matriz de riesgos asociados a la seguridad de la Información, con corte al 31 de diciembre del 2025, donde se verifica el cumplimiento de las actividades que deben ejecutar los procesos y/o Direcciones Territoriales de la UARIV, conforme a los entregables gestionados y reportados en la matriz de riesgos de la Entidad.

El informe está dirigido a la Dirección General, los integrantes del Comité Institucional de Control Interno, y dependencias interesadas. Son también destinatarios los entes de control y a los ciudadanos en general que deseen hacer control social.

El principal impacto de este informe es conocer la gestión desplegada por los responsables de la ejecución de las acciones planteadas como controles en los riesgos indicados en cada proceso, que le permite a la Alta Dirección tomar decisiones oportunas, pertinentes y conducentes para asegurar la adecuada custodia y tratamiento de la información y datos de la UARIV.

4. CONTEXTO DEL INFORME.

Teniendo en cuenta la importancia que representa todo lo relacionado con los riesgos asociados a la seguridad de la Información, los cuales pretenden de alguna manera permitir a los procesos garantizar un manejo y control de las posibles situaciones que impacten las diferentes metas y responsabilidades en cumplimiento de la misionalidad de la Entidad, y más aún el aseguramiento de los datos que se gestionan

en la UARIV, por lo tanto, es necesario visualizar y tener en cuenta las oportunidades de mejora que se puedan ejercer a los controles de los riesgos planteados con el objetivo de madurar y gestionar de una manera eficiente los riesgos de seguridad de la información según la matriz de riesgos emitida por parte de la Entidad asegurando su efectividad y eficacia.

Adicionalmente a lo indicado, es importante recordar que la gestión de los riesgos es un proceso de evaluación y maduración continuo, siendo esto de vital importancia para la Entidad donde se requiere monitoreo, seguimiento, control y ajustes constantes por parte de los lideres de los procesos para asegurar la sostenibilidad y el éxito de los procesos implementados en la Entidad permitiendo que las brechas de materialización de los riesgos sean mínimas para cada uno de los procesos de la Entidad.

La Oficina de Control Interno en cumplimiento de sus funciones a determinado realizar un análisis de la información de los procesos responsables de controlar y realizar seguimiento a los riesgos de seguridad de la información como son la Oficina de Tecnologías de la Información y la Subdirección Red Nacional de la Información. en donde se evalúa cada uno de los riesgos de mayor impacto con la seguridad de la información y específicamente la reservada y clasificada y el nivel de severidad de cada uno de estos riesgos.

Por su parte y teniendo como referente COBIT se deben asumir los riesgos de la información como un elemento integral de la gobernanza y gestión empresarial, no solo de TI, alineando la seguridad con los objetivos estratégicos. Se basa en identificar y gestionar la probabilidad de que amenazas impacten la confidencialidad, integridad o disponibilidad de los datos. Utiliza enfoques proactivos, evaluando riesgos continuamente y aplicando controles de seguridad.

5. RESULTADOS DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS.

La Oficina de Control Interno mediante correo electrónico del día 02 de febrero 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 diciembre 31 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 16 de febrero a las 16:37 en donde se indica:

> *"En atención a su solicitud, se remiten los siguientes informes de seguimiento generados en el segundo semestre de 2025, en relación con los controles y planes establecidos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la mencionada vigencia"*
>
> 1. *Informe 2DO Seguimiento Riesgos SGSI-Procesos May-Agos-2025.pdf*
> 2. *Informe 3ER Seguimiento Riesgos SGSI-Procesos Sep-Dic-2025 v2.pdf*

Adicionalmente, se habilitó acceso (consulta) a los soportes consolidados para dichos seguimientos:

2do Seguimiento: 2do Seguimiento Procesos 2025

3er Seguimiento: 3er Seguimiento Procesos 2025

Adicionalmente la Oficina de Control Interno solicito información complementaria mediante correo electrónico enviado el día 17 de marzo a las 10:27 am de la siguiente manera:

Ingenieros buenos días, de antemano agradecemos su oportuna respuesta a la información requerida, por otra parte, les solicitamos de la manera más atenta se nos envié el informe del primer seguimiento efectuado y la matriz de riesgos de seguridad de la información que fue tenida en cuenta para estos informes.

De igual manera se dé respuesta a las siguientes inquietudes:

La matriz de riesgos actualizada vigente para el año 2026 que fecha fue sensibilizada o socializada a los procesos.

los cambios en los riesgos que tienen un impacto negativo fueron soportados por los procesos? cuales evidencias fueron tenidas en cuenta?

Del anterior requerimiento se recibió respuesta por parte de la Oficina de Tecnologías de la Información el día 18 de febrero a las 10:46 am de la siguiente manera:

En atención a su solicitud me permito remitir:

Informe 1ER Seguimiento Riesgos SGSI-Procesos Ene-Abr-2025.pdf

- *Enlace de soportes del 1er seguimiento: 1er Seguimiento Procesos 2025*
- *Enlace matriz de riesgos fuente para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información: https://www.unidadvictimas.gov.co/documentos_bibliotec/mapa-de-riesgos-institucional-corrupcion-y-gestion-v2-2025/*
- *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 (Fuente para los informes de seguimiento): https://www.unidadvictimas.gov.co/documentos_bibliotec/plan-tratamiento-riesgos-de-seguridad-de-la-informacion-2025/*

Respecto a las inquietudes adicionales:

1. *La matriz de riesgos actualizada vigente para el año 2026 que fecha fue sensibilizada o socializada a los procesos.*

Respuesta:
Según el Procedimiento de administración de riesgos versión 8 del 4/12/2023, la actividad Socializar el mapa de riesgos al interior del proceso o DT´s, está a cargo del Enlace SIG del Proceso o Dirección Territorial. Por otra parte, el mismo procedimiento establece que la actividad Publicar y divulgar el mapa de riesgos institucional, está asignada a la Oficina Asesora de Planeación. En este sentido, desde el Sistema de Gestión

de Seguridad de la Información se apoya con la identificación y valoración de riesgos SGSI según las fechas establecidas en el marco del Plan de Implementación SIG 2025: https://www.unidadvictimas.gov.co/documentos_bibliotec/plan-de-implementacion-2025/

En este sentido, la actualización de riesgos para la vigencia 2026, según el Plan de Implementación SIG se programó para los meses de julio a septiembre de 2025.

En caso de requerir más información en relación con la sensibilización o socialización a los procesos, podríamos realizar una mesa de trabajo para abordar los soportes documentados en articulación con la Oficina Asesora de Planeación.

2. *¿Los cambios en los riesgos que tienen un impacto negativo fueron soportados por los procesos? cuales evidencias fueron tenidas en cuenta?*

   Respuesta:

   La atención de impactos negativos asociados a la gestión de riesgos se soporta directamente desde cada proceso, de acuerdo con el escenario específico que se presente, así:

   a. *Actualización de riesgos, controles y/o planes de tratamiento:*
      Cuando el impacto negativo se relaciona con cambios en la exposición al riesgo derivados de la actualización de riesgos, controles o planes de tratamiento, esta gestión es responsabilidad del propio proceso. La actualización es realizada por el Enlace SIG y cuenta con la aprobación del líder de proceso. Como evidencia se dispone de las actas de actualización de riesgos correspondientes a la vigencia 2026.
   b. *No ejecución de controles o planes de tratamiento:*
      En los casos en que el impacto negativo se origine por la no ejecución de controles o planes de tratamiento, el soporte también recae en el proceso involucrado. Durante las actividades de seguimiento, el proceso documenta el reporte de ejecución de las actividades, mientras que la Oficina de TI realiza la revisión de los soportes y retroalimenta oportunamente cualquier desviación o situación identificada.
   c. *Materialización del riesgo:*
      Cuando el impacto negativo corresponde a la materialización de un riesgo, la gestión es asumida por el proceso específico conforme a lo establecido por la OAP en el Procedimiento de administración de riesgos, versión 8 del 04/12/2023. En este escenario, el Enlace SIG del proceso debe diligenciar el Formato de monitoreo a la materialización de riesgos, en el marco de la actividad de monitoreo definida en dicho procedimiento.

      En todos los casos, los procesos actúan como primera línea de defensa, garantizando la trazabilidad, documentación y atención oportuna de los riesgos y sus impactos.

Adicionalmente la Oficina de Control Interno solicito información adicional mediante correo electrónico enviado el día 17 de marzo a las 10:27 am de la siguiente manera:

5.1 Antecedentes

Matriz de Riesgos Actualizada – Vigencia 2026

Proceso	Sigla del Proceso	Riesgos						Controles		
		Número de Riesgos	% de participacion por proceso	Nivel de Severidad de los riesgos				Número de Controles	Porcentaje de Participacion por controles	Número de Planes
				Alto	Moderado	Extremo	Bajo			
Comunicación Estratégica	CE	0	-	-	-	-	-	-	-	-
Control Interno Disciplinario	CID	2	6%	1	1	-	1	3	4%	1
Direccionamiento Estratégico	DE	1	3%	1	-	-	-	2	3%	2
Evaluación Independiente	EI	2	6%	-	1	-	-	3	4%	-
Gestión Administrativa	GA	2	6%	-	2	-	-	6	8%	1
Gestión Contractual	GC	2	6%	1	1	-	-	4	5%	2
Gestión de la Información	GI	10	31%	3	3	2	2	30	38%	12
Gestión Documental	GD	1	3%	-	-	1	-	3	4%	2
Gestión Financiera	GF	2	6%	-	2	-	-	4	5%	3
Gestión Interinstitucional	GI	1	3%	-	1	-	-	3	4%	1
Gestión Jurídica	GJ	2	6%	2	-	-	-	4	5%	2
Gestión para la asistencia	GPA	1	3%	-	1	-	-	1	1%	2
Gestión Talento Humano	GTH	1	3%	-	1	-	-	2	3%	1
Participación y visibilización	PV	1	3%	1	-	-	-	3	4%	1
Prevención Urgente y Atención en la Inmediatez	PUAI	0	0%	-	-	-	-	0	0%	0
Registro y Valoración	RV	1	3%	1	-	-	-	4	5%	1
Relación con el Ciudadano	RC	1	3%	1	-	-	-	3	4%	3
Reparación Integral	RI	1	3%	1	-	-	-	3	4%	1
Transversal Sistema de Seguridad y Privacidad de la información	TSSI	1	3%	1	-	-	-	1	1%	2
Total		32	100%	13 41%	13 41%	3 9%	3 9%	79	100%	37

Fuente: Tabla No. 1 – Datos tomados de la Matriz de riegos de la Entidad actualizada - 2026

A la fecha de corte del seguimiento, la matriz de riesgos donde se clasifican los riesgos de seguridad de la información presenta variaciones para la vigencia 2026 conforme a la actualización realizada, donde se presentan los siguientes aspectos:

- En el proceso de Comunicación Estratégica y Prevención urgente y atención a la Inmediatez no poseen riesgos de seguridad de la información.
- En algunos procesos se disminuyeron los riesgos
- En algunos riesgos cambio la calificación del nivel de severidad
- En algunos riesgos se disminuyeron los controles implementados
- En algunos riesgos se disminuyeron los planes de acción

Lo anteriormente indicado evidencia la necesidad de validar y documentar las causas de cada cambio (mitigación efectiva, reclasificación o error), restablecer o reforzar controles y planes de acción.

Se hace necesario tener en cuenta las siguientes recomendaciones cuando los aspectos de seguimiento y control sufren una serie de variaciones que representa a los procesos una menor gestión o que no se haya representado una eficacia o efectividad que garantice una probabilidad de materialización de los riesgos.

- Verificar y documentar la justificación de cada cambio.
- Reajustar la identificación, valoración y tratamiento de riesgos asegurando la coherencia con los criterios y la metodología como lo indica la guía de la Función Pública
- Asegurar Trazabilidad y evidencia para todas las decisiones y ajustes.

Matriz de Riesgos análisis de la Información del presente informe – Vigencia 2025

Proceso	Sigla del Proceso	Riesgos		Controles		
		Número de Riesgos	Porcentaje de Participacion por Proceso	Número de Controles	Porcentaje de Participacion por controles	Número de Planes
Comunicación Estratégica	CE	0	0%	0	0%	0
Control Interno Disciplinario	CID	2	6%	3	4%	1
Direccionamiento Estratégico	DE	1	3%	1	1%	1
Evaluación Independiente	EI	2	6%	2	3%	0
Gestión Administrativa	GA	2	6%	6	8%	1
Gestión Contractual	GC	2	6%	4	5%	2
Gestión de la Información	GI	10	30%	30	38%	12
Gestión Documental	GD	1	3%	3	4%	2
Gestión Financiera	GF	2	6%	4	5%	2
Gestión Interinstitucional	GI	1	3%	2	3%	1
Gestión Jurídica	GJ	2	6%	4	5%	2
Gestión para la asistencia	GPA	2	6%	2	3%	2
Gestión Talento Humano	GTH	1	3%	2	3%	1
Participación y visibilización	PV	1	3%	3	4%	1
Prevención Urgente y Atención en la Inmediatez	PUAI	1	3%	3	4%	1
Registro y Valoración	RV	1	3%	4	5%	1
Relación con el Ciudadano	RC	1	3%	3	4%	3
Reparación Integral	RI	1	3%	3	4%	1
Gestión del Cononocimiento y la Innovación (nuevo)	GCI	0	0%	0	0%	0
Totales		**33**	**100%**	**79**	**100%**	**34**

Fuente: Tabla No. 2 – Datos tomados de la Matriz de riegos de la Entidad – 2025

5.2 Análisis de la Informacion Oficina de Control Interno

Como se puede observar en la anterior tabla se evidencia una existencia de 33 riesgos en seguridad de la información, los cuales conforme a su definición y características implementadas cuentan con 79 controles y 34 planes a los cuales se les realiza un seguimiento de manera trimestral donde se evalúa el cumplimiento de los controles y sus planes conforme a los propuesto por cada uno de los responsables del proceso, adicionalmente conforme a su clasificación en cuanto a su nivel de severidad encontramos lo siguiente:

Nivel de Severidad de los riesgos				
Descripción	Extremo	Alto	Moderado	Bajo
No. Riesgos	1	10	13	9
% Participacion	9%	41%	41%	9%

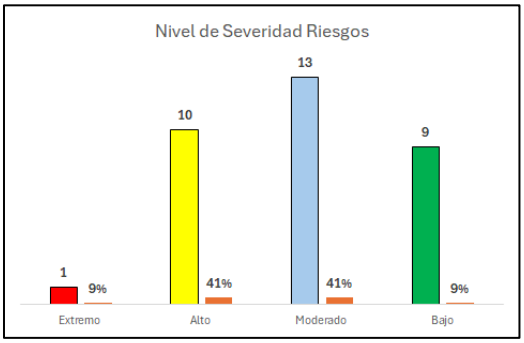


Tabla No. 3 – Datos tomados de la Matriz de riegos de la Entidad

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, estos seguimientos están programados de la siguiente manera:

No. Seguimiento	Fecha de Corte	Calificación Evaluación	Acumulado
1	Enero - Abril	Entre 0% y 33,33%	Resultado Seguimiento 1
2	Mayo - Agosto	Entre 0% y 33,33%	Resultado Seguimiento 1 + Resultado Seguimiento 2
3	Septimbre- Diciembre	Entre 0% y 33,33%	Suma del resultado 1 y 2 + Resultado Seguimiento 3

Fuente OTI: Tabla No. 4 – Programación de Seguimientos

Metodología de Calificación seguimiento

Teniendo en cuenta lo indicado por la Oficina de Tecnologías de la Información, la metodología implementada para la calificación de los seguimientos al cumplimiento de los controles y planes se fundamenta en la sumatoria del número de controles gestionados y del número de planes gestionados por cada proceso.

Posteriormente, este resultado se divide entre la calificación esperada, de acuerdo con el nivel de cumplimiento reportado en cada seguimiento efectuado, conforme a la siguiente fórmula:

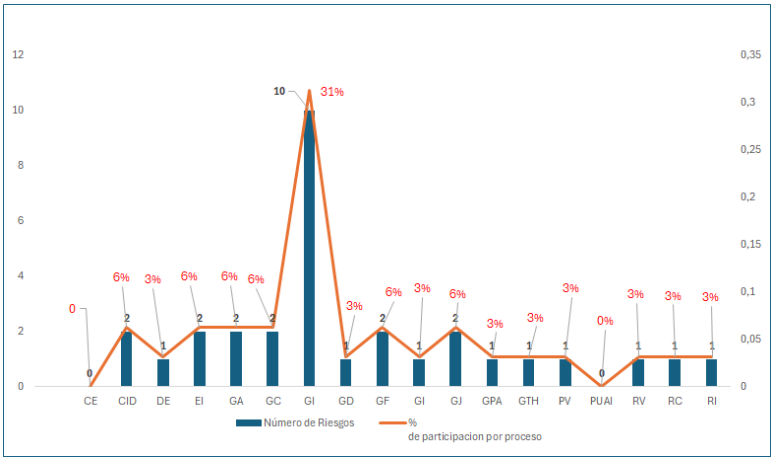
Número de Controles Gestionados + Número de Planes Gestionados /Calificación Esperada

Ejemplo:

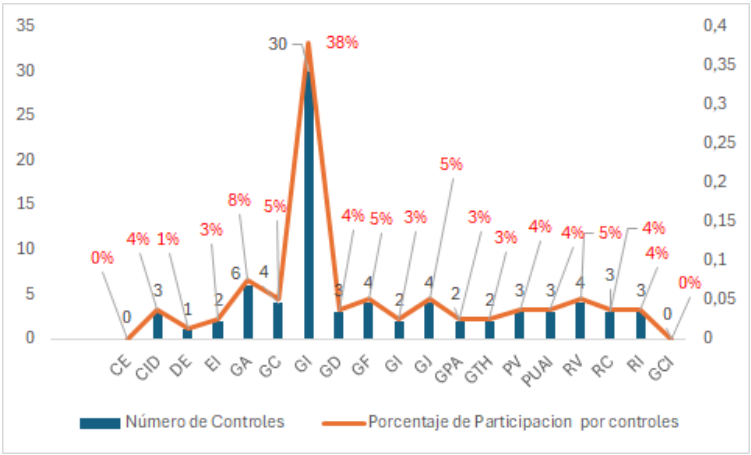
Proceso	Número de Controles	Número de Planes	Indicador Calificación (NC+NP)	Calificación Esperada	Valor por Indicador (NC+NP/Calificación Esperada
Comunicación Estratégica	1	1	2	33,33%	16,67%

Como se evidencia en el ejemplo anterior, la metodología aplicada no permite asignar calificaciones parciales con base en los indicadores previamente expuestos. En consecuencia, las calificaciones deben ser cerradas, en función del cumplimiento total en la entrega de los soportes establecidos para cada uno de los controles y planes de acción.

Participación de Riesgos por Procesos



Participación de Controles por Procesos



Como se puede observar en la anteriores graficas el proceso que cuenta con mayor número de riesgos y controles es el de **Gestión de la Información** determinando un impacto alto para las dependencias responsables de garantizar un adecuado manejo de los riesgos.

Cumplimiento de Ejecución de Controles y Planes de Acción por Proceso – Riesgos de Seguridad de la Información.

Proceso	Sigla del Proceso	Riesgos		Controles			Calificación Seguimientos 2025				
		Número de Riesgos	Porcentaje de Participacion por Proceso	Número de Controles	Porcentaje de Participacion por controles	Número de Planes	% Seguimiento Ene - Abril 33,33%	% Seguimiento May - Julio. 33,33%	% Seguimiento Agost.- Dic. 33,33%	Total Acumulado 2025	Desviación
Comunicación Estratégica	CE	0	0%	0	0%	0	0%	0%	0%	0%	-
Control Interno Disciplinario	CID	2	6%	3	4%	1	33,33%	25,00%	25,00%	83%	-17%
Direccionamiento Estratégico	DE	1	3%	1	1%	1	33,33%	33,33%	33,33%	100%	
Evaluación Independiente	EI	2	6%	2	3%	0	33,33%	33,33%	33,33%	100%	-
Gestión Administrativa	GA	2	6%	6	8%	1	33,33%	33,33%	33,33%	100%	-
Gestión Contractual	GC	2	6%	4	5%	2	33,33%	33,33%	33,33%	100%	-
Gestión de la Información	GI	10	30%	30	38%	12	33,33%	33,33%	33,33%	100%	-
Gestión Documental	GD	1	3%	3	4%	2	33,33%	33,33%	33,33%	100%	-
Gestión Financiera	GF	2	6%	4	5%	2	33,33%	33,33%	33,33%	100%	-
Gestión Interinstitucional	GI	1	3%	2	3%	1	33,33%	33,33%	33,33%	100%	-
Gestión Jurídica	GJ	2	6%	4	5%	2	33,33%	33,33%	33,33%	100%	-
Gestión para la asistencia	GPA	2	6%	2	3%	2	33,33%	33,33%	33,33%	100%	-
Gestión Talento Humano	GTH	1	3%	2	3%	1	33,33%	33,33%	33,33%	100%	-
Participación y visibilización	PV	1	3%	3	4%	1	33,33%	33,33%	33,33%	100%	-
Prevención Urgente y Atención en la Inmediatez	PUAI	1	3%	3	4%	1	33,33%	33,33%	33,33%	100%	-
Registro y Valoración	RV	1	3%	4	5%	1	33,33%	33,33%	33,33%	100%	-
Relación con el Ciudadano	RC	1	3%	3	4%	3	33,33%	33,33%	33,33%	100%	-
Reparación Integral	RI	1	3%	3	4%	1	33,33%	33,33%	33,33%	100%	-
Gestión del Cononocimiento y la Innovación (nuevo)	GCI	0	0%	0	0%	0	0%	0%	0%	0%	-
Totales		**33**	**100%**	**79**	**100%**	**34**	**33%**	**33%**	**33%**	**99,0%**	**-1%**

Tabla No. 5 – Análisis Cumplimiento Controles y Planes por proceso 2025

La anterior tabla conforme a la información suministrada por los responsables de los seguimientos a los riesgos de seguridad de la Información, presenta que un (1) proceso no alcanzan la meta del 100% siendo este el proceso de Control Interno Disciplinario alcanzando una calificación del 83%, los demás procesos evidencian un cumplimiento del 100% en su gestión de controles y planes definidos en la matriz de riesgos de seguridad de la información, sin embargo se presente que, los procesos de Comunicación Estratégica y Gestión del Conocimiento y la Innovación no reportan riesgos de seguridad y por ende ni controles ni planes, arrojando como resultado un cumplimiento consolidado de la siguiente manera:

Calificación	No. Procesos
0% a 50%	0
51% a 75%	0
76% a 95%	1
96% a 100%	16

Se hace necesario que los procesos que actualmente no reportan riesgos de seguridad de la información realicen un análisis conjunto con la Oficina de Planeación y la Oficina de Tecnologías de la Información, con el fin de validar la pertinencia de los riesgos que deben asociarse a sus funciones, obligaciones y a la información que gestionan.

Cabe resaltar la importancia de efectuar una adecuada identificación y definición de estos riesgos, considerando la misionalidad de la Entidad y la naturaleza sensible y crítica de la información que administra.

6. **ANÁLISIS DEL COMPORTAMIENTO HISTORICO**.

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

Tabla No. 6 – Comportamiento Histórico

De acuerdo con el análisis del comportamiento de gestión de los riesgos de información de los procesos durante las vigencias 2023, 2024 y 2025, se evidencia una dinámica institucional marcada por un ciclo de estabilidad, descenso y recuperación.

En la vigencia 2023 la Entidad presentó un nivel de cumplimiento alto (87%), con la mayoría de los procesos ubicados en rangos iguales o superiores al 80%, lo que reflejaba un desempeño adecuado en la implementación y seguimiento de los lineamientos evaluados.

Para 2024 se observa una disminución general del desempeño (79%), caracterizada por caídas significativas en varios procesos estratégicos y de apoyo. Esta variación negativa sugiere debilidades en la sostenibilidad del cumplimiento, posibles ajustes metodológicos en la medición o deficiencias en el reporte y soporte de evidencias.

En contraste, la vigencia 2025 muestra una recuperación sustancial (99%), con la mayoría de los procesos alcanzando el 100% de cumplimiento, lo que denota un fortalecimiento en los mecanismos de seguimiento, control y gestión interna. Este comportamiento evidencia capacidad de mejora institucional y respuesta efectiva frente a las brechas identificadas en la vigencia anterior.

No obstante, persisten alertas puntuales en procesos específicos que presentan comportamientos inestables o recuperaciones parciales, lo cual requiere análisis focalizado para garantizar la sostenibilidad del cumplimiento en el tiempo.

En términos generales, la evaluación permite concluir que la Entidad demuestra capacidad de corrección y mejora continua; sin embargo, es necesario fortalecer la estabilidad y consistencia del desempeño para evitar fluctuaciones significativas entre vigencias y asegurar un cumplimiento estructural y sostenido.

7. ENFOQUE BASADO EN RIESGOS.

La Oficina de Control interno, luego de revisar el nivel de cumplimiento y efectividad de los seguimientos propuestos en la vigencia 2025 encuentra los siguientes posibles riesgos que tiene la Entidad en lo que respecta a los riesgos de seguridad de la Información de la siguiente manera:

1. Posibilidad de que los procesos no identifiquen de manera integral los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información, generando vacíos en la gestión preventiva

2. Posibilidad de que los controles definidos en los procesos no reduzcan realmente la probabilidad o el impacto del riesgo, limitándose a un cumplimiento documental.

3. Posibilidad de que las acciones correctivas o preventivas definidas no se ejecuten dentro de los plazos establecidos.

4. Falta de gestión y control por parte de los líderes de los procesos en el cumplimiento de la entrega de evidencias o soportes de los controles y planes de acción asociados a la seguridad de la información.

5. Falta de aplicación de metodologías en la evaluación y seguimiento de los controles y planes establecidos en materia de seguridad de la información, lo que impide obtener una medición precisa de los indicadores y puede dar lugar a la materialización de riesgos asociados a los procesos del sistema integrado de gestión de la UARIV.

6. Falta de sensibilización sobre el manejo, administración, seguimiento y control de los riesgos de seguridad de la información, lo que impide identificar de manera específica las principales situaciones que podrían llevar a la materialización de los riesgos.

7. Falta de identificación y tratamiento de riesgos asociados a potenciales ransomware, especialmente en aquella información sensible de la entidad como es la directamente relacionada con las victimas

8. CONCLUSIONES DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS

El análisis y validación de evidencias permite concluir que el sistema de seguimiento presenta un nivel de cumplimiento alto y consistente (99%), evidenciando apropiación institucional del modelo de gestión de riesgos y controles. No obstante, se identifican oportunidades de mejora en:

- El cierre oportuno del proceso con desviación (Control Interno Disciplinario).
- La revisión y posible actualización del mapa de riesgos en procesos que reportan ausencia de riesgos y controles.
- El fortalecimiento cualitativo de la validación de evidencias para asegurar que el cumplimiento no sea únicamente formal sino sustancial.

En términos generales, el estado del seguimiento es favorable, con una leve desviación que puede ser corregida mediante acciones puntuales de mejora y seguimiento reforzado en los procesos con brechas identificadas.

9. CONCEPTO DE CONTROL INTERNO.

Si bien el resultado consolidado de la vigencia 2025 (99% de cumplimiento) refleja un desempeño institucional favorable, el control interno no se limita al resultado cuantitativo. Su verdadero alcance radica en asegurar que los controles reduzcan efectivamente la probabilidad e impacto de los riesgos sobre la confidencialidad, integridad y disponibilidad de la información, especialmente aquella catalogada como reservada o clasificada.

El control a la información y los datos a través de los riesgos son escenarios excepcionales que deben mantener sus lineamientos y requerimientos garantizando una adecuada gestión minimizando su materialización.

La gestión de la información en las entidades públicas debe desarrollarse bajo el principio general de publicidad y transparencia, atendiendo siempre a su nivel de clasificación y a las disposiciones legales que regulan su acceso. Cuando se trate de información reservada o clasificada, su restricción debe estar debidamente sustentada en criterios normativos claros y verificables, lo que otorga relevancia a los ejercicios de seguimiento y evaluación como el presente.

En este sentido, el adecuado control de la información exige un proceso previo de reconocimiento y clasificación, basado en el análisis del marco jurídico aplicable, las tablas de retención documental y la identificación formal de los activos de información. Esta gestión integral permite asegurar el cumplimiento de la normativa archivística, fortalecer la seguridad de la información y proteger los datos institucionales, garantizando un equilibrio entre el deber de transparencia y la obligación de salvaguardar la información sensible.

De lo anterior, y a partir del análisis de las evidencias y la información suministrada, se tiene que para la Oficina de Control Interno, el comportamiento institucional según la evaluación de los seguimientos a los riesgos de seguridad de la información efectuados en la vigencia 2025 presenta una calificación del 99%

presentando una desviación negativa del 1% que permite colegir que se han adelantado las acciones y gestiones pertinentes de seguimiento y control que permiten la obtención una calificación favorable, es necesario que las acciones de seguimiento, control y sensibilización se sigan gestionando con el propósito de fortalecer el objetivo y poder garantizar que los niveles de calificación de los procesos se cumplan según lo programado y lo dispuesto por la Oficina Asesora de Planeación, lo que implica por parte de la Oficina de Control Interno realizar una evaluación independiente para genera un valor agregado en su sistema de control interno y posibles acciones de mejoramiento.

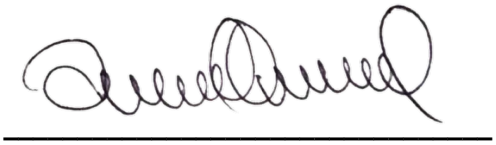
No obstante, y teniendo una visión holística de la seguridad de la información, es importante que la Oficina de Tecnologías de la Información acompañe con mayor frecuencia, rigor, y fortaleza técnica a cada uno de los procesos institucionales y dependencias en la identificación de riesgos, no dejando esa responsabilidad en los enlaces SIG, cual cuales no necesariamente son ingenieros de sistemas o personas versadas en estos especiales riesgos. Este acompañamiento tampoco se debe dejar como responsabilidad de la Oficina Asesora de Planeación, que, si bien tiene la metodología del DAFP sobre riesgos, está aún carece de la fortaleza en riesgos de la información en los escenarios contemporáneos.

Es recomendable que la OTI explore cotidianamente las nuevas tendencias de riesgos en materia de aseguramiento de la información, y trasmita esos datos a los procesos que potencialmente pueden ser afectos a ellos. En este escenario también es importante estar constantemente actualizados el los controles ante esos nuevísimos riesgos, aspecto que desde la Oficina de Control Interno se observa como una debilidad de la OTI para con la entidad.

De igual manera, es necesario que se haga una identificación de riesgos asociados al uso de la inteligencia artificial, la cual es incipiente en la entidad, pero no por ello importante, para el efecto, y solo como uno de muchos instrumentos internacionales, recomendamos mirar los 10 riesgos identificados por la IBM en el siguiente enlace.
https://www.ibm.com/es-es/think/insights/10-ai-dangers-and-risks-and-how-to-manage-them

Para finalizar, es necesario que tanta la OTI, la RED y la entidad en su conjunto tenga claro y presente que el principal y más costoso de sus activos es la información y por lo tanto la Oficina de Control Interno invita a que se tomen todas las precauciones para proteger ese activo.

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.