EVALUACIÓN Y VERIFICACIÓN SOBRE LOS AVANCES Y MEJORAS OBTENIDAS EN EL MARCO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INFORME FINAL
AUDITORIA INDEPENDIENTE

Oficina de Control Interno
Junio de 2026

1. Objetivo de la auditoría:

Evaluar el avance para el año 2025 y lo corrido de este año en el diseño, implementación y eficacia operativa de los controles de seguridad de la información y ciberseguridad implementados por la entidad, verificando la protección de la confidencialidad, integridad y disponibilidad de la información institucional, así como la gestión de vulnerabilidades.

2. Alcance de la auditoría:

En el marco del objetivo definido, se evaluará el avance en la implementación del Modelo de Seguridad y Privacidad de la Información del MJD y los controles de la política de Seguridad y Privacidad de la Información, con indicadores y evidencias de ejecución, en cuanto a:

- Análisis GAP, desarrollado para la vigencia 2025.
- Modelo de Seguridad y Privacidad de la Información (MSPI). Instrumento de evaluación MSPI, con corte al alcance de esta auditoría.
- Indicadores de gestión del Modelo de Seguridad y Privacidad de la Información (MSPI) para la vigencia 2025, con sus respectivas evidencias de ejecución.
- Controles de la política de seguridad de la información (vigente) con sus respectivas evidencias de ejecución, en cuanto a:
- Política de teletrabajo y trabajo remoto para la vigencia 2025
- Gestión de vulnerabilidades técnicas, en periodo comprendido entre enero a mayo de 2026. (Se efectuará análisis de vulnerabilidades de acuerdo con la evidencia entregada).

3. Criterios de auditoría o parámetros normativos:

Para el desarrollo de la presente auditoría, se tendrán en cuenta los siguientes criterios:

- Ley 87 de 1993 "Establece Las normas para el ejercicio del control interno en las entidades y organismos del Estado".
- Ley 1221 de 2008 "promueve y regula el teletrabajo en Colombia como instrumento de generación de empleo y autoempleo mediante el uso de tecnologías de la información y las telecomunicaciones (TIC)."
- Ley 1581 de 2012 "Establece las disposiciones generales para la protección de datos personales, garantizando el derecho de los ciudadanos a conocer, actualizar y rectificar la información que se recoja sobre ellos".
- Ley 1712 de 2014 "Establece la ley de transparencia y del derecho de acceso a la información pública nacional".
- Decreto 1072 de 2015 "expedido para compilar y racionalizar la normatividad laboral vigente en Colombia. Su propósito es simplificar y organizar en un solo cuerpo jurídico las disposiciones reglamentarias relacionadas con el trabajo,

seguridad social, riesgos laborales, teletrabajo, pensiones, capacitación y demás aspectos del sector".

- Decreto 1427 de 2017 del Ministerio de Justicia y del Derecho (en adelante MJD), "El cual define las dependencias internas y asigna sus funciones específicas".
- Decreto 767 de 2022 "El cual define los lineamientos generales de la Política de Gobierno Digital en el país."
- Resolución 384 de 2023 "Por el cual se implementa la modalidad de teletrabajo en el Ministerio de Justicia y del Derecho, se deroga la Resolución 0611 de 2022 y se dictan otras disposiciones".
- ISO/IEC 27001:2022, en lo aplicable a la seguridad de la información de los sistemas de información.
- Documento maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) v 5 de 2025 "Establece los lineamientos para implementar la seguridad y privacidad de la información en las entidades públicas".
- Guía para la Gestión integral del riesgo en entidades públicas v7 de 2025 de Función Pública "La cual define una metodología para identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que afectan los objetivos institucionales".
- COBIT 2019 DSS05 "Indica cómo administrar y garantizar la seguridad de los servicios de TI para proteger la información y soportar los objetivos organizacionales".

4. Metodología:

La metodología empleada por la Oficina de Control Interno (en adelante OCI), se basó en un levantamiento de información por medio de un cuestionario con treinta y seis (36) preguntas, de las cuales catorce (14) están relacionadas con la evaluación, seguimiento y gestión de la seguridad de la información y sus controles dentro de la gestión del riesgo y el gobierno institucional de la Política de seguridad de la información; diez (10) están enfocadas en los Controles de la Política de teletrabajo y trabajo remoto relacionados con la Política de seguridad de la información y doce (12) están enfocadas en los Controles de la política de seguridad de la información relacionados con la Gestión de vulnerabilidades técnicas; estas fueron enviadas con el plan específico; por otra parte, se utilizaron métodos de evaluación tales como la constatación de información y análisis sobre la misma; adicionalmente, se estableció comunicación continua con el área de tecnología, para resolver las inquietudes que se iban presentando en el desarrollo de la auditoria.

La apertura de la auditoría se realizó mediante reunión virtual el día 3 de junio de 2026, con la participación del Director de Tecnologías y Gestión de Información en Justicia (en adelante DTGIJ), el Subdirector de Tecnologías y Sistemas de Información (en adelante STSI), así como los profesionales encargados de atender la auditoría de ambas áreas y, por parte de la OCI, el Jefe de la Oficina de Control Interno y la auditora de la OCI. En el marco de la reunión de apertura, el área de Tecnología solicita la concesión de un plazo adicional para la remisión de las respuestas al cuestionario. En consecuencia, se

acuerda que dichas respuestas serán entregadas de manera parcial el 3 de junio y el 5 de junio de 2026, respectivamente.

En dicha reunión se presentaron el objetivo, alcance y cronograma general de las actividades previstas para el desarrollo de la auditoría; a su vez, se realizó la socialización de la información que debe ser allegada para la auditoria y se aclararon dudas relacionadas con el cuestionario remitido.

5. Desarrollo de la Auditoría

5.1. Antecedentes

En la vigencia 2024, la Oficina de Control Interno (OCI) realizó el informe de la auditoria denominada Evaluación y Verificación sobre los avances y mejoras obtenidas en el marco del proceso de seguridad de la información", el cual es tomado como insumo para esta auditoría, cuyo objetivo señalaba "*Evaluar y verificar los avances y mejoras obtenidas en el marco del proceso de seguridad de la información*[1]".

Dentro del respectivo informe se realizó la siguiente conclusión*:*

"Si bien es cierto que se encuentran avances importantes en cuanto a la documentación de la política de seguridad de la información, se insta al área de tecnología a validar la efectividad de los controles que contiene la misma, ya que no se encuentran lineamientos de seguimiento para determinar la efectividad y eficacia de las actividades que enmarcan dichos controles; además de asociar las respectivas responsabilidades de los diferentes roles que intervengan en las actividades de los controles y por último realizar un alineamiento de los procedimientos y/o guías que soportan los controles contenidos en la política en los ítems comunes[2]*."*

Y se realizaron las siguientes recomendaciones:

"La OCI sugiere articular el Procedimiento de Soporte a Usuarios y la Política de seguridad de la información en los ítems comunes:

- *Se sugiere incluir un control que permita realizar una validación de la vigencia en los accesos a los servicios tecnológicos para los funcionarios de planta activos, así como de los retiros, vacaciones, licencias, desvinculaciones o cambio de labores de los colaboradores de planta.*
- *Se sugiere articular el Procedimiento de Gestión de Accesos y la Política de seguridad de la información en los ítems comunes.*
- *Se sugiere robustecer el control "La STSI debe promover que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware, las bases de datos y demás elementos tecnológicos sean cambiados o suspendidos de acuerdo con las políticas y las mejores prácticas de seguridad" utilizando herramientas que brinden información detallada sobre el uso de los terminales y las actividades de los usuarios.*

[1] Auditoría Evaluación y Verificación sobre los avances y mejoras obtenidas en el marco del proceso de seguridad de la información; ítem 1. Objetivo de la auditoria; pág. 3; OCI MINJUSTICIA, Julio de 2024; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2024/Independiente/Informe-Final-seguridad-de-la-inf-2024-v-final.pdf

[2] Auditoría Evaluación y Verificación sobre los avances y mejoras obtenidas en el marco del proceso de seguridad de la información; ítem 7.1. Conclusiones; pág. 24; OCI MINJUSTICIA; Julio de 2024; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2024/Independiente/Informe-Final-seguridad-de-la-inf-2024-v-final.pdf

- *Definir un control que permita evaluar la efectividad de los mecanismos definidos para generar la cultura de seguridad en el MJD, así como lineamientos que le den soporte al mismo.*
- *Validar los permisos de acceso y modificación a la consola del antivirus para los usuarios del MJD, en caso de ser un lineamiento permitido se sugiere ajustar el control en la política.*
- *Fortalecer los controles para el uso del formato de "Acuerdos de confidencialidad de proveedores", validar la inclusión de parámetros de cumplimiento de la normatividad contenida en dichos acuerdos o como realizar un seguimiento efectivo para detectar posibles incumplimientos en la política de seguridad de la información y en el acuerdo de confidencialidad.*
- *Definir lineamientos para gestionar los riesgos asociados a los proveedores.*
- *Realizar análisis, revisión y posterior fortalecimiento de los controles para gestionar los cambios en las prácticas de seguridad de la información del proveedor y en la prestación de servicios mediante un conjunto de procedimientos y formatos específicos.*
- *Definir las características mínimas que debe cumplir la constancia de borrado seguro de la información, como se va a constatar que en dicho documento se encuentre toda la información, su clasificación en términos de confidencialidad y las bases de datos que hayan sido creada dentro del contrato en cumplimiento de las obligaciones contractuales y quien va a realizar dicha verificación en el acuerdo de confidencialidad para proveedores.*
- *Se sugiere hacer mención del acuerdo de confidencialidad en el contrato con el proveedor, ya sea como anexo de este o incluirlo tácitamente en la cláusula 3.*
- *Incluir en los controles de la política de seguridad el responsable de validar el diligenciamiento y/o a la calidad de la información diligenciada en los formatos de confidencialidad.*
- *Definir en la política de seguridad quien debe hacer la validación en las respectivas carpetas para evidenciar que se encuentren alojados en su contenido los formatos de confidencialidad.*
- *Incluir en los lineamientos de la política en qué casos se debe de volver a firmar el formato de confidencialidad.*
- *En los acuerdos de confidencialidad a proveedores, se deben determinar con claridad los montos pecuniarios que podrían ser susceptibles de multa y los hechos o actuaciones precisos que constituirían tal mecanismo correctivo sancionatorio. Por ello, se recomienda a la Dirección de Tecnología que se introduzcan multas con precisión en el marco de las minutas contractuales con proveedores que tienen acceso a los activos de información de esta cartera ministerial.*
- *Definir en la política de seguridad en qué casos se debe escalar el incidente de seguridad de la información a entidades tales como COLCERT o CSirt; adicionalmente, indicar donde se encuentran los números telefónicos, direcciones de correo electrónico, o nombres de los funcionarios para realizar dicha notificación.*
- *Robustecer la política de gestión de incidentes y la documentación completaría (procedimientos, guías).*
- *La OCI recomienda, validar la usabilidad del formato de planilla de acceso dado que no está diligenciando de forma correcta y completa; en caso de que se determine seguir usando dicho formato se recomienda robustecer el control para comprobar el adecuado diligenciamiento y dar los respectivos lineamientos en la política de operación del Procedimiento de gestión de acceso, en cuanto al quien, como y cuando se debe utilizar el formato mencionado; así como revisar el proceso el cual carece de controles y no cuenta con responsables de la revisión de las actividades ejecutadas.*
- *La OCI sugiere articular el Procedimiento de Gestión de Incidentes de seguridad y la Política de seguridad de la información en los ítems comunes.*

- *Incluir las actividades que se deben realizar en la detección, reporte, análisis, monitoreo y resolución de incidentes de seguridad de la información en el correspondiente procedimiento.*
- *Incluir las interacciones con los grupos de respuesta de acuerdo al vector del incidente,*
- *en el Procedimiento de Gestión de Incidentes de seguridad.*
- *Definir los lineamientos para reportar y gestionar un incidente de seguridad que provenga de un proveedor de servicios, indicar el rol del funcionario o contratista que actué como contacto entre tecnología y el proveedor y como se informaría del incidente al interior del MJD; adicionalmente contemplar las sanciones o multas que esto implicaría para el proveedor.*
- *Incluir las verificaciones que se deben realizar para probar que los incidentes de seguridad de la información reportados por la herramienta de mesa de servicio hayan sido solucionados de manera satisfactoria.*
- *Los incidentes de seguridad no son consignados en una bitácora, la cual permitiría validar el progreso o atraso en la respuesta de los incidentes con el fin de realizar el respectivo seguimiento; es de agregar que esta puede ser usada como insumo para determinar riesgos o posibles mejoras en el portal web, por lo cual se sugiere su implementación.*
- *Validar la formulación en las correspondientes celdas y realizar la respectiva corrección de ser necesario en la información del Instrumento de evaluación MSPI en cuanto a la "Calificación Frente a Mejores Prácticas en ciberseguridad (NIST)".*
- *Se sugiere completar la información faltante en la pestaña de levantamiento de información, columna "DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN" del Instrumento de evaluación MSPI, referente a "Inventario de áreas de procesamiento de información y telecomunicaciones, Inventario de partes externas o terceros a los que se transfiere información de la entidad, Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden, Aceptación de los riesgos residuales por parte de los dueños de los riesgos, Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.*
- *Se sugiere en las pestañas Administrativas y Técnicas del Instrumento de evaluación MSPI, completar las brechas en los ítems que no cumplen con el 100% de nivel de cumplimiento, indicando que le hace falta al control o requisito para cumplir frente a la Norma ISO 27001:2013.*
- *Elaborar planes de tratamiento para cada riesgo, incluso cuando el riesgo residual sea bajo o la opción de combatirlo sea evitarlo o reducirlo, con el fin de fortalecer los controles existentes y mitigar la materialización del riesgo.*
- *Se sugiere revisar las acciones a implementar en caso de que el riesgo se materialice, se debería realizar un nuevo análisis de las causas, establecer acciones correctivas y de mejora a implementar[3]".*

5.2. Evaluación del avance en la Política de seguridad de la información

De acuerdo con el documento maestro del modelo de seguridad y privacidad de la información elaborado por MinTIC, la política de seguridad y privacidad de la información "*Establece la base respecto al comportamiento personal y profesional de los*

[3] Auditoría Evaluación y Verificación sobre los avances y mejoras obtenidas en el marco del proceso de seguridad de la información; ítem 7.4. Recomendaciones; pág. 30 a la 33; OCI MINJUSTICIA; Julio de 2024; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2024/Independiente/Informe-Final-seguridad-de-la-inf-2024-v-final.pdf

funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad.
Orientar y apoyar por parte de la alta dirección de la entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente[4]", como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015, en la sección 2 "Elementos de la política de gobierno digital" en su ítem 3.2. Seguridad y Privacidad de la Información.

Actualmente, la Política de Seguridad y Privacidad de la Información del Ministerio de Justicia y del Derecho (MJD) se encuentra documentada en el instrumento con Código G-IC-14, versión 006 del año 2025, aprobado y publicado en el Sistema Integrado de Gestión (SIG).

En el marco de la evaluación realizada por la OCI, se evidencia que la política presenta un avance significativo en la adopción de buenas prácticas y en la incorporación de elementos fundamentales de la norma ISO/IEC 27001:2022, particularmente en lo relacionado con la definición de principios de seguridad, asignación de responsabilidades, gestión de activos de información y establecimiento de controles operacionales. Lo anterior refleja un compromiso institucional con la protección de la información y la alineación con estándares internacionales.

De igual forma, a partir de la validación del documento maestro de lineamientos del Modelo de Seguridad y Privacidad de la Información (en adelante MSPI), se determina que la política cumple con la base normativa exigida, asegurando coherencia con el marco de referencia establecido por MinTIC.

No obstante, desde una perspectiva de gobierno, desempeño y mejora continua del Sistema de Gestión de Seguridad de la Información (en adelante SGSI), se identifica que la política mantiene un enfoque predominantemente declarativo y operativo, sin consolidarse plenamente como un instrumento de gobernanza integral, control y medición, tal como lo requieren la ISO/IEC 27001:2022 y el MSPI en términos de madurez organizacional.

Actualmente, la efectividad de los controles se revisa y documenta en las reuniones individuales realizadas con cada área o proceso, escenario en el cual se ejecuta el seguimiento correspondiente. Adicionalmente, los controles de seguridad de la información sobre los activos bajo custodia se evalúan una vez al año, o ante cambios normativos o solicitudes de mejora por parte del MinTIC, utilizando la herramienta de autodiagnóstico del MSPI y la declaración de aplicabilidad.

En este contexto, la principal brecha identificada no radica en la ausencia de controles, sino en la falta de una estructuración formal, trazabilidad, incluyendo la definición de

[4] Maestro del modelo de seguridad y privacidad de la información v 5.0" en el ítem 7.2.2 "Política de seguridad y privacidad de la información" pág. 28, MinTIC, abril 2025.

evidencias verificables e indicadores de desempeño y eficacia, lo cual limita la capacidad de la Entidad para:

- Detectar oportunamente debilidades o desviaciones en la implementación de los controles.
- Responder con agilidad frente a riesgos emergentes.
- Consolidar una mejora continua efectiva del sistema de seguridad de la información.
- Garantizar un monitoreo permanente del estado de los controles.
- Sustentar decisiones estratégicas con información confiable, actualizada y verificable.

La ausencia de mecanismos formales de medición, seguimiento y trazabilidad puede limitar la capacidad institucional para identificar oportunamente debilidades en los controles y gestionar de manera preventiva los riesgos de seguridad de la información. Esto puede derivar en afectaciones a la confidencialidad, integridad y disponibilidad de la información, así como en debilidades en el cumplimiento normativo, pérdida de confianza institucional y limitaciones para demostrar la efectividad del Sistema de Gestión de Seguridad de la Información.

Con el fin de cerrar las brechas identificadas y fortalecer la alineación con ISO/IEC 27001:2022 y el MSPI, se recomienda:

- Fortalecer el lineamiento asociado a la gestión de controles de seguridad de la información sobre los activos bajo custodia, complementando lo establecido en la matriz de riesgos, mediante la definición explícita de los mecanismos de implementación, monitoreo y revisión de dichos controles. Esto debe incluir la asignación de responsables, periodicidad de ejecución y seguimiento, definición de evidencias verificables, así como indicadores de cumplimiento y eficacia, garantizando su trazabilidad, medición, auditabilidad y mejora continua.
- Definir e implementar indicadores clave de desempeño (KPI[5]) e indicadores clave de riesgo (KRI[6]) asociados a la seguridad de la información, con criterios claros de medición, seguimiento periódico y gestión formal, orientados a evaluar la eficacia de los controles, apoyar la toma de decisiones y fortalecer la mejora continua del SGSI.
- Fortalecer la articulación entre la Política de Seguridad de la Información y el Plan Estratégico de Seguridad de la Información (PESI), mediante la definición de mecanismos formales de alineación y trazabilidad que permitan vincular los lineamientos estratégicos con los objetivos, proyectos, controles, responsables,

[5] *Indicadores Clave de Desempeño (Key Performance Indicators – KPI) Los indicadores se diseñan desde el proceso de planeación y permiten que durante las demás etapas de la gestión se verifique el cumplimiento de objetivos y metas, así como el alcance de los resultados propuestos e introducir ajustes a los planes de acción, metas o actividades - Guía para la Gestión integral del Riesgo de Función pública -.*

[6] *Indicadores Clave de Riesgo (Key Risk Indicators- KRI) Estos indicadores proporcionan información oportuna sobre riesgos emergentes y potenciales que pueden tener impacto sobre el logro de los objetivos de la organización, así como las medidas en las cuales diferentes eventos o puntos desencadenantes - Guía para la Gestión integral del Riesgo de Función pública -.*

cronogramas e indicadores del plan, garantizando su implementación efectiva, seguimiento y medición en el marco del SGSI.

- Fortalecer la integración de los resultados del diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) y el nivel de madurez alcanzado, asegurando su incorporación explícita en la Política y su uso formal en el Plan Estratégico de Seguridad de la Información (PESI) como línea base para la definición de objetivos, priorización de controles y formulación de planes de mejora, garantizando su trazabilidad y alineación con las acciones y proyectos del SGSI.
- Revisar y ajustar el modelo de gobernanza del SGSI, asegurando la independencia funcional y organizacional del Oficial de Seguridad de la Información frente a las áreas operativas, con el fin de fortalecer la supervisión, control, evaluación y reporte, evitando conflictos de interés.
- Definir un esquema formal de respaldo y segregación de funciones, que garantice la continuidad de la gestión realizada por el Oficial de Seguridad de la Información y evite la concentración de responsabilidades en un único rol. Este esquema debe contemplar: Designación de suplentes o responsables alternos, con funciones claramente delimitadas; Segregación de funciones críticas, para reducir riesgos de dependencia y conflictos de interés; Protocolos de continuidad operativa, que aseguren la ejecución de actividades en caso de ausencia, rotación o contingencias.
- Diseñar e implementar un esquema estructurado de evaluación y auditoría periódica sobre los controles, la política y el SGSI, definiendo responsables, criterios, metodologías, periodicidad y evidencias, que permitan verificar el cumplimiento, medir la efectividad de los controles y soportar la mejora continua.

Por último, como resultado de la revisión de las recomendaciones emitidas en la auditoría de 2024, se evidencia que la política ha incorporado la mayoría de los aspectos críticos, especialmente en materia de:

- Gestión de accesos
- Gestión de incidentes
- Relación con proveedores
- Gestión del riesgo

Sin embargo, persisten brechas relevantes en materia de control, medición y trazabilidad, principalmente en los siguientes aspectos:

- "*Definir un control que permita evaluar la efectividad de los mecanismos definidos para generar la cultura de seguridad el MJD, así como lineamientos que le den soporte al mismo*." La política promueve capacitación y sensibilización, pero no define indicadores, métricas ni mecanismos de evaluación de efectividad.
- "*Definir en la política de seguridad quien debe hacer la validación en las respectivas carpetas para evidenciar que se encuentren alojados los formatos de confidencialidad*." No se evidencia la existencia de un control formal de auditoría sobre las carpetas documentales que permita realizar verificaciones sistemáticas, con responsables

definidos, periodicidad establecida y mecanismos de trazabilidad que garanticen la revisión y validación de la información.

- *"Incluir en los lineamientos de la política en qué casos se debe volver a firmar el formato de confidencialidad."* La política exige firma inicial, pero no define escenarios de renovación, como cambio de rol, extensión contractual, acceso a nueva información crítica.
- "*En los acuerdos de confidencialidad (…) determinar con claridad los montos pecuniarios (…) y los hechos que constituyen sanción*". Aunque hay sanciones generales, no se establecen: montos específicos, criterios detallados de multa, tipificación clara de incumplimientos.
- "*Incluir en los controles de la política el responsable de validar el diligenciamiento y/o la calidad de la información en los formatos de confidencialidad*". La política asigna responsabilidades generales, pero no define un control formal de calidad del diligenciamiento de formatos.

Por lo anterior, la OCI recomienda evaluar la incorporación de las acciones de mejora identificadas, con el fin de fortalecer el SGSI y avanzar hacia un mayor nivel de madurez institucional conforme a los lineamientos de ISO/IEC 27001:2022 y el MSPI.

5.2.1. Evaluación de la Política de teletrabajo y trabajo remoto

Marco normativo

Actualmente, el Ministerio de Justicia y del Derecho (MJD) cuenta con la Resolución 384 de 2023, mediante la cual se implementa la modalidad de teletrabajo en la entidad, se deroga la Resolución 0611 de 2022 y se dictan otras disposiciones. A continuación, se presentan y analizan los artículos que, a criterio del auditor o por definición, se relacionan con las actividades propias del área de Tecnología.

Artículo 6. Capacitación establece: "*El(la) teletrabajador(a) cuenta con prioridad de capacitación en promoción de la salud y prevención de riesgos laborales y psicosociales, así mismo, recibirá capacitación en las Tecnologías de la Información y Comunicaciones -TIC y en los parámetros de Seguridad de la Información*[7]." Esta actividad se analiza en la revisión del artículo 15.

Artículo 14. Condiciones relacionadas con los servicios TIC y seguridad de la información establece: "*La Dirección de Tecnologías y Gestión de Información en Justicia realizará la verificación de cumplimiento de requerimientos tecnológicos y de comunicación en el lugar del teletrabajo y/o en forma remota, así como la autorización del Oficial de seguridad de la información para el acceso desde redes externas a la red del Ministerio. El(la) teletrabajador(a) se compromete a*:

[7] Resolución 384 del 24 de marzo de 2023; Ministerio de Justicia y del Derecho; Artículo 6. Capacitación; Pág. 4; https://www.minjusticia.gov.co/normatividad- co/Resoluciones/Resoluci%C3%B3n%20No.%200384%20del%2024%20de%marzo%%20de%202023.pdf

a) *Acatar los lineamientos en materia de protección de datos personales y la política de privacidad y de seguridad de la información que el Ministerio tenga implementada y publicada en el portal Web.*
b) *Utilizar los datos de carácter personal a los que tenga acceso única y exclusivamente para cumplir con sus obligaciones para con la Entidad.*
c) *Cumplir con las medidas de seguridad implementadas para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso.*
d) *No ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.*
e) *No permitir que personas ajenas a la entidad, realicen o le colaboren en la realización de las funciones que se le asignen en desarrollo del Teletrabajo.*
f) *Cuando no se encuentre en el sitio donde se desarrolla la modalidad de Teletrabajo mantener el computador apagado o con clave.*
g) *Participar de todas las capacitaciones programadas por la Dirección de Tecnologías y Gestión de Información en Justicia.*

Parágrafo: El(la) servidor(a) público(a) se compromete a preservar los aspectos de confidencialidad, integridad, disponibilidad, autenticidad, auditabilidad, protección a la duplicación, no repudio y legalidad en tal medida que se garantice la seguridad de la información[8]".

Con el propósito de precisar si la DTGIJ y/o la STSI realiza la verificación del cumplimiento de los requerimientos tecnológicos y de comunicación en el lugar de teletrabajo o de manera remota respecto de los funcionarios en modalidad de teletrabajo y/o trabajo remoto, se remitió correo electrónico solicitando la respectiva aclaración. En respuesta, Tecnología informó lo siguiente mediante correo electrónico: "*La STSI, verifica la información de requisitos tecnológicos con evidencia fotográfica anexa al formato F-TH-13-05 que presenta el eventual teletrabajador al inicio de la convocatoria de teletrabajo.*

Posteriormente el procedimiento contempla visita presencial o virtual en el mes siguiente a la aprobación, para verificar lista de chequeo de los formatos F-TH-13-03 y F-TH-13-04 por los profesionales asignados por el GGH. En esta visita, en particular el formato F-TH-13-04 contempla verificar entre otros los siguientes ítems:

Recursos tecnológicos y soporte: Evaluar suficiencia tecnológica para el teletrabajo
Condiciones tecnológicas del trabajo - prestaciones de equipo de cómputo
Conectividad y acceso tecnológico - conexión a internet

Posterior a la verificación de todos los requisitos, se rinde un informe donde se emite un concepto con las recomendaciones y ajustes a realizar en la estación de teletrabajo, entre ellas:

El equipo de cómputo que utilices para teletrabajar debe tener todas las prestaciones (capacidad, memoria, velocidad, conexiones, etc.) necesarias para desarrollar correctamente tu trabajo.

Dentro del procedimiento no está contemplada una visita adicional por parte del STSI.

[8] Resolución 384 del 24 de marzo de 2023; Ministerio de Justicia y del Derecho; Artículo 14. Condiciones de servicio TIC y seguridad de la información; Pág. 5; https://www.minjusticia.gov.co/normatividad-co/Resoluciones/Resoluci%C3%B3n%20No.%200384%20del%2024%20de%20marzo%20de%202023.pdf

El área de Gestión humana y la STSI tienen previsto y se ha realizado gestiones para contratación de software especializado para monitoreo remoto, en particular para cumplimiento de los siguientes requisitos definidos en la política de seguridad de la información:

"Los funcionarios en modalidad de teletrabajo deben realizar sus actividades únicamente desde los dispositivos de MINJUSTICIA o autorizados por la entidad, configurando el inicio de sesión exclusivo para su perfil de acceso. La información utilizada o generada durante su gestión en las instalaciones de la entidad y durante el teletrabajo, debe ser almacenada en los medios autorizados para ello (OneDrive, unidades compartidas y SharePoint corporativos) sin descargar, almacenar y guardar información en sus dispositivos personales, móviles, USB o discos duros extraíbles, a menos que cuenten para ello con la autorización de los líderes de proceso y propietarios de los activos, y que los mismos sean encriptados por parte del personal de la STSI"".

Posteriormente se solicita aclarar a Tecnología si dicha validación se limita únicamente a la revisión de evidencia fotográfica, o si dentro de los funcionarios asignados por el GGH se incluye personal del área de tecnología para validar el cumplimiento de los requisitos técnicos correspondientes, a lo cual responden *"El área tecnológica, efectúa revisión de evidencia fotográfica y virtual. Lo anterior, mediante los casos de mesa de ayuda; apoyando al teletrabajador, en la verificación de los requisitos técnicos y/o cualquier otro problema que no le esté permitiendo el buen funcionamiento en su ejercicio en el equipo de cómputo. Para ello se trae como ejemplo la información de 3 casos de la funcionaria Cecilia Escobar en el archivo adjunto con nombre: Relación de Casos Filtrados Teletrabajo funcionaria Cecilia Escobar.pdf; tomado de la base de Excel de mesa de ayuda."*

La evidencia obtenida permite concluir que la verificación realizada por el área de Tecnología se limita principalmente a la revisión documental y fotográfica suministrada por el solicitante, así como a actividades de soporte técnico posteriores, sin evidenciarse un mecanismo formal de validación técnica integral, presencial o remota, orientado a verificar el cumplimiento efectivo de las condiciones tecnológicas y de conectividad exigidas para el teletrabajo[9]; por otra parte, no es claro para la OCI si la validación de dichos requerimientos debe gestionarse mediante la creación de casos en la mesa de ayuda ya que no se encuentra un lineamiento que lo mencione

Adicionalmente, se identifica que la validación de condiciones se realiza principalmente mediante evidencia fotográfica aportada por el funcionario postulado, lo cual limita la verificación efectiva de las condiciones tecnológicas y de comunicaciones. Por otra parte, en la visita domiciliaria, conforme a los formatos establecidos, se verifica el espacio de trabajo en el domicilio (dimensiones, pisos, escaleras, etc.), así como los riesgos de accidente, condiciones ergonómicas, riesgos físicos, químicos y biológicos (Formato F-TH-13-03), y la valoración psicosocial y psicolaboral (Formato F-TH-13-04). No obstante, estas verificaciones no incluyen de manera integral los aspectos tecnológicos y de conectividad que son competencia del área de Tecnología.

En consecuencia, se concluye que no se cumple con la verificación de las condiciones tecnológicas y de comunicación en el lugar de teletrabajo, ya sea de manera presencial

[9] Lo anterior se sustenta en la evidencia suministrada, la cual corresponde a la atención de casos a través de mesa de ayuda relacionados con errores en Word, conectividad VPN y acceso a la red LAN

o remota, configurándose un incumplimiento de la función asignada en el artículo 14 de la Resolución 384 de 2023 del Ministerio de Justicia y del Derecho.

Por otra parte, se solicitó vía correo electrónico la aclaración sobre si el Oficial de Seguridad de la Información genera algún tipo de autorización para el acceso desde redes externas a la red del Ministerio de Justicia y del Derecho (MJD) por parte de los funcionarios en modalidad de teletrabajo y/o trabajo remoto. En respuesta, se indicó lo siguiente: "*El Oficial de Seguridad de la Información no genera ningún tipo de autorización para el acceso desde redes externas a la red del Ministerio de Justicia y del Derecho (MJD), toda vez que en el procedimiento y en el alcance de las aprobaciones de teletrabajo no se realizan solicitudes de uso de redes externas especificas hacia la red del Ministerio*."

Lo anterior cobra relevancia considerando que los teletrabajadores acceden a herramientas institucionales desde redes domésticas, por lo cual se solicita aclaración, frente a esto, se indicó: "*Efectivamente se confirma que red externa es lo que usted plantea en el ejemplo; no obstante, es importante precisar que la solicitud o autorización de teletrabajo no implica necesariamente acceso a la red interna de MINJUSTICIA. Los teletrabajadores pueden utilizar herramientas institucionales disponibles en Internet, como correo electrónico, plataformas colaborativas u otros servicios autorizados, sin que esto represente conexión directa a la red interna. Para acceder a recursos internos o red interna de la Entidad se requiere la habilitación de servicios tecnológicos adicionales, como una VPN, la cual debe ser solicitada, y autorizada de manera independiente, y no constituye un requisito obligatorio ni automático dentro de la solicitud de teletrabajo*." Adicionalmente, la política de teletrabajo establece: "(…) *La Subdirección de Tecnologías y Sistemas de Información deberá realizar las actividades necesarias para asegurar la configuración y validación de equipos de cómputo, recursos de comunicación y conectividad, así como establecer los mecanismos para proveer la conexión remota segura a los equipos y sistemas de información de la entidad, y a los medios de almacenamiento autorizados* (…)".

En este contexto, se concluye que la Política de Seguridad de la Información, en lo relacionado con teletrabajo, no contempla este tipo de autorizaciones por parte del Oficial de Seguridad de la Información, lo que evidencia una desalineación entre la Resolución y la Política de Teletrabajo. Esta situación puede afectar la coherencia en la aplicación de controles y, eventualmente, configurar un posible incumplimiento de lo dispuesto en el artículo 14 de la Resolución 384 de 2023 del MJD.

Artículo 15. Obligaciones del Ministerio en el ítem 14 establece "*Capacitar al(la) teletrabajador(a) en actividades de prevención y promoción en riesgos laborales, principalmente en el autocuidado, en el cuidado de la salud mental y factores de riesgo ergonómico o biomecánico, así como uso y apropiación de TIC y seguridad digital para el Teletrabajo. Las capacitaciones podrán ser virtuales.*" Asimismo, en el ítem 20 se establece "*Informar al(la) teletrabajador(a) sobre las restricciones de uso de equipos y programas informáticos, la legislación vigente en materia de protección de datos personales, propiedad intelectual,*

seguridad de la información y en general las sanciones que puede acarrear por su incumplimiento[10]."

Se solicitó aclaración vía correo electrónico con respecto a si la DTGIJ tiene contempladas capacitaciones específicas para los funcionarios que van a iniciar en la modalidad o que están postulándose para adquirir la modalidad de Teletrabajo y trabajo remoto, relacionado con temas tecnológicos y de seguridad de la información:

> "*La Dirección de Tecnologías ha brindado apoyo en la implementación de herramientas tecnológicas que facilitan el desarrollo del teletrabajo; sin embargo, el liderazgo en la definición de lineamientos y directrices para su adecuada ejecución corresponde al Grupo de Talento Humano. Durante el primer semestre, la Dirección de Tecnologías ha desarrollado procesos de capacitación orientados al fortalecimiento de competencias digitales, mediante el uso de herramientas de Microsoft Office 365, tales como el correo electrónico, OneDrive, SharePoint y Forms.*
>
> *En estos espacios se han socializado las principales funcionalidades de cada herramienta, destacando su aplicación en el entorno de teletrabajo, así como las buenas prácticas para su uso eficiente, con el propósito de optimizar la gestión de la información, el trabajo colaborativo y la productividad de los colaboradores.*
>
> *Adicionalmente, en atención a la solicitud realizada por el Grupo de Talento Humano, la Dirección de Tecnologías elaboró un plan de apoyo en el que se identifican y describen las herramientas tecnológicas actualmente disponibles en la entidad que pueden ser utilizadas para fortalecer y facilitar el desarrollo de las actividades de teletrabajo. Este documento contempla funcionalidades orientadas a la comunicación, colaboración, almacenamiento y gestión documental, permitiendo a los colaboradores desempeñar sus funciones de manera eficiente, segura y alineada con los lineamientos institucionales.*"

Dado que la respuesta no da precisión a la pregunta formulada, se solicita aclarar si las capacitaciones realizadas estuvieron dirigidas específicamente a funcionarios en modalidad de teletrabajo o trabajo remoto, o si, por el contrario, fueron orientadas a los funcionarios en general a lo cual responden:

> "*Frente a la observación realizada, se aclara que las capacitaciones desarrolladas por la Dirección de Tecnologías fueron ejecutadas de manera masiva y estuvieron dirigidas a todos los colaboradores de la entidad, como una estrategia inicial orientada al fortalecimiento de las competencias digitales y al uso adecuado de las herramientas tecnológicas institucionales.*
> *Estas acciones buscaron brindar conocimientos y habilidades en el manejo de herramientas de Microsoft Office 365, tales como Outlook, OneDrive, SharePoint, Forms y Teams, las cuales facilitan el desarrollo de actividades tanto presenciales como en modalidades de trabajo flexible, incluyendo el teletrabajo.*
>
> *Es importante precisar que la definición de lineamientos, la coordinación, el seguimiento y la gestión de la modalidad de teletrabajo son responsabilidades del Grupo de Talento*

[10] Resolución 384 del 24 de marzo de 2023; Ministerio de Justicia y del Derecho; Artículo 15. Obligaciones del Ministerio; Pág. 6; https://www.minjusticia.gov.co/normatividad-co/Resoluciones/Resoluci%C3%B3n%20No.%200384%20del%2024%20de%20marzo%20de%202023.pdf

Humano, dependencia encargada de liderar las acciones relacionadas con la implementación y desarrollo de esta modalidad laboral dentro de la entidad."

Adicionalmente, se solicita aclaración de si han solicitado incluir capacitaciones específicas dentro del Plan Institucional de Capacitación (PIC) o fuera de él, para los funcionarios que ya se encuentran en teletrabajo y trabajo remoto, relacionado con temas tecnológicos y de seguridad de la información, a lo que responden:

"*En el marco del Plan Institucional de Capacitación (PIC), se han incluido jornadas de formación orientadas al fortalecimiento de las competencias digitales de los colaboradores, mediante capacitaciones en herramientas de Microsoft Office 365, tales como Outlook, OneDrive, SharePoint, Teams y Forms.*

De igual manera, se desarrollarán talleres, charlas y espacios de sensibilización relacionados con seguridad de la información, buenas prácticas en el uso de las tecnologías de la información, protección de datos, prevención de riesgos digitales y fortalecimiento de la cultura de ciberseguridad institucional.

Las actividades de capacitación y sensibilización realizadas son reportadas periódicamente al Grupo de Talento Humano, con el fin de consolidar la gestión del conocimiento, realizar el seguimiento correspondiente y evidenciar el cumplimiento de las acciones de formación definidas por la entidad."

Por lo anterior se establece cumplimiento parcial de la Resolución 384 de 2023 en los ítems 14 y 20 del artículo 15; no obstante, de acuerdo con las respuestas otorgadas, no existe evidencia suficiente que permita asegurar la participación efectiva de teletrabajadores en las capacitaciones realizadas, lo que genera un vacío de trazabilidad y limita la verificación del cumplimiento normativo.

Por otra parte, la Subdirección de Tecnologías y Sistemas de Información será responsable de verificar el correcto diligenciamiento del formato técnico de teletrabajo, con el propósito de determinar el cumplimiento de los requisitos tecnológicos mínimos por parte de cada candidato.

Esta actividad se encuentra formalmente establecida en la Actividad No. 4 del Procedimiento de Teletrabajo (Código P-TH-13, versión 2 del 11 de septiembre de 2023) y en el artículo 29. Plataformas y herramientas de tecnologías de la información y las comunicaciones TIC para el desarrollo del teletrabajo de la Resolución 384 de 2023 del MJD, en los siguientes términos: *"La Dirección de Tecnologías y Gestión de Información en Justicia revisará y validará de acuerdo con el formato establecido, las especificaciones técnicas de software y hardware, conexión de banda ancha y velocidad de internet, la selección del dispositivo adecuado dependerá de la necesidad de cada perfil, considerando el tipo de labor a realizar. También, brindará el soporte técnico necesario a los teletrabajadores y validará que los hardware de los equipos no sean manipulados.*

Parágrafo: Si la Dirección no valida en forma satisfactoria las condiciones técnicas, el servidor deberá realizar los ajustes pertinentes para poder acceder al teletrabajo[11]". Con base en la evidencia suministrada, se observó que la STSI realiza actividades orientadas al cumplimiento de la revisión documental de los requisitos técnicos establecidos para la postulación a la modalidad de teletrabajo, conforme al Procedimiento P-TH-13 y al artículo 29 de la Resolución 384 de 2023. No obstante, las oportunidades de mejora identificadas en relación con la verificación integral de las condiciones tecnológicas y de conectividad fueron desarrolladas en los apartados anteriores.

Análisis del cumplimiento de lineamientos de teletrabajo en la política de seguridad de la información

Con relación a, la Política de Seguridad de la Información del MJD, versión 6, en el ítem 4.4.4 "Política de teletrabajo y trabajo remoto", establece lineamientos para el cumplimiento de la normatividad de teletrabajo, asegurando el uso adecuado y seguro de las TIC, la protección de la información y la verificación de las condiciones tecnológicas. La Subdirección de Tecnologías es responsable de configurar, validar y monitorear los equipos, la conectividad y los accesos remotos seguros.

Los líderes de proceso deben autorizar y controlar el acceso a la información, especialmente la de carácter sensible, mientras que los funcionarios deben usar únicamente dispositivos y medios autorizados, reportar incidentes y cumplir las políticas de seguridad. Asimismo, contratistas y terceros deben cumplir requisitos técnicos y de seguridad antes de acceder a los sistemas, bajo control y validación de la entidad

Si bien la política establece que la STSI debe realizar actividades de configuración, validación de equipos y monitoreo del uso de recursos de teletrabajo para prevenir incidentes de seguridad, no se identifican mecanismos documentados que garanticen la validación continua y periódica de las condiciones tecnológicas una vez aprobado el teletrabajo. Esto constituye una debilidad en el esquema de control y limita la capacidad institucional para asegurar el cumplimiento sostenido de los requisitos técnicos y de seguridad establecidos.

La evidencia obtenida permitió identificar como principal mecanismo formal de validación el diligenciamiento inicial del Formato Técnico de Teletrabajo (F-TH-13-05), acompañado de registro fotográfico por parte del funcionario postulado a la modalidad de teletrabajo, lo cual corresponde a una validación declarativa y puntual, sin evidenciarse procedimientos documentados de reevaluación periódica que permitan verificar objetivamente la permanencia de las condiciones tecnológicas aprobadas. En este contexto, se identifican las siguientes debilidades de control:

[11] Resolución 384 del 24 de marzo de 2023; Ministerio de Justicia y del Derecho; Artículo 29. Plataformas y herramientas de tecnologías de la información y las comunicaciones, TIC para el desarrollo del teletrabajo; Pág. 11 y 12; https://www.minjusticia.gov.co/normatividad-co/Resoluciones/Resoluci%C3%B3n%20No.%200384%20del%2024%20de%20marzo%20de%202023.pdf

- En la visita domiciliaria realizada para realizar la verificación de las condiciones del teletrabajador no se tiene contemplado el acompañamiento de un funcionario o contratista de tecnología para validar los requisitos tecnológicos.
- No se contemplan mecanismos formales de reevaluación técnica periódica de los equipos de cómputo autorizados.
- No se definen frecuencias, responsables ni procedimientos para la validación continua de las condiciones tecnológicas.
- No se establece un control explícito que garantice el uso de software y sistemas operativos con soporte vigente y actualizados.
- No se establece la formalización de la autorización del Oficial de Seguridad de la Información para accesos desde redes externas.
- Si bien la normativa y las políticas institucionales establecen la necesidad de verificar las condiciones tecnológicas y de seguridad para el teletrabajo, dicha verificación debe considerar que los equipos utilizados pueden ser de propiedad del funcionario, pudiendo contener información personal o sensible. En este sentido, la entidad debe definir lineamientos claros que permitan realizar la validación de condiciones de seguridad sin vulnerar la privacidad del titular de la información, en concordancia con los principios de protección de datos personales (Ley 1581 de 2012) y los lineamientos de seguridad de la información.

A manera de ejemplo, la ausencia de mecanismos de reevaluación periódica podría impedir detectar oportunamente situaciones como la utilización de sistemas operativos sin soporte vigente por parte del fabricante[12], condición que incrementaría la exposición a vulnerabilidades de seguridad. Esta condición implica que:

- No recibe actualizaciones de seguridad.
- Presenta vulnerabilidades conocidas sin mitigación.
- Es susceptible a explotación mediante malware y ataques automatizados.
- Genera riesgos significativos para la confidencialidad, integridad y disponibilidad de la información institucional.

Esta situación impide garantizar que los equipos y entornos tecnológicos continúen cumpliendo con los estándares establecidos, incrementando la exposición a riesgos operativos y de seguridad de la información.

Por lo anterior, se recomienda fortalecer y alinear la Resolución, el procedimiento y la Política de teletrabajo mediante la implementación de controles iniciales y periódicos de validación tecnológica, que aseguren el uso de sistemas y software con soporte vigente, así como el cumplimiento continuo de las condiciones de seguridad, estableciendo mecanismos de seguimiento, trazabilidad y control que reduzcan la exposición a riesgos de ciberseguridad y garanticen la protección de la información institucional.

Por último, se identifican vacíos en la política de seguridad frente a componentes relevantes relacionados en la Resolución 384 de 2023 del MJD, que deben realizarse:

[12] Por ejemplo, uso de un equipo de cómputo con sistema operativo Windows 7

- Aunque la Política incorpora obligaciones generales de confidencialidad y control de acceso, no desarrolla expresamente la restricción prevista en el artículo 14 literal e) de la Resolución 384 de 2023 relacionada con la prohibición de apoyo o colaboración de terceros ajenos a la entidad en la ejecución de funciones bajo la modalidad de teletrabajo
- La política establece la "sensibilización y capacitación continua de funcionarios, contratistas y terceros" como parte de la cultura de seguridad, pero no diferencia ni prioriza a los teletrabajadores como población objetivo. Este vacío incumple lo dispuesto en el ítem 14 del artículo 15 de la Resolución 384 de 2023 del MJD, que establece el uso y apropiación de TIC y seguridad digital para el teletrabajo y en el ítem 20 del mismo artículo, que menciona que se debe informar a los teletrabajadores sobre restricciones de uso de equipos, normativa vigente en protección de datos y sanciones por incumplimiento.

La falta de diferenciación y priorización de los teletrabajadores en los programas de capacitación impide garantizar la apropiación efectiva de las políticas de seguridad digital y TIC, lo que incrementa la exposición a riesgos de ciberseguridad, incumplimiento normativo y pérdida de trazabilidad en el teletrabajo. Por lo anterior, se recomienda fortalecer y alinear la política de seguridad y la Resolución mediante la inclusión de controles específicos para esta modalidad, que aseguren:

- De manera expresa que el teletrabajador no reciba apoyo, asistencia o intervención de terceros en el desarrollo de sus funciones.
- La implementación de programas de capacitación diferenciados y obligatorios para teletrabajadores en TIC y seguridad digital o la validación efectiva de la asistencia a las capacitaciones realizadas por la DTGIJ.
- Mecanismos de seguimiento, trazabilidad y evidencia que garanticen la apropiación de las capacitaciones y el cumplimiento de las obligaciones normativas.
- Obligatoriedad de acatar los protocolos de seguridad de la información que la DTGIJ disponga, para ser beneficiario del teletrabajo, o para continuar en esa condición.

5.2.2. Gestión de vulnerabilidades Técnicas

Según el anexo A de la ISO/IEC 27001:2022, los controles para la gestión de vulnerabilidades técnicas tienen como objetivo "*obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a esas vulnerabilidades y se deben adoptar las medidas apropiadas.*"

Con relación a, la Política de Seguridad de la Información del MJD, versión 6, en el ítem 4.6.5 "Gestión de vulnerabilidades técnicas", establece lineamientos orientados a garantizar la gestión de pruebas periódicas de vulnerabilidades y hacking ético, con reporte y lineamientos de mitigación.

Sin embargo, el cumplimiento frente a ISO 27001:2022 es parcial, ya que se observa ausencia de:

- Evidencia formal y trazable de ejecución de pruebas, incluyendo la aplicación sistemática de pruebas de validación (en adelante retest) posterior a la remediación, como requisito indispensable para verificar la eficacia de las correcciones y cerrar el ciclo completo de gestión de vulnerabilidades.
- Integrar los resultados de pruebas y retest en el ciclo de mejora continua, generando retroalimentación sistemática hacia planes de acción e indicadores de desempeño, para fortalecer la eficacia de los controles.
- Incorporar indicadores de desempeño en la gestión de vulnerabilidades (ej. tiempo promedio de cierre de hallazgos críticos, % de vulnerabilidades corregidas en plazo, tasa de éxito en retest), para medir la eficacia de las correcciones.

Por lo anterior, la OCI recomienda fortalecer la gestión de vulnerabilidades mediante evidencia trazable de pruebas y retest, integrar resultados en el ciclo de mejora continua y establecer indicadores de desempeño que midan la eficacia de las correcciones; de esta forma se garantiza cierre completo del ciclo, eficacia de correcciones y reducción del riesgo residual.

Es de resaltar que la DTGIJ tiene identificada la infraestructura crítica y no critica, clasificando riesgos por impacto, probabilidad y nivel de criticidad. Se definen estrategias de tratamiento (mitigar, transferir, aceptar, eliminar) y responsables, con actividades de respaldo, redundancia, alta disponibilidad, pruebas de restauración y actualizaciones de seguridad, entre otras, por último, se contemplan fechas de inicio de la actividad; sin embargo, no establece un nivel de priorización diferenciado que refleje el impacto y la probabilidad del riesgo según la clasificación de los activos.

Dentro de las actividades realizadas por el área de Tecnología para dar cumplimiento a la gestión de vulnerabilidades, allegan cinco (5) informes de análisis de vulnerabilidades correspondientes a lo corrido de la vigencia 2026. Como soporte, se destaca un (1) informe técnico de remediación en el que se describen las acciones implementadas para el fortalecimiento de la seguridad, tanto a nivel de infraestructura —incluyendo protocolos y mecanismos de cifrado— como a nivel de aplicación —a través de la implementación de cabeceras de seguridad, controles para mitigar vulnerabilidades web y la configuración segura de cookies, entre otros—. De acuerdo con lo consignado en dicho informe, las acciones fueron ejecutadas en el periodo comprendido entre el 18 de marzo y el 10 de abril de 2026.

A continuación, se desarrolla el análisis comparativo entre los cinco (5) informes de análisis de vulnerabilidades y los resultados del retest efectuado por la OCI con la misma herramienta utilizada por Tecnología.

- **Análisis de vulnerabilidades a SUIN-JURISCOL**: Del análisis comparativo entre el informe de vulnerabilidades del 2 de marzo de 2026 (realizado por Tecnología) y el escaneo realizado el 22 de junio de 2026 (realizado por la OCI),

no se evidencia una mejora en la postura de seguridad asociada a las vulnerabilidades inicialmente identificadas; por el contrario, se observa un incremento significativo en el número y nivel de criticidad de los hallazgos.

En el informe del 2 de marzo se identificaron 5 vulnerabilidades, distribuidas en 3 de severidad media y 2 de severidad baja. Sin embargo, en el escaneo del 22 de junio se reportan 112 vulnerabilidades en total, correspondientes a 3 críticas, 1 alta, 36 medias y 72 bajas, lo cual evidencia un deterioro en el estado de seguridad del activo evaluado. En particular, la aparición de vulnerabilidades de nivel crítico y alto, inexistentes en el informe inicial, refleja una mayor exposición al riesgo, lo cual podría derivarse de configuraciones inseguras, falta de endurecimiento o ausencia de controles preventivos en el ciclo de gestión de vulnerabilidades.

En consecuencia, se concluye que, aunque pudieron haberse ejecutado acciones puntuales, no se evidencia una remediación efectiva ni sostenida de las vulnerabilidades reportadas en el informe del 2 de marzo de 2026, dado que el análisis del 22 de junio muestra un incremento significativo en la superficie de ataque y en el nivel de riesgo del sistema, evidenciando debilidades en el proceso de gestión y control de vulnerabilidades.

- **Análisis de vulnerabilidades a SICAAC**: Del análisis comparativo entre el informe del 2 de marzo de 2026 (realizado por Tecnología) y el escaneo realizado el 22 de junio de 2026 (realizado por la OCI), no se evidencia una remediación efectiva de las vulnerabilidades inicialmente identificadas, considerando el comportamiento global de los resultados.

  En el informe del 2 de marzo se identificaron siete (7) vulnerabilidades, distribuidas en 4 de severidad media y 3 de severidad baja. No obstante, en el escaneo del 22 de junio se reportan 98 vulnerabilidades, correspondientes a 1 crítica, 18 medias y 79 bajas, lo cual representa un incremento significativo tanto en volumen como en nivel de riesgo. Si bien no es posible descartar que algunas de las vulnerabilidades iniciales hayan sido tratadas de manera puntual, el aumento considerable en el número total de hallazgos y la presencia de vulnerabilidades críticas constituye un elemento relevante desde el punto de vista de auditoría, ya que indica que existen debilidades que podrían ser explotadas con un alto impacto, y que no fueron prevenidas ni mitigadas oportunamente dentro del proceso de gestión de vulnerabilidades.

  En consecuencia, se concluye que, aunque pudieron haberse realizado acciones correctivas puntuales, no se evidencia una mejora sostenida ni efectiva en la gestión de vulnerabilidades, toda vez que el análisis del 22 de junio no solo refleja la persistencia o sustitución de debilidades, sino también la incorporación de nuevos riesgos de mayor criticidad, lo cual denota debilidades en los mecanismos de control, priorización, seguimiento y aseguramiento de las actividades de remediación.

- **Análisis de vulnerabilidades a MICC**: Del análisis comparativo entre el informe de análisis de vulnerabilidades del 18 de marzo de 2026 (realizado por Tecnología) y el escaneo realizado el 22 de junio de 2026 (realizado por la OCI), se evidencia una disminución significativa en la cantidad de vulnerabilidades identificadas, pasando de 23 vulnerabilidades de severidad media y 32 de severidad baja en marzo, a 5 vulnerabilidades medias y 9 bajas en junio, lo cual indica que se llevaron a cabo acciones de remediación y mitigación por parte del área de Tecnología.

  No obstante, al analizar la naturaleza de las vulnerabilidades persistentes, se observa que aún subsisten debilidades en controles de seguridad fundamentales, particularmente en la configuración de los protocolos criptográficos, evidenciándose que continúan habilitados los protocolos TLS 1.0 y TLS 1.1, así como configuraciones que no garantizan un nivel óptimo de seguridad en las comunicaciones.

  En consecuencia, se concluye que, si bien existe evidencia de gestión y reducción del número de vulnerabilidades entre los periodos evaluados, persisten hallazgos relevantes que requieren fortalecimiento, lo que indica la necesidad de consolidar el proceso de remediación, priorizando la eliminación de vulnerabilidades estructurales y la implementación de controles de seguridad base, con el fin de garantizar un nivel de protección adecuado y sostenible.

- **Análisis de vulnerabilidades a portal web**: Del análisis comparativo entre el informe de vulnerabilidades del 19 de marzo de 2026 (realizado por Tecnología) y el escaneo realizado el 22 de junio de 2026 (realizado por la OCI), se evidencia una mejora parcial en la gestión de vulnerabilidades, reflejada en la reducción del número total de hallazgos y en la eliminación de vulnerabilidades de mayor criticidad intermedia (altas).

  En el informe de marzo se reportó 1 vulnerabilidad crítica, 4 altas, 6 medias y 115 bajas, mientras que en junio se identifican 1 crítica, 0 altas, 6 medias y 53 bajas, lo que evidencia que se logró la remediación de las vulnerabilidades de severidad alta, lo cual representa un avance relevante en la reducción del riesgo y se redujo significativamente el número de vulnerabilidades bajas, pasando de más de cien a poco más de cincuenta, lo que evidencia acciones de mitigación sobre controles de menor criticidad.

  En consecuencia, se concluye que sí se evidencian acciones de remediación parciales, particularmente en la eliminación de vulnerabilidades altas y en la reducción significativa de vulnerabilidades bajas; sin embargo, no se evidencia una remediación completa ni efectiva sobre los riesgos más críticos, dado que la vulnerabilidad crítica persiste sin corrección, se mantienen vulnerabilidades medias estructurales, lo que indica que las acciones implementadas no han sido suficientes para fortalecer de manera integral la seguridad del activo.

- **<u>Análisis de vulnerabilidades a SGDEA</u>:** Del análisis comparativo entre el informe de análisis de vulnerabilidades del 12 de mayo de 2026 y el escaneo realizado el 22 de junio de 2026, no se evidencia una remediación efectiva de las vulnerabilidades identificadas inicialmente, considerando la evolución y naturaleza de los hallazgos.

  En el informe de mayo se identificaron 1 vulnerabilidad crítica, 6 medias y 2 bajas, mientras que en el escaneo de junio se reportan 1 crítica, 7 medias y 2 bajas. Lo anterior evidencia que, además de la persistencia de vulnerabilidades previas, se incorporan nuevas debilidades en la configuración de seguridad, particularmente en el componente criptográfico.

  En consecuencia, se concluye que, aunque el volumen total de vulnerabilidades se mantiene relativamente estable, no se evidencia una mejora en la postura de seguridad ni un cierre efectivo de los hallazgos identificados en mayo.

Del análisis integral de los cinco ejercicios de comparación entre informes de vulnerabilidades y sus respectivos escaneos de validación (retest) realizados por la OCI, se evidencia un comportamiento heterogéneo en la gestión de vulnerabilidades por parte del área de Tecnología, con resultados que varían entre avances parciales, ausencia de remediación efectiva y deterioro de la postura de seguridad en algunos activos. Asimismo, se evidencia que, aun cuando se reducen vulnerabilidades en volumen, no siempre se prioriza adecuadamente la remediación de hallazgos críticos, los cuales en varios casos persisten sin tratamiento.

En consecuencia, se concluye que la Entidad presenta un proceso de gestión de vulnerabilidades activo, pero no completamente efectivo, con énfasis en la reducción cuantitativa de hallazgos, pero con debilidades en el enfoque estratégico, priorización por riesgo, cierre efectivo y sostenibilidad de las remediaciones, lo que impacta la madurez del control de seguridad.

Por lo anterior, la OCI sugiere fortalecer el proceso de gestión de vulnerabilidades mediante la implementación de un enfoque integral, basado en riesgo y orientado al cierre efectivo, que contemple como mínimo:

- Priorización basada en criticidad, asegurando que las vulnerabilidades críticas y altas sean atendidas de manera inmediata y verificadas mediante pruebas de validación (retest).
- Gestión de remediación estructural, orientada a eliminar causas raíz (actualización de componentes, endurecimiento de configuraciones, implementación de controles base), evitando la reaparición de vulnerabilidades.
- Ciclo formal de cierre y validación, garantizando que toda vulnerabilidad tratada sea verificada y documentada como cerrada, evitando tratamientos parciales.
- Monitoreo continuo y control de cambios, con el fin de prevenir la introducción de nuevas vulnerabilidades en los activos evaluados.

- Definición de indicadores de desempeño (KPIs), tales como tiempo de remediación, porcentaje de cierre por criticidad y reincidencia de vulnerabilidades, que permitan evaluar la efectividad del proceso.

Lo anterior con el fin de evolucionar hacia un modelo de gestión de vulnerabilidades preventivo, sostenible y alineado con buenas prácticas de seguridad, reduciendo de manera efectiva la exposición al riesgo de los sistemas de información.

Por último, Tecnología allega dos reportes generados por COLCERT[13], para los cuales ha definido un plan de trabajo orientado a la remediación. Se evidencia ejecución de actividades, aplicación de parches críticos, ventanas de mantenimiento y avances en la mitigación; no obstante, persisten actividades pendientes por iniciar y concluir. Por lo anterior, se recomienda formalizar la trazabilidad de las acciones, priorizar el cierre de las actividades críticas y documentar evidencia verificable de cada ejecución, con el fin de garantizar la eficacia de las correcciones y el cumplimiento pleno de los lineamientos de seguridad.

Dado lo anterior, se recomienda definir en la política un tratamiento diferenciado para infraestructura crítica (pruebas más frecuentes, trazabilidad reforzada, métricas de eficacia) y para infraestructura no crítica (controles básicos y revisiones periódicas), asegurando alineación con ISO 27001:2022 en gestión de riesgos y continuidad.

Por consiguiente, se recomienda establecer y ejecutar un ciclo formal de remediación y retest, que incluya la corrección de las vulnerabilidades identificadas, la validación posterior mediante nuevos escaneos de seguridad y el aseguramiento de que las medidas implementadas han mitigado efectivamente los riesgos, dejando evidencia del cierre de los hallazgos; esta recomendación cobra especial relevancia al evidenciarse coincidencias entre las vulnerabilidades identificadas por Tecnología y los hallazgos detectados por la Oficina de Control Interno (OCI), en el marco de esta auditoría.

Dado el carácter sensible de la información generada, los informes detallados serán entregados de manera restringida a la Dirección de Tecnologías y Gestión de Información en Justicia (DTGIJ).

5.3. Instrumento de evaluación MSPI

El "instrumento de evaluación MSPI" permite identificar de forma específica los controles implementados, mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y permite obtener insumos fundamentales para la fase de planificación. Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación y actualizar la información tras terminar la fase de evaluación de desempeño, para identificar los cambios en el nivel de madurez de la implementación

[13] Grupo de Respuesta a Emergencias Cibernéticas de Colombia, encargado de coordinar la prevención, gestión y respuesta ante incidentes de seguridad digital a nivel nacional.

del Modelo en la Entidad, el resultado que se obtenga después de la fase de evaluación de desempeño se incluirá como un insumo, en la fase de mejoramiento continuo[14].

De acuerdo con la evidencia allegada, se encuentra medición efectuada con fecha de evaluación octubre de 2025, realizada por el oficial de seguridad de la información. En el archivo analizado se encuentra la tabla de "Evaluación de Efectividad de controles", la cual resume los porcentajes de avance del resultado de nivel de implementación de controles y muestra el grado de cumplimiento para 4 de los dominios de acuerdo con la ISO/IEC 27001:2022 y su anexo A:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	88	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	93	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	90	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	81	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		88	100	OPTIMIZADO

Fuente: Instrumento de evaluación MSPI vigencia 2025, elaborado por Tecnología

A partir del análisis de la tabla y de la información consignada en el autodiagnóstico, es posible concluir que:

- El dominio A.5, correspondiente a los controles organizacionales, presenta una calificación de 88 puntos y un nivel de madurez "optimizado", lo que implica que las buenas prácticas se encuentran definidas, automatizadas y en proceso de mejora continua. Sin embargo, de los 37 ítems evaluados, solo el 73% alcanza 100 de nivel de cumplimiento, mientras que un 27% restante evidencia niveles parciales (80, 60 y 20), lo que refleja brechas relevantes que deben ser atendidas para consolidar la madurez institucional y garantizar la sostenibilidad del sistema.
- El dominio A.6, correspondiente a los controles de personas, presenta una calificación de 93 puntos y un nivel de madurez "optimizado", lo que implica que las buenas prácticas se encuentran definidas, automatizadas y en proceso de mejora continua. No obstante, de los 8 ítems evaluados, el 87,5% alcanza un 100 de nivel de cumplimiento, mientras que un 12,5% evidencia un nivel de cumplimiento de 40, reflejando una brecha crítica que debe ser atendida para consolidar la madurez institucional y garantizar la sostenibilidad del sistema de gestión de seguridad de la información.
- El dominio A.7, correspondiente a los controles físicos, presenta una calificación de 90 puntos y un nivel de madurez "optimizado", lo que implica que las buenas

[14] Maestro del modelo de seguridad y privacidad de la información v 5.0 en el ítem 6. Diagnostico; pág. 28, MinTIC, abril 2025.

prácticas se encuentran definidas, automatizadas y en proceso de mejora continua. Sin embargo, de los 14 ítems evaluados, solo el 85,7% alcanza 100 de nivel de cumplimiento, mientras que un 14,2% restante evidencia niveles parciales (60 y 0), lo que revela una brecha significativa que debe ser atendida para consolidar la madurez institucional y garantizar la sostenibilidad del sistema, en especial para el ítem de seguridad del cableado que tiene un nivel de cumplimiento de 0.

- El dominio A.8, correspondiente a los controles tecnológicos, presenta una calificación de 81 puntos y un nivel de madurez "optimizado", lo que implica que las buenas prácticas se encuentran definidas, automatizadas y en proceso de mejora continua. No obstante, de los 34 ítems evaluados, solo el 58,8% alcanza el 100% de cumplimiento, mientras que el 41,2% restante evidencia niveles parciales (80, 60 y 40), reflejando brechas que deben ser atendidas para consolidar la madurez institucional y garantizar la sostenibilidad del sistema.

En conjunto, los resultados muestran que la Entidad ha logrado automatizar y optimizar buenas prácticas, pero la existencia de ítems con cumplimiento parcial o crítico (especialmente en los dominios organizacional, físico y tecnológico) representa riesgos que pueden comprometer la sostenibilidad, trazabilidad y efectividad del sistema de gestión de seguridad de la información.

La atención prioritaria debe enfocarse en:

- Priorizar el cierre de brechas del MSPI iniciando por aquellos controles que presentan los niveles más bajos de cumplimiento.
- Fortalecer controles tecnológicos, dado su mayor nivel de rezago.
- Asegurar trazabilidad y evidencia verificable en la implementación de mejoras.
- Integrar acciones correctivas al plan estratégico institucional, garantizando alineación con estándares internacionales y sostenibilidad en el tiempo.

Con respeto a la Calificación frente a mejores prácticas en ciberseguridad (NIST[15]), se encuentra una tabla que muestra las brechas de cumplimiento entre el desempeño actual y el nivel esperado por el marco NIST.

A partir del análisis de la tabla y de la información consignada en el autodiagnóstico, es posible concluir que:

[15] National Institute of Standards and Technology (NIST): Es una agencia federal de los Estados Unidos que trabaja en colaboración con la industria y la academia para mejorar la seguridad económica y la calidad de vida. Su misión es promover la innovación y la competitividad industrial en el país

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
GOVERNAR	79	100
IDENTIFICAR	100	100
PROTEGER	90	100
DETECTAR	90	100
RESPONDER	80	100
RECUPERAR	82	100

Fuente: Instrumento de evaluación MSPI vigencia 2025, elaborado por Tecnología

- Governar: La Entidad presenta una calificación de 79 puntos frente al ideal de 100, con 6 ítems evaluados. De estos, el 33,3% alcanza una calificación de 100 puntos de cumplimiento, mientras que el 66,7% restante evidencia calificaciones entre 95, 80, 60 y 40, destacando como brecha crítica la categoría de "Supervisión". Esta situación refleja la necesidad de fortalecer los mecanismos de gobernanza para cerrar las brechas y garantizar la sostenibilidad del sistema de gestión de seguridad de la información.
- Identificar: La Entidad presenta una calificación de 100 puntos, alcanzando el nivel ideal establecido por el marco NIST. Los 3 ítems evaluados obtuvieron un 100% de cumplimiento, lo que demuestra la solidez de los procesos de identificación y la plena alineación con las buenas prácticas internacionales en ciberseguridad.
- Proteger: La Entidad presenta una calificación de 90 puntos frente al ideal de 100, con 5 ítems evaluados. De estos, el 60% alcanza la calificación de 100, mientras que el 40% restante evidencia calificaciones parciales de 77,5 y 70, lo que refleja brechas relevantes que deben ser atendidas para fortalecer la capacidad de protección y garantizar la sostenibilidad del sistema de gestión de seguridad de la información
- Detectar: La Entidad presenta una calificación de 90 puntos frente al ideal de 100, con 2 ítems evaluados. De estos, el 50% alcanza una calificación de 100 puntos de cumplimiento, mientras que el 50% restante evidencia un nivel de cumplimiento de 80 puntos, lo que refleja una brecha moderada que debe ser atendida para fortalecer la capacidad de detección y garantizar la sostenibilidad del sistema de gestión de seguridad de la información.
- Responder: La Entidad presenta una calificación de 80 puntos frente al ideal de 100, con 2 ítems evaluados. De estos, el 50% alcanza una calificación de 100 de cumplimiento, mientras que el 50% restante evidencia un nivel de cumplimiento de 60 puntos, lo que refleja una brecha significativa que debe ser atendida para fortalecer la capacidad de respuesta y garantizar la sostenibilidad del sistema de gestión de seguridad de la información.
- Recuperar: La Entidad presenta una calificación de 82 frente al ideal de 100. De estos, el 50% alcanza una calificación de 100 de cumplimiento, mientras que el 50% restante evidencia un nivel de cumplimiento de 60 puntos, lo que refleja una brecha significativa que debe ser atendida para fortalecer la capacidad de

recuperación y garantizar la sostenibilidad del sistema de gestión de seguridad de la información.

En conclusión, la entidad cuenta con una base sólida en identificación y protección, pero debe priorizar la gobernanza, la respuesta y la recuperación para alcanzar un nivel de madurez integral y sostenible frente al modelo NIST.

Por último, en cuanto a las diferentes pestañas que contiene el instrumento, la OCI encontró que:

- Levantamiento de información: Se sugiere completar la información faltante en la columna "Nombre del documento entregado".
- Clausulas: Se sugiere completar la información faltante en las columnas "Evidencia", "Brecha" y "Recomendación". Lo anterior cobra importancia teniendo en cuenta que esta información alimenta la tabla de "avance cláusulas modelo de operación (PHVA)".
- Organizacionales, Personas, Físicos, Tecnológicos: En los ítems cuya calificación es inferior a 100 no se encuentra diligenciada la columna "Brecha" y "Recomendación"; así como en algunas filas no se encuentra ingresada la evidencia que soporta el cumplimiento.

La OCI identificó vacíos en el diligenciamiento del instrumento: falta de información en columnas críticas (*documento entregado, evidencia, brecha y recomendación*) y ausencia de soporte en ítems con calificación parcial. Por lo anterior se sugiere completar la información faltante y estandarizar evidencias y brechas para asegurar trazabilidad y fortalecer la sostenibilidad del sistema.

6. Análisis de Riesgo

La Oficina de Control Interno, en el marco de su plan de auditoría con enfoque en riesgos, adelantó la evaluación y verificación a la política de seguridad y privacidad de la información, en la que se define que el Oficial de seguridad de la información es el responsable de "*Liderar y brindar acompañamiento a los procesos y proyectos de la entidad en la gestión de riesgos de seguridad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia*[16]".

Por otra parte, la mencionada Política contiene el ítem "4.3.4 Activos de información" mencionando que el MJD gestiona de forma integral sus activos de información mediante un inventario actualizado y clasificado (confidencialidad, integridad y disponibilidad), cumpliendo la normativa vigente. Se asignan responsables y custodios para cada activo, quienes garantizan la implementación de controles de seguridad,

[16] Política de seguridad y privacidad de la información v 6.0 en el ítem 4.3.1 Roles y responsabilidades del sistema de gestión de seguridad de la información/ Responsable u oficial de seguridad de la información; pág. 7, MJD, 9 de diciembre de 2025

gestión de riesgos y revisión periódica de accesos. Esto asegura protección, control y transparencia de la información institucional.

De acuerdo con lo expuesto, se procede al análisis de la matriz de riesgos de seguridad de la información de la vigencia 2025, identificando los siguientes aspectos relevantes:

- 40 activos de información relacionados en la matriz
- 23 activos de información están catalogados con riesgo inherente "Bajo"
- 9 activos de información están catalogados con riesgo inherente "Moderado"
- 5 activos de información están catalogados con riesgo inherente "Alto"
- 3 activos de información están catalogados con riesgo inherente "Extremo"
- Los controles están redactados con verbos que indican la acción: validar, coordinar, contratar, identificar, clasificar, divulgar, gestionar, implementar. Esto coincide con la estructura definida por el DAFP, pues se describe qué hace el control; aunque en algunos casos, la acción es repetitiva o genérica (ej. "coordina y contrata servicios"), lo que puede limitar la claridad sobre cómo se mitiga el riesgo.
- En algunos riesgos de la matriz se identifican causas genéricas (ej. "deficiencias de personal crítico", "falla de software", "condiciones ambientales"), pero no siempre se diferencian claramente de la circunstancia inmediata. Esto genera ambigüedad (el control puede estar atacando el síntoma y no la causa raíz).
- Dentro de los activos de información relacionados no se evidencian sistemas de información y aplicaciones de Software (Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas[17]).
- Se encuentran relacionados 83 controles, de los cuales 9 se encuentran catalogados con un rango de clasificación de diseño del control "débil" y 74 catalogados como "fuerte".

Dada la cantidad de activos de información y de controles asociados, la auditora determina evaluar de manera general la estructura de la descripción de los controles, conforme a lo establecido en la matriz y en la Guía de Gestión Integral del Riesgo, de la siguiente manera para el diseño del control:

- Tipología del control: Se especifica que los controles son preventivos, detectivos o correctivos.
- Objetivo del control: Se describe en relación con la vulnerabilidad o riesgo (ej. pérdida de disponibilidad, acceso no autorizado, divulgación indebida). Sin embargo, no todos los controles están formulados para atacar directamente la causa raíz del riesgo.
- Responsable asignado: En todos los casos se menciona que los controles cuentan con un responsable definido, con autoridad suficiente y con adecuada segregación de funciones en la ejecución.
- Oportunidad de ejecución: En todos los casos se menciona que es oportuna.

[17] *Guía para la Gestión integral del Riesgo de Función pública v 7.0 en el capítulo 5.1. 5.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados; pág. 95, DAFP, 7 de agosto de 2025*

- Confiabilidad de la información: En todos los casos se indica que la información es confiable.
- Medición y seguimiento (indicadores o métricas): En relación con la medición, 18 controles indican explícitamente que las métricas se tienen en cuenta en los indicadores, 64 señalan que se miden periódicamente o por demanda y se lleva un registro, y solo 1 control no se mide.

En cuanto a la ejecución del control se encuentra:

- Periodicidad de ejecución: De los 83 controles, 50 son "manuales", 20 son "semiautomáticos" y 13 son "automáticos".
- Formalización documental: 82 controles están "Aprobados y divulgados" y 1 "No documentado".
- Funcionamiento operativo:76 controles mencionan que son "Altamente efectivos" al momento de realizar las pruebas de recorrido, 6 están descritos como "Medianamente efectivo" y 1 como "No Aplica".
- Rango de calificación de la ejecución:68 controles están calificados como "débil" y 15 como "moderado".
- Solidez individual de cada control: 68 controles están calificados como "débil" y 15 como "moderado".
- Calificación de la solidez del conjunto de controles: En todos los casos está tipificada como "débil".

En cuanto al plan de tratamiento:

- Meta: De los 40 activos definidos; 23 no tienen una meta definida y 17 si la tienen.
- Inicio: De los 40 activos definidos; 23 tienen una fecha de inicio definida y 17 la tiene definida entre el 1 de febrero y el 1 de abril de 2024.
- Duración: De los 40 activos definidos; 5 tienen una duración de 3 meses; 5 tienen una duración de 6 meses; 7 tienen una duración de 1 año y 23 como no aplica.
- Acción si se materializa: De los 40 activos definidos; 23 no tienen una acción definida y 17 si la tienen.

En cuanto al seguimiento de los 83 controles; 31 indican "Pendiente documentar por el área" y 52 tienen las observaciones correspondientes a los seguimientos realizados, los cuales no evidencian una periodicidad en su realización.

En cuanto al seguimiento de los planes de tratamiento; 20 indican "N/A", 8 indican "Pendiente documentar por el área"; 8 tienen las observaciones correspondientes a los seguimientos realizados y 1 se encuentran en blanco; no evidencian una periodicidad en su realización; adicionalmente, se encuentra una diferencia entre los activos definidos y el seguimiento a los planes.

Se concluye que la entidad cuenta con una estructura formalizada de controles y planes de tratamiento, con responsables definidos y un alto porcentaje de controles efectivos

en pruebas de recorrido. Sin embargo, la solidez global de los controles se tipifica como débil, lo que refleja que, aunque existen mecanismos, estos no garantizan una reducción sostenible del riesgo residual.

Las principales brechas se concentran en:

- Cobertura incompleta de activos tecnológicos.
- Controles genéricos que no atacan causas raíz.
- Planes de tratamiento sin metas ni acciones definidas.
- Seguimiento sin periodicidad ni trazabilidad clara.

Esto limita la capacidad de la entidad para demostrar eficacia, sostenibilidad y mejora continua en la gestión de riesgos de seguridad de la información. Por lo anterior la OCI recomienda en el marco de la mejora continua:

- Ampliar la cobertura de activos: Incluir sistemas de información, aplicaciones y software crítico en la matriz.
- Fortalecer la descripción de controles: Redactar siguiendo la fórmula Responsable + Acción + Complemento. Evitar verbos genéricos y asegurar que la acción ataque la causa raíz.
- Revisar y robustecer controles débiles: Priorizar acciones correctivas sobre los 68 controles calificados como débiles y los 9 de diseño débil.
- Definir metas y acciones en planes de tratamiento: Establecer objetivos claros, fechas de inicio y acciones específicas en caso de materialización del riesgo.
- Mejorar la medición y seguimiento: Incorporar indicadores de eficacia (ej. % incidentes prevenidos, tiempo de respuesta, cumplimiento de ANS).
- Establecer periodicidad uniforme en el seguimiento de controles y planes.
- Consolidar evidencia y oficialidad: Garantizar que todos los controles estén documentados, divulgados y con evidencia verificable.

7. Conclusiones, hallazgos y/ recomendaciones

Se presentan las siguientes conclusiones, hallazgos y recomendaciones de acuerdo con la revisión y análisis de las evidencias.

7.1. Conclusiones

Se evidencia que, si bien el MJD cuenta con una Política de Seguridad de la Información, lineamientos de teletrabajo y un esquema definido para la gestión de vulnerabilidades, se identifican brechas en su articulación, implementación y seguimiento, particularmente en la validación tecnológica continua, la trazabilidad de los controles y el cierre efectivo del ciclo de gestión de riesgos y vulnerabilidades.

la Política de Seguridad de la Información se encuentra establecida, pero presenta debilidades en su operacionalización, especialmente en la definición de controles, indicadores, seguimiento y mecanismos de evaluación. Asimismo, se requiere mejorar su articulación con el PESI y con los resultados del MSPI, así como fortalecer el modelo de gobernanza, la independencia del Oficial de Seguridad y la gestión de la confidencialidad, con el fin de garantizar un SGSI más robusto, medible y sostenible.

Aunque existen lineamientos definidos para el teletrabajo, estos requieren mayor articulación y fortalecimiento en su implementación, especialmente en lo relacionado con validaciones tecnológicas, controles de seguridad y seguimiento continuo. La ausencia de mecanismos formales de verificación, trazabilidad y actualización de condiciones tecnológicas incrementa la exposición a riesgos de ciberseguridad y puede afectar la protección de la información institucional.

Los lineamientos de teletrabajo incluidos en la política requieren mayor precisión y fortalecimiento en aspectos clave como control de terceros, validación de equipos, protección de datos personales y capacitación. La ausencia de mecanismos formales de seguimiento y evidencia limita la verificación del cumplimiento y la apropiación de las medidas de seguridad por parte de los teletrabajadores.

La gestión de vulnerabilidades presenta oportunidades de mejora en cuanto a la formalización de su ciclo completo, desde la identificación hasta la validación del cierre. La falta de indicadores, trazabilidad, priorización diferenciada y monitoreo continuo limita la efectividad del proceso, limitando la capacidad de la entidad para demostrar la reducción efectiva del riesgo asociado a vulnerabilidades de seguridad

Los resultados del instrumento de evaluación MSPI evidencian la existencia de brechas significativas en el nivel de cumplimiento, especialmente en aquellos ítems con niveles críticos, así como rezagos en la implementación de controles tecnológicos. Adicionalmente, se identifican debilidades en la trazabilidad, disponibilidad de evidencias y estandarización de la información, lo cual limita la verificación del avance y la efectividad de las acciones implementadas.

Las matrices de riesgos requieren fortalecimiento en la identificación de activos, definición de controles, medición de su eficacia y establecimiento de planes de tratamiento. Las debilidades en la documentación, seguimiento e indicadores limitan la gestión efectiva del riesgo, reduciendo la capacidad preventiva y la respuesta oportuna ante eventos adversos.

La implementación de estas acciones permitirá incrementar el nivel de madurez del SGSI, mejorar la capacidad de prevención y respuesta ante riesgos cibernéticos, y asegurar de manera integral la protección de la información institucional.

7.2. Hallazgos

Para la DTGIJ y el GGH: Se evidenció que la validación de las condiciones tecnológicas y de comunicación de los funcionarios postulados a la modalidad de teletrabajo se realiza mediante la revisión documental del Formato Técnico de Teletrabajo (F-TH-13-05) y la evidencia fotográfica aportada por el servidor, sin aplicar mecanismos adicionales que permitan corroborar de manera efectiva el cumplimiento inicial, ni mecanismos documentados y estandarizados que permitan efectuar una verificación integral y periódica de las condiciones tecnológicas y de conectividad, ya sea de manera presencial o mediante herramientas remotas de validación que permitan corroborar el cumplimiento del artículo 14 de la Resolución 384 de 2023. Lo cual ocurre por la falta de definición e implementación de procedimientos e instrumentos estandarizados que permitan realizar verificaciones integrales (presenciales o remotas), limitando el proceso a revisión documental basada en evidencia fotográfica.

Esta situación limita la capacidad institucional para demostrar el cumplimiento integral de los requisitos tecnológicos y de seguridad establecidos para el teletrabajo, incrementando la exposición a riesgos asociados con configuraciones inadecuadas, conectividad insegura, uso de tecnologías no autorizadas y afectaciones a la confidencialidad, integridad y disponibilidad de la información institucional.

Recomendación para el hallazgo (plan de mejora): Se recomienda definir e implementar un procedimiento que garantice que la Dirección de Tecnologías y Gestión de Información en Justicia realice dicha verificación de manera efectiva, ya sea de forma presencial o remota, incorporando mecanismos que permitan validar directamente el cumplimiento de los requerimientos tecnológicos y de comunicación en el entorno real de trabajo del funcionario.

7.3. Socialización informe de auditoria

Mediante memorando MJD-MEM26-0003623 del día 25 de junio de 2026, se remite informe preliminar de esta auditoría, a la Dirección de Tecnologías y Gestión de la Información en Justicia (En adelante DTGIJ), Subdirección de Tecnologías y Sistemas de Información (En adelante STSI) y al Grupo de Gestión Humana (En adelante GGH); mediante el cual se informa que pueden remitir sus comentarios o promover una reunión de socialización con la OCI, dentro de los tres (3) días siguientes a la recepción de este informe, conforme lo dispone el procedimiento de Auditoría Interna.

Mediante comunicación radicada No. MJD-MEM26-0003704 del 1 de julio de 2026, la DTGIJ presentó respuesta al hallazgo consignado en el informe de auditoría, manifestando su aceptación. Adicionalmente, solicitó la vinculación del GGH en la formulación y ejecución de las acciones correspondientes, indicando para tal efecto:

"Si bien es cierto que en el Ministerio existe un procedimiento P-TH-13 Vr 002,de teletrabajo teniendo como responsable al coordinador del Grupo de Gestión Humana, cuyo objetivo "es el de establecer las actividades a realizar para que los funcionarios públicos del Ministerio de Justicia y del Derecho que cumplan los requisitos normativos puedan acceder a la modalidad de teletrabajo, así mismo, señalar las actividades a efectuar posterior a la validación y aprobación de la solicitud de teletrabajo", la Dirección de Tecnologías y Gestión de la Información, no debe crear un procedimiento, sino incluir dentro del existente una actividad que permita realizar dicha verificación de manera efectiva, ya sea de forma presencial o remota, incorporando mecanismos que permitan validar directamente el cumplimiento de los requerimientos tecnológicos y de comunicación en el entorno real de trabajo del funcionario, para de esta manera evitar las afectaciones a la confidencialidad, integridad y disponibilidad de la información institucional. En este orden de ideas, el hallazgo no es solamente dirigido a el área de TI, sino también para el área de Gestión Humana, siendo ella la responsable del procedimiento P-TH-13 Vr 002.En conclusión, debemos estar las dos áreas incluidas en el hallazgo, para cumplirlo establecido en la Resolución 384 de 2023".

Dado lo anterior, la Oficina de Control Interno (OCI) manifiesta que, de conformidad con los lineamientos establecidos en el numeral 15 del artículo 15 de la Resolución 384 de 2023 del Ministerio de Justicia y del Derecho, correspondiente a las obligaciones del Ministerio, según el cual se debe "*verificar que el lugar de trabajo donde reside el(la) teletrabajador(a) cumpla en todo momento con las condiciones técnicas y de seguridad y salud en el trabajo, con apoyo de la ARL*", así como con lo dispuesto en el numeral 5 del artículo 27 de la misma resolución, referente a las acciones del(la) Coordinador(a) del Grupo de Gestión Humana, que establece como responsabilidad "*programar y adelantar las visitas de verificación pertinentes al lugar de domicilio de los(as) funcionarios(as) que se encuentren en proceso de acceder a la modalidad de teletrabajo, así como a aquellos(as) que ya se encuentren en dicha modalidad cuando se requiera*", y considerando lo manifestado por la Dirección de Tecnología, la OCI concluye que es procedente vincular al Grupo de Gestión Humana (GGH) dentro del presente hallazgo. Lo anterior, teniendo en cuenta que dicha dependencia es responsable del procedimiento de teletrabajo código P-TH-13, versión 02 del 11 de septiembre de 2023, y tiene asignadas funciones directamente relacionadas con la verificación y seguimiento de las condiciones requeridas para el desarrollo de esta modalidad laboral.

En consecuencia, la OCI determina que el Grupo de Gestión Humana comparte responsabilidad en los aspectos observados dentro del hallazgo, por lo que deberá participar en la definición, formulación e implementación de las acciones correctivas y de mejora que se establezcan en el respectivo plan de mejoramiento, con el fin de fortalecer los mecanismos de control, seguimiento y verificación asociados a la modalidad de teletrabajo y prevenir la materialización de situaciones similares en el futuro.

7.4. Recomendaciones:

Se consignan algunas recomendaciones que no son obligatorias de asumir, sin embargo, desde la perspectiva de la oficina de control interno pueden ser importantes para seguir asegurando el proceso:

Para la DTGIJ y el GGH: En relación con la política de teletrabajo incluida en la política de seguridad de la información, el procedimiento de teletrabajo y la Resolución 384 de 2023, se recomienda:

- Fortalecer y alinear la Resolución, el procedimiento y la Política de teletrabajo mediante la implementación de controles iniciales y periódicos de validación tecnológica, que aseguren el uso de sistemas y software con soporte vigente, así como el cumplimiento continuo de las condiciones de seguridad, estableciendo mecanismos de seguimiento, trazabilidad y control que reduzcan la exposición a riesgos de ciberseguridad y garanticen la protección de la información institucional.
- Incluir el acompañamiento de un funcionario del área de Tecnología en las visitas domiciliarias realizadas para la verificación de las condiciones del teletrabajador, con el fin de validar el cumplimiento de los requisitos tecnológicos establecidos o por medios virtuales.
- Definir las frecuencias, responsables y procedimientos para la validación continua de las condiciones tecnológicas del teletrabajador, garantizando un control sistemático y documentado.
- Establecer un control explícito que garantice el uso de software y sistemas operativos con soporte vigente y debidamente actualizados en los equipos autorizados para el teletrabajo (propios o suministrados por el MJD).
- Formalizar la autorización del Oficial de Seguridad de la Información para los accesos a los sistemas institucionales desde redes externas, definiendo el procedimiento y los controles correspondientes o el posible ajuste de esta actividad de acuerdo con las actividades realizadas por Tecnología.
- Definir como política de operación del teletrabajo el cumplimiento obligatorio, por parte de los funcionarios beneficiarios, de las directrices de seguridad de la información emitidas por la Entidad.

Para la DTGIJ: En relación con la Política de seguridad de la información, se recomienda:

- Fortalecer el lineamiento asociado a la gestión de controles de seguridad de la información sobre los activos bajo custodia, complementando lo establecido en la matriz de riesgos, mediante la definición explícita de los mecanismos de implementación, monitoreo y revisión de dichos controles. Esto debe incluir la asignación de responsables claros, periodicidad de ejecución y seguimiento, definición de evidencias verificables, así como indicadores de cumplimiento y eficacia, garantizando su trazabilidad, medición, auditabilidad y mejora continua.
- Definir e implementar indicadores clave de desempeño (KPI) e indicadores clave de riesgo (KRI) asociados a la seguridad de la información, con criterios claros de medición, seguimiento periódico y gestión formal, orientados a evaluar la eficacia de los controles, apoyar la toma de decisiones y fortalecer la mejora continua del SGSI.
- Fortalecer la articulación entre la Política de Seguridad de la Información y el Plan

Estratégico de Seguridad de la Información (PESI), mediante la definición de mecanismos formales de alineación y trazabilidad que permitan vincular los lineamientos estratégicos con los objetivos, proyectos, controles, responsables, cronogramas e indicadores del plan, garantizando su implementación efectiva, seguimiento y medición en el marco del SGSI.

- Fortalecer la integración de los resultados del diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) y el nivel de madurez alcanzado,asegurando su incorporación explícita en la Política y su uso formal en el Plan Estratégico de Seguridad de la Información (PESI) como línea base para la definición de objetivos, priorización de controles y formulación de planes de mejora, garantizando su trazabilidad y alineación con las acciones y proyectos del SGSI.
- Revisar y ajustar el modelo de gobernanza del SGSI, asegurando la independencia funcional y organizacional del Oficial de Seguridad de la Información frente a las áreas operativas, con el fin de fortalecer la supervisión, control, evaluación y reporte, evitando conflictos de interés.
- Definir un esquema formal de respaldo y segregación de funciones, que garantice la continuidad de la gestión realizada por el Oficial de Seguridad de la Información y evite la concentración de responsabilidades en un único rol. Este esquema debe contemplar: Designación de suplentes o responsables alternos, con funciones claramente delimitadas; segregación de funciones críticas, para reducir riesgos de dependencia y conflictos de interés; protocolos de continuidad operativa, que aseguren la ejecución de actividades en caso de ausencia, rotación o contingencias.
- Diseñar e implementar un esquema estructurado de evaluación y auditoría periódica sobre los controles, la política y el SGSI, definiendo responsables, criterios, metodologías, periodicidad y evidencias, que permitan verificar el cumplimiento, medir la efectividad de los controles y soportar la mejora continua.
- Incorporar indicadores y mecanismos de evaluación que permitan medir la efectividad de la capacitación y sensibilización promovidas por la política.
- Definir un responsable e implementar un control formal de auditoría sobre las carpetas documentales de formatos de confidencialidad que garantice la trazabilidad y verificaciones sistemáticas de la información.
- Incluir en los lineamientos de la política los casos en los cuales debe realizarse la renovación de la firma del formato de confidencialidad, tales como el cambio de rol, la extensión contractual o el acceso a nueva información crítica.
- Fortalecer los acuerdos de confidencialidad mediante la definición de montos pecuniarios específicos, criterios detallados para la aplicación de sanciones y la tipificación clara de los hechos que constituyen incumplimiento.
- Fortalecer la política mediante la definición de un control formal de calidad sobre el diligenciamiento de los formatos de confidencialidad, asignando un responsable específico para su validación.

En relación con la política de teletrabajo incluida en la política de seguridad de la información:

- Establecer de manera expresa en la política la prohibición de que el teletrabajador reciba apoyo, asistencia o intervención de terceros en el desarrollo de sus funciones.
- Implementar controles periódicos de verificación sobre los equipos utilizados en teletrabajo, orientados a validar que los sistemas operativos, aplicaciones, mecanismos de protección, configuraciones de seguridad y condiciones de conectividad continúen cumpliendo los requisitos definidos por la entidad para la protección de la información institucional.
- Definir e implementar lineamientos y procedimientos formales para la validación de las condiciones de seguridad de los equipos de cómputo de propiedad de los teletrabajadores, estableciendo criterios, alcance, responsabilidades, mecanismos de verificación y evidencias requeridas, garantizando que dichas actividades se realicen bajo principios de necesidad, proporcionalidad y confidencialidad, sin acceder ni afectar información personal del titular. Lo anterior en concordancia con la Ley 1581 de 2012, la Política de Seguridad de la Información y los lineamientos institucionales de protección de datos personales.
- Implementar programas de capacitación diferenciados y de carácter obligatorio dirigidos a los teletrabajadores, enfocados en Tecnologías de la Información y las Comunicaciones (TIC) y seguridad digital o establecer mecanismos de seguimiento y control que garanticen la participación efectiva de los teletrabajadores en las capacitaciones incluidas en el Plan Institucional de Capacitación (PIC), especialmente en temas tecnológicos y de seguridad de la información.
- Definir e implementar mecanismos de seguimiento, trazabilidad y generación de evidencias que permitan garantizar la apropiación de las capacitaciones y el cumplimiento de las obligaciones normativas por parte de los teletrabajadores.

En relación con la gestión de vulnerabilidades, incluida en la política de seguridad de la información:

- Fortalecer la gestión de vulnerabilidades mediante evidencia trazable de pruebas y retest, integrar resultados en el ciclo de mejora continua y establecer indicadores de desempeño que midan la eficacia de las correcciones; de esta forma se garantiza cierre completo del ciclo, eficacia de correcciones y reducción del riesgo residual.
- Definir en los lineamientos un tratamiento diferenciado para infraestructura crítica (pruebas más frecuentes, trazabilidad reforzada, métricas de eficacia) y para infraestructura no crítica (controles básicos y revisiones periódicas).
- Establecer un ciclo formal de cierre y validación, garantizando que toda vulnerabilidad tratada sea verificada y documentada como cerrada, evitando tratamientos parciales.
- Priorización basada en criticidad, asegurando que las vulnerabilidades críticas y altas sean atendidas de manera inmediata y verificadas mediante pruebas de validación (retest).
- Monitoreo continuo y control de cambios, con el fin de prevenir la introducción de nuevas vulnerabilidades en los activos evaluados.

- Definición de indicadores de desempeño (KPIs), tales como tiempo de remediación, porcentaje de cierre por criticidad y reincidencia de vulnerabilidades, que permitan evaluar la efectividad del proceso.

En relación con el instrumento de evaluación MSPI, se recomienda:

- Priorizar el cierre de brechas del MSPI iniciando por aquellos controles que presentan los niveles más bajos de cumplimiento
- Fortalecer controles tecnológicos, dado su mayor nivel de rezago.
- Asegurar trazabilidad y evidencia verificable en la implementación de mejoras.
- Integrar acciones correctivas al plan estratégico institucional, garantizando alineación con estándares internacionales y sostenibilidad en el tiempo.
- Completar la información faltante y estandarizar evidencias y brechas para asegurar trazabilidad y fortalecer la sostenibilidad del sistema.

En relación con las matrices de riesgos, se recomienda:

- Ampliar la cobertura de activos: Incluir sistemas de información, aplicaciones, bases de datos y software crítico en la matriz.
- Fortalecer la descripción de controles: Redactar siguiendo la fórmula "Responsable + Acción + Complemento". Evitar verbos genéricos y asegurar que la acción ataque la causa raíz.
- Revisar y robustecer controles débiles: Priorizar acciones correctivas sobre los controles calificados como débiles.
- Definir metas y acciones en planes de tratamiento: Establecer objetivos claros, fechas de inicio y acciones específicas en caso de materialización del riesgo.
- Mejorar la medición y seguimiento: Incorporar indicadores de eficacia (ej. % incidentes prevenidos, tiempo de respuesta, cumplimiento de ANS).
- Establecer periodicidad uniforme en el seguimiento de controles y planes.
- Consolidar evidencia y oficialidad: Garantizar que todos los controles estén documentados, divulgados y con evidencia verificable.

Cordial saludo,

Cristina Alarcón Tapiero	Elder Herney Villar Castro
Profesional especializado – Contratista	Jefe (e) Oficina de Control Interno
Auditor Líder	