Comercio, Industria y Turismo

OFICINA DE CONTROL INTERNO
OCI-018-2025

Informe de seguimiento a la Gestión del Riesgo

Aprobó: Ángela Mónica Castro Mora - Jefe Oficina de Control Interno
Elaboró: Ingrid Yiseth Camargo Morales – Profesional Universitario Grado 11
Paola Andrea Blandón Salazar – Contratista
Juan Carlos Cabuya Navarrete-Contratista

TRD OCI – 107–34,38

CONTENIDO

1. UNIDAD OBJETO SEGUIMIENTO ____ ***4***

2. RESPONSABLE UNIDAD OBJETO SEGUIMIENTO ____ ***4***

3. OBJETIVOS ____ ***4***

3.1 General ____ **4**

3.2 Específicos ____ **4**

4. ALCANCE ____ ***4***

6. RESULTADOS DEL SEGUIMIENTO ____ ***6***

6.1. Evaluación general de la gestión del riesgo. ____ **6**

6.1.1. Política y metodología para la administración de riesgos ____ **6**

6.1.2. Matrices de riesgos ____ **6**

6.2. Seguimiento Riesgos de Corrupción ____ **7**

6.2.2. Validación del diseño de los controles ____ **9**

6.2.3. Monitoreo y reporte ____ **9**

6.3 Seguimiento Riesgos de Gestión ____ **9**

6.3.1. Evaluación de la identificación ____ **10**

6.3.2. Validación del diseño de los controles ____ **11**

6.3.3. Monitoreo y reporte ____ **12**

6.4.1. Evaluación de la identificación ____ **13**

6.4.2. Validación del diseño de los controles ____ **13**

6.4.3. Monitoreo y reporte ____ **14**

6.5. Seguimiento Riesgos Seguridad y Privacidad de la información ____ **15**

6.5.1. Identificación de Riesgos ____ **15**

6.5.2. Validación del diseño de los controles ____ **16**

6.5.3. Monitoreo y reporte ____ **16**

7. HALLAZGOS _____ ***17***

8. REVISIÓN EFECTIVIDAD _____ ***20***

9. CONCLUSIONES _____ ***21***

10. RECOMENDACIONES _____ ***21***

11. PLAN DE MEJORAMIENTO _____ ***22***

1. UNIDAD OBJETO SEGUIMIENTO

Matrices de riesgos de corrupción, gestión, fiscales, seguridad y privacidad de la información.

2. RESPONSABLE UNIDAD OBJETO SEGUIMIENTO

Oficina Asesora de Planeación Sectorial (OAPS).
Oficina de Sistemas de Información (OSI)

3. OBJETIVOS

3.1 General

Evaluar la identificación, análisis y gestión del riesgo en la entidad, así como la efectividad de los controles establecidos en el Ministerio de Comercio, Industria y Turismo, durante el primer cuatrimestre de la vigencia 2025.

3.2 Específicos

- Verificar el monitoreo efectuado por la primera y segunda línea de defensa a los riesgos de corrupción, riesgos de gestión, fiscales y seguridad y privacidad de la información SPI.

- Verificar la efectividad de los controles implementados para mitigar los riesgos de corrupción, gestión, fiscales y SPI.

- Evaluar la efectividad de los planes de mejoramiento de anteriores trabajos realizados por la Oficina de Control Interno respecto a la gestión del riesgo.

4. ALCANCE

La Oficina de Control Interno en cumplimiento de lo establecido en el artículo 2.2.21.5.4 del Decreto 1083 2015 (Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública), efectuó el seguimiento a las matrices de riesgos de corrupción, gestión, fiscales y seguridad y privacidad de la información, cuya valoración de riesgos residual se encuentra en zona extrema o alta, teniendo en cuenta la Política de Administración del Riesgo establecida en el MinCIT, y la guía para la Administración del Riesgo y el diseño de controles en entidades públicas.

Para tal fin, se tomó el reporte de monitoreo realizado por la segunda línea de defensa correspondiente al primer cuatrimestre de 2025, para los riesgos con valoración residual alta y extrema.

Tipo de Riesgo	Numero de riesgos con valoración residual Alta, Extrema
Riesgos de Corrupción	21
Riesgos de Gestión	11
Riesgos Fiscales	8
Riesgos SPI	385

Fuente: Seguimiento consolidado de riesgos primer Cuatrimestre de 2025

Para los riesgos de seguridad y privacidad de la información, se tomó una muestra utilizando el formato de muestreo de la Función Pública, obteniendo una muestra de 23 riesgos a evaluar, con un nivel de confianza del 90%.

5. CRITERIOS DEL SEGUIMIENTO

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

Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública".

Decreto 1081 de 1015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República".

Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6

Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

DE-DR-001- Política de Administración del Riesgo, versión 4 del 26 de noviembre de 2024.

NTC ISO IEC 27001:2022

GTI-DE-002 Manual de políticas de seguridad y privacidad de la información.

GTI-DE-003 Manual del sistema de gestión de seguridad y privacidad de la información.

DE-001 Guía de Activos de Información.

GTI GTI-DE-006 Guía para el Análisis de Eventos e Incidentes de Seguridad y Privacidad de la Información.

GTI-PR-002 Gestión Operativa

TI. GTI-PR-003 Gestión de Información.

GTI-PR-004 Gestión de incidentes de seguridad y privacidad de la información. GTI-PR-014 Control acceso servicios TI

6. RESULTADOS DEL SEGUIMIENTO

6.1. Evaluación general de la gestión del riesgo.

6.1.1. Política y metodología para la administración de riesgos

La Oficina de Control Interno verificó que el MinCIT cuenta con la política de gestión del riesgo, la cual fue establecida mediante la Resolución Interna No. 0894 del 30 de agosto de 2021. "*Por la cual se actualiza y se adopta la política y metodología para la administración de riesgos del Ministerio de Comercio, Industria y Turismo"*

Posteriormente se observó, que la Oficina Asesora de Planeación Sectorial adelantó la actualización de la Política y Metodología para la administración de riesgos en el MinCIT - DE-DR-001, a la versión 4 de fecha 26 de noviembre del 2024, cumpliendo con los parámetros definidos por el Departamento Administrativo de la Función Pública (DAFP) respecto a la versión 6 de la "*Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP de noviembre de 2022"*

6.1.2. Matrices de riesgos

Se realizó verificación de la información publicada en la página web del MinCIT, evidenciando la publicación de las matrices de riesgos de corrupción, riesgos de gestión, riesgos fiscales y riesgos de seguridad y privacidad de la información, así como los respectivos monitoreos realizados por la primera y segunda línea de defensa durante el primer cuatrimestre de la vigencia 2025, de acuerdo con la periodicidad establecida en la política y metodología para la administración de riesgos vigente; a continuación se relacionan las versiones actualizadas y publicadas:

Tabla N° 1 – Matrices de Riesgos MinCIT

Matriz de riesgo	Versión	Fecha
Corrupción	14	30-12-2024
Gestión	15	30-12-2024
Fiscales	3	30-11-2024
Seguridad y privacidad de la información	-	30-09-2024

Fuente: Elaboración propia

6.2. Seguimiento Riesgos de Corrupción

6.2.1. Identificación de riesgos.

Durante el seguimiento realizado, se observó que la matriz de Riesgos de Corrupción del MinCIT Versión 14, cuenta con veintiún (21) riesgos identificados, los cuales se encuentran asociados a diez (10) procesos y uno (1) a un proyecto de inversión.

Tabla N° 2 – Cantidad de riesgos por tipo de proceso

TIPO DE PROCESO	N° DE RIESGOS	N° DE CONTROLES	PARTICIPACIÓN RIESGOS	PARTICPACIÓN DE CONTROLES
Apoyo	6	12	29%	24%
Misional	9	26	43%	52%
Estratégicos	5	11	24%	22%
Proyecto de Inversión (PI)	1	1	5%	2%
Total general	**21**	**50**	**100%**	**100%**

Fuente: Elaboración propia

De acuerdo a la información de la tabla No. 2, se observó que los procesos misionales cuenta con la mayor participación del total de los riesgos, con el 43 % (9 riesgos) con 26 controles definidos; el 29% (6 riesgos) corresponde a riesgos relacionados con los procesos de apoyo con 12 controles definidos; el 24% (5 riesgos) se encuentran asociados a los procesos estratégicos con 11 controles definidos y finalmente con una participación de 5% un riesgo (1) asociado al proyecto de inversión "Fortalecimiento de los estándares de calidad en la infraestructura productiva nacional a partir del reconocimiento y desarrollo nacional e internacional del Subsistema Nacional de la Calidad Nacional".

Se evidenció que en la matriz de riesgos se establecen dos tipologías de riesgos (corrupción y fraude), observando que (18) riesgos identificados son de corrupción y

(3) de fraude los cuales se encuentran relacionados a los siguientes procesos y proyecto de inversión (PI).

- Los riesgos de fraude se encuentran relacionados con los procesos Gestión del Talento Humano, Gestión de Recursos Financieros, y Adquisición de Bienes y Servicios.
- La mayor concentración de los riesgos de corrupción se encuentra relacionados al proceso misional Desarrollo Empresarial con una participación del 24% (5 riesgos).

Del seguimiento realizado se verificó si el total de eventos de riesgos descritos y registrados en la matriz de riesgos de corrupción, cumplen con los componentes y parámetros establecidos por la secretaria de Transparencia de la Presidencia de la República, (acción u omisión, uso del poder, desvió de la gestión, beneficio privado) como se describe en la tabla:

Tabla N° 3 – Número de Riesgos de Corrupción por cumplimiento de componentes definición riesgos de corrupción

ACCION OMISIÓN	USO DEL PODER	DESVIACION	BENEFICIO PRIVADO O PARTICULAR
17	19	21	21

Fuente: Elaboración propia

- El total de los riesgos en su descripción contemplan la desviación de la gestión hacia beneficio propio o particular.
- En el 29% (6) de los riesgos se identificó como hecho generador las "quejas o las investigaciones por parte de los entes de control o personas interesadas", lo cual no corresponde a hecho generador, porque no se identifica el evento o circunstancia que, al ocurrir, tiene el potencial de causar el riesgo de corrupción.
- Se analiza la "acción u omisión" como hacer o dejar de hacer, por lo que en 81% de los eventos de riesgo, la situación contempla el criterio revisado.

Por lo anterior se observa que, los riesgos de corrupción y fraude no cumplen en su descripción con alguno de los parámetros establecidos en la "Guía para la administración del riesgo y el diseño de controles en Entidades Públicas versión 6."

Sin embargo, es importante señalar en virtud de la actualización de la Política de Administración de Riesgos, la Oficina Asesora de Planeación viene adelantado un ejercicio de revisión y ajuste a los Riesgos de Corrupción identificados inicialmente, no obstante, con corte al 30 de abril 2025 se han actualizado el 14 % de los eventos de riesgo, (1) correspondiente al proceso de gestión del Talento Humano, (1) del proceso de relación con el ciudadano y (1) facilitación del comercio y la defensa comercial, por lo que se hace necesario continuar el proceso de la actualización de los riesgos.

6.2.2. Validación del diseño de los controles

Durante el seguimiento y análisis efectuado a los 50 controles establecidos en la matriz de riesgos de corrupción Versión 14, se realizó verificación de las variables para evaluar el diseño de los controles (responsable, periodicidad, propósito, cómo se realiza la actividad, observaciones o desviación resultante de aplicar el control, y evidencia de ejecución del control), las cuales se encuentran establecidas en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas versión No. 4 ", o*bservando lo siguiente:

- La totalidad de los controles definidos presentan aspectos por fortalecer tanto en su diseño como en su redacción, lo cual no permite evaluar su efectividad frente a los riesgos identificados. En general, no se especifican aspectos como el responsable del control, su periodicidad, el propósito, el procedimiento de ejecución, observaciones o desviaciones derivadas de su aplicación, ni evidencia que respalde su implementación y se identificó que el 96 % de los controles no definen su periodicidad de ejecución.

6.2.3. Monitoreo y reporte

Se evidenció monitoreo por parte de primera y segunda línea de defensa, de acuerdo con lo establecido en la Política y metodología para la administración de riesgos del MinCIT, el cual fue verificado mediante el reporte de la información registrado en el formato DE-FM-043 matriz de riesgos de corrupción.

Respecto a la aplicabilidad de los controles definidos se observó:

- Dificultad para acceder a los soportes documentales, debido a la metodología dispuesta por la OAPS para el monitoreo, donde las evidencias reposan en carpetas compartidas por la primera línea, lo que condiciona el acceso a la información.
- Aplicabilidad de controles sin soportes documentales.
- Controles no aplicados, debido a que la actividad generadora del riesgo no ocurrió durante el primer cuatrimestre de la vigencia 2025.

6.3 Seguimiento Riesgos de Gestión

La versión 15 de la matriz de riesgos de gestión del MinCIT contempla un total de 71 riesgos, de los cuales veintinueve (29) se encuentran en proceso de reformulación y cuarenta y dos (42) han sido reformulados. Estos riesgos están asociados a sesenta y siete (67) controles en revisión y ciento tres (103) que han sido reformulados.

Tabla N° 4 – Riesgos de gestión por nivel de riesgo residual

Zona de riesgo residual	Número de riesgos en revisión	Número de riesgos Reformulados
Baja	17	5
Moderada	11	27
Alta	1	8
Extrema	0	2
Total	**29**	**42**

Fuente: Mapa de Riesgos de Gestión Versión 15 de 2024

De acuerdo con la tabla No. 4 se encuentran en zona de riesgo alta o extrema un total de once (11) riesgos, los cuales son objeto del monitoreo cuatrimestral, conforme a lo indicado por la política y metodología para la administración de riesgos del MinCIT.

Para efectos del presente seguimiento, se tomaron los once (11) riesgos de gestión que se encuentran en zona residual alta y extrema, los cuales se encuentran asociados a seis (06) procesos como se muestra a continuación:

Tabla N° 5 – Riesgos de gestión evaluados por clasificación.

TIPO DE PROCESO	N° DE RIESGOS	N° DE CONTROLES	PARTICIPACIÓN RIESGOS	PARTICPACIÓN DE CONTROLES
Apoyo	2	2	18%	11%
Misional	7	14	64%	74%
Estratégicos	2	3	18%	16%
Total general	**11**	**19**	**100%**	**100%**

Fuente: Elaboración propia

Según la información presentada en la tabla N.º 5, se observa que para los riesgos revisados se concentran la mayor proporción en los procesos misionales, con un 64 % (7 riesgos), los cuales cuentan con catorce (14) controles definidos. Por su parte, los procesos de apoyo representan el 18 % (2 riesgos), con dos (2) controles definidos, y los procesos estratégicos también abarcan el 18 % (2 riesgos), con tres (3) controles definidos.

6.3.1. Evaluación de la identificación

Se realizó un análisis de la descripción del riesgo, aplicando la estructura de redacción basada en el qué, cómo y por qué, con el propósito de determinar su impacto, causa

inmediata y causa raíz. Como resultado, se estableció que los once (11) riesgos evaluados cumplen con los parámetros establecidos por la política.

6.3.2. Validación del diseño de los controles

De los diecinueve (19) controles identificados para los riesgos de gestión evaluados, se realizó la revisión de los elementos para la efectividad del control, tales como: descripción, atributos informativos y de eficiencia como lo indica la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas versión No.6".*

- Descripción: Conforme a los parámetros establecidos para la redacción del control (responsable, acción y complemento) se obtuvo:

Tabla N° 6 – Controles Evaluados según descripción

Descripción	Cumplen	No cumple	Cumple	No cumple
Responsable	12	7	63%	37%
Acción	18	1	95%	5%
Complemento	18	1	95%	5%

Fuente: Elaboración propia

De acuerdo con la información de la tabla que contiene los diecinueve (19) controles evaluados, se identificó que siete (7) controles, equivalentes al 63 %, presentan inconsistencias en la identificación del responsable, en relación con el cargo de quien efectúa el control o con la información registrada en la columna *"Cargo Ejecutor del Control"* de la matriz. Se presenta un riesgo cuya descripción no incluye la acción ni el complemento, conforme a la estructura de redacción establecida en la *Política y Metodología para la Administración de Riesgos*.

- Totalidad de controles identificados: Teniendo en cuenta que *"la identificación de los controles se realiza a partir de cada una de las causas raíz que se hayan identificado para cada riesgo[i]"*, se evidenció que, para los once (11) riesgos evaluados, se identificaron un total de veintiún (21) causas raíz, a partir de las cuales se establecieron controles para dieciséis (16), lo que representa una cobertura del 76 %.
- Atributos de eficiencia: Se presenta la identificación de los elementos de tipo de control (defectivos o correctivos) e implementación (manual) para los once (11) controles evaluados.
- Atributos Informativos: En cuanto a la frecuencia, se identificó que catorce (14) de los diecinueve (19) controles, equivalentes al 74 %, se ejecutan por evento. Respecto a la documentación, siete (7) controles (37 %) no cuentan con registro

documental. En relación con el registro de la evidencia, la totalidad de los controles evaluados incluye el nombre del documento o soporte asociado.

6.3.3. Monitoreo y reporte

Se evidenció monitoreo por parte de primera y segunda línea de defensa, de acuerdo con lo establecido en la guía Política y metodología para la administración de riesgos del MinCIT, el cual fue verificado mediante el reporte de la información registrado en el formato DE-FM-022 matriz de riesgos de gestión.

Respecto a las actividades de seguimiento y monitoreo, se evidenció que los soportes de la ejecución de los controles para el primer cuatrimestre de 2025 presentan diferencias respecto al registro o falta de descripción en las observaciones que permitan establecer que se ejecutaron todos los controles para la totalidad de los eventos generados en el periodo.

6.4 Seguimiento Riesgos Fiscales

La versión 03 de la matriz de riesgos fiscales del MinCIT contempla un total de doce (12) riesgos que se encuentran asociados a veintiún (21) controles.

Tabla N° 7 – Riesgos de gestión por nivel de riesgo residual

Zona de riesgo residual	Número de riesgos fiscales
Baja	2
Moderada	2
Alta	2
Extrema	6
Total	**12**

Fuente: Mapa de Riesgos Fiscales Versión 03 de 2024

De acuerdo con la tabla No. 7 se encuentran en zona de riesgo alta o extrema un total de ocho (08) riesgos, los cuales son objeto del monitoreo cuatrimestral, conforme a lo indicado por la política y metodología para la administración de riesgos del MinCIT.

Para efectos del presente seguimiento, se tomaron los ocho (08) riesgos fiscales que se encuentran en zona residual alta y extrema, los cuales se encuentran asociados a cuatro (04) procesos como se muestra a continuación:

Tabla N° 8 – Riesgos fiscales evaluados por clasificación.

TIPO DE PROCESO	N° DE RIESGOS	N° DE CONTROLES	PARTICIPACIÓN RIESGOS	PARTICPACIÓN DE CONTROLES
Apoyo	3	4	38%	31%
Misional	4	6	50%	46%
Estratégicos	1	3	13%	23%
Total general	**8**	**13**	**100%**	**100%**

Fuente: Elaboración propia

Según la información presentada en la tabla N.º 8, se observó que para los riesgos revisados se concentran la mayor proporción en los procesos misionales, con un 50 % (4 riesgos), los cuales cuentan con seis (6) controles definidos. Por su parte, los procesos de apoyo representan el 38% (3 riesgos), con cuatro (4) controles definidos, mientras que los procesos estratégicos abarcan el 13% (1 riesgo), con tres (3) controles definidos.

6.4.1. Evaluación de la identificación

Se realizó un análisis de la descripción del riesgo, aplicando la estructura de redacción basada en el qué, cómo y por qué, con el propósito de determinar su impacto, causa inmediata y causa raíz.

Tabla N° 9 – Cumplimiento de los elementos de la descripción de riesgos Fiscales

Elementos de la descripción del riesgo fiscal	Cumple	Participación de cumplimiento	No cumple	Participación de incumplimiento
¿Qué? Impacto	8	100%	0	0%
¿Cómo? Causa Inmediata	3	38%	5	63%
¿Por qué? Causa Raíz	6	75%	2	25%

Fuente: Elaboración propia

De acuerdo con la información presentada en la tabla No. 9, se evidenció que, de los ocho (8) riesgos evaluados, cinco (5), equivalentes al 63%, no cuentan con la identificación de su causa inmediata y en dos (2) riesgos, que representan el 25%, no se ha identificado la causa raíz, conforme a lo establecido para la composición del riesgo fiscal.

6.4.2. Validación del diseño de los controles

De los trece (13) controles identificados para los riesgos fiscales evaluados, se realizó la revisión de los elementos para la efectividad del control, tales como: descripción,

atributos informativos y de eficiencia como lo indica la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas".*

- Descripción: Conforme a los parámetros establecidos para la redacción del control (responsable, acción y complemento) se obtuvo:

Tabla N° 10 – controles evaluados según descripción

Descripción	Cumplen	No cumple	Cumple	No cumple
Responsable	10	3	77%	23%
Acción	13	0	100%	0%
Complemento	9	4	69%	31%

Fuente: Elaboración propia

De acuerdo con la tabla, de los trece (13) controles evaluados, se identificó que tres (3), equivalente al 23 %, no cuenta con la descripción del responsable o es diferente al indicado en la columna *"Cargo Ejecutor del Control"* de la matriz. Cuatro (4) controles, que representan el 31 % del total, no incluyen el complemento necesario para identificar el objeto del control, lo cual no se ajusta a la estructura de redacción establecida en la Política y Metodología para la Administración de Riesgos.

- Atributos de eficiencia: Se presenta la identificación de los elementos de tipo de control (defectivos o correctivos) e implementación (manual o automática) para los trece (13) controles evaluados.

- Atributos Informativos: En cuanto a la frecuencia, se identificó que seis (06) de los catorce (14) controles, equivalentes al 43%, se ejecutan por evento. Respecto a la documentación, seis (6) controles (43 %) no cuentan con registro documental. En relación con el registro de la evidencia, la totalidad de los controles evaluados incluye el nombre del documento o soporte asociado.

6.4.3. Monitoreo y reporte

Se evidenció monitoreo por parte de primera y segunda línea de defensa, de acuerdo con lo establecido en la guía Política y metodología para la administración de riesgos del MinCIT, el cual fue verificado mediante el reporte de la información registrado en el formato DE-FM-022 matriz de riesgos fiscales.

Respecto a las actividades de seguimiento y monitoreo, se evidenció que los soportes de la ejecución de los controles para el primer cuatrimestre de 2025 presentan diferencias respecto al registro o falta de descripción en las observaciones que

permitan establecer que se ejecutaron todos los controles para la totalidad de los eventos generados en el periodo.

6.5. Seguimiento Riesgos Seguridad y Privacidad de la información

6.5.1. Identificación de Riesgos

La matriz de riesgos de seguridad y privacidad de la información con fecha de actualización a 10 de mayo de 2025 presenta un total de 368 riesgos cuya zona de riesgo residual se encuentra en Extremo y Alto.

Para el seguimiento a la gestión del riesgo del primer cuatrimestre de 2025, se calculó el tamaño de la muestra con la herramienta de la función pública a través de un muestreo aleatorio simple arrojando un total de 23 riesgos que fueron revisados.

Los riesgos evaluados corresponden al tipo de activo denominado "servicios" y se encuentran distribuidos en los siguientes tipos de activo asociado a servicios:

Tabla N° 11– Riesgos evaluados según tipo de activo asociado

Tipo de Activo	Cantidad
Sitio Web Externo	4
Almacenamiento Servidor de Datos	5
Licencia Uso Firma / Certificado Digital	2
Almacenamiento One Drive / Share Point	11
Correo Electrónico Institucional	1

Fuente: Elaboración propia

En todos los riesgos evaluados, se observa que en la descripción del riesgo no cumple con los criterios definidos en las instrucciones establecidas en la Matriz de Riesgos, que se encuentran mediante comentarios en la celda, dicha descripción debe exponer de manera clara las situaciones no deseadas, incorporando los elementos ¿qué?, ¿cómo? y ¿por qué?, y ser comprensible para cualquier persona.

De acuerdo con las directrices del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC; "Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita" y en relación con la valoración del riesgo, éste Modelo, estable que, "Posterior a la identificación de los riesgos de seguridad de la información con sus respectivas amenazas y

vulnerabilidades enunciadas…, "se deberá continuar con el Paso 3. Valoración del Riesgo, de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" del Departamento Administrativo de la Función Pública – DAFP.

6.5.2. Validación del diseño de los controles

Durante el seguimiento y análisis efectuado a los controles establecidos en la matriz de riesgos de seguridad y privacidad de la información con fecha de actualización a 10 de mayo de 2025, se realizó verificación de las variables para evaluar el diseño de los controles (responsable, acción y objeto del control), observando lo siguiente:

- La totalidad de los controles definidos presentan su responsable, discriminando los grupos de la Oficina de Sistemas de Información que tienen la responsabilidad de implementar el control.
- La totalidad de los controles definidos presentan la respectiva acción a realizar con el control y el resultado esperado u objeto del control.

6.5.3. Monitoreo y reporte

Se evidenció monitoreo por parte de primera y segunda línea de defensa, de acuerdo con lo establecido en la guía Política y metodología para la administración de riesgos del MinCIT, el cual fue verificado mediante el reporte de la información registrado en el formato "Seguimiento Consolidado Riesgos SPI 1C-2025" con corte a mayo 10 de 2025.

El monitoreo a los riesgos de seguridad y privacidad de la información se realizan de acuerdo con la agrupación por el tipo de activo asociado, es decir, Sitio Web Externo, Almacenamiento Servidor de Datos, Almacenamiento One Drive / Share Point, Licencia Uso Firma / Certificado Digital y Correo Electrónico Institucional.

Respecto a las actividades de seguimiento y monitoreo, se evidenció que la ejecución de los controles para el primer cuatrimestre de 2025 presenta las siguientes acciones de acuerdo con el tipo de activo asociada a cada riesgo evaluado, así:

- Almacenamiento One Drive / Share Point" y "Almacenamiento Servidor de Datos" (16 riesgos)

Se evidencia que la OSI, realiza el respectivo monitoreo según los extractos de informes de FortiDeceptor Quincenal Report.

Se reporta que no se ha presentado materialización de riesgos.

- Sitio web externo (4 riesgos)

Se evidencia que la OSI, realiza el respectivo monitoreo según los extractos de informes de FortiDeceptor Quincenal Report.

Se reporta que no se ha presentado materialización de riesgos.

"Licencia Uso Firma / Certificado Digital" (2 riesgos)

Se evidencia que la OSI, realiza el respectivo monitoreo según los soportes del Grupo de EPM Microdata Ltda, referentes a la prestación del Servicio de Mantenimiento Preventivo y Correctivo para Servidores.

Se reporta que no se ha presentado materialización de riesgos

"Correo Electrónico Institucional" (1 riesgo)

Se evidencia que la OSI, realiza el respectivo monitoreo según los extractos de informes de FortiDeceptor Quincenal Report.

Se reporta que no se ha presentado materialización de riesgos.

7. HALLAZGOS

Hallazgo 1. Ccontroles sin soportes de su ejecución o que no corresponden al documento registrado de la matriz.

Condición: Revisado el monitoreo realizado por la primera línea de defensa, se observó que para los siguientes riesgos no se aportaron evidencias de cumplimiento de aplicación de los controles descritos en las matrices de riesgo como se relaciona en la siguiente tabla:

MATRIZ DE RIESGO	N° RIESGO	AREA RESPONSABLE	RIESGO	OBSERVACIÓN
Corrupción	RC-10	Dirección de Análisis Sectorial y Promoción - Grupo del Análisis sectorial y RNT del Viceministerio del Turismo	Posibilidad de afectación reputacional, debido a favorecimiento indebido a terceros en la expedición de certificaciones de exención de renta para hoteles nuevos y remodelados.	De acuerdo con el monitoreo realizado por la primera línea de defensa en el cual informan que el control se está ejecutando, no fue posible verificar la aplicabilidad de los controles, toda vez que no se adjuntaron soportes de su ejecución. Se recomienda revisar la descripción de los controles de tal manera que se identifique responsable, periodicidad, propósito, como se realiza, observaciones o desviaciones, y la evidencia de aplicación.
Corrupción	RC-11	Grupo de planificación y	Posibilidad de afectación de la imagen	De acuerdo con el monitoreo realizado por la primera línea de defensa, no fue

MATRIZ DE RIESGO	N° RIESGO	AREA RESPONSABLE	RIESGO	OBSERVACIÓN
		desarrollo sostenible del turismo	del ministerio por de recibir o solicitar dádiva o beneficio particular o de terceros al emitir de manera anticipada concepto DIMAR.	posible verificar la aplicabilidad de los controles, toda vez que el soporte de ejecución no corresponde a la vigencia 2025. Se recomienda revisar la descripción de los controles de tal manera que se identifique responsable, periodicidad, propósito, como se realiza, observaciones o desviaciones, y la evidencia de aplicación.
Gestión	FC-RG5	Grupo Análisis y Gestión de la Cadena Logística de Comercio Exterior	Posibilidad de afectación reputacional por perjuicios a los actores de la cadena logística, debido a fallas en las funcionalidades del aplicativo o interoperabilidades con las entidades que intervienen para la inspección de la carga en puertos y aeropuertos y/o uso inadecuado del aplicativo por parte de los usuarios declarantes, entidades de control o puertos.	Control 2. El soporte es el formato de control de trámites manuales, sin embargo, no se adjunta correos que indiquen la autorización Control 4. El soporte corresponde a la relación de las capacitaciones realizadas. No se observan las listas de asistencia

Criterios: Política y metodología para la administración de riesgos DE-DR-001 Versión 6. En la cual estable que la primera línea "*se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos"*

Causa: Fallas en las actividades de monitoreo y seguimiento.

Consecuencia: Posible inefectividad de los controles definidos para mitigar los riesgos.

Hallazgo 2. Estructura de redacción de los riesgos y controles sin la totalidad de los elementos los establecidos.

Condiciones:

- Los riesgos de corrupción RC-2, RC-3, RC-7, RC-8, RC-12, RC-15, RC-20, RC-22, no se identifica el hecho generador de corrupción.

- Los controles definidos en la matriz de riesgos de corrupción no contemplan alguno o algunos de los elementos (responsable, periodicidad, propósito, cómo se realiza la actividad, observaciones o desviación resultante de aplicar el control, y evidencia de ejecución del control).

- Desde la primera recomendación registrada en el informe OCI-014-2023 al primer cuatrimestre 2025, se han logrado actualizar 3 riesgos de corrupción de 21 establecidos.

- La descripción de los controles definidos para los riesgos de gestión FC-RG2, FC-RG5, FC-RG9, IC-RG3, BS-RG1, GD-R2, no presentan la identificación del responsable o es diferente a la registrada en la columna responsable de la matriz.

- La descripción de los riesgos fiscales FP-RF1, FP-RF4, FP-RF5, BS-RF1, TH-RF1, BS-RF2, BS-RF3, no cumplen con la estructura que identifique la causa inmediata o causa raíz.

- La descripción de los controles definidos para los riesgos fiscales FP-RF1, FP-RF4, presentan inconsistencias en la identificación del responsable y el complemento del control.

- La descripción de los riesgos de seguridad y privacidad de la información no aplica el criterio establecido en las instrucciones documentadas, como comentario en la celda de la Matriz de riesgos del MinCIT; que indica "Descripción de los riesgos: Expone de manera clara las situaciones no deseadas, asegurando que contenga los criterios ¿qué? ¿cómo? Y ¿por qué? y sea comprensible para cualquier persona". Así como tampoco inicia con la frase "posibilidad de" como parte de la estructura propuesta para redacción del riesgo, en la Guía para la Administración de Riesgos del DAFP.

Criterio:

- Política y metodología para la administración de riesgos DE-DR-001 Versión 4.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 y 6.

Causa: Fallas en la estructuración de riesgos y controles

Consecuencia: Posible materialización de riesgos.

8. REVISIÓN EFECTIVIDAD

Se realizó revisión de efectividad de las acciones de mejoramiento relacionadas con la gestión del riesgo del MinCIT, observando que, de 20 acciones de mejoramiento, el 55% fueron efectivas y el 45% inefectivas, como se relaciona en la siguiente tabla:

Tabla N° 12 – Acciones efectivas

CÓDIGO DEL INFORME	NOMBRE DEL INFORME	HALLAZGO	COD. ACCIÓN
OCI-018-2023	Informe Final Auditoría Interna de Gestión al Proyecto de Inversión "Fortalecimiento de los servicios brindados a los usuarios de Comercio Exterior a nivel nacional -VUCE" Código BPIN: 2018011000279	Observación No. 4	23-022-A
OCI-032-2023	Informe de auditoría interna de gestión, a la supervisión y seguimiento del patrimonio autónomo ProColombia	Observación No. 3.	23-050-A
OCI-021-2023	Informe Final Seguimiento a la Planeación Estratégica del Ministerio 2025	Hallazgo No. 3	23-012-A 23-012-B
OCI-023-2023	Informe de auditoría interna de gestión financiera y ejecución presupuestal	Hallazgo N° 1.	23-035-A
OCI-043-2023	Auditoría asociada a la Gestión de la Administración del Riesgo del Ministerio de Comercio, Industria y Turismo.	Hallazgo No. 1	23-060-A 23-060-B
		Hallazgo No. 4	23-063-A
		Hallazgo No. 8.	23-067-E
		Hallazgo No. 2	23-061-A
		Hallazgo No. 6	23-065-A

Fuente: Elaboración propia

Tabla N° 13 – Acciones inefectivas

CÓDIGO DEL INFORME	NOMBRE DEL INFORME	HALLAZGO II	COD. ACCIÓN	ACCCIÓN A REALIZAR
OCI-021-2023	Informe Final Seguimiento a la Planeación Estratégica del Ministerio 2024	Hallazgo No. 2 Falta de oportunidad y efectividad de la revisión de riesgos que inducen a generar debilidades en el diseño y aplicación de controles.	23-011-A	Reformular acción
OCI-043-2023	Auditoría asociada a la Gestión de la Administración del Riesgo del Ministerio de Comercio, Industria y Turismo.	Hallazgo No. 3 Reporte de monitoreo sin la evidencia que soporte las actividades de control	23-062-A	Formular plan de mejoramiento de acuerdo al hallazgo 1 del presente informe
		Hallazgo No. 5 Debilidades en la gestión de Riesgos de Seguridad de Información (Rol enfoque hacia la prevención)	23-064-A	Reformular acción
		Hallazgo No. 7 Desatención en los lineamientos de la Resolución 720 de 2022 y la Política y	23-066-A	Reformular acción

		Metodología para la Administración de Riesgos y Oportunidades anexo 1, (Rol enfoque hacia la prevención)		
		Hallazgo No. 8. Debilidad en la efectividad de los controles	23-067-A 23-067-C 23-067-B	Formular plan mejoramiento de acuerdo al hallazgo 2 del presente informe
OCI-049-2021	Informe definitivo de AIG a la gestión de los riesgos en el MinCIT (2021)	Observación 2. Debilidad en el control de verificación de la información registrada en la matriz de riesgos del MinCIT	21-067-A	Reformular acción
OCI-049-2021			21-067-B	

Fuente: Elaboración propia

9. CONCLUSIONES

- No se materializaron riesgos de corrupción, gestión, fiscales, seguridad y privacidad de la información durante el primer cuatrimestre 2025.

- Las matrices de riesgos del MinCIT, no contemplan plan de acción de tratamiento para riesgos residuales que se encuentran en zona extrema o alta, y la acción de tratamiento según la política y metodología para la administración de riesgos es "reducir".

- Los soportes documentales que respaldan la ejecución de los controles presentan diferencias con el registro o no se anexaron en el seguimiento.

- La descripción de los riesgos de seguridad y privacidad de la información, no se encuentra alineada con las instrucciones establecidas en la Matriz de Riesgos, que se encuentran mediante comentarios en la celda "Descripción del Riesgo", dicha descripción debe exponer de manera clara las situaciones no deseadas, incorporando los elementos ¿qué?, ¿cómo? y ¿por qué?, y ser comprensible para cualquier persona.

10. RECOMENDACIONES

- Establecer mecanismos para el monitoreo de los riesgos por parte de la primera línea de defensa que garantice que la información y los documentos soporte de aplicación de los controles mantengan confidencialidad y no sean susceptibles de modificación.

- Verificar la pertinencia de implementar planes de acción para los riesgos residuales en zona extrema y alta y que su acción de tratamiento es "reducir" atendiendo a lo establecido en la "*Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, en la cual indica que se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento. Y El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.*"

11. PLAN DE MEJORAMIENTO

Se solicita articular la formulación de las acciones de mejoramiento con la primera línea de defensa de acuerdo con los hallazgos registrados, así mismo se solicita tomar las acciones que permitan atender las recomendaciones informadas.