



La justicia
es de todos

Minjusticia

INFORME DE AUDITORÍA SOBRE EL
PROCESO DE MODELACIÓN DEL
RIESGO EN EL MINISTERIO DE
JUSTICIA Y DEL DERECHO

Oficina de
Control
Interno.
Noviembre
de 2021

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

1. Objetivo de la auditoría

Evaluar y verificar, desde la tercera línea de defensa, el cumplimiento del proceso de modelación del riesgo en el Ministerio de Justicia y del Derecho (en adelante MJD)

2. Alcance de la auditoría

En el marco del objetivo definido, se evaluará el periodo comprendido entre el 1º de marzo de 2020 y el 1º de octubre de 2021.

3. Criterios o parámetros normativos

- ✓ Constitución Política de Colombia, artículos 209 y 269.
- ✓ 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
- ✓ 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.
- ✓ 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.
- ✓ Decreto 507 de 2016, por medio del cual se modifica el Decreto Único Reglamentario del Sector Justicia y del Derecho.
- ✓ Decreto 1083 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- ✓ Guía 7 sobre Gestión de Riesgos, del Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones. 2016.
- ✓ Guía para la administración del riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de Función Pública (en adelante DAFP), versión 6 de diciembre del 2020.
- ✓ Manual Operativo del Modelo Integrado de Planeación y Gestión, versión 4, de marzo de 2021.
- ✓ Guía de administración de riesgos, código G-MC-04, del 31 de diciembre de 2019, versión 6, del Sistema Integrado de Gestión -SIG-del Ministerio de Justicia y del Derecho.

4. Metodología

Para el desarrollo de la presente auditoría, la Oficina de Control Interno (en adelante OCI), tomará como base la información proveniente del grupo de Calidad y Transformación Organizacional de la Oficina Asesora de Planeación -OAP-, que aportó la información respecto a la modelación del riesgo en el MJD, y se contrastará con lo indicado en la Guía del Departamento Administrativo de la Función Pública -DAFP-, versión 6 de diciembre del 2020, y en la Guía de Administración del Riesgo del Ministerio de Justicia y del Derecho; identificada con el código G-MC-04, del 31 de diciembre de 2019, versión 6.

	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Se diseñó un formulario de nueve (9) preguntas dirigido a la OAP, por medio del cual se buscó conocer el cumplimiento de las diferentes etapas definidas en las guías ya mencionadas e información relevante para esta auditoría.

Se realizó la solicitud de evidencias e información de importancia para la auditoría, por medio del memorando MJD-MEM21-0007622 del 30 de septiembre de 2021, dirigido a la OAP. La dependencia auditada dio respuesta mediante los memorandos MJD-MEM21-0007954 del 12 de octubre de 2021 y MJD-MEM21-0008079 del 15 de octubre de 2021 adjuntado lo solicitado. También se realizaron entrevistas al personal involucrado en el tema y acompañamiento a reuniones de identificación de riesgos y diseño de controles.

Con la entrega de las evidencias, los auditores diseñaron diversas listas de chequeo, donde se consignarán los datos más relevantes encontrados por esta auditoría, para verificar el cumplimiento de cada una de las etapas definidas en la guía del Departamento Administrativo de la Función Pública, y que corresponde a la metodología para la administración del riesgo. Esta guía se comparó con la incorporada en el SIG del Ministerio de Justicia y del Derecho, identificada con el Código G-MC-O4 versión 6 sobre el mismo tema.

Igualmente, se diseñaron cuadros de seguimiento para totalizar los riesgos identificados con sus respectivos controles, tanto de gestión, corrupción y seguridad de la información, como para verificar que el diseño esté debidamente realizado, y que cumpla con las indicaciones del DAFP y la guía propia del MJD.

5. Desarrollo de la Auditoría

5.1 Política de Administración del Riesgo

La política de administración del riesgo¹ determina las orientaciones que deben tenerse en cuenta para la gestión del riesgo; esta es una tarea propia del equipo directivo y se debe hacer desde el ejercicio de direccionamiento estratégico y de planeación, por lo cual se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

La administración de los riesgos es un proceso diseñado para identificar los eventos que puedan afectar la organización, y manejar los riesgos que estén dentro de su apetito de riesgo², para proveer seguridad razonable con miras a la consecución de los objetivos del MJD.

En cuanto a la aprobación de la política de administración del riesgo en el MJD, se encuentra que la OAP, en reunión del Comité Institucional de Gestión y Desempeño (CIGD) del día 15 de febrero de 2019 a través del acta N°2, presentó las modificaciones

¹ En la política se determina la estructura para la administración del riesgo, con aspectos metodológicos para cada una de las etapas de la gestión del riesgo.

² El apetito de riesgo es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

 <div style="display: flex; justify-content: space-between; align-items: center;"> La justicia es de todos Minjusticia </div>	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

a realizar a la Política de Gestión del Riesgo; modificaciones realizadas y firmadas por la Jefe de Oficina de la OAP, como representante de la Alta Dirección³, dicha actualización fue aprobada por el Comité Institucional de Coordinación de Control Interno (CICCI) en sesión realizada el día 18 de diciembre de 2019, e incorporada en el SIG el 31 de diciembre de 2019, y que se plasma en la Guía de Administración del Riesgo, identificada con el Código SIG G-MC-04 versión 6.

En la guía G-MC-04, del 31 de diciembre de 2019, en el punto 4.2 se consigna que:

“El Ministerio de Justicia y del derecho, con el liderazgo de la alta dirección, representada en el Comité Institucional de Coordinación de Control Interno y con el apoyo de los líderes de procesos y sus equipos de trabajo gestionará, orientará, implementará y fortalecerá las etapas de administración de todo tipo de riesgos (gestión, corrupción, seguridad digital, etc.), que impidan el logro de los objetivos estratégicos, institucionales y de procesos con base en las orientaciones establecidas en el presente manual, a través de su tratamiento, manejo y seguimiento”.

La OCI constató la participación permanente de la alta dirección del MJD, en la formulación de la política de riesgos, como el conocimiento y la aplicación de ella dentro del proceso de mejora integral de la gestión institucional⁴, que tiene como objetivo el de: “coordinar y administrar la implementación del sistema Integrado de Gestión del Ministerio de Justicia y del Derecho, con el fin de asegurar su mejora continua, conveniencia, eficacia y eficiencia conforme con los estándares adoptados”.

La actividad⁵ de: *“orientar la administración de los riesgos de gestión, de corrupción de la entidad y de seguridad de la información, dentro de los sistemas de Gestión de Calidad, de acuerdo con los establecido en el documento G-MC-04-Guía para la administración del Riesgo”*, se encuentra a cargo de la OAP.

5.2 Proceso de Identificación y Modelación del Riesgo.

La identificación de riesgos consiste en determinar los posibles eventos potenciales, que pueden estar o no bajo el control del ministerio, que ponen en peligro el logro de la visión y los objetivos institucionales; estableciendo los agentes generadores, las causas y los efectos si llegasen a ocurrir. En la identificación de riesgos, se debe tener en cuenta que un riesgo es diferente a una deficiencia de control interno; por lo tanto, se requiere efectuar un análisis para no dejar una causa como un riesgo.

Para la modelación del riesgo, el MJD tiene prevista una herramienta de ayuda en Excel, identificada -en el SIG- con el Código F-MC-G04-01, con hojas independientes para la identificación de cada uno de los riesgos y controles de gestión, de corrupción y de seguridad de la información, herramienta que se encuentra incluida en la guía del MJD, de diciembre del 2109, y publicada en la página WEB.

³ De acuerdo a la Resolución 1940 del 2019, “por medio de la cual se articula el Sistema Integrado de Gestión - SIG con la versión actualizada del Modelo Integrado de Planeación y Gestión - MIPG en el Ministerio de Justicia y del Derecho, se establece su equipo operativo y se dictan otras disposiciones”.

⁴ Que figura en el SIG con código C-MC, versión 5, con fecha de vigencia del 28 de febrero de 2020.

⁵ A cargo de los profesionales del Grupo de Calidad y Transformación Organizacional

	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

La Oficina Asesora de Planeación y la Dirección de Tecnologías y Gestión de Información en Justicia -DTGIJ-, realizaron diversas jornadas de socialización a cada una de las dependencias, tanto del formato incorporado en el SIG, como de la metodología prevista en la guía, para la identificación de los riesgos.

En concordancia con lo anterior, se realizaron reuniones con las diferentes dependencias encaminadas a socializar el plan de trabajo para la implementación de la Política de Riesgos, entre las cuales se presentaron los lineamientos para la identificación, de los riesgos, tanto de gestión, corrupción y seguridad de la información; como también el diseño, y calificación de los controles para atacar las causas de las amenazas.

Se verificó por la OCI, la realización de reuniones virtuales con las diferentes dependencias del Ministerio de Justicia y del Derecho por el aplicativo Teams; las cuales comprenden capacitación, revisión de las matrices formuladas por cada dependencia, correcciones y aprobación final de estas.

En relación a los riesgos de gestión y corrupción, la OCI corroboró que la OAP, posterior a la aprobación de la política de administración del riesgo, celebró un total de 72 mesas de trabajo con las dependencias; actividades realizadas de manera individual con el enlace y/o servidor designado -para este ejercicio- por la dependencia.

Por otro lado, en la identificación de riesgos de seguridad de la información⁶, y su plan de tratamiento, se realizaron reuniones con la OAP y la DTGIJ, para la realización del plan de trabajo⁷ y las acciones respectivas a desarrollar; igualmente, se realizaron diversas mesas de trabajo con los líderes de transparencia de cada dependencia para socializar el plan de trabajo en lo concerniente a identificación de los activos de la información y riesgos de seguridad de la información, como también la capacitación de gestión de riesgos por parte de la DTGIJ.

En el año 2020 se totalizaron 62 reuniones con los líderes de transparencia, encaminadas a la identificación y levantamiento de los riesgos y controles de seguridad de la información; así mismo, durante el año 2021 se realizaron 69 reuniones con el propósito de hacerles seguimiento y actualización a esos riesgos, generándose una nueva matriz. Como resultado de estos ejercicios se cuenta con el mapa de riesgos y controles de activos de la información, con un total de 399 activos y riesgos identificados.

Los auditores realizaron confirmación de cada una de las etapas del proceso de modelación del riesgo, esto se realizó por medio de los audios grabados y que son incorporados como evidencia e igualmente asistiendo a una sesión presencial realizada - el día 12 de noviembre de 2021- con la Dirección Financiera, en la que se realizó la primera parte del levantamiento de los riesgos y controles de tesorería.

⁶ Que afectan alguno de los tres pilares de la seguridad de la información, como son la pérdida de la confidencialidad de los activos, la pérdida de integridad de los activos y la pérdida de disponibilidad de los activos

⁷ De los años 2020 y 2021

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

En la actividad anterior se observó que, a partir de la metodología lluvia de ideas, con la ayuda de la herramienta Excel, se identifica riesgo, causas, consecuencias y controles, cumpliendo y siguiendo los lineamientos definidos en la guía de administración del riesgo del Ministerio.

También es importante resaltar que la DTGIJ, para el proceso de modelación del riesgo relacionado con seguridad de la información, junto a la guía de Ministerio, también tiene como referente -a aplicar- el Marco del Modelo de Seguridad y Privacidad de la Información (en adelante MSPI), expedido por El Ministerio de Tecnologías de la Información y las Comunicaciones.

5.3 Cumplimiento Normativo Identificación y Tratamiento del Riesgo.

La OCI realiza la verificación de cada una de las etapas establecidas en la Guía para la Administración de Riesgos, versión 6 de diciembre del 2020, emanada del Departamento Administrativo de la Función Pública-DAFP, comparándola con la guía incorporada en el SIG, del Ministerio de Justicia y de Derecho. Para este efecto, se diseñó el cuadro que se presenta a continuación, abordando cada una de las etapas definidas:

Convenciones:

SIGNIFICADO	
X	Cumple
X	Cumple o incumple parcialmente
X	Incumple

Pasos modelación del riesgo	Actividad a desarrollar		Cumplimiento Guía del MJD		Comentarios OCI
			SI	NO	
Actividades previas al inicio de la modelación del riesgo.	Conocimiento de la entidad	Cumple con la misión, visión, objetivos estratégicos y planeación institucional.	X		Actividades plasmadas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numeral 4.5
	Cumple con el modelo de operación	Cumple con la caracterización de los procesos	X		Actividades incorporadas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numeral 4.5

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Pasos modelación del riesgo	Actividad a desarrollar	Cumplimiento Guía del MJD		Comentarios OCI
		SI	NO	
	Cumple con los objetivos de los procesos.	X		Actividades incluidas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numeral 4.5
	Cumple con los planes, programas o proyectos asociados	X		Actividades previstas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numeral 4.5
Paso 1. Política de administración de riesgos.	1.1 Lineamientos de la política	X		Se encuentran en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019, numeral 4.3.1. Alta Dirección o su representante Legal y el CICCI- línea estratégica; como también en la Resolución 1940 del 20 de diciembre de 2019, por medio de la cual se articula el Sistema Integrado de Gestión - SIG con la versión actualizada del Modelo Integrado de Planeación y Gestión, se establece su equipo operativo y se nombra el representante de la alta dirección.
	1.2 Marco conceptual para el apetito del riesgo		X	En la guía actual del MJD, no se encuentra definido el marco conceptual para el apetito de riesgo del MJD, punto establecido en la última guía de administración de riesgos y controles del DAFP -2020-. El apetito del Riesgo es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. Se recomienda actualizar la guía, previa aprobación de la alta dirección, quien es la responsable de establecer el apetito de riesgo y el marco conceptual. Entendemos que, antes de la emisión de este informe, se presentó ante el CICCI llevado a cabo el 23 de noviembre de 2021, una fórmula de aceptación del riesgo sobre la base de los lineamientos relacionados con el apetito del riesgo. circunstancia sobre la cual se ahondará en el curso del seguimiento frente a este informe.
Paso 2. Identificación del riesgo.	2.1. Análisis de objetivos estratégicos y de los procesos	X		Se encuentran en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numerales 4.5 y 4.7
	2.2. Identificación de los puntos de riesgo.	X		
	2.3. Identificación de áreas de impacto.	X		
	2.4. Identificación de áreas de factor de riesgo	X		
	2.5. Descriptor de riesgo.	X		
	2.6. Clasificación del riesgo.	X		Actividades consagradas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numeral 4.10

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Pasos modelación del riesgo	Actividad a desarrollar	Cumplimiento Guía del MJD		Comentarios OCI
		SI	NO	
Paso 3. Valoración del riesgo.	3.1 Análisis de riesgo.	X		Actividades inmersas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numeral 4.11; se anota que, aunque la guía del MJD lo tiene previsto; en el nuevo documento del DAFP, de diciembre de 2020, se presenta una actualización en la metodología de la evaluación del riesgo, precisando el análisis de la probabilidad e impacto, con tablas de referencia con porcentajes, así como el mapa de calor resultante. Se recomienda a la OAP evaluar su incorporación, para una nueva actualización de la guía del MJD.
	3.2 Evaluación del riesgo.	X		
	3.3 Estrategias para combatir el riesgo.	X		
	3.4 Herramientas para la gestión del riesgo.	X		
	3.5 Monitoreo y revisión.	X		
4. Lineamientos riesgos relacionados con posibles actos de corrupción.		X		Actividades establecidas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numerales 4.14 y 4.15
5. Lineamientos riesgos de seguridad de la información.		X		Actividades plasmadas en la Guía Administración de Riesgos G-MC-04 de 31 de diciembre de 2019; numerales 4.6 y 4.7.6, aunque se aclara que en la última guía del DAFP se usa el termino de "lineamientos riesgos de seguridad de la información", como lo tiene definido el MINTIC y no seguridad digital, como se consigna en la guía del MJD. El Riesgo de Seguridad de la Información es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (de la guía 2020 del DAFP)

Esta auditoría, al realizar la verificación de cada una de las etapas de la última guía de riesgos, del DAFP ya mencionada observó que, en general, el Ministerio da cumplimiento a los lineamientos generados en el mencionado documento -que es posterior a la guía del MJD-. No obstante, se recomienda a la OAP, evaluar la necesidad de actualizarla, teniendo en cuenta las observaciones realizadas en el cuadro anterior, puntos 1.2, 3.1, 3.2 y 5, que hablan de la explicación del nivel de aceptación del riesgo -apetito-, la calificación de probabilidad e impacto, así como las responsabilidades, frente a la gestión y materialización de riesgos, y se dan los lineamientos referentes a la seguridad de la información.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02	
		Versión: 03	

Como se evalúa el riesgo hoy en el MJD

Actualmente, para la calificación del riesgo, el MJD analiza el nivel de probabilidad y el nivel de impacto del riesgo, siguiendo los lineamientos de la guía interna -con la cual la OCI realiza el seguimiento de la modelación- que se basó en la anterior guía del DAFP (2018).

Para la probabilidad, el MJD actualmente usa el siguiente cuadro:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos dos años o nunca se ha presentado
2	Improbable	Pudo ocurrir en algún momento, es poco común o frecuente	Se ha presentado al menos una vez en el último año
3	Moderada	Puede ocurrir en algún momento	Se ha presentado al menos una vez en los últimos 8 meses
4	Probable	probablemente ocurrirá en la mayoría de las circunstancias	Se ha presentado al menos una vez en los últimos cuatro meses
5	Casi certeza	Se espera que ocurra en la mayoría de las circunstancias	Se ha presentado más de una vez durante los últimos cuatro meses

Para el impacto de los riesgos de gestión, se usa la siguiente tabla:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la entidad

Para establecer el impacto de los riesgos de corrupción, se tienen en cuenta los parámetros de calificación incluidos en la herramienta de ayuda de la guía del MJD y se acude a la siguiente tabla:

N°	PREGUNTA	RESPUESTA	
		SI	NO
	Si el riesgo de corrupción se materializa podría:		
1	¿Afecta el grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, Servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Una vez se haya diligenciado el cuadro, se calcula el impacto del riesgo identificado así:

- Responder si, de una a cinco preguntas, genera un impacto moderado.
- Responder si, de seis a once preguntas genera un impacto mayor.
- Responder si, de doce a veinte preguntas genera un impacto catastrófico.

Posteriormente se pasa a la siguiente tabla de impactos:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Moderado	Genera medianas consecuencias sobre la entidad
2	Mayor	Genera altas consecuencias para la entidad
3	Catastrófico	Genera consecuencias desastrosas para la entidad

Cómo propone evaluar el riesgo la guía 2020 del DAFP

En la guía de riesgos del DAFP (2020) se establecen unos nuevos criterios para medir la probabilidad, relacionada con la frecuencia con que se ejecuta cada actividad que, a juicio de la OCI, permitiría más fácilmente determinar el nivel de probabilidad, aunque mantiene la estructura de cinco niveles, que actualmente se maneja:

NIVEL	DESCRIPTOR	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
1	Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
2	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
3	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
4	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
5	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

También, en la guía del DAFP del 2020, se establecen nuevos criterios, para establecer el impacto:

NIVEL	DESCRIPTOR	AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
1	Leve 20%	Afectación menor a 10 SMMLV	El riesgo afecta la imagen de algún área de la organización
2	Menor 40%	Entre 10 y 50 SMMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
3	Moderado 60%	Entre 50 y 100 SMMLV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4	Mayor 80%	Entre 100 y 500 SMMLV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
5	Catastrófico 100%	Mayor a 500 SMMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

En este sentido, se recomienda a la OAP, verificar para la etapa de valoración de los riesgos de gestión, la realización de una actualización de la guía interna del MJD, o para futuras actualizaciones, consignar que los cambios que proponga el DAFP sean incorporados de manera inmediata en la guía del ministerio, o que se tomará como referencia metodológica la guía actualizada del DAFP⁸. En esta actualización, que se efectuó a diciembre de 2020, se precisan los análisis de probabilidad e impacto y sus tablas de referencia, así como el mapa de calor resultante.

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía DAFP 2018, para la administración del riesgo y el diseño de controles en entidades públicas. Sobre este particular, se rescata que la OAP generó unos lineamientos a todas las dependencias de esta cartera ministerial para la identificación y correcta administración del riesgo de corrupción, fundados en un informe de la OCI con unas recomendaciones que, justamente, tenían que ver con aquellos.

Por otro lado, esta auditoría, realizó la verificación de las matrices de riesgos que corresponden a gestión, corrupción y seguridad de la información, para cada uno de los dieciocho (18) procesos de la cadena de valor del MJD; para este propósito se diseñó una tabla de seguimiento -que se verá más adelante-, en la que se cuantifica el total de riesgos y controles existentes en el MJD, y que permitirá mitigar las amenazas para los objetivos de cada proceso.

En lo concerniente a gestión y corrupción, es importante decir que, para la identificación de los riesgos y controles, se llevaron a cabo capacitaciones, acompañamientos y asesorías técnicas lideradas por la OAP; en total, para esos riesgos, se realizaron 72 reuniones⁹, en las cuales se socializó la política de riesgos, y se dio explicación al manejo del formato herramienta de riesgos identificado con el código F-MC-G04.

Se constató que en las reuniones de asesoría técnica brindadas por la OAP, a partir de una lluvia de ideas se ejecuta la identificación del riesgo, sus causas y controles, y que se ha avanzado en el tema de tener en cuenta las observaciones y recomendaciones realizadas por la Oficina de Control Interno, en relación, tanto a los seguimientos hechos con anterioridad al mapa de riesgos de corrupción, así como los hallazgos de las auditorías desarrolladas por esta oficina para los riesgos de gestión; es de aclarar que estas asesorías técnicas se efectúan de manera individual con el referente de cada dependencia.

En relación con la identificación de los riesgos y controles asociados a seguridad de la información¹⁰, se constató que la identificación del riesgo se desarrolla teniendo en cuenta la Guía de Administración del Riesgo del MJD y las indicaciones del MSPI¹¹ y que es un proceso nuevo

⁸ Dice el DAFP que en el paso de valoración del riesgo, se establecen los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad, proponiéndose en la tabla para el análisis de probabilidad con un enfoque en la exposición al riesgo, análisis que le permite a los líderes de proceso contar con elementos objetivos para su definición; en cuanto a la tabla de impacto, se consideran la afectación económica y reputacional como aspectos principales frente a la posible materialización de los riesgos, en tal sentido, se ajusta la matriz de calor de acuerdo con la escala de severidad definida en 5 zonas (baja, moderada, alta y extrema), elementos que, en su conjunto, plantean un análisis más ácido, es decir de mayor profundidad y estricto, teniendo en cuenta el entorno cambiante en el cual se desenvuelven las entidades públicas del país

⁹ En el periodo comprendido entre abril de 2020 y septiembre de 2021.

¹⁰ Proceso que fue liderado por la DTGJ

¹¹ Modelo de Privacidad y Seguridad de la Información del MINTIC.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

en el MJD -a partir de marzo de 2020-, que aún está en desarrollo, levantando los riesgos y controles para los activos de información que se han identificado en el MJD¹².

5.4 Riesgos y controles

A continuación, se presenta una tabla que resume la cantidad de los riesgos y controles establecidos por las dependencias, para cada uno de los procesos de la cadena de valor del MJD:

Riesgos identificados por procesos.	Gestión		Seguridad en la Información		Corrupción		Total, riesgos	Total, controles
	Riesgos	Controles	Riesgos	Controles	Riesgos	Controles		
Acceso a la Justicia	2	4	59	12	2	6	63	22
Direccionamiento y planeación institucional	2	8	21	0	No identificado	0	23	8
Formulación y seguimiento de las políticas públicas	1	3	25	14	No identificado	0	26	17
Formulación y seguimiento de proyectos normativos	1	3	17	6	No identificado	0	18	9
Fortalecimiento del principio de seguridad jurídica	4	12	14	2	No identificado	0	18	14
Gestión administrativa	3	8	11	11	1	2	15	21
Gestión contra la criminalidad y la reincidencia	11	26	26	14	3	10	40	50
Gestión contractual	1	3	17	0	3	5	21	8
Gestión de la información y las comunicaciones	2	7	43	9	1	2	46	18
Gestión de la Relación con los Grupos de Interés	1	6	18	18	No identificado	0	19	24
Gestión de las Tecnologías y la Información	2	9	11	3	No identificado	0	13	12

¹² Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA		Código: F-SE-01-02
			Versión: 03

Riesgos identificados por procesos.	Gestión		Seguridad en la Información		Corrupción		Total, riesgos	Total, controles
	Riesgos	Controles	Riesgos	Controles	Riesgos	Controles		
Gestión del conocimiento	No identificado	0	5	4	No identificado	0	5	4
Gestión del talento humano	7	19	19	1	3	7	29	27
Gestión documental	2	6	14	1	1	1	17	8
Gestión financiera	4	12	26	0	2	3	32	15
Gestión del jurídica	6	18	55	0	No identificado	0	61	18
Mejora integral de la gestión institucional	2	5	6	0	No identificado	0	8	5
Seguimiento y evaluación	2	7	12	3	1	3	15	13
Total	53	156	399	98	17	39	469	293

De la tabla anterior, podemos concluir que:

- En las matrices aportadas se identificaron un total de 469 líneas de riesgos, discriminados así: de gestión 53, que equivalen al 11.30% del total, de seguridad de la información 399, que corresponden al 85.07%, y corrupción 17, que representan el 3.63% del total de riesgos. Se aclara, en cuanto a los riesgos de seguridad de la información, que la OCI al realizar la revisión de las matrices aportadas por la DTGIJ, encuentra que, para los 399 activos de información identificados, y que corresponden a los dieciocho (18) procesos de la entidad, se vinculan con 399 riesgos, pero al revisar la matriz, en realidad se establecieron quince (15) riesgos de seguridad de la información que se están repitiendo, para los 399 activos de información, por ello al sumar nos totalizan 399 filas de riesgos, que arrojan la sumatoria.
- Para tratar los riesgos se han diseñado 293 controles¹³ discriminados así: ciento cincuenta y seis, 156, que equivalen al 53,24%, relacionados con gestión, noventa y ocho, 98 (33,44%) para los riesgos de seguridad de la información y treinta y nueve, 39 (13,32%) de corrupción.
- La OCI entiende, en cuanto a los riesgos de seguridad de la información, que es un proceso iniciado en 2020, y por lo tanto aún se encuentra en implementación el levantamiento de los riesgos y controles; pero, en todo caso, se invita a la DTGIJ, como a

¹³ En las matrices reportadas como evidencias (gestión, seguridad y corrupción) por la OAP y la DTGIJ

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

la OAP para que revisen los riesgos que aún no tienen controles, de tal suerte que se determine de nuevo su riesgo inherente e implemente su seguimiento, lo cual permitiría mitigar las causas generadoras, por cuanto lo deseable es que cada riesgo tenga -al menos- un control asociado, que mitiga la posibilidad de materialización de la amenaza, a menos que la decisión, de la alta dirección, en relación con su administración sea la de la aceptación.

5.4.1 Análisis de Riesgos y controles

La OCI procede a realizar la verificación de los riesgos y controles, los cuales deben cumplir con las pautas definidas en la guía de administración de riesgo del MJD. Para cumplir con ello se diseñó una tabla, que se observará más adelante, dando prioridad a los calificados con riesgo inherente alto o extremo, circunstancia por la cual se seleccionaron, a criterio de la auditoría, cuatro (4) riesgos de gestión, tres (3) de corrupción y dos (2) de seguridad de la información asociados al proceso TIC, para efectuar el análisis respectivo.

Riesgos de Gestión y controles

Para la verificación de los controles de gestión, se tuvieron en cuenta los parámetros de calificación incluidos en la herramienta de ayuda de la guía del MJD y se acude a la siguiente tabla:

VERIFICACIÓN DISEÑO DE LOS CONTROLES						
1. ¿Existe un responsable asignado de la ejecución?	2. ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	3. ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	4. ¿Las actividades que desarrollan en el control realmente buscan por sí solas prevenir o detectar las causas que puedan dar origen al riesgo; ejemplo: Verificar, Validar, Cotejar, Comparar, Revisar	5. ¿La fuente de Información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	6. ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	7. ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?
Asignado=15 No asignado=0	Adecuado=15 Inadecuado=0	Oportuna=15 Inoportuna=0	Prevenir=15 Detectar=10 No es un control=0	Confiable=15 No confiable=0	Se investigan y se resuelven oportunamente =15 No se investigan y se resuelven oportunamente asignado=0	Completa=10 Incompleta=5 No existe=0

Tabla de calificación controles

En las siguientes tablas se analizarán los riesgos de gestión, causas y controles. En la primera fila se consigna el proceso asociado en la cadena de valor; en la segunda, el riesgo identificado por la primera y segunda línea de defensa y se le realiza su análisis; posteriormente, se consigna la causa determinada por la dependencia y la descripción del control diseñado, la clase de control y el comentario de la OCI:

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	GESTIÓN DE LA RELACIÓN CON LOS GRUPOS DE INTERÉS		COMENTARIO OCI
RIESGO	Incumplimiento de los términos para responder PQRD a los grupos de interés del Ministerio		<p>Aunque el riesgo está identificado, considera la OCI que se encuentra incompleto, faltando por incluir el riesgo de ausencia de respuesta, como también lo concerniente a los parámetros procedimentales - internos- que el MJD ha instituido para responder, con calidad, a los grupos de interés.</p> <p>El GSC identificó seis (6) causas y, a cada una, le incluye un control, como se verá a continuación.</p>
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIO OCI
1.Falta de conocimiento por parte de servidores y contratistas para el correcto manejo del Sistema de Gestión Documental que soporta la gestión de las PQRSD	El Grupo de Gestión Documental, al menos una vez al año, y a fin de fortalecer el conocimiento sobre el manejo de la herramienta para el trámite de PQRSD, realizará una capacitación sobre el uso adecuado del Sistema de Gestión Documental, según los lineamientos del Manual de Archivo y Correspondencia de la Entidad, a servidores y contratistas de las diferentes dependencias, En caso de que las personas citadas a la capacitación no asistiesen a estas el Coordinador del GGD debe realizar la solicitud a la dependencia en donde se presentó inasistencia mediante memorando informando la fecha y hora de la nueva capacitación haciendo énfasis en una posible obligatoriedad.	Detectivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles. El control permitiría realizar el seguimiento a las actividades desarrolladas, que buscan garantizar el buen manejo del Sistema de Gestión documental, y con esto, se ataca una de las causas generadoras del riesgo.
2.Incorrecto reparto de las PQRSD a las dependencias a través del Sistema de Gestión Documental.	El Grupo de Gestión Documental cada año, a fin de generar una adecuada distribución de correspondencia al interior de la entidad, programará una serie de capacitaciones con cada dependencia sobre las tipologías documentales de su competencia, en caso de que las personas citadas a la capacitación no asistiesen a estas, el coordinador GGD debe realizar la solicitud a la dependencia en donde se presentó inasistencia mediante memorando informando la fecha y hora de la nueva capacitación haciendo énfasis en una posible obligatoriedad.	Preventivo	La OCI, considera que la capacitación, en tipologías permite a las dependencias identificar oportunamente los documentos que le son entregados por el Grupo de Gestión Documental; con esto se evitan reprocesos y se garantizan las respuestas de manera oportuna. El control se encuentra debidamente identificado, con calificación de cien (100) en la evaluación realizada por la auditoría.
3.Inadecuado seguimiento a la respuesta de las PQRD dentro de las dependencias, en su	Los enlaces de PQRSD de las dependencias una vez al mes, para generar alertas tempranas respecto al cumplimiento de los términos de las PQRSD, realizarán seguimientos	Detectivo	La OCI, al evaluar el control encuentra que este es de carácter detectivo y permite realizar seguimiento, con alertas tempranas, a las respuestas

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	GESTIÓN DE LA RELACIÓN CON LOS GRUPOS DE INTERÉS	COMENTARIO OCI
rol de primera línea de defensa.	internos a la gestión de estas, de acuerdo con las directrices del Grupo de Servicio al Ciudadano En caso de que el enlace de PQRSD no realice el seguimiento, el GSC procederá a hacer un requerimiento al líder de la dependencia para que este de cumplimiento a la tarea asignada. Si al momento de realizar el seguimiento, el enlace detalla PQRSD próximas a vencerse, de forma inmediata informará a la persona responsable en EPX de esta situación para evitar su vencimiento	de las PQRD que se encuentran activas. El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. También atacaría otra causa que podría ser la de elaborar y firmar a tiempo el oficio de respuesta de las PQRD en el gestor documental, pero no realizar las gestiones de envío de la comunicación al peticionario; el cual está asociado a un indebido control a la gestión de envío por parte de la dependencia.
4. Falta de autocontrol de los colaboradores (servidores y contratistas) del Ministerio para dar respuesta a las PQRD recibidas de manera oportuna	El Grupo de Servicio al Ciudadano una vez publicado el informe trimestral de PQRD, para promover el autocontrol de los colaboradores en el tema, realizará el reconocimiento institucional de las tres (3) dependencias con los mejores desempeños en cada periodo de medición, a través de su divulgación vía mail interno. En caso de que se presenten empates se incluirán en el reconocimiento y si una dependencia presenta una reducción significativa (más del 10%) en sus resultados se enviará un correo alertando sobre la situación para la revisión interna de esta.	Se encuentra que el control 4 de la matriz, contempla que el GSC realizará un reconocimiento a las dependencias con mejores desempeños, en realidad promueve la calidad y mejora continua. El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-.
5. Indebido seguimiento y control en la atención de PQRD por parte del GSC	El Grupo de Servicio al Ciudadano semanalmente, con el fin de generar alertas oportunas a las dependencias de la Entidad y en su rol de segunda línea de defensa, enviará correo electrónico a todas las dependencias que tengan PQRS asignadas, sobre próximos vencimientos de términos para responder. En caso de que el destinatario se encuentre en alguna situación administrativa que signifique su no lectura, se remitirá el reporte al personal asignado por el enlace.	La OCI acota que el control permitiría realizar un seguimiento al trámite interno de las respuestas. El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. Se recomienda que el correo se active de manera automática, según la parametrización hecha al ePX.
6. Indebido seguimiento y control en la atención de PQRD por parte del GSC	El Grupo de Servicio al Ciudadano trimestralmente para realizar control y seguimiento del estado de PQRSD realizara un informe sobre estas, el cual publicará en la página WEB y se llevará al Comité Institucional de Gestión y Desempeño En caso de que se identifiquen incumplimientos en términos de respuesta se realizará el envío de un reporte a la OCID y así mismo se realizará una divulgación con las diferentes dependencias sobre los resultados del informe.	La OCI considera que el control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. Permite al MJD establecer las responsabilidades en caso de incumplimientos legales y/o procedimentales en la gestión de respuesta.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	FORMULACIÓN Y SEGUIMIENTO DE LAS POLÍTICAS PÚBLICAS		COMENTARIO
RIESGO	Incumplimiento de metodología del proceso de formulación de políticas públicas competencia del Ministerio de Justicia y el Derecho.		El riesgo de incumplimiento se encuentra correctamente identificado. Se han establecido en el MJD, tres (3) causas y, a cada una, se les ha incluido un control, como se ve enseguida.
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIO OCI
1.Desconocimiento de la metodología de formulación de políticas públicas	El funcionario o contratista designado por cada viceministerio, al menos dos veces al año, a fin de fortalecer el conocimiento en la metodología vigente para la formulación de política pública, realiza capacitación y divulgación de la misma a los funcionarios encargados de formular política pública. Si al momento de realizar la capacitación, el personal asistente es menor a la tercera parte, se deberá reprogramar la capacitación o realizar un proceso de divulgación de la metodología a los no asistentes para de esta forma lograr la cobertura total de las personas involucradas en este proceso	Preventivo	La OCI, realizó verificación del control; su calificación sería 100 - según la tabla de diseño de controles-. Al capacitar oportunamente, en la metodología, a los funcionarios responsables de las políticas públicas, se permitiría una buena apropiación y, por lo tanto, una adecuada formulación de las políticas públicas a cargo del MJD.
2.Tiempos limitados o insuficientes	Los viceministros en coordinación con los directores, cada vez que se vaya a formular política pública, a fin de controlar los tiempos y poder actuar frente a situaciones que impidan el oportuno desarrollo de las actividades, establece un cronograma con fechas y responsables para cada una de las etapas del proceso de formulación de política. Si en el transcurso de las labores se presenta algún factor externo o interno que impida el oportuno cumplimiento de los tiempos previamente establecidos se procederá a modificar el cronograma a fin de poder adelantar las actividades en los tiempos requeridos y que impidan el incumplimiento de las actividades de la metodología de formulación.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 - según la tabla de diseño de controles-. Al establecer un cronograma, con fechas y responsables, para la formulación de las políticas y sus ajustes en caso de algún inconveniente, se permitiría la formulación y/o ajustes, en los tiempos esperados.
3.Falta de competencias específicas en las temáticas para la formulación de política pública.	Los viceministros en coordinación con los directores, cada vez que se vaya a formular política pública, a fin de seleccionar al personal más idóneo para las temáticas a tratar en la formulación de políticas públicas y teniendo en cuenta el manual de funciones del Ministerio, procederá a distribuir internamente ya sea el proceso completo de formulación o las actividades relacionadas en la metodología al personal a cargo. Si en el proceso de distribución de actividades o temáticas, se presenta una deficiencia en conocimientos o experiencia interna se podrá recurrir a una entidad externa o a expertos, para solicitar el apoyo requerido.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 - según la tabla de diseño de controles-. Al seleccionar a los servidores y/o apoyos más competentes, se logra mitigar el riesgo de incumplimiento en la metodología.

 <div style="display: inline-block; background-color: #0056b3; color: white; padding: 2px;"> La justicia es de todos </div> <div style="display: inline-block; background-color: #0056b3; color: white; padding: 2px; margin-left: 10px;"> Minjusticia </div>	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	GESTIÓN CONTRA LA CRIMINALIDAD Y LA REINCIDENCIA	COMENTARIO OCI	
RIESGO	No realizar el traslado de las solicitudes de visita al Sistema de Responsabilidad Penal para Adolescentes - SRPA y al Sistema Penitenciario y carcelario que no son competencia del Ministerio de Justicia y el Derecho.	Es un riesgo que afecta las capacidades de atención de las entidades que conforman el sistema penitenciario y carcelario; que se encuentra correctamente identificado. Se han establecido, en el MJD, tres (3) causas y tres controles, como se ve enseguida.	
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIO OCI
1.Olvido por parte del personal de la solicitud	El coordinador del grupo penitenciario y carcelario diariamente, para llevar un control de las solicitudes que llegan a la dirección y el debido proceso de respuesta a las mismas cuando no son competencia del ministerio, realizara un seguimiento a través de un cuadro de control donde se consigna si son o no competencia del ministerio y el paso a seguir. Si en el momento de realizar el seguimiento, se identifican solicitudes recibidas el día anterior que no han sido trasladadas se debe realizar el traslado de forma inmediata, informando a las entidades que recibirán la solicitud para que la prioricen, así mismo se deberá informar de la situación al director quien podrá realizar un requerimiento al funcionario que no ha realizado el traslado.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. Permite verificar un seguimiento oportuno a las solicitudes y sus respuestas, e igualmente el cuadro de control permite realizar la verificación oportuna, minimizando posibles olvidos por parte de los responsables.
2.Falta de conocimiento de las obligaciones misionales por parte del personal asociado a la Dirección de Política Criminal y Penitenciaria	El coordinador del grupo penitenciario y carcelario semanalmente, para llevar un control de las solicitudes que llegan a la dirección y el debido proceso de respuesta a las mismas cuando no son competencia del ministerio, realizara un seguimiento a través de un cuadro de control donde se consigna si son o no competencia del ministerio y el paso a seguir. Si en el momento de realizar el seguimiento, se identifican solicitudes recibidas la semana anterior que no han sido trasladadas se debe realizar el traslado de forma inmediata, informando a las entidades que recibirán la solicitud para que la prioricen, así mismo se deberá informar de la situación al director quien podrá realizar un requerimiento al funcionario que no ha realizado el traslado.	Preventivo	El control definido está bien diseñado, su calificación sería 100 -según la tabla de diseño de controles-. Permite discriminar las solicitudes que son competencia y/o trasladar las que no.
3.Desconocimiento de la normatividad asociada	El funcionario designado por el líder de la Dirección de Política Criminal y Penitenciaria, al menos una vez cada semestre, a fin de fortalecer el conocimiento en las obligaciones misionales de la Dirección, especialmente en los temas relacionados con el Sistema Penitenciario y Carcelario y el SRPA y así mismo en la normatividad asociada al proceso, realizará un proceso de sensibilización y capacitación a todo el personal de la DPCP. En caso de que, al momento de la ejecución de la actividad hallase un faltante de citados mayor o igual a la tercera parte, se deberá o reprogramar la actividad o realizarla una segunda vez, si aún después de esto se sigue presentando inasistencia se enviará por correo electrónico la información a los no asistentes para su consulta.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100. La OCI, considera que se ataca la causa.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	GESTIÓN CONTRA LA CRIMINALIDAD Y LA REINCIDENCIA		COMENTARIO OCI
RIESGO	Errores en el proceso de expedición del Certificado de Carencia de Informes por Tráfico de Estupefacientes.		La OCI considera que el error en el proceso de expedición es una causa generadora del verdadero riesgo, que sería el incumplimiento en el procedimiento de expedición del certificado. Se recomienda a la OAP, en conjunto con la dependencia, revisar la redacción del riesgo.
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIO OCI
1. Errores en el diligenciamiento de los datos solicitados en la plataforma SICOQ para la solicitud.	Los funcionarios designados por la Subdirección de Control y Fiscalización de Sustancias Químicas y Estupefacientes- Grupo Control de Sustancias Químicas- cada vez que se presente una modificación o actualización normativa y/o de la plataforma, a fin de minimizar la posibilidad de errores al momento del diligenciamiento de la información en esta, actualizará el material necesario relacionado con el uso de la plataforma SICOQ y de las Sustancias Químicas (instructivos, manuales, circulares y guías). Dependiendo del impacto en el proceso se debe realizar la modificación o actualización en el menor tiempo posible. Se debe acompañar el proceso de actualización o modificación con capacitaciones a los usuarios, teniendo en cuenta la demanda y las cargas laborales internas.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. Permite actualizar la información del trámite por cambios en la norma y/o en el procedimiento, así como la capacitación a los solicitantes, para minimizar o evitar los errores en el diligenciamiento de los datos.
2. Fallas en el proceso de revisión de los datos diligenciados en la plataforma SICOQ	Los funcionarios designados por la Subdirección de Control y Fiscalización de Sustancias Químicas y Estupefacientes- Grupo Control de Sustancias Químicas- cada vez que se presente una modificación o actualización normativa y/o de la plataforma, a fin de minimizar la posibilidad de errores al momento del diligenciamiento de la información en esta, actualizará el material necesario relacionado con el uso de la plataforma SICOQ y de las Sustancias Químicas (instructivos, manuales, circulares y guías). Dependiendo del impacto en el proceso se debe realizar la modificación o actualización en el menor tiempo posible. Se debe acompañar el proceso de actualización o modificación con capacitaciones a los usuarios, teniendo en cuenta la demanda y las cargas laborales internas. Evidencia: Material actualizado Asistencia a las capacitaciones	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. La OCI, verificó el control encontrando que permite actualizar la información en el momento de suceder alguna modificación o actualización, con la correspondiente capacitación a los funcionarios responsables del proceso de revisión de los datos en el SICOQ; con esto, se evita la ocurrencia de errores en el proceso de análisis.

La OCI observó que la mayoría de los riesgos de gestión evaluados, se encuentran debidamente identificados, y sus controles son adecuados; sin embargo, considera que algunos deben ser ajustados, de acuerdo a las recomendaciones realizadas en la columna de comentarios OCI.

Riesgos y controles de seguridad de la información

La OCI, al realizar la revisión de las matrices aportadas por la DTGIJ, encuentra que, para los 399 activos de información, correspondientes a los dieciocho (18) procesos de la entidad, existen en realidad quince (15) riesgos de seguridad de la información, que se repiten, a saber:

1. Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros).

 <div style="display: inline-block; background-color: #0056b3; color: white; padding: 2px;"> La justicia es de todos </div> <div style="display: inline-block; background-color: #0056b3; color: white; padding: 2px; margin-left: 10px;"> Minjusticia </div>	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

2. Acción Industrial / Espionaje (infiltración canales de comunicación, servicios de información, servicios informáticos)
3. Actos vandálicos y/o terrorismo
4. Arquitectura insegura de la red.
5. Degradación del rendimiento de las aplicaciones o la red, Retraso o interrupción de los sistemas de información y/o la información
6. Destrucción de equipos o medios
7. Destrucción, pérdida, extravío, robo, daño o alteración de información en medio físico o lógico.
8. Fuga, revelación o divulgación de información sensible y/o confidencial
9. Hurto, fraude o sabotaje de equipos, medios, información o documentos.
10. Incumplimiento contractual y/o sanciones.
11. Indisponibilidad del servicio por gestión de cambio (plataforma o portales).
12. Interrupción total o parcial de los procesos del negocio por falla/daño/degradación de los equipos informáticos, equipos de comunicaciones (dispositivos de red, planta telefónica, servidores, UPS, entre otros), debido a cualquier evento o incidente
13. Pérdida de información debido a errores en la ejecución del procedimiento de backup, fallas en el software de backup.
14. Pérdida, alteración, acceso no autorizado, divulgación no autorizada y/o fuga de información confidencial/sensible procesada y/o almacenada.
15. Problemas, fallas o no disponibilidad de los servicios esenciales (internet, teléfonos, aire acondicionado, energía, agua, etc.)

Por lo anterior, en las matrices aportadas existen 399 filas de riesgos para los 399 activos de información del MJD, de los cuales, según la matriz de evaluación de la dirección, se contabilizan de la siguiente manera, teniendo en cuenta el riesgo inherente:

- 342 presentan un riesgo inherente bajo, cuya opción de manejo, establecida por la dirección¹⁴, es asumir el riesgo y algunos tienen controles.
- 43 presentan riesgo inherente moderado, cuya opción de manejo es reducir el riesgo, a través de controles.
- 12 presentan riesgo inherente alto, cuya opción de manejo es reducir el riesgo, a través de controles.
- 2 presentan riesgo inherente extremo, cuya opción de manejo es reducir el riesgo, a través de controles.

Se recomienda a la DTGIJ, como se dijo líneas arriba, seguir con el proceso de evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, como también que se revisen los riesgos de activos de información, que aún no tienen controles, determinando de nuevo su riesgo inherente e implemente su seguimiento, que permitiría mitigar las causas generadoras; por cuanto lo deseable es que cada riesgo tenga al menos un control asociado, que mitigaría la posibilidad de materialización de la amenaza. Se sugiere que este ejercicio se realice con el acompañamiento y asesoría de la OAP.

En las siguientes tablas se analizarán dos (2) riesgos del proceso de gestión de las tecnologías de la información. En la tercera columna se consigna el comentario OCI; en la segunda, sobre el

¹⁴ Apetito de riesgo, que será aprobado por el Comité correspondiente.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

riesgo identificado, se realiza su análisis; posteriormente, se consigna la causa determinada por la dependencia y la descripción del control diseñado, la clase de control y el comentario de la OCI:

PROCESO	GESTIÓN DE LAS TECNOLOGÍAS Y LA INFORMACIÓN		COMENTARIO OCI
RIESGO	Actos vandálicos y/o terrorismo		<p>La OCI considera que el riesgo está mal identificado; en realidad lo descrito como riesgo (actos vandálicos y/o terrorismo) es una causa que puede afectar la plataforma y servidores del MJD.</p> <p>La OCI se permite recomendar el siguiente riesgo -que será evaluado por la DTGIJ-:</p> <p>Afectación de la plataforma tecnológica del MJD, que impacta en sus canales, servicios, correos institucionales, servidores, aplicaciones, etc.</p> <p>En lo concerniente a causas se puede decir que podrían haber más, además de los actos vandálicos, como por ejemplo, la falta de implementación de buenas prácticas en TIC, o que no se cuente con el respaldo en cuanto a servidores o en cuanto a suministro de energía eléctrica, o que la plataforma se encuentra obsoleta y/o desactualizada, entre otras; y para cada uno, se tendrían que implantar uno o más controles.</p>
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIOS OCI
Arquitectura insegura de la red.	<p>1. Se modificó el direccionamiento del dominio minjusticia.gov.co, a través de IFX</p> <p>2. El sitio de minjusticia.gov.co tendrá como primera línea de contención el firewall del Ministerio de Defensa.</p> <p>3. Se cambiaron las IP's relacionadas al sitio web para dejar de recibir ataques masivos desde diferentes partes del mundo, puesto que ya había un descubrimiento por parte de los ciber atacantes, lo cual provocaban la caída del servicio cada vez que se reestablecía.</p>	Detectivo/ correctivo	<p>La OCI encuentra que una arquitectura insegura de red es una causa que podría afectar la plataforma tecnológica del MJD.</p> <p>En cuanto al diseño del control, la OCI considera que no es adecuado, ya que no cumple con los parámetros de valoración definidos en la guía tanto del MJD, como del DAFP, ni con los establecidos en el MSPI -que también tiene una tabla de valoración cuantitativa de los controles-.</p> <p>Se recomienda a la DTGIJ adecuar las calificaciones con puntaje, como lo determina la guía del DAFP o con la guía del MSPI de MINTIC y no como se encuentra actualmente -respondiendo sí o no- en la calificación observada en la matriz aportada</p> <p>La OCI considera que el control es de carácter correctivo, aunque debe redactarse en forma adecuada- ya que lo consignado corresponde a las medidas correctivas tomadas, después de haberse materializado el riego este año.</p>

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	GESTIÓN DE LAS TECNOLOGÍAS Y LA INFORMACIÓN	COMENTARIO OCI	
RIESGO	Fuga, revelación o divulgación de información sensible y/o confidencial	<p>La OCI encuentra que es un riesgo posible para el proceso de TIC, y está bien definido</p> <p>Otras causas, que podrían tener un control, además de las establecidas por la DTGIJ podrían ser:</p> <ul style="list-style-type: none"> - Debilidad en los procesos de detección de fallas tempranas y mantenimiento para los sistemas de información - Interés de atacantes externos en borrar y/o modificar información para afectar el funcionamiento de la entidad - Los servidores y/o contratistas pueden tener interés en borrar y/o modificar información de los sistemas para afectar el funcionamiento de la entidad 	
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIOS OCI
Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros.	Asignación de responsabilidades para la seguridad de la información.	Preventivo	<p>La OCI considera que es un riesgo inherente extremo. La opción de manejo no es adecuada, ya que lo que se debe evitar es el riesgo de posible pérdida o fuga de información. Igualmente, no se encuentra cual es el riesgo residual luego de aplicar el control (no hay evaluación de la probabilidad y el impacto residual). Como también no es claro quién es el responsable de su ejecución; por lo tanto, se debe rediseñar el control.</p> <p>Diseñar un mecanismo de control de acceso a los diferentes usuarios internos o externos-</p>

La OCI encuentra que existe un riesgo directamente del proceso TIC¹⁵, que ha sido advertido por esta oficina en anteriores ocasiones y que corresponde a la adquisición de bienes y servicios informáticos desarticulados con las necesidades del Ministerio, cuyas causas podrían ser debidas, según la OCI, a:

- Deficiencias en las asesorías técnicas o con información de baja calidad o poco confiable que dificulte tomar decisiones de adquisición de bienes o servicios tecnológicos
- Falta de priorización de los proyectos de tecnología que requieren las dependencias del MJD.
- Incumplimiento de los requerimientos de calidad de proyectos de TIC, asociados a bienes o servicios informáticos.

¹⁵ Se recomienda evaluar.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Las causas advertidas pueden generar para la entidad consecuencias como: Realizar adquisiciones innecesarias o inadecuadas, dejando atrás otros proyectos prioritarios de tecnología, detrimento patrimonial, reprocesos en los proyectos, pérdida de esfuerzos, hasta llegar a la insatisfacción con los resultados de los proyectos de tecnologías de la información.

Por lo anterior, la OCI recomienda evaluar la inclusión, en la matriz de riesgos del proceso de gestión de tecnologías y la información, de un control para la fase de planeación, otro para la de ejecución y uno posterior a la implementación. Se recomiendan los siguientes controles:

-Semestralmente el director de la DTGIJ, en conjunto con su equipo, revisará la viabilidad y prioridad de todas las necesidades de proyectos de TICs identificados durante el semestre, analizando su complejidad, compatibilidad, componentes, prioridad y tiempo de implementación. En caso de identificar proyectos inviables para el MJD, se emite el respectivo concepto sobre el proyecto de TICs solicitado, dejando evidencia en una matriz de priorización.

-Cada vez que se requiera, el director de la DTGIJ verificará si la solución contratada e implementada en el proyecto, aportó los resultados que se esperaban, constatando con la dependencia involucrada los resultados obtenidos y la efectividad de la solución en la resolución de la necesidad. Se evaluarán las inconformidades encontradas, informando al proveedor para su ajuste en el periodo de la garantía, de lo cual se dejará evidencia en un informe por proyecto ejecutado.

Por todo lo anterior, la OCI considera que el nivel de madurez del modelo seguridad y privacidad de la información del MJD, es respetable, según la tabla siguiente¹⁶ :

NIVEL	DESCRIPCIÓN
Inicial	En este nivel se encuentran las entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad disponibilidad y privacidad de la información.
Respetable	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente planificación del MSPI
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuentan con métricas, indicadores y realizan auditorias al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Análisis Riesgos de Corrupción

En las siguientes tablas se analizarán tres riesgos de corrupción, sus causas y controles. En la primera fila se consigna el proceso asociado en la cadena de valor, en la segunda el riesgo identificado por la primera y segunda línea de defensa y se le realiza su análisis; posteriormente,

¹⁶ Del instrumento de identificación de la línea base de seguridad, que publica MINTIC

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

se consigna la causa determinada por la dependencia y la descripción del control diseñado, la clase de control y el comentario de la OCI:

PROCESO	GESTIÓN DEL TALENTO HUMANO	COMENTARIOS OCI	
RIESGO	Posibilidad de que se beneficie a un funcionario o un tercero a partir de la ejecución indebida de los recursos públicos, en el marco de la gestión del talento humano	El riesgo identificado se encuentra bien definido, que presenta un impacto mayor	
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIOS OCI
Presiones internas o externas al funcionario que elabora la certificación.	El Coordinador del Grupo de Gestión Humana cada vez que se realiza un evento y con el fin de garantizar la adecuada ejecución de los planes de bienestar y capacitación, revisa y aprueba las actividades a realizar en el marco del fortalecimiento de la gestión humana de acuerdo con el plan de gestión de talento humano, en el caso de no ejecutar el plan de conformidad a lo establecido se actualiza el plan para el desarrollo efectivo de las actividades.	Preventivo.	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles. Al contar con la revisión, visto bueno y aprobación del coordinador del GGH, y que este obedece al plan de gestión, se puede mitigar el riesgo de corrupción en la emisión de la certificación de conformidad.
Vulnerabilidad de los aplicativos en los cuales se generan las certificaciones (acceso a terceros).	Los profesionales del Grupo de Gestión Humana cada vez que se realice una actividad de fortalecimiento, con el fin de asegurar la participación, llevarán registro de las actividades realizadas, adjuntando los soportes y evidencias cuando se requieran. En caso de no contar con un registro, en el momento, se levantará un acta de la actividad.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles. La causa, para la OCI es la vulneración al sistema de información. La falta de controles es una debilidad en el control interno del grupo. El control cuenta con responsables y tiempos definidos en su ejecución.
Falta de controles en los sistemas de generación de información que impidan su alteración.			

PROCESO	GESTIÓN DEL TALENTO HUMANO	COMENTARIO OCI	
RIESGO	Manipular la información laboral para favorecer el ingreso de personas a la planta de personal o por el contrario manipularla para suscitar la salida de un funcionario	El riesgo se encuentra definido para el ingreso y salida de personal, pero no contempla actividades como las novedades y liquidación de nómina. Se sugiere el siguiente: manipular la información laboral en los procesos asociados a la gestión del personal del MJD.	
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIOS OCI
Falta de control en la instancia de verificación de perfiles y requisitos	El Coordinador del Grupo de Gestión Humana cada vez que se realiza la incorporación de un funcionario, con el fin de verificar la idoneidad de la persona, revisa las certificaciones laborales contra la información de la hoja de vida, verificando el cumplimiento de requisitos y la legalidad de dichos documentos. En el caso de encontrar inconsistencias, solicita completar la información y realizar las aclaraciones necesarias.	Preventivo.	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-, y este ataca la causa establecida.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Modificación de los requisitos para favorecer un tercero	El auxiliar del GGH, cada vez que solicitan el préstamo de una hoja de vida, con el fin de salvaguardar la información contenida en ella y teniendo en cuenta que información reservada, registra el préstamo y devolución de las mismas en el formato destinado para este fin, verificando los folios y la integridad del documento. En caso de inconsistencias en el expediente, requiere al solicitante para que allegue la carpeta completa o informa el hecho ante el CGGH.		Aunque se observa que el control está bien diseñado, realmente la causa sería la modificación o sustracción de documentos para favorecer a un tercero
Presiones de un tercero	El Coordinador del Grupo de Gestión Humana cada vez que solicitan una certificación laboral, y con el fin de garantizar la veracidad de la información, revisa las certificaciones laborales contra la información de la hoja de vida; en caso de encontrar inconsistencias solicita al profesional ajustar la certificación, de tal manera que esta cumpla con los requisitos solicitados o la información contenida en el expediente.		El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. El control implementado al tener como responsable de revisión tanto de la hoja de vida como los documentos incorporados y la certificación generada,

PROCESO	GESTIÓN CONTRA LA CRIMINALIDAD Y LA REINICIENCIA		COMENTARIO OCI
Riesgo	Manipulación del proceso de certificado de carencia por parte de los profesionales que evalúan las solicitudes a fin de obtener un beneficio propio.		El riesgo se encuentra correctamente identificado. Al evaluar su impacto, arroja una calificación de 13, la cual corresponde a un impacto catastrófico. Sin embargo, hay que añadir que puede ser para beneficio propio o de un tercero.
CAUSA	DESCRIPCIÓN DEL CONTROL	CLASE DE CONTROL	COMENTARIOS OCI
Manipulación indebida de la información	Las personas designadas por el Grupo de Control de Sustancias Químicas para llevar a cabo los tramites de certificado de carencia, cada vez que se va a realizar el estudio de la solicitud, a fin de controlar el acceso a la información de las solicitudes, solicitarán el acceso a la información exclusivamente del proceso asignado. En el caso que una o más personas soliciten acceso a información que no corresponde al proceso asignado, las personas encargadas al interior de la subdirección del manejo de la correspondencia informarán del hecho al coordinador del grupo Control de Sustancias Químicas - Control de Cannabis, según corresponda y este último tomará las medidas del caso.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-. El control evita que se presente manipulación de la información, ya que el acceso al estudio de la solicitud es autorizado solo para el responsable de realizar el trámite y en el caso de que se solicite ingreso por una persona diferente, esto se debe reportar al coordinador del grupo, para que tome las medidas pertinentes.

 <div style="display: flex; justify-content: space-between; align-items: center;"> La justicia es de todos Minjusticia </div>	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Prebendas a los ingenieros químicos	Los miembros del Grupo de Control de Sustancias Químicas, cada vez que se reciba un requerimiento de un externo, de datos de contacto de quien tiene a cargo el estudio del trámite de certificado de carencia, a fin de evitar el acceso del solicitante a los datos de las personas que realizan el estudio del trámite, responderán que no es posible dar esta información por ningún canal y que si requieren de alguna otra información relacionada con el trámite, esta se recibirá por los canales establecidos formalmente. En el caso que el solicitante del trámite reitere el requerimiento, se pondrá en conocimiento del subdirector este hecho para que se tomen las medidas del caso.	Preventivo	El control se encuentra bien diseñado; su calificación sería 100 -según la tabla de diseño de controles-
Prebendas al personal jurídico			Se observó, por la auditoria, que el control evita que se conozca la identidad de los funcionarios que tienen a cargo el estudio de los requisitos técnicos y jurídicos; evitando así el ofrecimiento de dadas o prebendas por parte de externos, o al interior del ministerio.
Prebendas al personal técnico			

La OCI, al realizar la evaluación del diseño de los riesgos de corrupción y sus controles, realizó consulta al seguimiento, efectuado por la OCI, con corte al 30 de agosto de 2021, encontrando que han mejorado en su identificación y diseño, garantizando la mejora para la adecuada identificación y administración del riesgo. Con esto se reducen las posibles afectaciones que se puedan generar por una deficiente modelación del riesgo; adicional a esto invita a la segunda línea de defensa a seguir con el mejoramiento del diseño de los riesgos y controles, teniendo en cuenta las observaciones realizadas por la OCI, en los informes de auditoría y observando los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

6. Análisis de Riesgo

La Oficina de Control Interno, en el marco de su plan de auditoría con enfoque en riesgos, adelantó la presente auditoría evaluando los riesgos asociados al proceso de mejora integral de la gestión institucional¹⁷, que tiene como objetivo el de: “coordinar y administrar la implementación del sistema Integrado de Gestión del Ministerio de Justicia y del Derecho, con el fin de asegurar su mejora continua, conveniencia, eficacia y eficiencia conforme con los estándares adoptados”, y específicamente a la actividad¹⁸ de: “orientar la administración de los riesgos de gestión de los procesos, de corrupción de la entidad y de seguridad de la información, dentro de los sistemas de Gestión de Calidad, de acuerdo con los establecido en el documento G-MC-04-Guía para la administración del Riesgo”.

En ese sentido, es importante precisar que, revisado el mapa de riesgos en el Sistema Integrado de Gestión, se observó que existen los siguientes dos (2) riesgos identificados:

¹⁷ De código C-MC, versión 5, con fecha de vigencia del 28 de febrero de 2020.

¹⁸ A cargo de los profesionales del Grupo de Calidad y Transformación Organizacional

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

PROCESO	Mejora integral de la gestión institucional	
RIESGO 1. R1	Información desactualizada en el Sistema Integrado de Gestión -SIG-	
RIESGO 2. R2	Seguimiento inoportuno al sistema integrado de gestión -SIG-	
Causas	Descripción del Control	Comentarios OCI al riesgo y al control
R1C1 No tener la última versión del documento.	El coordinador del grupo de calidad y transformación organizacional al menos dos veces al año a fin de identificar posible documentación desactualizada o incompleta en el SIG realizará verificación de la documentación cargada en el sistema, en caso de encontrar información incompleta o desactualizada, requerirá a través de correo electrónico al responsable y facilitador del proceso él envió de la información actualizada. Evidencia: correo electrónico solicitando la información, respuesta enviada por el responsable o facilitador del proceso.	<p>La OCI se permite comentar que los dos riesgos establecidos, pueden ser consecuencias del riesgo asociado a la mejora integral de la gestión institucional, y que no permitiría la consecución de los objetivos del proceso, por lo cual la OCI recomienda el siguiente riesgo para el proceso, que será evaluado por la OAP:</p> <p>Incumplimiento por parte del MJD a los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión -MIPG-, al no estar conformes con los atributos de calidad de las políticas institucionales de gestión y desempeño, enmarcadas en las siete (7) dimensiones del modelo.</p> <p>Las causas, además de las establecidas, que también lo son, podría ser:</p> <p>-La debilidad en el seguimiento a la implementación del Modelo Integrado de Planeación y Gestión -MIPG- en el MJD -que hoy se encuentra como un riesgo R2-, otra causa -que ahora está como riesgo R1- sería no contar con información actualizada en el SIG, al no tener la última versión de los documentos aprobados, que genera un uso inadecuado de la documentación.</p>
R2C2 No reportar información a tiempo por parte de los responsables del proceso	La persona designada o el coordinador del grupo de calidad y transformación organizacional trimestralmente a fin de identificar información o documentación desactualizada o incompleta en el SIG, realizará verificación de la información cargada en el sistema, en caso de encontrar información incompleta o desactualizada, requerirá a través de correo electrónico al responsable y facilitador del proceso él envió o cargue de la información actualizada. Evidencia: correo electrónico solicitando la información, respuesta enviada por el responsable o facilitador del proceso.	<p>Los controles definidos, que están bien diseñados, permiten a la OAP verificar semestralmente la documentación del SIG, para poder así solicitar a las áreas responsables su actualización y envío de la información actualizada, así como el cargue de la misma en la matriz o sistema correspondiente.</p> <p>La OCI encuentra que, en el caso de esta auditoría, el documento actualizado sería la guía de riesgos del MJD, cuyo documento se encuentra publicado en la página WEB del MJD y fue constatado por esta auditoría.</p> <p>La OCI se permite anotar que respecto a la causa de no reportar información a tiempo por parte de los responsables y/o facilitadores de los procesos, en este caso, el facilitador es la misma OAP, y verificada la matriz aportada, la OAP no consignó en la matriz Excel, ningún seguimiento a la ejecución de los dos controles, a su cargo, en los cuatrimestres de seguimiento.</p> <p>Se recomienda al grupo, diligenciar la matriz en la parte correspondiente a los seguimientos de cada uno de los riesgos identificados en el sistema de gestión del MJD, para evitar el riesgo de incumplimiento a los lineamientos del MIPG, en este caso a la guía de administración de riesgos.</p>

6.1 Herramientas para la identificación y control del riesgo en el MJD

a. Herramienta Excel con código del SIG: F-MC-G04-01

Actualmente el MJD está atendiendo la estructuración y seguimiento de los riesgos y controles de gestión, de corrupción y de seguridad de la información, a través de una tabla Excel de guía, identificada con el código del SIG: F-MC-G04-01.

	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Esta es una herramienta en la cual se registra la información correspondiente a la identificación del riesgo del proceso, y también es una herramienta de control donde los líderes del proceso en cada dependencia registran sus seguimientos cuatrimestrales, y se consigna el seguimiento por parte de la segunda línea de defensa.

La OAP explica, en cuanto al seguimiento de los riesgos de gestión y corrupción que: “Las dependencias responsables de los riesgos, como primera línea de defensa, realizan el seguimiento cuatrimestral a los mapas de riesgos de gestión y corrupción, para lo cual remiten los correos de seguimiento y eventualmente se realizan reuniones con las dependencias para las actualizaciones o modificaciones. La Oficina Asesora de Planeación, como segunda línea de defensa, revisa los riesgos y el seguimiento realizado por las dependencias, consolida la información y de ser requerido publica las matrices actualizadas.”

En ese sentido, la OCI se permite acotar que

En cuanto a la identificación y seguimiento de los riesgos y controles de seguridad de la información, se constató que -desde el año 2020- se implementó en el MJD la gestión de riesgos de seguridad de la información a cargo de la Dirección de Tecnologías y Gestión de la Información en Justicia, realizándose su proceso de identificación y análisis en la misma herramienta Excel de código F-MC-G-04-01. Se comprueba que se ha avanzado en la identificación, análisis, de riesgos y controles, y este año se realizó un primer monitoreo; aunque se encuentra que en las matrices aportadas aún no tienen diligenciada la parte correspondiente al plan de tratamiento de esos riesgos de seguridad de la información y menos el monitoreo para todos los controles implementados. Por lo anterior, la OAP aclara que: “aún no se ha cerrado el ciclo PHVA, porque falta la mejora continua que se espera tener en la próxima vigencia”.

b. Módulo de riesgos en DARUMA

El aplicativo DARUMA tiene un módulo de riesgos, que hace parte de una de las preguntas elevadas por la auditoría, sobre el estado actual de dicho módulo.

La OCI encuentra que el módulo se encuentra en etapa de pruebas y no ha entrado en producción, actualmente según lo corroborado -noviembre de 2021- se están incorporando -en un ambiente de pruebas- los riesgos que se encuentran en la herramienta Excel F-MC-G04-01, para posteriormente poder entrar a incorporar los riesgos, controles y seguimientos en el aplicativo¹⁹

Se recomienda avanzar en la primera incorporación de las matrices de riesgos, en el módulo de riesgos del sistema DARUMA, en ambiente de producción, previa capacitación a las diferentes dependencias sobre su uso, módulo que debe ser la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad de la información en el MJD.

Se recomienda, también, asociar los indicadores de la política de gestión del riesgo en el módulo de indicadores de DARUMA.

¹⁹Cuando entre a producción el módulo y todo el proceso de modelación y seguimiento se pueda efectuar en dicho aplicativo, para obviar el Excel.

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

6.2 Indicadores de la gestión del riesgo

En la información suministrada por la OAP, se evidenció que esta dependencia tiene tres indicadores de seguimiento de la política, de lo cual aportó los resultados:

No	Indicador	Objetivo	Fórmula	Cumplimiento según la OAP
1	Cumplimiento de los controles establecidos en los riesgos	Determinar la efectividad de los controles establecidos en los riesgos	# de controles no efectivos / # de controles identificados en los riesgos*100	100
2	Seguimiento a la materialización de riesgos	Determinar el porcentaje de riesgos materializados en el período	# de riesgos materializados / # de riesgos identificados*100	97,1
3	Mapas de riesgos con observaciones de la OCI	Establecer de los riesgos identificados, cuánto tienen observaciones de la OCI	# de riesgos con observaciones OCI / # de riesgos identificados*100	82,06

La DTGIJ ha establecido un indicador de implementación, denominado nivel de implementación del modelo de Seguridad y Privacidad de la información que tiene como fórmula

No	Indicador	Objetivo	Fórmula	Cumplimiento según la DTGIJ
1	Nivel de implementación del modelo de Seguridad y Privacidad de la información	Implementar el modelo de seguridad y privacidad de la información	Σ (IND. OP. 1 * PESO PONDERADO) En %	70

Según la información aportada por la DTGIJ el avance del cumplimiento de dicho indicador es del 70%, ante lo cual la OCI considera que el avance es menor, según el análisis visto líneas atrás en el que se concluyó que el MJD se encuentra en un nivel respetable, y en este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información, y aunque existen controles que permiten detectar posibles incidentes de seguridad, no se encuentran gestionados dentro del componente planificación del MSPI

 La justicia es de todos Minjusticia	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

Ante la pregunta, elevada por la OCI, de la ficha técnica de los indicadores, no fue presentada, por cuanto los indicadores son nuevos y hasta ahora se están estructurando. Por lo tanto, se recomienda diligenciar la hoja de vida por cada uno de los indicadores en el formato incorporado en el SIG, con el Código: F-MC-G-05-01 versión 3.

7. Conclusiones, hallazgos y recomendaciones

Resultado de la auditoría se concluye que la OAP, a través del grupo de calidad y transformación organizacional, tanto como la DTGIJ, actualmente están atendiendo la estructuración y seguimiento de los riesgos y controles de gestión, de corrupción y de seguridad de la información, a través de la herramienta Excel dispuesta para ello, identificada con el código del SIG: F-MC-G04-01.

La OCI pudo comprobar que, dentro del proceso de mejora integral de la gestión institucional²⁰, que tiene como objetivo el de: “coordinar y administrar la implementación del sistema Integrado de Gestión del Ministerio de Justicia y del Derecho, con el fin de asegurar su mejora continua, conveniencia, eficacia y eficiencia conforme con los estándares adoptados” se tiene prevista la actividad²¹ de: “orientar la administración de los riesgos de gestión de los procesos, de corrupción de la entidad y de seguridad de la información, dentro de los sistemas de Gestión de Calidad, de acuerdo con los establecido en el documento G-MC-04-Guía para la Administración del Riesgo”.

La OCI considera que la herramienta dispuesta, por el MJD, a través del formato Código: F-MC-G04-01 permite a los profesionales tener una guía paso a paso, para poder llegar a identificar los riesgos, así como el diseño de los controles, y además hacerle seguimiento, cuatrimestral, a la materialización de los riesgos. Sin embargo, observó la OCI que en las matrices allegadas no se está consignado el seguimiento, aunque si se constató que las dependencias, cada cuatro meses, envían un reporte a la OAP del seguimiento de los controles. Se recomienda a la OAP, como segunda línea de defensa encargada del seguimiento periódico, recordar que dicha actividad se efectúa en la herramienta dispuesta para ello, como lo define la guía del MJD.

Se observa que, en cuanto a la identificación de los riesgos de seguridad de la información, se está teniendo como base la afectación de la integridad, confidencialidad y la disponibilidad de un activo o grupos de activos del MJD dentro del proceso.

Se encuentra que en la fase de identificación y análisis de causas, o fuentes de riesgo, se está realizando a partir del contexto interno, externo del proceso y, para este análisis, se están considerando posibles fuentes de información adicionales, como el resultado de auditorías, informes de seguimientos desarrollados por la OCI, análisis de riesgos materializados en periodos anteriores; se comprobó igualmente que, en el periodo de la auditoría, se realizaron un total de 203 reuniones de asesoría y asistencia técnica entre la OAP, la DTGIF y las dependencias para identificar debidamente los riesgos y controles, que afectan los diferentes procesos del Ministerio.

La auditoría observó que, en general, se cumplen las orientaciones de la Guía del MJD, en el proceso de modelación del riesgo, pero considera importante fortalecer la etapa de seguimiento.

²⁰ De código C-MC, versión 5, con fecha de vigencia del 28 de febrero de 2020.

²¹ A cargo de los profesionales del Grupo de Calidad y Transformación Organizacional

	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

También se espera que, próximamente, el módulo de riesgos del aplicativo DARUMA pueda efectuar todo el proceso de identificación, evaluación y seguimiento a los mapas de riesgos y que, de una vez, se actualice con la metodología dispuesta por el DAFP, en la versión del 2020.

Recomendaciones

En consecuencia, generamos las siguientes pautas, fundamentalmente orientadas al robustecimiento de la segunda línea de defensa, en la que participan la OAP y la DTGIJ, a saber:

1. Realizar la actualización de la guía incorporada en el SIG, poniéndola a tono con la última versión del DAFP.
2. Identificar los riesgos y controles con códigos, para cada uno de los procesos, lo que permite hacer un mejor control a la dependencia encargada del tema y a la OCI, como tercera línea de defensa.
3. Continuar teniendo en cuenta las observaciones realizadas por la OCI, tanto en las auditorías internas, como en el seguimiento al mapa de riesgos de la entidad.
4. Diligenciar la hoja de vida de los indicadores en el formato identificado con el Código: F-MC-G-05-01 versión 3.
5. Avanzar en la primera incorporación de las matrices de riesgos, en el módulo de riesgos del sistema DARUMA, en ambiente de producción, previa capacitación a las diferentes dependencias sobre su uso, módulo que debe ser la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad de la información en el MJD
6. Solicitar a las diferentes dependencias, al inicio de cada vigencia, que deleguen el funcionario que servirá de enlace para el acompañamiento en el proceso de administración del riesgo.
7. Diligenciar la matriz en la parte correspondiente a los seguimientos de cada uno de los riesgos identificados en el sistema de gestión del MJD, para evitar el riesgo de incumplimiento a los lineamientos del MIPG, en este caso, a la guía de administración de riesgos, que prevé esa tarea. Así mismo que se evalúe el seguimiento con una periodicidad menor, a los cuatro meses, para ciertos riesgos de alta probabilidad e impacto.
8. A la DTGIJ, realizar revisión al mapa de riesgos de seguridad de la información en lo concerniente al diseño de los controles; es recomendable que cada riesgo tenga al menos un control asignado que permita mitigar su impacto, a menos que la decisión, de la alta dirección, en relación con su administración sea la de la aceptación.
9. A la DTGIJ, evaluar la inclusión, en la matriz de riesgos del proceso de gestión de tecnologías y la información, de un control para la fase de planeación, otro para la de ejecución y uno posterior a la implementación. Se recomiendan los siguientes controles:

	FORMATO INFORME DE AUDITORÍA INTERNA	Código: F-SE-01-02
		Versión: 03

- Semestralmente el director de la DTGIJ, en conjunto con su equipo, revisará la viabilidad y prioridad de todas las necesidades de proyectos de TICs identificados durante el semestre, analizando su complejidad, compatibilidad, componentes, prioridad y tiempo de implementación. En caso de identificar proyectos inviables para el MJD, se emite el respectivo concepto sobre el proyecto de TICs solicitado, dejando evidencia en una matriz de priorización.
- Cada vez que se requiera, el director de la DTGIJ verificará si la solución contratada e implementada en el proyecto, aportó los resultados que se esperaban; verificando con la dependencia involucrada los resultados obtenidos y la efectividad de la solución en la resolución de la necesidad. Se evaluarán las inconformidades encontradas, informando al proveedor para su ajuste en el periodo de la garantía, de lo cual se dejará evidencia en un informe por proyecto ejecutado.

Elaboraron:

CARLOS ALBERTO PUENTES
Profesional líder de auditoría

ELDER HERNEY VILLAR CASTRO
Profesional apoyo de auditoría

Revisó y aprobó:

DIEGO ORLANDO BUSTOS FORERO
Jefe Oficina de Control Interno