MINISTERIO DE JUSTICIA Y DEL DERECHO

EVALUACIÓN Y VERIFICACIÓN AL PROCESO DE SEGURIDAD DE LA INFORMACIÓN

INFORME FINAL

Oficina de Control Interno

Noviembre de 2022

Tabla de contenido

1. Objetivo de la auditoría:

Evaluar y verificar el estado actual del Modelo de Seguridad y Privacidad de la Información del Ministerio de Justicia y del Derecho.

2. Alcance de la auditoría:

En el marco del objetivo definido, se evaluará el avance a 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 en cuanto a “Gestión de medios removibles”, “Seguridad física y del entorno _ Áreas seguras” y “Controles contra códigos maliciosos”, desde el 1° de octubre de 2021 hasta el 30 de septiembre de 2022.

3. Criterios de auditoría o parámetros normativos:

Para el desarrollo de la presente auditoría se tendrán en cuenta los siguientes criterios: Documento maestro del Modelo de Seguridad y Privacidad de la Información (MSPI); Guía 8 Controles de Seguridad y Privacidad de la Información; Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas" y su anexo 4 denominado "Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas "; G-MC-04 Guía para la Administración de Riesgos del MJD; Ley 1712 de 2014;ISO 27001:2013 e ISO 27002:2013, Ley 1581 de 2012; artículo 77 de la Ley 1474 de 2011.

4. Metodología:

Para el desarrollo de la presente auditoría la Oficina de Control Interno (en adelante OCI), realizó una revisión de los criterios y parámetros normativos, asociados con seguridad y privacidad de la información.

La apertura de la auditoría se realizó reunión el día 1 de noviembre de 2022 con el Subdirector de Tecnología y Gestión de la Información en Justicia, profesional encargada de atender la auditoría y el equipo auditor; en dicha reunión se informó el objetivo, alcance y fechas de las actividades principales para el desarrollo de la auditoría; a su vez, se realizó la socialización de la información que debe ser allegada para la auditoria.

A continuación, se detalla la información que fue solicitada y recibida:

#	Información Solicitada	Recibida	Observaciones
1	Política de seguridad de la información del MJD.	SI	Anexan política 2021 y borrador 2022
2	Roles y Responsabilidades de Seguridad y Privacidad de la Información	SI	

#	Información Solicitada	Recibida	Observaciones
3	Controles de la política de seguridad digital en cuanto a "Gestión de medios removibles", "Seguridad física y del entorno _ Áreas seguras" y "Controles contra códigos maliciosos"	SI	
4	Acuerdos de confidencialidad de funcionarios, contratistas y terceros que manejen información del MJD	SI	
5	Análisis GAP MSPI	SI	Entrega parcial 2021
6	Nivel de madurez de acuerdo con el MSPI	SI	Entrega parcial 2021
7	Indicadores de gestión del Modelo de Seguridad y Privacidad de la Información (MSPI), con sus respectivas evidencias de ejecución, con corte al alcance de esta auditoría	SI	Entrega parcial 2021
8	Instrumento de evaluación MSPI, con corte al alcance de esta auditoría.	SI	Entrega parcial 2021
9	Monitoreo y seguimiento de los riesgos de seguridad digital, con corte al alcance de esta auditoría	SI	Entrega parcial 2021 y 2022
10	Activos de información con vigencia 2021 y 2022, con sus respectivas aprobaciones por parte de los líderes de área.	SI	Entrega parcial de aprobaciones
11	Gestión de incidentes de la seguridad digital	SI	
12	Plan y avance en la ejecución del plan de tratamiento de riesgos.	SI	Entrega parcial 2021

El día 17 de noviembre de 2022, se realiza una reunión virtual con personal de la Dirección de Tecnología y los auditores de la OCI para resolver inquietudes con respecto a la información allegada para la auditoria de seguridad de la información. Adicionalmente, la auditora líder realiza visita en sitio a las instalaciones del centro de datos y cuarto de UPS; lo anterior, con el objetivo de verificar los controles sobre las áreas seguras, el día 18 de noviembre.

5. Desarrollo de la Auditoría:

Política de Seguridad y Privacidad 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 funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad*[1]", como parte del Modelo de Seguridad y Privacidad de la

[1] Maestro del modelo de seguridad y privacidad de la información v 4.0" en el ítem 7.2.2 "Política de seguridad y privacidad de la información" pág. 27, MinTIC, octubre 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

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 se registra en el documento con Código: G-IC-14 versión 2 año 2021 la política de seguridad y privacidad de la información, la cual se encuentra publicada en la página del MJD en el sistema integrado de gestión; al evaluar el documento -por parte de la OCI- se encuentra que:

- La política de seguridad de la información cuenta con objetivos y alcance definidos.

- La política establece la asignación de las responsabilidades específicas para la gestión de la seguridad de la información, a través de roles definidos, en el ítem 4.2. Organización de la seguridad de la información, roles y responsabilidades del sistema de gestión de seguridad de la información.

- La política establece que, en caso de que funcionario y/o contratista cometa una violación a la seguridad de la información, se ejecutará el código disciplinario.

- La Dirección de Tecnología Gestión e Información en Justicia (DTGIJ), viene adelantando una nueva actualización de la política de seguridad de la información versión 3 año 2022, la cual modifica lo siguiente:

    - Se define cada uno de los términos del glosario.
    - Modificación a la sección: “Equipo del Proyecto de Seguridad de la Información”: Se incluye la Subdirección de Información en Justicia.
    - Se modifica el título “Terminación de vinculación, vacaciones, licencias o terminación de contratos”.
    - Se adecúa el ítem “4.3 Política de Seguridad en los Recursos”.
    - Se modifica el numeral “4.5 La Política de Gestión de Acceso”, anexando lineamientos para el almacenamiento y debido tratamiento de la información laboral. Se anexa ítem para realizar Backup, a los equipos dados de baja.

- La política de seguridad y privacidad de la información se revisa anualmente por el Comité de Gestión y Desempeño del MJD y se actualiza según las necesidades por el oficial de seguridad (labor que no se encuentra consignada en las funciones descritas en la política de seguridad de la información).

- Cuando los controles de la política no son efectivos la DTGIJ, realiza un análisis y diagnostico del control en particular, evalúan qué control puede suplirlo y ser mas efectivo en cuanto al escenario en particular. Este procedimiento no está definido en la política.

- El documento no cuenta con marco legal y regulatorio del MJD para los aspectos de seguridad de la información.

- La política no define cuáles son las partes interesadas.

- A criterio de la auditoria, el documento carece de políticas específicas que promuevan la implementación de controles de Seguridad de la Información.

- Se valida el documento contra los controles del anexo A de la ISO/IEC 27001:2013 y no se encuentran controles con respecto a:

    - Política para dispositivos móviles.
    - Teletrabajo.
    - Áreas seguras.
    - Controles físicos de entrada.
    - Seguridad del cableado.
    - Mantenimiento de equipos.
    - Retiro de activos.
    - Seguridad de equipos y activos fuera de las instalaciones.
    - Disposición segura o utilización de medios.
    - Controles contra códigos maliciosos (Detección, prevención, recuperación).
    - Procedimientos de operación documentados.
    - Restricciones sobre la instalación de software.

- La guía 2 “Elaboración de la política general de seguridad y privacidad de la información.” del MSPI del MinTIC, presenta algunas recomendaciones de políticas de seguridad de la información, como: No repudio: La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. La política deberá incluir mínimo los siguientes aspectos (trazabilidad, retención, auditoria, intercambio electrónico de información[2]).

- Teniendo en cuenta lo anterior, se recomienda incluir las políticas sugeridas en la guía 2 y el anexo A de la ISO/IEC 27001:2013.

Para realizar la validación de los controles de la política mencionada anteriormente y de acuerdo con lo contemplado en el anexo A de la ISO/IEC 27001:2013, la OCI realizó la toma de una muestra aleatoria (definidos en el alcance), tanto como una reunión con el área de tecnología y la validación de la evidencia allegada, encontrando lo siguiente:

[2] Guía 2 “Elaboración de la política general de seguridad y privacidad de la información v 1.0” en el ítem 9.4 “No repudio” pág. 20, MinTIC, mayo 2016. https://gobiernodigital.mintic.gov.co/692/articles-5482_G2_Politica_General.pdf

Roles y responsabilidades

El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones en referencia a las responsabilidades que cada personaje tiene[3].

En la resolución 1939 de 2019 expedida por el Ministerio de Justicia y Derecho (MJD) se adopta la versión actualizada del Modelo Integrado de Planeación y Gestión - MIPG, se conforman los Comités Sectorial e Institucional de Gestión y Desempeño, se establecen los líderes temáticos y se dictan otras disposiciones.

La política de seguridad y privacidad de la información del MJD describe los roles y responsabilidades del sistema de gestión de seguridad de la información en su ítem “4.2. Organización de la seguridad de la información, roles y responsabilidades del sistema de gestión de seguridad de la información”, encontrando:

- Comité de seguridad: El Comité Institucional de Gestión y Desempeño del MJD hará las veces de Comité de Seguridad de la Información; dentro de sus funciones están promover la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, entre otras. Para diciembre de este año está programada la reunión de revisión de la actualización de la política. El Comité Institucional de Gestión y Desempeño estará integrado por los siguientes miembros:

    - El Secretario General, quién lo presidirá.
    - El Director Jurídico.
    - El Director de Asuntos Internacionales
    - El Director de Tecnologías y Gestión de Información en Justicia.
    - El Director de Métodos Alternativos de Solución de Conflictos.
    - El Director de Justicia Formal.
    - El Director de Desarrollo del Derecho y Ordenamiento Jurídico.
    - El Director de Justicia Transicional.
    - El Director de Política Criminal y Penitenciaria.
    - El Director de Política de Drogas y Actividades Relacionadas.
    - El Jefe de la Oficina Asesora de Planeación.
    - El Jefe de la Oficina de Prensa y Comunicaciones
    - El Jefe de la Oficina de Control Interno, quien será invitado permanente con voz, pero sin voto.

[3] Guía 4 “Roles y Responsabilidades v 1.0” en el ítem 6 “Definición de roles y responsabilidades” pág. 11, MinTIC, abril 2016. https://gobiernodigital.mintic.gov.co/692/articles-5482_G4_Roles_responsabilidades.pdf

- Oficial de seguridad de la información: Es el encargado de desarrollar, evaluar y realizar control y seguimiento de actividades encaminadas al fortalecimiento de la seguridad de la información, y demás actividades en el marco de la implementación del SGSI basado en el MSPI en el Ministerio de Justicia y del Derecho. Es de agregar que en la actualidad no se cuenta con este rol en la DTGIJ (está en proceso de contratación), por lo cual es necesario que, en ausencias temporales del funcionario o contratista, se prevea qué cargo ha de suplir el liderazgo en torno al tema.

- Líder de seguridad informática: Es el encargado de establecer los controles, medidas técnicas y administrativas necesarias para proteger la infraestructura tecnológica, los sistemas y los activos de información del Ministerio. Evaluar, emitir conceptos y avalar las nuevas soluciones o plataformas tecnológicas a adquirir o implementar en la Entidad, teniendo en cuenta el cumplimiento de los requisitos de seguridad de la información, entre otras. Actualmente se están replanteando las funciones de este rol.

- Oficial de protección de datos personales: Es el encargado de estructurar, diseñar y administrar el programa que permita a la entidad cumplir el marco regulatorio sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente, entre otras. Cabe agregar que en la actualidad no se cuenta con este rol en la DTGIJ, por lo cual es necesario que, en ausencias temporales del funcionario o contratista, se prevea qué cargo ha de suplir el liderazgo en torno al tema. Actualmente las funciones de este rol están repartidas entre dos colaboradores y serán asumidas de forma parcial por el nuevo oficial de seguridad.

- Equipo del proyecto de seguridad de la información: Debe conformarse un equipo para el cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de tener disponible la información relevante del MJD de manera oportuna. Miembros del equipo de seguridad y privacidad de la información, teniendo en cuenta los siguientes perfiles:

    - Director de Tecnologías y Gestión de Información en Justicia
    - Área responsable del proyecto
    - Oficial de Seguridad de la información.
    - Líder de infraestructura
    - Líder de sistemas de información
    - Líder de servicios
    - Líder de calidad
    - Partes interesadas

La siguiente imagen presenta los perfiles de manera genérica, y el nivel al cual pertenecerían según lo propuesto por la Guía 4 de Roles y responsabilidades de MinTIC.

Figura No. 1 – Equipo de Gestión de Seguridad de la Información en las entidades

Fuente: Guía N°4 de Roles y responsabilidades de MinTIC

Dado lo anterior, en el desarrollo de la presente auditoría se evidenciaron los siguientes aspectos:

- La política de seguridad de la información no contempla los roles y responsabilidades de los proveedores.

- La política no define las partes interesadas del equipo del proyecto.

- Actualmente, la Dirección de Tecnología no cuenta con funcionarios para desempeñar los roles del oficial de seguridad de la información (en este momento en proceso de contratación), y del oficial de protección de datos personales por lo cual se incumple con lo consignado en la política en el ítem 4.2. Organización de la seguridad de la información, roles y responsabilidades del sistema de gestión de seguridad de la información.

Gestión de medios removibles

Según el anexo A de la ISO/IEC 27001:2013, los controles para la gestión de medios removibles tienen como objetivo: *"Implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización*[4]".

En la política de seguridad de la información, se encuentra en el ítem "4.4. Gestión de activos, manejo de medios".

[4] Maestro del modelo de seguridad y privacidad de la información v 4.0" en el ítem 11.1 "Controles y objetivos de control" pág. 44, MinTIC, octubre 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

El documento carece de políticas específicas con respecto a la gestión de medios, por lo cual la OCI realiza validación de la evidencia allegada y, de acuerdo con lo señalado en la reunión con el área de tecnología, se encuentra lo siguiente:

- Por medio de políticas la consola del antivirus permite el cifrado y bloqueo de memorias (USB[5]) y discos duros de equipos de cómputo. No está documentada en la política.

- Listado de 50 equipos de cómputo ubicados en áreas estratégicas y críticas del MJD (de acuerdo con la información manejada), los cuales cuentan con el respectivo bloqueo de USB.

- Se realiza un proceso de borrado seguro por mesa de ayuda, cuando los medios removibles van a ser desechados o donados.

- El tercero contratado es el encargado de realizar la protección (transporte y factores ambientales) y embalaje de los medios físicos transportados, para este caso las cintas magnéticas, una vez que salen del MJD son responsabilidad de este. Para la entrega de las cintas se realiza un documento (Formato F-TI-04-01 de entrega en custodia de copias de seguridad), es de agregar que las cintas van etiquetadas.

- En los estudios previos del contrato con el tercero se encuentra establecido cómo se deben entregar las cintas y cómo solicitarlas.

- La OCI recomienda validar la aplicación de la política de cifrado, bloqueo de discos y USB a un mayor número de equipos de cómputo, de acuerdo con la criticidad y manejo de la información e incluir controles específicos en la política al respecto.

Seguridad física y del entorno_ Áreas seguras

Según el anexo A de la ISO/IEC 27001:2013, los controles para el acceso a las áreas seguras tienen como objetivo “Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización[6]”.

[5] Una memoria USB (de Universal Serial Bus), es un dispositivo de almacenamiento que utiliza una memoria flash para guardar información.

[6] Maestro del modelo de seguridad y privacidad de la información v 4.0” en el ítem 11.1 “Controles y objetivos de control” pág. 45, MinTIC, octubre 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

En la actual política, estos controles no se encuentran documentados, por lo cual la OCI realiza la validación de la evidencia allegada y, de acuerdo con lo determinado en la reunión con el área de tecnología, se encuentra lo siguiente:

- Las áreas seguras definidas para el MJD son: centro de datos, cuartos de switch (centros de cableado), cuarto de UPS.

- Se tienen controles definidos únicamente para el datacenter (control biométrico, planilla de control de acceso datacenter (Formato F-TI-02-03 Versión 3).

- Las áreas seguras están monitoreadas por cámaras con control del área de seguridad

- Las UPS[7] cuentan con una consola, donde se puede validar su comportamiento.

- Los responsables de las áreas seguras son 3 funcionarios del DTGIJ, los cuales ejercen funciones dentro de las mismas.

La OCI recomienda a la DTGIJ incluir estos controles en la respectiva política

Controles contra Códigos maliciosos

Según el anexo A de la ISO/IEC 27001:2013, los controles contra códigos maliciosos tienen como objetivo “Implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos[8].” En la política de seguridad de la información, se encuentra en el ítem “4.8. política de seguridad en las operaciones, control contra software malicioso”. El documento carece de políticas específicas con respecto a los controles contra códigos maliciosos, por lo cual la OCI realiza validación de la evidencia allegada y, de acuerdo con lo revisión en la reunión con el área de tecnología, se encuentra lo siguiente:

- Frente a la configuración de la herramienta de anticifrado, si bien es cierto que se indica su existencia y licenciamiento formalizado, no se presentan informes que permitan determinar si la misma es eficiente frente a lo requerido por el MJD.

[7] La sigla UPS es la abreviación de su nombre en inglés Uninterruptable Power Supply, Dicho dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.
[8] Maestro del modelo de seguridad y privacidad de la información v 4.0” en el ítem 11.1 “Controles y objetivos de control” pág. 46, MinTIC, octubre 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- La actual consola de antivirus en el MJD es Kaspersky Security Antivirus, la cual cuenta con licenciamiento vigente.

- Se presenta documento con la configuración de MFA[9] donde se identifica dicha configuración para el acceso a los servicios autenticados con cuentas Microsoft, más no especifica el control que efectúa el MFA frente a la ejecución de código malicioso.

- Se presenta documentación relacionada con el monitoreo y seguimiento de UTM hasta septiembre 30 del año en curso; estos presentan información consistente con el funcionamiento de la UTM[10]; sin embargo, no se presentan las acciones realizadas para mitigar lo observado en el monitoreo ni se encuentran recomendaciones pertinentes.

- Se presenta documentación relacionada con las reglas de acceso al recurso parametrizadas en el firewall para las zonas interior, exterior y DMZ[11], con su correspondiente zonificación en el esquema lógico.

- Se presenta documento con el procedimiento de respaldo y restauración de los Sistemas de información donde se especifican las políticas de operación y el desarrollo de las actividades, deduciendo su importancia en la reducción del impacto en caso de un riesgo materializado. Sin embargo, es importante determinar si este procedimiento logra determinar que las copias de respaldo no guarden información que sea comprometida por código malicioso en su estructura.

- Se presenta información relacionada con los comunicados emitidos por US Cert (Cybersecurity & infrastructure security agency) donde se informa acerca de vulnerabilidades presentadas y llamado a recursos de solución y parchado de la vulnerabilidad. Sin embargo, no hay indicio alguno de la gestión realizada frente a cada comunicado, ya sea en el análisis de la vulnerabilidad o en el parchado y corrección de lo notificado.

Por lo anterior, es importante documentar las acciones que se deben realizar con base en la información entregada por el monitoreo y por el reporte de las entidades aliadas en materia de ciberseguridad, como también realizar el análisis y la documentación de las acciones derivadas para la contención de los posibles riesgos.

[9] La sigla MFA hace referencia a Múltiple Factor de Autenticación el cual agrega una capa de protección al proceso de inicio de sesión. Cuando se accede a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional; por ejemplo, tienen que escanear su huella digital o especificar un código que reciben en su teléfono.
[10] La gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad y, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red.
[11] Una zona desmilitarizada (demilitarized zone, DMZ) es una red perimetral que protege la red de área local (local-area network, LAN) interna contra el tráfico no confiable.

Adicionalmente, la OCI realiza análisis de vulnerabilidades sobre la página web del MJD, encontrando lo siguiente:

- 34 vulnerabilidades de alto riesgo (pueden comprometer sistema).
- 2758 vulnerabilidades de riesgo medio (pueden comprometer data).
- 60 de bajo riesgo.
- 2159 advertencias internas.

Este análisis se realizó como una muestra, con una duración de 10 horas, 28 minutos y 30 segundos, donde no se alcanzó la totalidad de las URL[12] de la página mencionada. Es de agregar que el informe del análisis será entregado al área de tecnología de forma interna, ya que posee información sensible.

De igual manera, se realiza una prueba de SSL[13] encontrando que están habilitados los protocolos TLS[14] 1.0 y 1.1, los cuales son obsoletos y no recomendados dada la debilidad de las suites de cifrado.

Acuerdos de confidencialidad o de no divulgación

Según el anexo A de la ISO/IEC 27001:2013, los controles para los acuerdos de confidencialidad tienen como objetivo: *"identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información"*. En la política de seguridad de la información, se encuentra en el ítem " 4.9. Política de seguridad en las comunicaciones**,** acuerdos de confidencialidad o de no divulgación".

La OCI realiza validación de la política, la evidencia allegada y, de acuerdo con lo establecido en la reunión con el área de tecnología, se encuentra lo siguiente:

- El Acuerdo de Confidencialidad para Funcionarios tiene el código F-IC-G14-01, el cual se valida y se encuentra en el Sistema integrado de Gestión (SIG); el Grupo de Gestión Contractual es el encargado de validar el diligenciamiento. Dentro de las evidencias allegadas, anexan 8 formatos diligenciados, encontrando campos en blanco en cuanto a los ítems 4, 5 y la fecha de la firma del documento.

- El acuerdo de Confidencialidad para Contratistas tiene el código F-IC-G14-02, el cual se encuentra en el SIG. El Grupo de Gestión Contractual es el encargado de

[12] La sigla URL (Uniform Resource Locator – Localizador de Recursos Uniforme) y es la dirección única y específica que se asigna a cada uno de los recursos disponibles.
[13] La sigla SSL (Secure Sockets Layer o Capa de Sockets Seguros) proporciona un canal seguro entre dos computadoras o dispositivos que operan a través de Internet o de una red interna.
[14] La sigla TLS (Transport Layer Security, o Seguridad de la Capa de Transporte), es el protocolo criptográfico que garantiza las comunicaciones en Internet.

validar el diligenciamiento. Dentro de las evidencias allegadas, anexan 9 formatos diligenciados, encontrando campos en blanco en cuanto a los ítems 4, 5 y 8.

- El acuerdo de Confidencialidad para Proveedores tiene el código F-IC-G14-03, el cual se encuentra en el SIG. El supervisor del contrato debe solicitar el diligenciamiento del formato. Dentro de las evidencias allegadas, anexan 3 formatos diligenciados, encontrando 1 formato sin el código, versión y vigencia del documento.

- El acuerdo de Confidencialidad para Convenios tiene el código F-IC-G14-04, el cual se encuentra en el SIG. El director, subdirector, jefe o funcionario a cargo de la supervisión del convenio deben gestionar las firmas de este. La DTGIJ no allega evidencia a este respecto.

- Es responsable de la revisión y seguimiento de los acuerdos el oficial de seguridad. Lo anterior no se puede validar ya que actualmente la Dirección de Tecnología no cuenta con el profesional en mención.

- Dentro de los controles de la política no se hace referencia al diligenciamiento y/o a la calidad de la información diligenciada en los formatos de confidencialidad.

- No se anexan soportes de capacitación a los involucrados en la firma de los acuerdos de confidencialidad mencionados.

- Por lo anterior, se hace necesario realizar un seguimiento más estricto al diligenciamiento completo y adecuado de los acuerdos de confidencialidad mencionados, para evitar campos en blanco en los mismos. Adicionalmente, se recomienda capacitar a los actores involucrados en el correcto diligenciamiento del formato.

Gestión de incidentes de la seguridad digital

Según la ISO/IEC 27000:2018, la Gestión de Incidentes de Seguridad tiene como objetivo: *"detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información*[15]". Para el caso del MJD cuenta con el procedimiento de Gestión de Incidentes de Seguridad, con Código: P-IC-04, versión 1 del año 2020.

Para los meses de septiembre a diciembre del año 2021 se reportaron tres (3) incidentes de Seguridad de la Información (2 por incidentes con el correo institucional, 1 por incidente con la información en carpetas compartidas); los tres casos no fueron cerrados

[15] Maestro del modelo de seguridad y privacidad de la información v 4.0" en el ítem 3. "Definiciones" pág. 13, MinTIC, octubre 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

oportunamente, teniendo en cuenta los ANS[16]. El nivel de efectividad en la respuesta a los casos de seguridad de la información a través de Aranda, con un porcentaje de cumplimiento de solución de ANS del 0%; por lo tanto, no cumplieron con el indicador de cumplimiento de solución.

RESUMEN POR ANS CUMPLIMIENTO SOLUCIÓN

MES	CUMPLE	NO CUMPLE	TOTAL GENERAL	PORCENTAJE DE CUMPLIMIENTO
SEPTIEMBRE	0	2	2	0%
OCTUBRE	0	1	1	0%
NOVIEMBRE	0	0	0	-
DICIEMBRE	0	0	0	-
Total general	**0**	**3**	**3**	**0%**

RESUMEN POR TIPO SERVICIO

MES	INCIDENTE	REQUERIMIENTO	TOTAL GENERAL
SEPTIEMBRE	2	0	2
OCTUBRE	1	0	1
NOVIEMBRE	0	0	0
DICIEMBRE	0	0	0
Total general	**3**	**0**	**3**

Para los meses de enero a octubre del año 2022 se reportaron treinta y cuatro (34) incidentes o requerimientos de Seguridad de la Información, 30 de los cuales son incidentes (29 por incidentes con el correo, 1 por incidente con la información en carpetas compartidas), y 4 son requerimientos (por requerimientos con el correo institucional). De 34 casos, 2 no fueron cerrados oportunamente.

Se tienen 14 casos generados en el mes de octubre, en estado suspendido, los cuales aún no se han cerrado porque corresponden a una campaña de seguridad con un correo enviado de forma intencional y se está realizando el análisis respectivo del comportamiento de los usuarios. El nivel de efectividad en la respuesta a los casos de seguridad de la información a través de Aranda, con un porcentaje de cumplimiento de solución de ANS del 94%, por lo tanto, no cumplieron con el indicador de cumplimiento de solución.

[16] La sigla ANS hace referencia a Acuerdos de Niveles de Servicio

RESUMEN POR ANS CUMPLIMIENTO SOLUCIÓN

MES	CUMPLE	NO CUMPLE	Total general	PORCENTAJE DE CUMPLIMIENTO
ENERO	1	0	1	100%
FEBRERO	0	0	0	
MARZO	2	0	2	100%
ABRIL	0	1	1	0%
MAYO	5	0	5	100%
JUNIO	0	0	0	
JULIO	5	0	5	100%
AGOSTO	2	0	2	100%
SEPTIEMBRE	3	1	4	75%
OCTUBRE	14	0	14	100%
Total general	**32**	**2**	**34**	**94%**

RESUMEN POR TIPO SERVICIO

MES	INCIDENTE	REQUERIMIENTO	TOTAL GENERAL
ENERO	1	0	1
FEBRERO	0	0	0
MARZO	2	0	2
ABRIL	1	0	1
MAYO	3	2	5
JUNIO	0	0	0
JULIO	4	1	5
AGOSTO	1	1	2
SEPTIEMBRE	4	0	4
OCTUBRE	14	0	14
Total general	**30**	**4**	**34**

Instrumento de evaluación MSPI

La herramienta de diagnóstico permite obtener un resultado preciso, el cual le permite a cada entidad generar un plan de seguridad de la información para ser desarrollado en su interior y, de esta manera, dar cumplimiento con lo estipulado en el manual de gobierno en línea en su cuarto componente[17].

El instrumento se encuentra incompleto, no se encuentran diligenciadas todas las pestañas del archivo, y el archivo fue modificado.

Se puede evidenciar que se desconoce cómo se debe diligenciar el instrumento, por los siguientes motivos:

[17] Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información v 1.0" en el ítem "3. Introducción" pág. 6, MinTIC, junio 2017. https://gobiernodigital.mintic.gov.co/692/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf

Alteración del instrumento. El instrumento fue modificado; cuenta con una pestaña adicional denominada “Evolución MSPI 2021 enero”; se recomienda utilizar el formato original suministrado por el Ministerio TIC, ya que este formato se encuentra clasificado como público con reserva para uso exclusivo de las entidades del Estado, y, por lo tanto, no debe ser modificado, así como tampoco las fórmulas del instrumento.

Avance del ciclo de funcionamiento del modelo de operación (PHVA). En el marco de la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), el diligenciamiento de la herramienta diagnóstico del MSPI permite a las entidades servir de guía u orientación para identificar las mejoras de los estándares de seguridad de la información con 5 fases o niveles de madurez (inicial, repetible, definido, administrado y optimizado).

Este instrumento basado en el Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es decir, que el ciclo de funcionamiento del PHVA para llegar a las conclusiones, debe verse desde el momento que se expide el Decreto 1078 de 2015, el cual se asocia a la implementación del modelo de seguridad y privacidad de la información para todas las entidades del Estado, según lo establecido en su artículo 2.2.17.4.3 Obligaciones comunes de los prestadores de servicios ciudadanos digitales en su numeral 7 *“Implementar sistemas de gestión de seguridad y controles que permitan disminuir y gestionar el riesgo asociado a la integridad, confidencialidad y disponibilidad de la información para lo cual adoptarán el cumplimiento de estándares de amplio reconocimiento nacionales o internacionales de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la información de la política de Gobierno Digital”*

Para obtener un resultado preciso de la evolución de la madurez es preciso contar con la medición en el instrumento, desde su comienzo desde el año 2015 hasta la última medición, de manera que se pueda evidenciar la medida del progreso o avance en cada uno de los componentes del ciclo PHVA (planificación, implementación, evaluación de desempeño y mejora continua). Cuando nos referimos al año 2015, significa a partir de la implementación del Decreto 1078 de 2015 y no solo contar desde la vigencia anterior. Lo anteriormente mencionado, no es posible evaluarlo, ya que actualmente el instrumento no cuenta con dicha información. Tener en cuenta para futuras mediciones el *Instructivo No 1 - Instrumento para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información, versión 1 del Ministerio TIC*, para llevar a cabo la autoevaluación de la madurez del MSPI.

Una implementación de este marco debe ser evaluado, al menos, una vez al año, y en la información entregada dentro de esta auditoría solo se puede evidenciar la evaluación con corte 2021 elaborada el 1° de febrero de 2021. A pesar de tener un informe entregable del modelo y marco metodológico del MSPI del Ministerio, con

fecha de elaboración al 31 de agosto de 2022, la Subdirección de Tecnologías y Sistemas de Información no cuenta con el instrumento base de medición.

Siendo de esta manera, la información de la entidad, independiente de quien la diligencie o si hay rotación de personal, estos documentos son del Ministerio y deben ser controlados y asegurados para facilitar la evaluación de la gestión institucional en materia de la implementación del MSPI.

En términos de seguridad de la información y según el *Instructivo No 1 - Instrumento para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información*, en el año 2020 las entidades deberían tener implementado el MSPI al 100%. Aunque es preciso mencionar que siempre va a existir una brecha en la implementación, este resultado debería estar cercano al 100%.

En la medición con fecha de evaluación 1° de febrero de 2021, no diligencian la pestaña levantamiento de información y Áreas involucradas, lo cual soporta la evaluación llevada a cabo en la siguiente hoja denominada *Administrativa* y *Técnicas;* dicha información debería evidenciar el cumplimiento de la información recolectada para evaluar la madurez del MSPI. Es así que, también al analizar la respuesta de autoevaluación de la hoja *PHVA,* la evidencia no es precisa y tampoco objetiva y no corresponde al nivel de cumplimiento de la escala de evaluación, según cada criterio.

Información parcialmente suministrada. Dentro de la auditoría y como parte de la información solicitada se requirió de acuerdo con el alcance de la misma, el instrumento del MSPI, corte vigencia 2021 y 2022, para lo cual solo fue entregado el instrumento MSPI medianamente diligenciado vigencia 2021, con fecha de evaluación al 1° de febrero de 2021 y los Informes del modelo y marco metodológico del MSPI del Ministerio entregable 1, sin soporte que evidencie su análisis versión 2021 con fecha de elaboración 1/12/2021, e informe entregable 1 versión 2022 con fecha de elaboración del 31/08/22; este último sin instrumento MSPI diligenciado que permita analizar el resultado del informe.

En conclusión, la entidad no cuenta con información confiable acerca de la madurez de la implementación del MSPI, existiendo dificultad en el diligenciamiento del instrumento para evaluar dicha madurez y, por último, no mantienen la información histórica de la medición. A continuación, se presenta un análisis de algunos elementos de su contenido:

Análisis GAP de acuerdo con el MSPI

El objetivo del análisis GAP es identificar el estado actual de la entidad respecto a la adopción del MSPI[18].

Dentro de la información allegada para la presente auditoría el área de tecnología no hace entrega del instrumento de evaluación MSPI para el año 2022; por lo cual, no fue posible validar su diligenciamiento y no se puede precisar su cumplimiento; cabe resaltar que actualmente la DTGIJ no cuenta con el oficial de seguridad.

Para este caso, el análisis GAP se encuentra en el análisis de brechas frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la Información, al validar la información de los dominios de seguridad del año 2021 entregados en el "Modelo y marco metodológico del MSPI del Ministerio" no es consistente con la información ingresada en el instrumento de evaluación MSPI, por lo cual no se analiza.

Por lo anterior, se insta a la DTGIJ a diligenciar el formato de instrumento de evaluación MSPI para el año 2022, validar la información ingresada en el análisis de brechas para el año 2021 y completar la información en el documento Modelo y marco metodológico del MSPI del Ministerio para el año 2022.

Nivel de madurez de acuerdo con el MSPI

"La evaluación del nivel de madurez pretende determinar cómo se encuentra la entidad frente a las mejores prácticas en ciberseguridad definidas por el NIST[19], con miras a ir realizando un diagnóstico frente a los lineamientos de la política de ciberseguridad y ciberdefensa definidos en el documento Conpes 3701 y el Conpes 3854[20]".

El instrumento de evaluación del MSPI no fue entregado por Tecnología para el 2022, por lo cual solo se analiza el año 2021.
El nivel de madurez en el que se encuentra el MJD con respecto al Modelo de Seguridad y Privacidad de la Información para el año 2021, es:

[18] Maestro del modelo de seguridad y privacidad de la información v 4.0" en el ítem 6 "Diagnostico" pág. 21, MinTIC, octubre 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf
[19] El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology)
[20] Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información v 1.0" en el ítem 5.8. "HOJA 8 CIBERSEGURIDAD" pág. 25, MinTIC, junio 2017. articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf (mintic.gov.co)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	69	100
DETECTAR	70	100
RESPONDER	71	100
RECUPERAR	53	100
PROTEGER	71	100

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% A 35 %
INTERMEDIO	36% A 70%
SUFICIENTE	71% A 100%

- Identificar: En esta sección se analizan seis categorías: gestión de activos, entorno empresarial, dirección (gobernanza), evaluación de riesgos, estrategia de gestión de riesgos y gestión de riesgos, que desarrolla una comprensión organizativa para gestionar el riesgo de la seguridad cibernética de los sistemas, las personas, los activos, los datos y las capacidades. Para el año 2021, este núcleo para el MJD se encontraba en un nivel intermedio con el 69%.

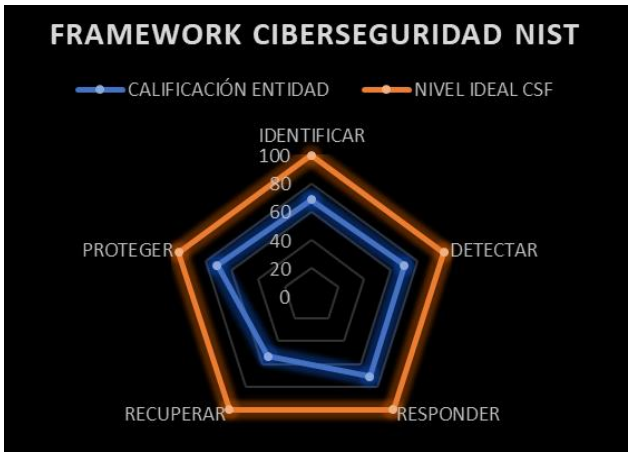
- Detectar: En esta sección se analizan tres categorías: Anomalías y eventos, control continuo de seguridad y procesos de detección. Para el año 2021, este núcleo para el MJD se encontraba en un nivel intermedio con el 70%.

- Responder: En esta sección se analizan cinco categorías: Planificación de respuestas, comunicaciones, análisis, mitigación y mejoras. Para el año 2021, este núcleo para el MJD se encontraba en un nivel suficiente con el 71%.

- Recuperar: En esta sección se analizan tres categorías: Planificación de la recuperación, mejoras y comunicaciones. Para el año 2021, este núcleo para el MJD se encontraba en un nivel intermedio con el 53%.

- Proteger: En esta sección se analizan seis categorías: Control de acceso, concientización y formación, seguridad de los datos, procesos y procedimientos de protección de la información, mantenimiento y tecnología de protección[21]. Para el año 2021, este núcleo para el MJD se encontraba en un nivel suficiente con el 71%.

[21] Marco de seguridad cibernética NIST en los ítems “Función del núcleo del CSF: Identificar, pág. 6”, “Función del núcleo del CSF: Proteger, pág. 10”,” Función del núcleo del CSF: Detectar, pág. 12”, “Función del núcleo del CSF: Responder, pág. 14”, “Función del núcleo del CSF: Recuperar, pág. 15” AWS, enero 2019. https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf



La grafica muestra la brecha entre la calificación alcanzada por el MJD para el año 2021 y la calificación objetivo.

Análisis de Riesgo:

Riesgos de seguridad de la información:

Se revisa la matriz de riesgos de seguridad de la información vigencia 2021 y 2022, encontrando las siguientes deficiencias:

La matriz de riesgos de seguridad de la información para la vigencia 2021 y 2022, cuenta con 15 riesgos identificados para el año 2021 y 7 riesgos identificados en el año 2022, de los cuales se encuentra la matriz parcialmente diligenciada, en cuanto la definición y evaluación de los controles, así como el plan de tratamiento del riesgo.

No se evidencia el monitoreo y seguimiento de los riesgos de seguridad de la información para la vigencia 2021 y 2022, por parte de la primera línea de defensa (líderes de proceso) y la segunda línea de defensa (Dirección de Tecnologías y Gestión de Información en Justicia).

Se evidencia que no se evalúan los controles y, por tanto, no es posible verificar la efectividad de estos; se desconoce si dichos controles funcionan o no, y se podría estar desconociendo la posible materialización de un riesgo de seguridad digital y, por tanto, no se puede identificar la disminución del riesgo inherente (riesgo residual).

El proceso no cuenta con las evidencias suficientes que determinen la aprobación de los riesgos de seguridad digital y las modificaciones justificadas llevadas a cabo en la vigencia 2021 y 2022.

De acuerdo con la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del DAFP,* la articulación entre los riesgos de gestión, corrupción y seguridad digital, de acuerdo con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la Secretaría de Transparencia y la de Gobierno Digital, la integración con respecto a la gestión del riesgo no debe ser limitante para evaluar de manera integral tanto los riesgos como los controles, de manera, que se puedan coordinar o definir controles lo bastante robustos para proteger y evitar la materialización de los riesgos a nivel institucional.

Actualmente el SIG, por las segundas líneas de defensa, refiriéndonos a la Oficina Asesora de Planeación y la Dirección de Tecnologías y Gestión de Información en Justicia, no se articulan frente a este tema en particular, viéndose como islas independientes al igual que los riesgos asociados a la gestión institucional. Se recomienda analizar profundamente las causas, los riesgos y controles en los tres tipos de riesgos para generar un propósito común, que permita generar las alertas necesarias y oportunas que eviten la continuidad del negocio y el cumplimiento de los objetivos institucionales del MJD.

Activos de información

El proceso entregó el registro de activos de información 2021 aprobado y publicado mediante Resolución 1853 del 17 de noviembre de 2021 y el proyecto de actualización del registro de activos de información 2022, el cual aún se encuentra en proceso de validación y aprobación.

Se verifican los criterios asociados al cumplimiento del registro de acuerdo con la Ley 1712 de 2014, encontrando que no se articula a las tablas de retención documental (TRD) e inventarios documentales dispuesto por la mencionada Ley.

Es importante que parte de la actualización de los registros de activos de información se han identificado de manera objetiva por parte de cada área de la entidad con la asesoría brindada por la Dirección de Tecnologías y Gestión de Información en Justicia, la Oficina Asesora Jurídica y el Grupo de Gestión Documental.

6. Conclusiones, hallazgos y/ recomendaciones

Se presentan las siguientes conclusiones, hallazgos y recomendaciones para la mejora del proceso de seguridad de la información en el Ministerio de Justicia y del Derecho.

Conclusiones

La política de seguridad de la información requiere una revisión a profundidad con el fin de establecer qué controles se deben ingresar, cuáles se deben actualizar, y cuáles se deben eliminar, para que estén acorde a las actividades realizadas por la Dirección Tecnología, y así garantizar la seguridad de la información en el MJD.

Como resultado del análisis del instrumento del MSPI, por el estado del diligenciamiento, la entidad no puede identificar su brecha en la implementación del modelo de seguridad y privacidad de la información.

Lo mismo ocurre con los riesgos de seguridad digital, con la incompletitud del análisis, valoración y evaluación de los riesgos no es posible determinar la efectividad de los controles. Existe ausencia en el monitoreo de los pocos controles y plan de tratamiento definidos por los líderes de proceso, así como el seguimiento realizado por la segunda línea de defensa (Dirección de Tecnologías y Gestión de Información en Justicia).

Aún falta madurez en la identificación de activos de información y por tanto la identificación de los riesgos de seguridad digital. El proceso tiene un reto importante para mejorar frente a los instrumentos de medición y desempeño del proceso que impacta significativamente la gestión institucional.

Socialización de informe preliminar contentivo de hallazgos a cargo de la Dirección de Tecnología y la Subdirección de Tecnologías y Sistemas de Información

El día 29 de noviembre bajo memorando número MJD-MEM22-0009600-OCI-10300 la OCI envía informe preliminar a la Dirección de Tecnología, indicando que dicha dependencia debe remitir sus comentarios o promover una reunión de socialización, dentro de los tres (3) días siguientes a la recepción del informe en mención, conforme lo dispone el procedimiento de Auditoría Interna.

La DTGIJ, genera comunicación radicada bajo el número MJD-MEM22-0009722-DTI-10500 del 2 de diciembre de 2022, a través de la cual envían respuesta frente a los hallazgos evidenciados en el informe.

Con sujeción a lo anterior, y en aras de ser lo más pedagógico posible para el entendimiento del lector, procederemos a analizar cada uno de los hallazgos, en función de cada una de las respuestas efectuadas, teniendo en cuenta lo consignado en el siguiente cuadro de datos:

HALLAZGO	RESPUESTA DTGI	RESPUESTA OCI
1. Al no contar con un oficial de seguridad, se evidencia un presunto incumplimiento en lo relacionado con la política de seguridad y privacidad de la información en el ítem 4.2. "Organización de la seguridad de la información, roles y responsabilidades del sistema de gestión de seguridad de la información", donde se indica que el MJD debe contar con dicho oficial.	La Dirección de Tecnologías y la Subdirección de Tecnologías y Sistemas de Información han realizado la gestión requerida para contratar una profesional a cargo de las actividades específicas requeridas para lo que resta de la vigencia 2022, en cumplimiento del rol de Oficial de Seguridad de la Información. Se perfeccionó el día 30 de noviembre, el contrato No. 793-2022 con la ingeniera Adriana Esperanza Aranguren Prieto, el cual tiene la siguiente descripción del objeto: "Prestación de servicios profesionales para la actualización, consolidación y seguimiento del modelo de seguridad y privacidad de la información en el MJD". Así mismo, se están realizando las gestiones pertinentes para la contratación correspondiente a la vigencia 2023, con las mismas características. Con base en lo anterior, solicitamos retirar el hallazgo, dejando el registro de que se ha subsanado y se está asegurando mantener el cumplimiento para la siguiente vigencia.	Si bien es cierto que la Dirección de Tecnologías y la Subdirección de Tecnologías y Sistemas de Información han realizado la gestión requerida para contratar un oficial de seguridad, en la fecha de realización de la auditoria, la DTGIJ no contaba con el oficial de seguridad; es de agregar que la entidad estuvo dos meses (octubre y noviembre) sin este rol; por tanto, no hubo continuidad en las labores realizadas, lo cual se ve reflejado en la entrega de la documentación solicitada en esta auditoría, como por ejemplo el instrumento de evaluación del MSPI para el año 2022; Adicional a lo anterior, el oficial de seguridad está contratado solo por el mes de Diciembre de 2022. En conclusión: Se confirma el hallazgo.
2. Al no contar con un Oficial de Protección de Datos Personales o la definición de quién asumiría sus funciones, se evidencia un presunto incumplimiento del artículo 23 del Decreto 1377 de 2013 y, en lo relacionado en la política de seguridad y privacidad de la información, en el ítem 4.2. Organización de la seguridad de la información, roles y responsabilidades del sistema de gestión de seguridad de la información.	Efectivamente, se presenta en el Ministerio un incumplimiento en la delegación de un Oficial o área de protección de datos personales. Sin embargo, es un hallazgo que no debe quedar a cargo de la Dirección o Subdirección de Tecnologías y Sistemas de Información; dado que corresponde a la Alta Dirección, a través de la instancia decisoria de gobierno corporativo en la materia, es decir el Comité Institucional de Gestión y Desempeño. En tal sentido, se solicita trasferir la responsabilidad del plan de mejoramiento e informar del hallazgo a dicho Comité. Finalmente, es importante anotar que, a pesar de que no se ha realizado la delegación, la Dirección de Tecnología reservó un presupuesto para la contratación de un profesional que pueda ejercer el rol de Oficial de	La respuesta ofrecida reconoce la falta del oficial de Protección de Datos Personales y, con relación al responsable del hallazgo, se tiene en cuenta, lo siguiente: • La definición del rol es dada desde la política de seguridad de la información. • La política está a cargo de la DTGIJ. • El área auditada es la dirección de tecnología. • La dirección lidera el proceso de seguridad de la información. • El rubro para la contratación del rol mencionado está a cargo de la dirección. Como consecuencia de lo anterior, el hallazgo se mantiene. En conclusión: Se confirma el

HALLAZGO	RESPUESTA DTGI	RESPUESTA OCI
	protección de datos personales, a partir de la vigencia 2023. Acogiendo la recomendación de la Oficina de Control Interno, sugerimos que la supervisión de su contrato esté a cargo del área que sea delegada oficialmente por la Alta Dirección para tal efecto, evitando conflictos con el rol de Oficial de Seguridad de la Información, con quien dicho profesional deberá coordinar esfuerzos, para dar cumplimiento a la normatividad en materia de seguridad y de protección de datos personales.	hallazgo.
3. Se evidencia incumplimiento en el diligenciamiento del instrumento de evaluación MSPI para el año 2022, el cual no fue realizado en su momento por el oficial de seguridad o quien en su momento haya llevado a cabo sus funciones u obligaciones; adicionalmente, en lo encontrado en el instrumento diligenciado para el año 2021, la entidad no cuenta con información confiable acerca de la madurez de la implementación del MSPI, pues existe dificultad en el diligenciamiento del instrumento para evaluar dicha madurez y, por último, no mantienen la información histórica de la medición; por lo anterior se presume un incumplimiento al Decreto 1078 de 2015 Artículo 2.2.9.1.1.3. y Artículo 2.2.9.1.2.2, así como también el Documento Maestro modelo de seguridad y privacidad de la información v 4.0 en el ítem 6. Diagnostico.	La profesional que asumió el rol de Oficial de Seguridad de la Información tendrá la responsabilidad de retomar el correcto diligenciamiento del instrumento de evaluación MSPI a partir de la vigencia 2023, con el fin de dar cumplimiento a la normatividad y conservar la información que permita verificar el avance en la implementación del modelo.	La respuesta reconoce la falta del diligenciamiento del instrumento de evaluación MSPI y la responsabilidad del nuevo oficial de seguridad de realizar dicha labor. En conclusión: Se confirma el hallazgo.
4. Al encontrarse campos en blanco en los formatos del acuerdo de confidencialidad para funcionarios y contratistas, se evidencia incumplimiento en su correcto diligenciamiento, se presume un incumplimiento a la política de seguridad y privacidad de la información en los ítems 4.4 Gestión de activos y 4.9. Política de seguridad en las comunicaciones, acuerdos de	Dado que la Subdirección de tecnologías y Sistemas de Información ha detectado que los formatos de acuerdos de confidencialidad poseen debilidades en la definición de algunos campos y deben ser revisados, se está trabajando en la actualización de los mismos, la cual será divulgada a los colaboradores, una vez se aprueben las nuevas versiones. Como parte del mejoramiento continuo, se actualizará la política de seguridad de la información a	La respuesta otorgada reconoce debilidades en la definición de algunos campos de los acuerdos de confidencialidad y su posterior actualización y divulgación. En conclusión: Se confirma el hallazgo.

HALLAZGO	RESPUESTA DTGI	RESPUESTA OCI
confidencialidad o de no divulgación	profundidad, a lo largo de la vigencia 2023.	
5. Al verificar los registros de activos de información vigencia 2021 y 2022, estos no aseguran el cumplimiento o su articulación con las tablas de retención documental (TRD) y los inventarios documentales dispuestos en el artículo 13 numeral d) de la Ley de Transparencia, incumpliendo lo definido en la Ley 1712 de 2014 artículo 13 numeral c.	Es importante aclarar que, la responsabilidad en la identificación y actualización de los activos de información es del líder de cada proceso de la entidad y la misma incluye la armonización con las tablas de retención documental. Desde la primera identificación de activos de información del Ministerio de Justicia y del Derecho, se ha realizado una articulación y armonización con la gestión documental y las TRD, lo cual se lleva a cabo a través de una reunión de revisión en la cual participan: el Oficial de Seguridad de la Información, Profesional Especializado de la SGIJ, Dirección Jurídica y Gestión Documental; la cual se llevó a cabo el año anterior y se realizará próximamente para la actualización correspondiente a la vigencia 2022. Se tendrá en cuenta la recomendación, en cuanto a la mejora o complemento en el formato de activos, aunque se aclara que la responsabilidad de liderar esta actividad es compartida con la Subdirección de Gestión de Información en Justicia y la ejecución de la misma es transversal a la entidad, en cabeza de los líderes de cada proceso. Se solicita retirar este hallazgo, dado que no constituye incumplimiento y en cualquier caso, no está a cargo de la Dirección y/o Subdirección de Tecnologías y Sistemas de Información.	De acuerdo con lo mencionado por el auditado, nos permitimos confirmar el hallazgo mencionado, teniendo en cuenta que tal como lo establece la Ley 1712 de 2014 se debe asegurar la relación entre los activos de información y las tablas de retención documental. Dentro del ejercicio de auditoría se revisaron los activos y se evidencia que: • El formato no contiene dicha relación; • Los activos identificados vigencia 2021 y el preliminar de 2022 no cuenta con dicha articulación, es más se relaciona más con los productos de la caracterización de cada proceso. Teniendo en cuenta lo anteriormente descrito se mantiene el hallazgo, y se recomienda tal como lo menciona la Subdirección se tenga en cuenta dicho cambio dentro de la actualización de los activos de información y se defina el liderazgo o coordinación del levantamiento de estos. En conclusión: Se confirma el hallazgo.

Recomendaciones

- Incluir en la política de seguridad del MJD el marco legal y regulatorio, los controles faltantes de acuerdo con el anexo A de la ISO/IEC 27001:2013 y la guía 2 Elaboración de la política general de seguridad y privacidad de la información.

- Incluir controles específicos que apoyen los controles existentes en la política.

- Definir en la política de seguridad las partes interesadas del equipo del proyecto, los roles y responsabilidades de los proveedores.

- Incluir dentro de las labores del oficial de seguridad la revisión y actualización de las políticas de seguridad de la información.

- Definir la responsabilidad demostrada del oficial de protección de datos personales y del Oficial de Seguridad de la información en funcionarios o áreas distintas; si bien es cierto que sus funciones pueden ser complementarias, la respuesta de su rol frente a solicitudes se entrega a instancias distintas.

- Validar la aplicación de la política de cifrado, bloqueo de discos y USB a un mayor número de equipos de cómputo, de acuerdo con la criticidad y manejo de la información.

- Determinar si el procedimiento de respaldo y restauración logra comprobar que las copias de respaldo no guardan información que sea comprometida por código malicioso en su estructura.

- Documentar las acciones que se deben realizar, con base a la información entregada por el monitoreo y por el reporte de las entidades aliadas en materia de ciberseguridad, como también realizar el análisis de las acciones derivadas para la contención de los posibles riesgos.

- Se recomienda realizar un diagnóstico al análisis de vulnerabilidades emitido por la OCI, con el fin de determinar la remediación a realizar sobre el mismo.

- Se recomienda actualizar los protocolos TLS 1.0 y 1.1 de la página web del MJD.

- Capacitar a los actores involucrados en el correcto diligenciamiento de los formatos de los acuerdos de confidencialidad.

- Se recomienda al área de tecnología habilitar un repositorio donde el oficial de seguridad aloje la respectiva documentación generada dentro de sus funciones, con el fin que, cuando esta sea requerida, sea encontrada de manera fácil y oportuna.

- El registro de activos de información 2022 se encuentra incompleto, tal como se puede evidenciar en la fila 61, 70 no tiene nombre el activo de información, pese que se encuentra diligenciado en todas las demás casillas del formato. Se recomienda complementar el registro y desarrollar un ejercicio a profundidad que permita identificar mayores insumos para la identificación de los riesgos de seguridad digital.

Con un muy cordial saludo,

_____	_____
Cristina Alarcón Tapiero Profesional OCI Auditor Líder	Luisa Fernanda Santiago Delvasto Profesional OCI Auditor de Apoyo

_____
Diego Orlando Bustos Forero
Jefe Oficina de Control Interno