SEGUIMIENTO A LAS MATRICES DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1. INFORMACIÓN GENERAL DE LA AUDITORIA O SEGUIMIENTO

Tabla 1- Información general

Tipo de informe	**Preliminar**		**Final**	**X**
No. Informe	OCI-18-2026			
Fecha del informe	29-05-2026			
Objetivo	Efectuar seguimiento a la ejecución de los controles definidos en los mapas de riesgos de seguridad de la información, de acuerdo con el Manual y Política de Riesgos de la Entidad, y la normatividad vigente. Para el presente seguimiento se tuvieron en cuenta los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), la Guía para la Gestión Integral del Riesgo del Departamento Administrativo de la Función Pública, y los lineamientos internos definidos por la entidad para la gestión de riesgos.			
Alcance	1 de septiembre de 2025 al 30 de abril de 2026. Se incluyó la revisión de la identificación de activos de información, la formulación y valoración de los riesgos, la definición e implementación de controles, los planes de tratamiento y las actividades de monitoreo y seguimiento, así como la verificación de la efectividad de las acciones derivadas de seguimientos previos.			
Periodo de ejecución	04 al 31 de mayo			
Equipo Auditor	Crhistian Augusto Amador León			
Documentación analizada	Se analizó la documentación remitida por el proceso para el seguimiento a las matrices de riesgos de Seguridad y Privacidad de la Información – SPI, correspondiente a: Manual para la Gestión de Riesgos MN-PSG-004 versión 5; inventarios de activos de información por proceso en formato Excel; matriz de riesgos de Seguridad de la Información del proceso Gestión de Tecnologías de la Información y Comunicaciones – Seguridad; matrices propuestas de riesgos SPI por proceso; documento relacionado con el plan de tratamiento de riesgos SPI; documentos de registro de evidencias de riesgos; soportes asociados a controles, tales como reportes de respaldos, requerimientos de servicio, documentación técnica, archivos de configuración y anexo contractual; así como documento de roles y responsabilidades en la gestión de riesgos SPI. La documentación fue revisada frente a los criterios definidos en la metodología interna de gestión de riesgos, la Guía para la			

	Administración del Riesgo y el Diseño de Controles del DAFP y los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI de Ministerio de Tecnologías de la Información y las Comunicaciones.

2. DESARROLLO DEL SEGUIMIENTO

2.1 Verificación del marco metodológico para la gestión de riesgos de Seguridad y Privacidad de la Información – SPI

Frente al seguimiento realizado, se evidenció que la entidad cuenta con documentación formal relacionada con la gestión de riesgos y la gestión de Seguridad y Privacidad de la Información – SPI, así:

- El Manual para la Gestión de Riesgos (código MN-PSG-004 versión 5): establece lineamientos relacionados con la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de riesgos, incluyendo lineamientos específicos para riesgos de seguridad de la información, identificación y valoración de activos, identificación de amenazas y vulnerabilidades, definición de controles y seguimiento de riesgos residuales.
- La Política General de Seguridad de la Información: involucra el compromiso institucional frente a la protección de los activos de información y la implementación de controles orientados a preservar la confidencialidad, integridad y disponibilidad de la información institucional.
- El procedimiento "*PR-GGC-003 Identificación, clasificación y etiquetado de activos de información digitales*": define lineamientos para la identificación, clasificación y etiquetado de activos de información digitales, estableciendo criterios asociados a confidencialidad, integridad y disponibilidad de la información, así como responsabilidades para su gestión y actualización.
- Procedimientos relacionados con gestión de incidentes tecnológicos y análisis de riesgos asociados a proveedores con acceso a activos de información.

La documentación anterior es consistente con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información – MSPI, particularmente en lo relacionado con identificación de activos de información, valoración de riesgos, planes de tratamiento, seguimiento y mejora continua, así como con los principios establecidos en la norma ISO/IEC 27001:2022 relacionados con gestión de riesgos y controles de seguridad de la información.

2.2 Verificación de la Identificación y Clasificación de Activos de Información

La Oficina de Control Interno revisó los inventarios de activos de información remitidos por el GT Gestión de Plataforma de Tecnologías de Información de la Dirección de Gestión de Información, con el fin de verificar la identificación,

clasificación, actualización y trazabilidad de los activos utilizados como base para la gestión de riesgos de Seguridad y Privacidad de la Información – SPI.

Frente a la información remitida, se evidenció que la entidad cuenta con inventarios de activos de información asociados a diferentes procesos institucionales; se realizaron actividades de acompañamiento, mesas de trabajo, revisión, retroalimentación y actualización de los inventarios durante la vigencia 2025, orientadas a fortalecer la identificación, clasificación y valoración de activos de información críticos para los procesos institucionales: se evidenciaron correos electrónicos, reuniones de trabajo y remisión de versiones ajustadas de inventarios por parte de diferentes procesos, relacionados con la revisión y actualización de activos de información, así como solicitudes de complementación y validación efectuadas por el GT Gestión de Plataforma de Tecnologías de Información y el GT Planeación.

Así mismo, se evidenció gestión relacionada con la identificación y priorización de activos críticos, revisión de componentes asociados a software, hardware, servicios y recurso humano, así como retroalimentación técnica frente a la consolidación y ajuste de la información reportada por los procesos.

No obstante, se identificaron situaciones que requieren fortalecimiento, así:

Oportunidad de mejora No. 1. Debilidades en la gestión y trazabilidad del inventario de activos de información: Al validar los archivos de inventario de activos de información remitidos para cada uno de los diferentes procesos institucionales, se identificaron situaciones relacionadas con integridad, consistencia, actualización y trazabilidad de la información registrada, las cuales podrían afectar la adecuada asociación entre activos, riesgos, controles y planes de tratamiento definidos dentro de la gestión de riesgos de Seguridad y Privacidad de la Información – SPI.

Durante la revisión de los inventarios de activos de información remitidos por los diferentes procesos institucionales, se evidenciaron situaciones relacionadas con integridad, consistencia, completitud, actualización, trazabilidad y consolidación de la información registrada, así como oportunidades de mejora frente a la asociación de determinados componentes y la formalización del proceso de validación y articulación institucional de los inventarios utilizados dentro de la gestión de riesgos de Seguridad y Privacidad de la Información – SPI, lo que presenta debilidades frente a los siguientes lineamientos:

Situación identificada	Criterio normativo	Criterio relacionado
Registros sin código de identificación y duplicidad de códigos para activos diferentes. **Ejemplo:** Archivo 2025_Activos_Inf-Planeación: - 59 activos sin código asociado - 127 activos con códigos duplicados. Archivo 2025_Activos_Inf-Monitoreo de Amenazas Geológicas: - 26 activos sin código asociado - 127 activos con códigos duplicados. Adicionalmente, se evidenciaron: - 66 registros con código "GTIC00XXX" - 7 registros con código "GTIC00XX"	Manual para la Gestión de Riesgos MN-PSG-004	**5.11.1 Identificación de los activos de seguridad de la información** Id del activo: Es el identificador único de cada activo. Inicia con la codificación establecida en el SGC para cada proceso, ej.: CI-GM-01.
Registros con campos sin diligenciar relacionados con ubicación del activo y fecha de actualización del activo. **Ejemplo:** Archivo 2025_Activos_Inf-Monitoreo de Amenazas Geológicas: - 566 activos sin ubicación - 11 activos sin fecha de actualización - 49 activos que registran " 45517" como fecha de actualización. Archivo 2025_Activos_Inf-GD:	Procedimiento PR-GGC-003 "Identificación, clasificación y etiquetado de activos de información digitales" Manual de Operación MO-TEC-002	**PR-GGC-003 - Actividad 6: Revisar el inventario de los activos de la información** Revisar el inventario de activos de información digitales, la identificación, la clasificación y su correcto etiquetado en el formato de inventario de activos de información digitales." **MO-TEC-002 - Inventario y propiedad de los activos** El SGC, como propietario de los activos de información, debe mantener un inventario actualizado con todos los activos institucionales, identificados,

Situación identificada	Criterio normativo	Criterio relacionado
- 586 activos sin ubicación - 11 activos sin fecha de actualización - 49 activos que registran " 45517" como fecha de actualización.		clasificados y protegidos según su valor, criticidad, sensibilidad, nivel de reserva y funcionalidad.
Se evidenciaron registros o información asociada a otros procesos dentro de algunos archivos de levantamiento de activos, sin claridad frente a su correspondencia con el proceso evaluado, lo cual dificulta la trazabilidad, identificación y consolidación de los activos de información utilizados dentro de la gestión de riesgos SPI. **Ejemplo:** En archivos de procesos como IERM, Planeación, DRM y Monitoreo de Amenazas Geológicas se observaron registros asociados al código "CPC0001 – Informes de Gestión Institucional, Informe de Rendición de Cuentas", sin evidenciar claridad sobre su correspondencia con el proceso evaluado.	Procedimiento PR-GGC-003 "Identificación, clasificación y etiquetado de activos de información digitales"	**PR-GGC-003 - Actividad 7: Validar el inventario de activos de información digitales** Revisar la identificación, la clasificación, el etiquetado y la valoración del inventario de activos de información digitales.
Se evidenciaron registros en los que no se observa claridad frente a la clasificación o asociación de determinados componentes dentro del inventario. **Ejemplo:** en el archivo "2025_Activos_Inf_DH.xlsx", hoja "1. Inventario de Activos", los registros	Manual para la Gestión de Riesgos MN-PSG-004	**5.11.1 Identificación de los activos de seguridad de la información** "Tipo de activo: Los tipos de activos pueden ser: Información (...), Software, Hardware, Recurso Humano, Servicios."

Situación identificada	Criterio normativo	Criterio relacionado
"Zetaware (Módulos Genesis, Kinex y Trinity)" y "Linux - Ubuntu 24 - Python - R" no presentan diligenciado el campo "Tipo de activo".		
Aunque se evidenciaron actividades de revisión, acompañamiento y retroalimentación frente al levantamiento de activos de información, no se observó evidencia consolidada relacionada con la validación y aprobación formal de los inventarios remitidos por parte de los responsables o jefes de dependencia, ni mecanismos que permitieran identificar su estado de validación, consolidación o aprobación institucional conforme a los lineamientos definidos para la gestión de activos de información.	Documento Maestro – Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional	**4. Revisión y aprobación de los activos de información** "Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los líderes de los procesos o sus delegados y que esta haya sido validada y aprobada por los jefes de cada dependencia, se debe enviar la matriz para su consolidación y validación (…)"" **Gestión inventario clasificación de activos e infraestructura critica Cibernética** "Revisión y Aprobación: Corresponde a la etapa en donde se valida la clasificación y valoración dada a los activos de información, para la presentación y aprobación por parte del dueño o responsable de los activos."
Durante la revisión no se evidenció claridad frente a la articulación entre los inventarios de activos de información utilizados para la gestión de riesgos SPI y otros instrumentos institucionales relacionados con activos de información y gestión documental objeto de publicación en el micrositio de transparencia.	Documento Maestro – Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional	**5. Publicación de los activos de información** "El área, proceso, grupo interno, funcionario o rol responsable de la custodia del inventario de activos de información debe enviar el consolidado del inventario de Activos de Información para la respectiva publicación de la información en la página web de la entidad, Link

Situación identificada	Criterio normativo	Criterio relacionado
Ejemplo: en los archivos revisados no se identificaron campos, referencias o mecanismos que permitieran relacionar de manera clara los activos utilizados dentro de la gestión de riesgos SPI con los inventarios de activos de información objeto de publicación institucional.		de transparencia y acceso a la Información Pública (…)"

2.3 Verificación de la formulación, aprobación y seguimiento de matrices de riesgos de Seguridad y Privacidad de la Información – SPI

Revisadas las matrices de riesgos de Seguridad y Privacidad de la Información – SPI remitidas por el GT Gestión de Plataforma de Tecnologías de Información para los diferentes procesos institucionales, con el fin de verificar su formulación, estructura, asociación con activos de información, definición de controles, estado de aprobación y seguimiento, conforme a los lineamientos definidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP, el Manual para la Gestión de Riesgos, el Modelo de Seguridad y Privacidad de la Información – MSPI y demás documentación institucional aplicable, se evidenció que la entidad ha adelantado actividades relacionadas con levantamiento de activos de información, mesas de trabajo, acompañamiento técnico, formulación de propuestas de matrices SPI y retroalimentación frente a riesgos y controles asociados a los procesos institucionales. Así mismo, se evidenciaron correos electrónicos relacionados con revisión, remisión de propuestas, observaciones y solicitudes de ajuste frente a activos de información y formulación de matrices SPI.

No obstante, se identificaron situaciones que requieren fortalecimiento:

Oportunidad de mejora No. 2. Debilidades en la formulación, formalización y seguimiento de matrices de riesgos SPI: Durante la validación efectuada a las matrices de riesgos SPI propuestas para los diferentes procesos institucionales, **exceptuando la matriz correspondiente a la Dirección de Gestión de Información – DGI**, se identificaron debilidades relacionadas con la formulación metodológica de riesgos, diseño y trazabilidad de controles, asociación entre activos, riesgos y controles, contextualización de riesgos, definición de responsables y operacionalización de la gestión de riesgos de Seguridad y Privacidad de la Información – SPI, las cuales podrían afectar el

adecuado seguimiento, monitoreo y evaluación de la gestión de riesgos de Seguridad y Privacidad de la Información – SPI, particularmente frente a la trazabilidad entre activos, riesgos y controles, así como en la definición, ejecución y seguimiento de los controles establecidos y la verificación de su efectividad.

Lo anterior presenta debilidades frente a los siguientes lineamientos:

Situación identificada	**Criterio normativo**	**Criterio relacionado**	**Documento donde se evidenció (Ejemplos)**
A. Formalización y contextualización de las matrices			
Las matrices remitidas por el GT Gestión de Plataforma de Tecnologías de Información y GT Planeación se encuentran en estado de propuesta y no se evidenció aprobación ni socialización formal con los procesos responsables.	Manual para la Gestión de Riesgos MN-PSG-004 v5	**5.2.1. Objetivos de la política** "Garantizar que se desarrollen cada una de las etapas previstas para la actualización, implementación y seguimiento del mapa de riesgos en el marco de la política para la gestión de riesgos del SGC."	Todas las matrices propuestas revisadas
En algunos procesos que gestionan información sensible, reservada o especializada, no se evidenció una contextualización específica de riesgos y controles acorde con la naturaleza de la información administrada por el proceso, observándose matrices con estructuras y tratamientos similares pese a la diferencia en criticidad, sensibilidad o especialidad de la información gestionada. **Ejemplo:** En matrices correspondientes a procesos como Gestión Disciplinaria, Gestión Jurídica, Gestión	Manual para la Gestión de Riesgos MN-PSG-004 Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	**MN-PSG-004 - 5.11 LINEAMIENTOS PARA SEGURIDAD DE LA INFORMACIÓN** "A partir del inventario de activos de información con el que cuenta el SGC; se hace necesario establecer una clasificación de acuerdo con el Manual de Gestión del Riesgo del Departamento Administrativo de la Función pública que establece tres pilares o principios de la Seguridad de la Información (…)	Gestión Disciplinaria Gestión Jurídica Gestión de Talento Humano Investigaciones y Aplicaciones Nucleares y Radiactivas

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
Documental, Gestión de Talento Humano, Investigaciones y Aplicaciones Nucleares y Radiactivas y Licenciamiento y Control de Instalaciones Radiactivas, no se evidenció diferenciación clara en la definición de riesgos y controles frente a información reservada, sensible, jurídica, disciplinaria o técnica especializada administrada por dichos procesos.		alineada a la definición de clasificación del activo en términos de confidencialidad, integridad y disponibilidad.”	
B. Formulación y valoración del riesgo			
No se evidenció identificación o clasificación explícita de factores de riesgo conforme a la estructura definida en la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP, particularmente frente a factores relacionados con tecnología, talento humano, ejecución de procesos o eventos externos asociados a los riesgos SPI formulados.	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	**3.3 Identificación de áreas de factores de riesgo** “Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa.” “Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con su complejidad”	Todas las matrices propuestas revisadas
Se evidenciaron inconsistencias entre el tipo de riesgo definido y la descripción del escenario de riesgo formulado, particularmente frente a la	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	**Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 - 5.4 Descripción del riesgo**	Investigaciones y Aplicaciones Nucleares Radioactivas Gestión Jurídica

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
aplicación de los principios de confidencialidad, integridad y disponibilidad sobre determinados activos de información. **Ejemplo:** En algunas matrices SPI el riesgo se clasifica como "Pérdida de confidencialidad"; sin embargo, la descripción del escenario incorpora simultáneamente afectaciones relacionadas con integridad y disponibilidad.	Manual para la Gestión de Riesgos MN-PSG-004	**Tipo de Riesgo:** Este campo solo admite uno de estos 3 valores: • Pérdida de Disponibilidad • Pérdida de Integridad • Pérdida de Confidencialidad **Descripción del Riesgo:** En este campo se describe la situación específica que da como resultado el correspondiente riesgo. **MN-PSG-004 - 5.11 LINEAMIENTOS PARA SEGURIDAD DE LA INFORMACIÓN.** "A partir del inventario de activos de información con el que cuenta el SGC; se hace necesario establecer una clasificación de acuerdo con el Manual de Gestión del Riesgo del Departamento Administrativo de la Función Pública que establece tres pilares o principios de la Seguridad de la Información (…) alineada a la definición de clasificación del activo en términos de confidencialidad, integridad y disponibilidad."	Gestión Disciplinaria Gestión Documental Talento Humano

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
C. Diseño y seguimiento de controles			
Se evidenciaron oportunidades de mejora frente al nivel de detalle y documentación de algunos controles definidos en las matrices SPI propuestas, observándose casos en los cuales la descripción del control no permitía identificar de manera clara aspectos relacionados con la ejecución operativa, validación, trazabilidad, tratamiento de desviaciones o mecanismos específicos de seguimiento del control implementado, incluyendo soporte o evidencia de su ejecución. **Ejemplo:** En matrices correspondientes a Gestión Contractual y Gestión de Bienes y Servicios se definieron controles relacionados con "implementar control formal de asignación, revisión periódica y revocación de permisos"; sin embargo, no siempre se evidenciaba claridad frente a actividades específicas de validación, tratamiento de desviaciones o mecanismos concretos de seguimiento y verificación del control.	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 Manual para la Gestión de Riesgos MN-PSG-004 v5	**Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 - 5.8 Estructura para la Descripción del Control** "Descripción del Control: Este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad." **Manual para la Gestión de Riesgos MN-PSG-004 v5** "Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración." "Complemento (¿cómo lo hace?, ¿cuál es la evidencia?): corresponde a los detalles que permiten identificar claramente el objeto del control." "Es importante identificar el responsable de ejecutar el control"	Gestión Contractual Gestión de Bienes y Servicios Geoamenazas
Se evidenciaron oportunidades de mejora frente a la operacionalización	Guía para la Gestión Integral del Riesgo en	"Descripción del Control: Este campo corresponde a una	Gestión Contractual

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
y contextualización de algunos controles definidos en las matrices SPI propuestas, observándose casos en los cuales la descripción del control correspondía principalmente a referencias generales de controles asociados a ISO/IEC 27001 y 27002, sin evidenciar de manera clara su implementación específica dentro del proceso evaluado. **Ejemplo:** En matrices correspondientes a Gestión de Bienes y Servicios y Geoamenazas se evidenciaron controles asociados a gestión de accesos, revisión de permisos o aplicación de controles de seguridad alineados con ISO/IEC 27001 y 27002; sin embargo, en algunos casos la descripción del control no detallaba de manera específica cómo se ejecuta, valida, monitorea o evidencia operativamente el control dentro del proceso evaluado.	Entidades Públicas v7 – DAFP	descripción de la forma en la cual el control seleccionado será implementado en la entidad." "NOTA: Las entidades pueden crear controles adicionales a los listados en el anexo A de la norma ISO 27001:2022 de acuerdo a sus necesidades."	Gestión de Bienes y Servicios Geoamenazas
Se evidenciaron oportunidades de mejora frente a la coherencia entre la periodicidad definida para algunos controles y la descripción operativa de ejecución establecida en las matrices SPI propuestas, observándose casos en los cuales la frecuencia definida	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	"La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna."	Direccionamiento Estratégico Evaluación Independiente

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
no guardaba total correspondencia con la dinámica operativa o seguimiento descrito para el control.			
Se evidenciaron oportunidades de mejora frente a los indicadores o mecanismos definidos para seguimiento de riesgos y controles en algunas matrices SPI propuestas, observándose casos en los cuales las métricas definidas se orientaban principalmente a medir actividades de implementación, revisión o documentación de controles, sin evidenciar criterios claros para evaluar la efectividad del control implementado, tendencias del riesgo o contribución en la mitigación del riesgo asociado. **Ejemplo:** En matrices correspondientes a Gestión de Bienes y Servicios, Gestión Contractual y Relacionamiento se evidenciaron métricas orientadas principalmente a verificar implementación, revisión o documentación de controles; sin embargo, no siempre se observaban criterios específicos para medir tendencias del riesgo, efectividad del control o disminución de la exposición al riesgo asociado.	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	"Los Indicadores Clave de Riesgos (KRI), son métricas diseñadas con el fin de identificar, estimar y monitorear la ocurrencia y severidad de eventos y posibles amenazas (…)" "Estos indicadores permiten (…) evaluar a través de su tendencia la efectividad de los controles que se disponen para mitigarlos."	Gestión de Bienes y Servicios Gestión Contractual Relacionamiento
D. Estructura, trazabilidad y consistencia de la información			
Se evidenció similitud en estructuras y descripciones	Guía para la Gestión Integral	La guía establece que la identificación y	Gestión Documental

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
de algunos riesgos, impactos, controles e indicadores entre diferentes procesos, limitando en ciertos casos la contextualización específica de los riesgos frente a las características, operación y naturaleza particular de cada proceso institucional. **Ejemplo:** Se evidenciaron matrices correspondientes a procesos con naturalezas distintas que incorporaban riesgos, controles e indicadores con estructuras y descripciones similares, pese a administrar información, servicios y dinámicas operativas diferentes.	del Riesgo en Entidades Públicas v7 – DAFP	análisis del riesgo deben realizarse considerando las características y contexto del proceso.	Gestión Jurídica Investigación en Geociencias Básicas
Se identificaron errores de referencia o cálculo en algunas matrices remitidas, evidenciados en campos con resultados como "#REF!", "NULL" o inconsistencias de visualización, lo cual podría afectar la integridad, trazabilidad y valoración residual de los riesgos definidos.	Manual para la Gestión de Riesgos MN-PSG-004 v5 / Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	La guía establece lineamientos relacionados con valoración, análisis y monitoreo del riesgo.	Direccionamiento Estratégico

2.4 Verificación de ejecución, monitoreo y efectividad de controles SPI- Dirección Técnica de Gestión de la Información

Se revisaron las evidencias remitidas por el GT Gestión de Plataforma de Tecnologías de Información de la Dirección de Gestión de Información – DGI, relacionadas con la ejecución, monitoreo y seguimiento de controles asociados a la gestión de riesgos de Seguridad y Privacidad de la Información – SPI definidos para el proceso Gestión de TIC, con el fin de verificar su

implementación, trazabilidad, evidencia de ejecución y mecanismos de seguimiento y monitoreo aplicados.

Durante la validación efectuada se evidenció que el proceso ha adelantado actividades relacionadas con la implementación y ejecución de controles de Seguridad y Privacidad de la Información, gestión de accesos, monitoreo de eventos de seguridad, administración de plataformas tecnológicas, ejecución de actividades de respaldo, revisión de controles de seguridad, seguimiento a vulnerabilidades, gestión de incidentes y generación de evidencias operativas asociadas a la gestión de riesgos SPI.

Así mismo, se evidenció remisión de soportes relacionados con ejecución de controles técnicos y operativos, registros de monitoreo, reportes de seguimiento, evidencias de revisión y documentación asociada a controles implementados por el GT Gestión de Plataforma de Tecnologías de Información. Teniendo en cuenta que el proceso Gestión de Tecnologías de la Información y las Comunicaciones soporta transversalmente la operación institucional y la administración de diferentes activos tecnológicos e información institucional, toma relevancia el adecuado monitoreo, ejecución y seguimiento de los controles SPI implementados dentro de la infraestructura y servicios tecnológicos administrados por la DGI.

No obstante, se identificaron situaciones que requieren fortalecimiento:

Oportunidad de mejora No. 3. Fortalecimiento del monitoreo, trazabilidad y evaluación de efectividad de controles SPI

Durante la revisión efectuada a las evidencias relacionadas con ejecución, monitoreo y seguimiento de controles SPI implementados por el GT Gestión de Plataforma de Tecnologías de Información, se identificaron oportunidades de mejora relacionadas con formalización del seguimiento, trazabilidad operativa, evaluación de efectividad de controles, consolidación de evidencias y mecanismos de monitoreo asociados a la gestión de riesgos de Seguridad y Privacidad de la Información – SPI.

Situación identificada	**Criterio normativo**	**Criterio relacionado**	**Documento donde se evidenció (Ejemplos)**
A. Evidencias de ejecución y trazabilidad de controles			
Se evidenció que algunos controles definidos en la matriz SPI no contaban con soporte completo o evidencia claramente asociada durante el seguimiento	Guía para la Gestión Integral del Riesgo en Entidades	**Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – 5.5.3**	MR Gestión-Tecnología_Información_Comunicaciones-Seguridad.xlsx;

Situación identificada	**Criterio normativo**	**Criterio relacionado**	**Documento donde se evidenció (Ejemplos)**
realizado, observándose en algunos casos registros operativos, muestras documentales o soportes parciales frente a determinados controles implementados. **Ejemplo:** Aunque la matriz define múltiples controles asociados a gestión de accesos, respaldos, conectividad y seguridad de servicios de red, las evidencias remitidas corresponden principalmente a registros operativos, capturas o muestras documentales de determinados controles.	Públicas v7 – DAFP Manual para la Gestión de Riesgos MN-PSG-004 v5	**Estructura para la descripción del control**. Complemento (¿cómo lo hace?, ¿cuál es la evidencia?): corresponde a los detalles que permiten identificar claramente el objeto del control. Manual para la Gestión de Riesgos MN-PSG-004 v5. "Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración."	
En algunos casos las evidencias remitidas permiten validar la ejecución operativa de los controles definidos; sin embargo, no evidencian de manera integral mecanismos formales de monitoreo, seguimiento, medición o evaluación de efectividad de los controles implementados. **Ejemplo:** Se remitieron evidencias relacionadas con ejecución de respaldos, configuraciones de red, logs y gestión de accesos; sin embargo,	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7	La guía establece lineamientos relacionados con seguimiento, monitoreo y revisión de riesgos y controles asociados a la gestión del riesgo "En esta etapa se revisa la efectividad de los controles…" "Seguimiento: En este campo se especifica la	Información de respaldos_BD; Esquema Técnico SD-WAN y Conectividad - SGC; Registros de evidencias riesgo 1 y 2.xlsx

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
no se evidenció de manera integral seguimiento periódico documentado sobre efectividad, desviaciones, resultados de monitoreo o análisis consolidado de los controles implementados.		periodicidad del seguimiento a la implementación del control.”	
B. Monitoreo y efectividad de controles			
Algunos indicadores o mecanismos definidos para seguimiento de riesgos y controles no fueron evidenciados dentro de los soportes remitidos, dificultando verificar el seguimiento, monitoreo y medición de efectividad de determinados controles implementados. **Ejemplo:** En las evidencias revisadas no siempre se observaron métricas o mecanismos asociados a tendencias del riesgo, efectividad del control o disminución de la exposición al riesgo relacionado con los controles implementados.	Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 – DAFP	“Los Indicadores Clave de Riesgos (KRI), son métricas diseñadas con el fin de identificar, estimar y monitorear la ocurrencia y severidad de eventos y posibles amenazas (…)” “Estos indicadores permiten (…) evaluar a través de su tendencia la efectividad de los controles que se disponen para mitigarlos.”	MR Gestión-Tecnología_Información_Comunicaciones-Seguridad.xlsx
C. Conservación y disponibilidad de registros			
Se evidenciaron limitaciones frente a la disponibilidad histórica de algunos registros técnicos asociados a controles SPI, particularmente relacionados con logs y respaldos de información. **Ejemplo:** Dentro de las evidencias remitidas se indicó que algunos registros disponibles corresponden únicamente a periodos limitados de retención operativa, como logs almacenados por periodos aproximados de tres meses o respaldos asociados a ventanas	Documento Maestro MSPI / Guía DAFP v7 / MO-TEC-002	Lineamientos relacionados con monitoreo, trazabilidad, conservación de registros y gestión de eventos de seguridad de la información.	Información de respaldos_BD; Esquema Técnico SD-WAN y Conectividad - SGC

Situación identificada	Criterio normativo	Criterio relacionado	Documento donde se evidenció (Ejemplos)
limitadas de conservación técnica.			

Las situaciones identificadas evidencian oportunidades de mejora frente al fortalecimiento del monitoreo, trazabilidad, centralización y medición de efectividad de los controles asociados a la gestión de riesgos SPI, particularmente en relación con el seguimiento formal de los controles implementados, la consolidación de evidencias y la verificación periódica de efectividad de los mecanismos de control definidos.

No obstante, durante la revisión se evidenció que el GT Gestión de Plataforma de Tecnologías de Información cuenta con avances en la ejecución operativa de controles relacionados con respaldos de información, conectividad, gestión de accesos y administración de servicios tecnológicos, soportados mediante evidencias técnicas y registros operativos remitidos durante el seguimiento.

2.5 Roles y responsabilidades en la gestión de riesgos SPI y líneas de defensa

Durante la revisión se evidenció que la entidad cuenta con lineamientos institucionales que establecen funciones, responsabilidades y actividades relacionadas con la gestión de riesgos, principalmente a través del Manual para la Gestión de Riesgos MN-PSG-004 versión 5 y la Resolución No. 1281 de 2024.

En este sentido, la Resolución No. 1281 de 2024 establece para el Grupo de Trabajo Planeación, entre otras funciones, la de: *"Coordinar la administración de la gestión del riesgo en los diferentes procesos de la entidad con la periodicidad y oportunidad requeridas*".

De igual forma, el Manual para la Gestión de Riesgos MN-PSG-004 versión 5 en su numeral "*5.2.4. Niveles de responsabilidad y autoridad"* establece para la segunda línea de defensa (Grupo de Trabajo Planeación, Directores Técnicos y Coordinadores de Grupo de Trabajo), entre otras responsabilidades:

- "Acompañar, orientar y entrenar a los responsables de procesos en la identificación, análisis y valoración del riesgo".
- "Promover ejercicios de autoevaluación para establecer eficacia y eficiencia de los controles y de la gestión del riesgo"

- "Consolidar el mapa de riesgos institucional y presentarlo para análisis y seguimiento ante el CIGD"
- "Generar alertas cuando se requieran cambios en los riesgos o se materialicen riesgos al interior de los procesos"
- "Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad".

Así mismo, el numeral **5.7.3 "Monitoreo y seguimiento del mapa de riesgos"** de este mismo manual, establece que:
1ª . Línea de defensa: "Los líderes de proceso deben monitorear y revisar el cumplimiento de los controles de manera constante con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la materialización de riesgos."

2ª . Línea de defensa: "El Grupo de trabajo de Planeación realizará un seguimiento cuatrimestral a la aplicación de los controles y planes de acción o tratamiento como parte de su rol de acompañamiento permanente a la Gestión de Riesgos", y adicionalmente "apoyará y articulará la consolidación de las evidencias de estos y el reporte del seguimiento".

Por su parte, la Resolución **No. 1281 de 2024** establece para **el Grupo de Trabajo Tecnologías de Información** funciones relacionadas con:

- "Realizar y mantener actualizado el inventario de la información de plataforma e infraestructura tecnológica, software, aplicaciones y sistemas de información de apoyo a la gestión"
- "Proponer, administrar y ejecutar las estrategias en cuanto a seguridad de la información, para los sistemas administrativos y de soporte, conforme a las decisiones, políticas y lineamientos del Comité de Gobierno de TI".
- "Garantizar la aplicación de los estándares, lineamientos del Comité de gobierno de TI, buenas prácticas, principios para la administración y soporte de tecnologías de información en los aspectos relacionados con los sistemas administrativos y de soporte institucional."

Bajo este marco institucional, la gestión de riesgos SPI involucra responsabilidades distribuidas entre los líderes de proceso, el Grupo de Trabajo Planeación en su rol de segunda línea de defensa y las dependencias responsables de la gestión técnica y operativa de la seguridad de la información.
Lo anterior se complementa con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG, la Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP y el Modelo de Seguridad y Privacidad de la Información – MSPI, los cuales promueven la articulación entre las líneas de

defensa, la definición clara de responsabilidades y el fortalecimiento de mecanismos para la gestión, monitoreo y seguimiento de riesgos.

No obstante, frente a la información revisada durante el seguimiento, se identificaron oportunidades de mejora relacionadas con la articulación operativa, formalización y aplicación práctica de los mecanismos de coordinación, articulación, monitoreo, seguimiento y reporte asociados a la gestión de riesgos SPI entre las dependencias involucradas, de conformidad con las responsabilidades definidas institucionalmente.

Oportunidad de mejora No. 4. Fortalecimiento de la articulación y definición de roles y responsabilidades frente a la gestión y seguimiento de riesgos SPI. Se identificaron situaciones que evidencian debilidades en la articulación institucional, y la definición operativa de responsabilidades y consolidación de mecanismos de seguimiento y monitoreo asociados a la gestión de riesgos SPI, particularmente en relación con la aplicación práctica del esquema de líneas de defensa y el seguimiento institucional de riesgos y controles de seguridad de la información, así:

Situación identificada	Criterio normativo	Criterio relacionado
Se evidenciaron oportunidades de mejora frente a la articulación operativa y aplicación práctica de los roles y responsabilidades asociados a la gestión de riesgos SPI entre las dependencias involucradas.	Resolución 1281 de 2024 Manual para la Gestión de Riesgos MN-PSG-004 v5	**Resolución 1281 de 2024 – Grupo de Trabajo Planeación** "Coordinar la administración de la gestión del riesgo en los diferentes procesos de la entidad con la periodicidad y oportunidad requeridas." **Manual para La Gestión de Riesgos - 5.7.3 Monitoreo y seguimiento del mapa de riesgos.** **2ª línea de defensa.** "El Grupo de trabajo de Planeación realizará un seguimiento cuatrimestral a la aplicación de los controles y planes de acción o tratamiento como parte de su rol de acompañamiento permanente a la Gestión de Riesgos, de acuerdo con los lineamientos definidos por el Departamento Administrativo

Situación identificada	Criterio normativo	Criterio relacionado
		de la Gestión Pública DAFP. Adicionalmente, apoyará y articulará la consolidación de las evidencias de estos y el reporte del seguimiento. **5.2.4. Niveles de responsabilidad y autoridad.** Responsabilidades por línea de defensa 2ª Línea (Grupo de Trabajo Planeación; Directores Técnicos; Coordinadores Grupo de Trabajo) ”Acompañar, orientar y entrenar a los responsables de procesos en la identificación, análisis y valoración del riesgo “Consolidar el mapa de riesgos institucional y presentarlo para análisis y seguimiento ante el CGDI”. “Generar alertas cuando se requieran cambios en los riesgos o se materialicen riesgos al interior de los procesos”. “Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.”
No se evidenció un mecanismo institucional consolidado para el seguimiento integral de riesgos SPI que permitiera articular activos de información, riesgos, controles, monitoreo, seguimiento y	Manual para la Gestión de Riesgos MN-PSG-004 v5 Resolución 1281 de 2024	**5.2.4. Niveles de responsabilidad y autoridad.** Responsabilidades por línea de defensa 2ª Línea (Grupo de Trabajo Planeación; Directores Técnicos; Coordinadores Grupo de Trabajo)

Situación identificada	Criterio normativo	Criterio relacionado
responsables institucionales.		”Presentar periódicamente información al CICCI y CGDI sobre la Gestión de riesgos en el SGC, incluyendo riesgos materializados, con el objetivo de generar toma de decisiones frente a los mismos.” “Generar alertas cuando se requieran cambios en los riesgos o se materialicen riesgos al interior de los procesos”. **Manual para La Gestión de Riesgos - 5.7.3 Monitoreo y seguimiento del mapa de riesgos.** **2ª línea de defensa.** “El Grupo de trabajo de Planeación realizará un seguimiento cuatrimestral a la aplicación de los controles y planes de acción o tratamiento como parte de su rol de acompañamiento permanente a la Gestión de Riesgos, de acuerdo con los lineamientos definidos por el Departamento Administrativo de la Gestión Pública DAFP. Adicionalmente, apoyará y articulará la consolidación de las evidencias de estos y el reporte del seguimiento. **Resolución 1281 de 2024** **2.3. Grupo de Trabajo Planeación** 12) Coordinar la administración de la gestión del riesgo en los diferentes procesos de la entidad con la periodicidad y oportunidad requeridas.

Situación identificada	Criterio normativo	Criterio relacionado
Las matrices SPI remitidas se encontraban en estado de propuesta y sin aprobación formal, dificultando la formalización institucional de mecanismos de seguimiento, monitoreo y consolidación de evidencias asociadas a riesgos SPI.	Manual para la Gestión de Riesgos MN-PSG-004 v5	**Manual para la Gestión de Riesgos – 5.7.3 Monitoreo y seguimiento del mapa de riesgos:** "Los líderes de proceso deben monitorear y revisar el cumplimiento de los controles de manera constante…" / "El Grupo de trabajo de Planeación realizará un seguimiento cuatrimestral…"
Aunque se evidenciaron actividades de acompañamiento y construcción metodológica de matrices SPI, no se identificó un esquema formal consolidado que permitiera verificar periódicamente el estado, efectividad y seguimiento institucional de los riesgos y controles SPI implementados.	Manual Operativo MIPG Manual para la Gestión de Riesgos MN-PSG-004 v5	<u>Modelo Estándar de Control Interno</u> Esquema de responsabilidades 2ª Línea (se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC) "Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión." "Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente." **Manual para la Gestión de Riesgos – 5.7.3 Monitoreo y seguimiento del mapa de riesgos:** "Los líderes de proceso deben monitorear y revisar el cumplimiento de los controles de manera constante…" / "El Grupo de trabajo de Planeación realizará un seguimiento cuatrimestral…"

Situación identificada	Criterio normativo	Criterio relacionado
No se evidenció trazabilidad consolidada frente a mecanismos institucionales de reporte, monitoreo o generación de alertas asociados a la gestión y seguimiento de riesgos SPI.	Manual para la Gestión de Riesgos MN-PSG-004 v5	**5.2.4. Niveles de responsabilidad y autoridad.** Responsabilidades por línea de defensa 2ª Línea (Grupo de Trabajo Planeación; Directores Técnicos; Coordinadores Grupo de Trabajo) "Promover ejercicios de autoevaluación para establecer eficacia y eficiencia de los controles y de la gestión del riesgo ".

3. RECOMENDACIONES

Tabla 2 - Recomendaciones por proceso

No.	PROCESO	RECOMENDACIÓN
1	Dirección de Gestión de Información – GT Gestión de Plataforma de Tecnologías de Información Procesos institucionales	Fortalecer los mecanismos de gestión, consolidación, revisión y actualización del inventario institucional de activos de información, garantizando la identificación única de los activos, la completitud y trazabilidad de la información registrada, la articulación con otros instrumentos institucionales y la validación formal de los levantamientos realizados, conforme a los lineamientos definidos en el PR-GGC-003, el MN-PSG-004, el MO-TEC-002 y el MSPI.
2	Dirección de Gestión de Información – GT Gestión de Plataforma de Tecnologías de Información Grupo de Trabajo Planeación Procesos institucionales	Fortalecer el proceso de formulación, formalización, aprobación, implementación y seguimiento de las matrices de riesgos SPI, garantizando la adecuada articulación entre activos de información, riesgos, controles, responsables, periodicidad, evidencias de ejecución e indicadores de seguimiento, conforme a los lineamientos definidos por el DAFP, el MSPI y la documentación institucional aplicable.
3	Dirección de Gestión de Información – GT Gestión de Plataforma de Tecnologías de Información Grupo de Trabajo Planeación	Fortalecer los mecanismos de seguimiento, monitoreo y evaluación de efectividad de los controles SPI implementados, garantizando la consolidación y trazabilidad de evidencias, la definición de mecanismos periódicos de validación y monitoreo, la conservación histórica de registros técnicos relevantes y la articulación entre riesgos, controles, indicadores y evidencias de ejecución,

No.	PROCESO	RECOMENDACIÓN
		conforme a los lineamientos definidos por el DAFP, el MSPI y las buenas prácticas aplicables en gestión de seguridad de la información.
4	Dirección de Gestión de Información – GT Gestión de Plataforma de Tecnologías de Información Grupo de Trabajo Planeación Procesos institucionales	Fortalecer la definición, articulación y formalización de roles y responsabilidades asociados a la gestión de riesgos SPI dentro del esquema institucional de líneas de defensa, garantizando mecanismos claros de seguimiento, monitoreo, reporte, consolidación y generación de alertas frente a riesgos y controles de Seguridad y Privacidad de la Información, conforme a los lineamientos definidos por el MIPG, el DAFP, el MSPI y la documentación institucional aplicable.

4. CONCLUSIONES.

Como resultado del seguimiento efectuado a la gestión de riesgos de Seguridad y Privacidad de la Información – SPI, se evidenció que la entidad cuenta con avances relacionados con la definición de lineamientos institucionales, levantamiento de activos de información, formulación de matrices de riesgos SPI y ejecución de algunos controles asociados a la gestión de seguridad de la información.

No obstante, se identificaron oportunidades de mejora relacionadas con la formalización y aprobación de matrices SPI, la trazabilidad entre activos, riesgos y controles, la definición y monitoreo de controles, la evaluación de efectividad de los mecanismos implementados y la articulación institucional de roles y responsabilidades dentro del esquema de líneas de defensa.

Las situaciones identificadas evidencian la necesidad de continuar fortaleciendo la madurez institucional de la gestión de riesgos SPI, particularmente frente a los mecanismos de seguimiento, monitoreo, trazabilidad y coordinación institucional definidos en el marco del MIPG, el MSPI y la metodología institucional de gestión de riesgos.

5. APROBACIÓN

EMHM Erika Marcela Huari Mateus	CAAL Crhistian Augusto Amador León
Jefa de Oficina de Control Interno	**Auditor Interno**