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

INFORME FINAL

Oficina de Control Interno
5 de Julio de 2024

Tabla de contenido

1. Objetivo de la auditoría:

Evaluar y verificar los avances y mejoras obtenidas en el marco del proceso de seguridad de la información.

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 en la vigencia 2023 y los controles de la política de Seguridad y Privacidad de la Información versión 3 en cuanto a:

- Gestión de acceso
- Seguridad física y del entorno
- Seguridad en las operaciones/ control contra software malicioso
- Gestión de la prestación de servicios de proveedores

3. Criterios de auditoría o parámetros normativos:

Para el desarrollo de la presente auditoría se tendrán en cuenta los siguientes criterios: Ley 1581 de 2012; Ley 1712 de 2014; ISO 27000:2017 e ISO 27001:2022; Documento maestro del Modelo de Seguridad y Privacidad de la Información (MSPI); Guía 8 Controles de Seguridad y Privacidad de la Información de MINTIC; 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"; Guía 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información de MINTIC; G-MC-04 Guía para la Administración de Riesgos del Ministerio de Justicia y del Derecho (en adelante MJD); P-IC-04 Procedimiento Gestión de Incidentes de seguridad de la información del MJD; G-IC-14 Política de seguridad de la información versión 03 del 19 de diciembre de 2022 del MJD; Informe de auditoría “Evaluación y verificación al proceso asociado de seguridad de la información” generado en noviembre de 2022.

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 dieciséis (16) preguntas basadas en el Informe de auditoría “Evaluación y verificación al proceso asociado de seguridad de la información de noviembre de 2022 enviadas con el plan específico y posteriormente con un cuestionario con doce (12) preguntas basadas en la evidencia allegada; 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 presencial el día 27 de Mayo de 2024, con el Director Técnico de Tecnologías y Gestión de Información en Justicia (en adelante DTGIJ), el Subdirector de Tecnologías y Sistemas de Información (en adelante STSI), los profesionales encargados de atender la auditoría, el jefe de la Oficina de Control Interno y las auditoras de la OCI; 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.

5. Desarrollo de la Auditoría

5.1. Antecedentes

En la vigencia 2022, la Oficina de Control Interno (OCI) realizó el informe de la auditoria denominada Evaluación y Verificación al Proceso de Seguridad de la Información, el cual es tomado como insumo para esta auditoría, cuyo objetivo señalaba "*Evaluar y verificar el estado actual del Modelo de Seguridad y Privacidad de la Información del Ministerio de Justicia y del Derecho*[1]".

Dentro del respectivo informe se realizaron las siguientes 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*[2]*".*

Y se realizaron las siguientes recomendaciones:

[1] Auditoría Evaluación y Verificación al Proceso de seguridad de la información; ítem 1. Objetivo de la auditoria; pág. 3; OCI MINJUSTICIA, noviembre de 2022; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2022/Informe%20Final%20seguridad%20de%20la%20inf%202022%20(1).pdf

[2] Auditoría Evaluación y Verificación al Proceso de seguridad de la información; ítem 6. Conclusiones, hallazgos y/ recomendaciones; pág. 23; OCI MINJUSTICIA, noviembre de 2022; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2022/Informe%20Final%20seguridad%20de%20la%20inf%202022%20(1).pdf

- "*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* [3]."

[3] Auditoría Evaluación y Verificación al Proceso de seguridad de la información; ítem 6. Conclusiones, hallazgos y/ recomendaciones; pág. 26 y 27; OCI MINJUSTICIA, noviembre de 2022; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2022/Informe%20Final%20seguridad%20de%20la%20inf%202022%20(1).pdf

Por último, en la auditoria en mención, se detectaron 5 hallazgos de los cuales y a la fecha de la actual auditoria, 4 fueron cerrados quedando uno pendiente por gestionar "*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*[4]".

5.2. Política de seguridad de la información

En la reunión de apertura de la auditoria, el subdirector de tecnología solicita que se audite la versión 3 de la Política de seguridad y privacidad de la información con Código: G-IC-14 del 19 de diciembre de 2022; puesto que el documento vigente (versión 4) del 26 de diciembre de 2023, a la fecha no cuenta con la suficiente madurez en sus controles.

Dado lo anterior, y en vista que el contenido entre versiones tiene cambios significativos, que denotan un avance considerable en la política, se contempla que se auditarán los controles que sean comunes en las versiones ya mencionadas.

5.2.1. Gestión de activos de información

Según el anexo A de la ISO/IEC 27001:2022, los controles para la gestión de activos de información tienen como objetivo "*Se debe elaborar y mantener un inventario de información y otros activos asociados, incluidos los propietarios*".

En la versión 3 de la política de seguridad de la información, los lineamientos se encuentran definidos en el ítem "4.4. Gestión de activos de información". La auditora de la OCI realiza validación de la evidencia allegada encontrando:

- Los lineamientos para la gestión de activos de información se encuentran en el procedimiento con el mismo nombre, con código P-CI-06 del 25 de julio de 2023.

- Los activos de información se deben revisar mínimo una vez al año, para identificar posibles actualizaciones y generar los ajustes correspondientes. Así mismo, los propietarios deben actualizar los activos y reportar al oficial de seguridad de la información, cualquier cambio o inclusión en la información. Al examinar la documentación allegada se encuentran 25 actas de aprobación de los activos de información de las diferentes áreas del MJD; adicionalmente, se encuentra acta de reunión del comité de gestión y desempeño el 12 de diciembre de 2023 en donde se informa que se aprueba el inventario de activos de información del MJD y se indica que "*Con el inventario de activos de información actualizado, se logró identificar que, de acuerdo con la criticidad, se cuenta con 136 activos en alta, 215 en media*

[4] Auditoría Evaluación y Verificación al Proceso de seguridad de la información; ítem 6. Conclusiones, hallazgos y/ recomendaciones; pág. 24; OCI MINJUSTICIA, noviembre de 2022; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2022/Informe%20Final%20seguridad%20de%20la%20inf%202022%20(1).pdf

y 98 en baja, de aquí la importancia de realizar el ejercicio de revisión de manera anual con la aplicación de la nueva metodología de levantamiento de la información".

- Se encuentra publicada en la página web del MJD la Resolución de 2081 del 06 de diciembre de 2023 mencionando "*Artículo 1.- Actualización de los Instrumentos de Gestión de la Información pública del Ministerio de Justicia y del Derecho. Actualizar los instrumentos de gestión de la información pública del Ministerio de Justicia y del Derecho, entendiéndose como éstos: (i) Registros de Activos de Información, (ii) índice de Información Clasificada y Reservada, (iii) Esquema de Publicación de Información y (iv) Programa de Gestión Documental, de acuerdo con lo establecido en la Ley 1712 de 2014 y el Decreto 1081 de 2015, adoptados mediante la Resolución NO.1853 del 17 de noviembre de 2021 y actualizados mediante la Resolución NO.0367 del 22 de marzo de 2023*[5]*".*

5.2.2. Gestión de acceso

Según el anexo A de la ISO/IEC 2001:2022, los controles para la gestión de acceso tienen como objetivo "*Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos de seguridad de la información y del negocio"* y *"Los derechos de acceso a la información y a otros activos asociados se deben proveer, revisar, modificar y eliminar de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.*"

En la versión 3 de la política de seguridad de la información, los lineamientos se encuentran definidos en el ítem "4.5. Política de Gestión de acceso". La auditora de la OCI realiza validación de la evidencia allegada y de la política, entre los cuales se destacan:

"*La asignación de usuario tipo administrador local del equipo debe ser asignado únicamente para los usuarios que lo requieran previa autorización y validación de la STSI; se llevara un registro digital de las autorizaciones concedidas para acceder a un equipo con perfil de administrador local junto con su justificación y autorización* [6]*"*. Al validar la evidencia allegada se encuentra que el personal de Mesa de ayuda, contratado por el MJD, es el único autorizado para el ingreso a los equipos de cómputo con perfil de administrador local para la instalación y configuración de software en las estaciones de trabajo. Para la vigencia 2023, no se autorizó a ningún funcionario diferente de mesa de ayuda para hacer uso del usuario administrador local; es de agregar que el control de la política igualmente se encuentra documentado en las políticas de operación del P-TI-01 Procedimiento Soporte a Usuarios, versión 6 del 30 de junio de 2020. Dado lo anterior, la OCI sugiere articular el procedimiento y la política mencionada, en cuanto a los ítems comunes.

"Todos los accesos a los servicios tecnológicos deben tener vigencia de uso[7]". En cuanto a los contratistas se refiere, al crear los perfiles de usuario en el directorio activo, se incluye la fecha de final del contrato o periodo laboral; lo cual, determina la utilización de los servicios tecnológicos. Para los funcionarios de planta se incluye en el directorio activo una restricción de

[5] Resolución de 2081 del 06 de diciembre de 2023; MJD; Pág. 3; https://www.minjusticia.gov.co/transparencia/Documents/Resolucion-No-2081-del-6-de-diciembre-de-2023.pdf#search=RESOLUCI%C3%93N%202081%20DE%202023

[6] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.5 Política de Gestión de Acceso; Pág. 14.

[7] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.5 Política de Gestión de Acceso; Pág. 14

inicio de sesión en la red para un grupo definido de equipos. Dado lo anterior, la OCI 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.

"*Toda solicitud de creación, modificación, bloqueo o eliminación de usuarios de acceso a los servicios de red a través de VPN* [8]*, debe realizarse a través de la mesa de ayuda* [9]". En la vigencia 2023, se registraron y atendieron por medio del aplicativo de mesa de ayuda Aranda 100 solicitudes por VPN. Los lineamientos de acceso de los funcionarios y contratistas a los diferentes sistemas de información del MJD, se encuentran documentados en el Procedimiento de Gestión de Accesos con Código P-TI-02 versión 9 del 1 de febrero de 2024. La OCI sugiere articular el procedimiento y la política en mención en cuanto a los ítems comunes.

"La STSI debe velar por que los equipos ajenos a MINJUSTICIA no accedan a la red local de la entidad[10]*".* La Subdirección ejecuta un control basado en la aplicación del protocolo IEEE 802.1X[11] el cual identifica un estándar de seguridad para redes LAN y WAN que permite la autenticación de dispositivos antes de que se conceda acceso a la red, con lo cual se protege la red de usuarios no autorizados y ataques cibernéticos.

"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[12] *".* Lo cual se realiza: En servidores: A la cuenta "Administrador" que viene por defecto en el sistema operativo Windows Server se le cambia de contraseña y solo es utilizada por personal autorizado. En equipos PC: A la cuenta "Administrador" que viene por defecto se le cambia la contraseña y solo es utilizada por el personal de mesa de ayuda. La OCI sugiere robustecer dicho control utilizando herramientas que brinden información detallada sobre el uso de los terminales y las actividades de los usuarios.

"*La STSI debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos*[13]". La STSI gestiona actualmente los repositorios por medio de la herramienta Azure Devops[14], la cual, actúa como repositorio principal, donde reposa la información de los 18 sistemas de información. Esta plataforma permite gestionar roles de acceso gestionando la

---

[8] Virtual Private Network (VPN) Red Privada Virtual, A diferencia de una red local tradicional, una VPN crea una conexión virtual a través de Internet. Permite que tus dispositivos se comuniquen como si estuvieran en la misma red local, incluso si están en diferentes ubicaciones geográfica.

[9] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.5 Política de Gestión de Acceso / Política de Acceso a Servicios De Red; Pág. 15.

[10] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.5 Política de Gestión de Acceso / Política de Acceso a Servicios De Red; Pág. 15.

[11] La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puertos. Forma parte del grupo de protocolos IEEE 802 (IEEE 802.1) y permite la autenticación de dispositivos conectados a un puerto LAN.

[12] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.5 Política de Gestión de Acceso / Política de seguridad de uso de altos privilegios y utilitarios de administración; Pág. 16.

[13] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.5 Política de Gestión de Acceso / Política de seguridad de control de acceso a sistemas de información y aplicativos; Pág. 16.

[14] Azure DevOps: Es una plataforma que admite una cultura colaborativa y un conjunto de procesos para desarrollar software. Puede trabajar en la nube con Azure DevOps Services o local con Azure DevOps Server, y acceder a servicios integrados de planificación, control de código, compilación, prueba y artefactos

seguridad y el control de los cambios realizados; actualmente se tienen configurados 7 roles de acceso a la herramienta.

5.2.3. Seguridad física y del entorno

Según el anexo A de la ISO/IEC 27001:2022, los controles para la seguridad física y del entorno tienen como objetivo "*Las áreas seguras deben protegerse mediante controles de entrada y puntos de acceso adecuados"* y *"Deben diseñarse y aplicarse medidas de seguridad para trabajar en zonas seguras".*

En la versión 3 de la política de seguridad de la información, se encuentra en el ítem "4.7. Política de seguridad física y del entorno"; es de aclarar que, en esta versión de la política estos controles no se encuentran documentados, por lo cual, la OCI realiza la validación de la evidencia allegada encontrando lo siguiente:

- La DTGIJ determina que un área se considera segura, cuando debido a la información u otros activos críticos que administran, deben estar aisladas del resto de la entidad y tener controles adicionales implementados, como ingreso autorizado y con registro.

- Tecnología estableció como área segura el Datacenter, el cual, aloja toda la infraestructura de Servidores, equipos de comunicación y los centros de cableado estructurado o backbone[15].

- El DataCenter está monitoreado por un sistema de video vigilancia, por medio del cual, se registran las actividades de ingreso y salida de personal interno o externo al MJD; adicionalmente, cuenta con dispositivo biométrico por huella y reconocimiento facial para controlar el ingreso al Datacenter.

- Uno de los controles de acceso al Datacenter se realiza mediante el formato F-TI-02-01 Versión 4 del 16 de agosto de 2023 "Planilla de control de acceso"; dentro de la evidencia allegan 9 planillas que comprenden los accesos realizados en la vigencia 2023, encontrando 6 formatos con campos en blanco en cuanto a "Nombre del visitante", "Entidad y/o dependencia", "Objeto ingresado", "Funcionario que autoriza", "Firma de quien autoriza", "Trabajo realizado", "Hora de salida" y "Firma visitante"; adicionalmente, se encontraron campos con comillas en las filas, incumpliendo presuntamente el principio de integridad[16] en cuanto a la completitud[17] de la información se refiere y la política de operaciones del procedimiento de gestión de acceso.

De acuerdo a lo anterior, 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

[15] Backbone: Es una red troncal que conecta numerosos routers interconectados entre sí. Puede utilizarse para conectar sedes de una organización, edificios gubernamentales, universidades e incluso países o continentes.

[16] Integridad: Propiedad de la información relativa a su exactitud y completitud

[17] La completitud de la información se refiere a garantizar que todos los datos y elementos relevantes estén presentes y no falten en un sistema o conjunto de información

Procedimiento de gestión de acceso, en cuanto al quién, cómo y cuándo 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. Es de resaltar que, la documentación de los controles se encuentra en la versión 4 de la política, en el ítem "4.5 Controles Físicos".

5.2.4. Seguridad en las operaciones/ control contra software malicioso

Según el anexo A de la ISO/IEC 27001:2022, los controles contra malware tienen como objetivo "*La protección contra el malware debe implementarse y respaldarse con el conocimiento adecuado del usuario*".

En la versión 3 de la política de seguridad de la información, los lineamientos se encuentran definidos en el ítem "4.8. Política de Seguridad en las operaciones / Control contra software malicioso". La OCI realiza validación de la evidencia allegada y de los controles comunes en las dos versiones de la política, entre los cuales se destacan:

- "*Además, proporcionará los mecanismos para generar cultura de seguridad entre los colaboradores frente a los ataques de software malicioso*[18]*".* Se destaca la realización de pruebas de ingeniería social[19] junto con un taller virtual al que asistieron 200 funcionarios y contratistas del MJD ; adicionalmente, se realizaron 3 charlas virtuales entre las cuales se destaca "Buenas de prácticas de ciberseguridad"; es de agregar que, se realiza una encuesta de precepción, por medio de la cual evalúan la opinión de los participantes sobre la formación que recibieron. La OCI sugiere 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.

- *"La STSI debe velar por que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico*[20]*".* El agente de red del antivirus está configurado para que se inicie automáticamente con el sistema operativo y parametrizado para que realice escaneo en tiempo real de la actividad de la estación de trabajo. En cuanto a la información que es transmitida por correo electrónico es escaneada por la misma suite de Microsoft.

- *El/La Oficial de Seguridad de la Información, debe implementar y documentar lineamientos para verificar la información relacionada con el software malicioso, y emitir boletines de advertencia informativos*[21]". El oficial de seguridad implementa y documenta lineamientos por medio de planes de seguridad de la información, los cuales están orientados a la ejecución de:

[18] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.8 Control contra software malicioso; Pág. 20

[19] Pruebas de ingeniería social: El objetivo de estas pruebas es obtener información confidencial al suplantar cuentas de funcionarios, clientes o proveedores, utilizando estrategias de persuasión. Estos ataques pueden incluir técnicas como el phishing (mediante correo electrónico), vishing (mediante llamadas telefónicas), smishing (mediante mensajes SMS) o incluso la manipulación en persona o a través de redes sociales.

[20] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.8 Control contra software malicioso; Pág. 20

[21] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.8 Control contra software malicioso; Pág. 20

análisis de vulnerabilidades, ejecución de herramientas de escaneo cómo antivirus para detectar software malicioso y plan operativo de seguridad de la información; adicionalmente, para la vigencia 2023 se emitieron ocho (8) boletines informativos enviados por correo institucional y se dictaron cuatro (4) charlas virtuales de temas relacionados con seguridad de la información, usando la plataforma Teams.

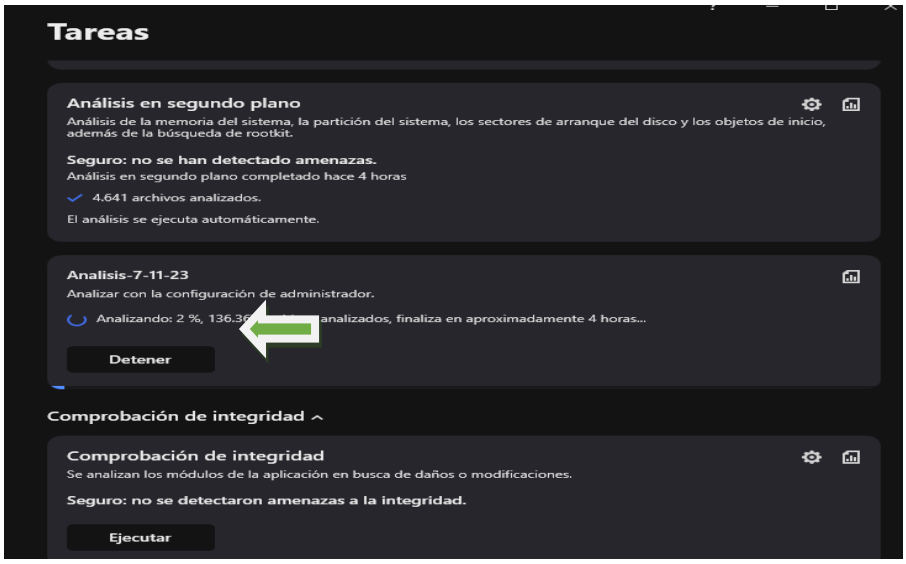
- *"La STSI, a través de sus colaboradores, debe impedir que los usuarios realicen cambios en la configuración del software de antivirus, antispyware, antispam y antimalware[22]".* Para realizar cambios o modificaciones en el software instalado en los equipos del MJD, se requiere de las credenciales y permisos de un usuario administrador, el cual utiliza únicamente mesa de ayuda. Los lineamientos para este control se encuentran documentados en las políticas de operación del procedimiento de soporte a usuarios y en la versión 4 de la política de seguridad de la información en el ítem 4.6.8 Instalación de software. Para validar lo anterior la OCI ingresa a la consola del antivirus y se evidencia que:

  - No se pueden realizar cambios en su configuración de protección frente a amenazas, las opciones las deja en marca agua[23].

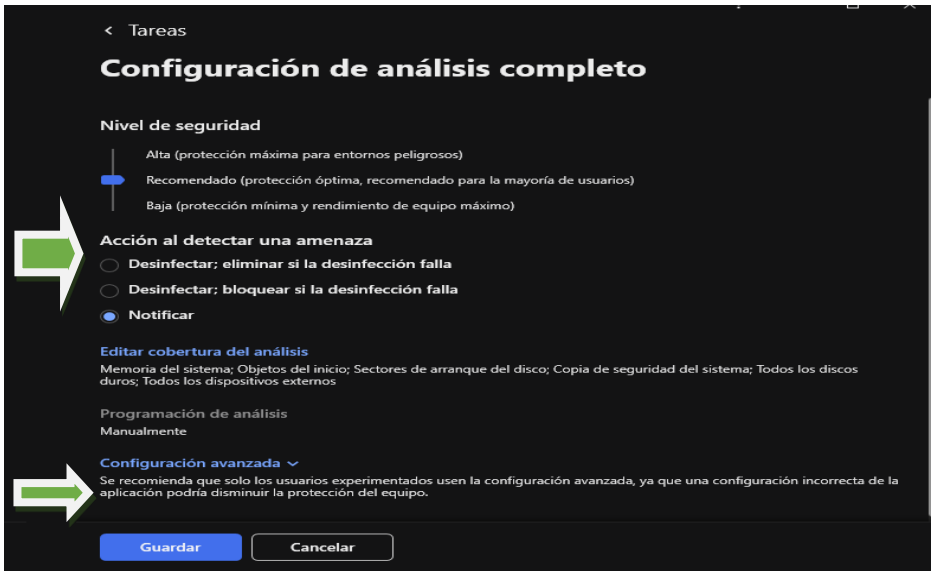
[22] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.8 Control contra software malicioso; Pág. 20

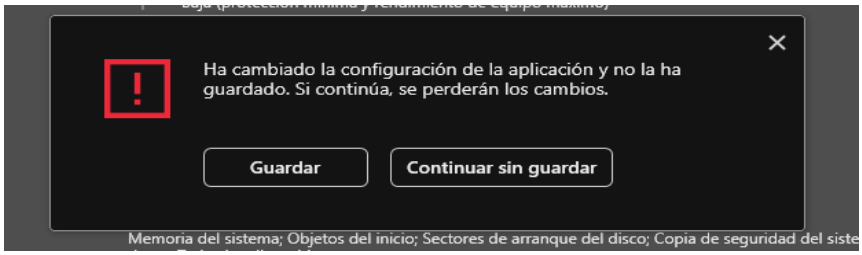
[23] Marca de agua: Se refiere a que el botón aparece deshabilitado o con una apariencia atenuada. Esto significa que no se puede interactuar con él o que su funcionalidad está restringida en ese momento

- Permite ejecutar tareas de análisis, activándolas de forma manual.

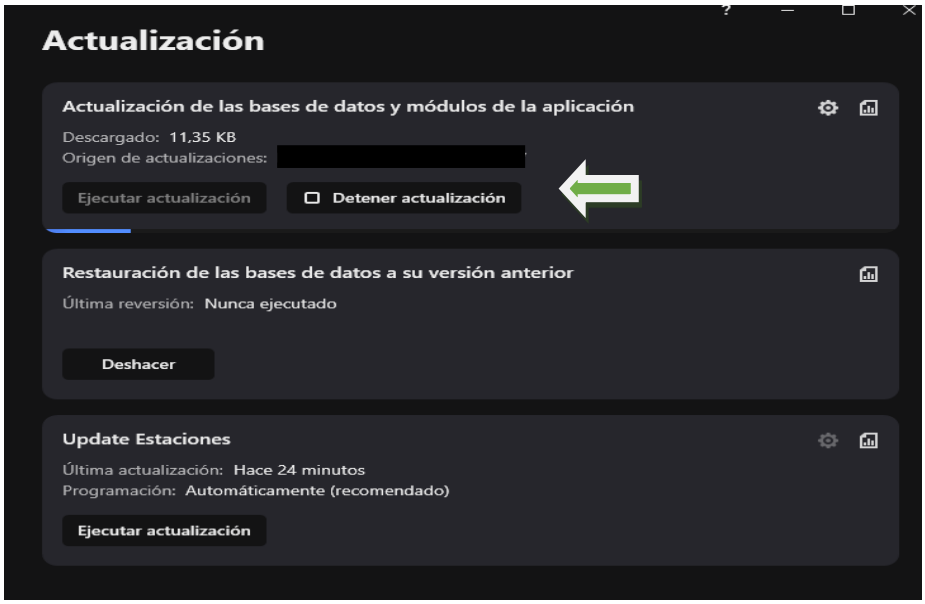


- Permite cambiar la configuración, cuando se selecciona un analisis completo al equipo.





- Realizar de forma manual actualizaciones en sus bases de datos y módulos de aplicación.



Dado lo anterior, la OCI sugiere 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.

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

- 1087 vulnerabilidades de alto riesgo (pueden comprometer sistema).
- 315 vulnerabilidades de riesgo medio (pueden comprometer data).
- 603 vulnerabilidades de bajo riesgo.
- 1848 advertencias internas.

Este análisis contó con una duración de 15 horas,10 minutos y 5 segundos, alcanzando la totalidad de las rutas del portal mencionado. 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 resalta que al realizar la prueba de SSL[24] se encuentran deshabilitados los protocolos TLS[25] 1.0 y 1.1, los cuales son obsoletos y no recomendados dada la debilidad de las suites de cifrado.

[24] 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.
[25] La sigla TLS (Transport Layer Security, o Seguridad de la Capa de Transporte), es el protocolo criptográfico que garantiza las comunicaciones en Internet.

5.2.5. Gestión de la prestación de servicios de proveedores

Según el anexo A de la ISO/IEC 27001:2022, los controles para los proveedores tienen como objetivo "*Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor*" , "*Los requisitos de seguridad de la información pertinentes debieran establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor* " y "*La organización debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información del proveedor y en la prestación de servicios*"

En la versión 3 de la política de seguridad de la información, los lineamientos se encuentran definidos en el ítem "4.11. Política para la gestión de la prestación de servicios de proveedores". La auditora de la OCI realiza validación de la evidencia allegada encontrando lo siguiente:

- *"El supervisor del contrato debe solicitar el diligenciamiento y firma al proveedor del acuerdo de confidencialidad [26]".* En la documentación se encuentran 3 formatos de acuerdos de confidencialidad para proveedores diligenciados en su totalidad, los cuales tienen como supervisor al Subdirector de tecnología.

Con el fin de validar lineamientos que la auditoria considera importantes, se solicitó a tecnología vía correo electrónico:

- ¿Cómo validan el cumplimiento de los requisitos de seguridad por parte del tercero y/o proveedor?

  Respuesta emitida por Tecnología: "*Se valida a partir del diligenciamiento del Formato F-IC-G14-03 - Política de seguridad de la información, ítem 4.11*". Si bien es cierto que la política define algunos lineamientos para el uso del formato de "Acuerdos de confidencialidad de proveedores", no se encuentra definido como validar el cumplimiento de la normatividad contenida en dichos acuerdos o como realizar un seguimiento efectivo para detectar posibles incumplimientos; por lo cual, la OCI recomienda fortalecer los controles, validar la inclusión de estos parámetros en la política de seguridad de la información y en el acuerdo de confidencialidad.

- ¿Cómo validan la efectividad de la política a proveedores?

  Respuesta emitida por Tecnología: "*El supervisor del contrato debe solicitar el diligenciamiento y firma al proveedor del acuerdo de confidencialidad, una vez se tenga el documento se debe compartir con el/la Oficial de Seguridad de la Información para su revisión y seguimiento. ítem de la política 4.11".* Actualmente, no se encuentra definida una métrica cuantificable que permita evaluar la efectividad de los controles de la política y de la documentación complementaria a la misma; por lo cual, la OCI recomienda validar su inclusión.

- Mencione los procesos y/o procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

[26] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.11. Política para la gestión de la prestación de servicios de proveedores; Pág. 32

Respuesta emitida por Tecnología: "*La guía de Administración de Riesgos, que se encuentra publicada en el SIG de la entidad*". La OCI realiza análisis del contenido de la guía en mención, encontrando que se encuentran definidos los parámetros para riesgos de corrupción, gestión y seguridad digital de forma general, pero no se encuentra definido en el documento cómo gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor; se valida si existe documentación complementaria que mencione cómo tratar este tipo de riesgos y no se encuentran parámetros al respecto; por lo anterior, la OCI recomienda definir lineamientos para gestionar los riesgos asociados a los proveedores.

- Mencione cómo el MJD supervisa, revisa, evalúa y gestiona los cambios en las prácticas de seguridad de la información del proveedor y en la prestación de servicios.

Respuesta emitida por Tecnología: "*El Ministerio de Justicia y Derechos (MJD) supervisa, revisa, evalúa y gestiona 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. A continuación, se detallan las acciones con base en los procedimientos y formatos del MJD:*

1. *Supervisión y Revisión: Formato F-TI-06-04 Pruebas Funcionales y no Funcionales: Este formato se utiliza para llevar a cabo pruebas exhaustivas de las funcionalidades y aspectos no funcionales del sistema de información. Las pruebas incluyen la verificación de la seguridad de la información y aseguran que los cambios propuestos no introduzcan vulnerabilidades.*
2. *Evaluación: Evaluaciones de Impacto: Antes de implementar cualquier cambio, se realizan evaluaciones de impacto para determinar cómo las modificaciones afectarán la seguridad de la información y la prestación de servicios. Estas evaluaciones se documentan y revisan minuciosamente.*
3. *Pruebas de Seguridad: Se llevan a cabo pruebas de penetración y simulacros de ataque utilizando el formato F-TI-06-04 para evaluar la efectividad de las nuevas prácticas de seguridad implementadas por el proveedor.*
4. *Gestión de Cambios: Formato F-TI-03-01 Implementación en Producción de Software: Este formato se utiliza para documentar y gestionar la implementación de software en producción, asegurando que todos los cambios sean aprobados y validados antes de su despliegue. Formato F-TI-03-02 Recibo a Satisfacción Puesta en Producción: Una vez implementados los cambios, este formato se utiliza para confirmar que los mismos se han realizado de manera satisfactoria y cumplen con los requisitos de seguridad establecidos*".

Si bien es cierto que, el área de tecnología tiene definidos controles para la implementación de cambios en el software proporcionado por un proveedor, no se encontró en la documentación allegada, controles que permitan revisar y/o evaluar las modificaciones o ajustes que se realizan en las políticas, procedimientos y controles relacionados con la seguridad de la información por parte del proveedor. Estos cambios pueden incluir actualizaciones en las medidas de seguridad, ajustes en los acuerdos contractuales, mejoras en la gestión de riesgos o cualquier otro aspecto que afecte la seguridad de los datos y la continuidad del servicio en el contexto de la prestación de servicios por parte de un proveedor; por la cual, la OCI insta a tecnología a realizar análisis, revisión y posterior fortalecimiento de los respectivos controles.

- ¿Cómo validan que los proveedores y terceros que manejan activos de información de la entidad devuelvan dichos activos, cuando finaliza la relación contractual o convenio de intercambio de información?

  Respuesta emitida por Tecnología: "*Basados en el artículo 24 de la ley 1437 que indica "Teniendo en cuenta que, la confidencialidad es un concepto inherente a la condición del proveedor, el cual se ve obligado a mantener aun después de su vinculación la reserva del documento y/o información a la que tuvo acceso y que en virtud de la ley tiene tal carácter, es imperioso que se revise cada uno de los ítems a los cuales se les imprime confidencialidad". Se establece en los acuerdos de confidencialidad del ministerio la cláusula 5 que indica: EL CONTRATISTA se compromete a guardar reserva sobre toda la información confidencial y estratégica a la que tenga acceso en el desarrollo del contrato celebrado con EL MINISTERIO DE JUSTICIA Y DEL DERECHO. La cláusula 8: EL CONTRATISTA reconoce que la información confidencial del MINISTERIO DE JUSTICIA Y DEL DERECHO es y permanecerá siendo de propiedad del MINISTERIO DE JUSTICIA Y DEL DERECHO. No se permitirá ningún uso de esta información distinto del que se prevé en el Contrato. Después de entregada la información y finalizada la relación contractual todas las bases de datos e información generada, producto del contrato deben ser eliminadas o borradas de los equipos e infraestructura utilizada por EL CONTRATISTA"*. La OCI revisa los lineamientos del acuerdo de confidencialidad para proveedores encontrando que la cláusula 8 adicionalmente menciona que el contratista "*el cual deberá presentar un documento que sirva de constancia de la aplicación de un método de borrado seguro*[27] *(WIPE) para garantizar la eliminación total de la información obtenida en la ejecución del contrato. Una vez culminadas las obligaciones contractuales, en caso de no cumplir el contratista con lo pactado si era exigible la cláusula penal pactada en el contrato*". Es de resaltar que en el acuerdo de confidencialidad y en la política de seguridad de la información, no se encuentran definidas las características mínimas que debe cumplir la constancia de borrado seguro de la información, cómo 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 creadas dentro del contrato en cumplimiento de las obligaciones contractuales, quién va a realizar dicha verificación, en qué momento se va a solicitar (con la última cuenta de cobro, como parte de los entregables …) ; por lo cual, la OCI recomienda validar su inclusión. Adicionalmente, para la vigencia 2023 no se presentaron labores de eliminación de información con proveedores donde fuera requerido el borrado seguro.

- Qué sanción o multa se tiene definida en caso de incumplimiento de las políticas de seguridad por parte de los proveedores.

  Respuesta emitida por Tecnología: "*En el Acuerdo de Confidencialidad para Proveedores, la cláusula 8 establece que en caso de incumplimiento de lo pactado "..... se hará exigible la cláusula penal pactada en el contrato*." La OCI valida el acuerdo de confidencialidad para proveedores encontrando en el ítem 3. CONSIDERACIONES "*Que la Ley 1273 de 2009, modificó el Código Penal y creó un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", además de establecer disposiciones que busquen preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Así, en su Artículo 269A establece "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no*

[27] El borrado seguro es un proceso que garantiza la eliminación permanente y segura de información sensible de un dispositivo de almacenamiento, como un disco duro, una memoria USB o incluso servicios en la nube1. A diferencia de simplemente borrar o eliminar archivos, el borrado seguro utiliza software especializado para sobrescribir los datos con ceros u otros patrones, lo que hace que los datos eliminados sean irrecuperables

*con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo**, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes*** …" De igual manera, en su Artículo 269F señaló: "*El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes*." Adicionalmente, menciona: "*Teniendo en cuenta que, la confidencialidad es un concepto inherente a la condición del proveedor, el cual se ve obligado a mantener aun después de su vinculación la reserva del documento y/o información a la que tuvo acceso y que en virtud de la ley tiene tal carácter, es imperioso que se revise cada uno de los ítems a los cuales se les imprime confidencialidad, para que guarde relación con lo dispuesto en el Artículo 24 de la ley 1437 de 2011."* Si bien cierto que en el acuerdo de confidencialidad se estipulan las posibles sanciones a las que estaría sujeto el proveedor en caso de incumplimiento del acuerdo, a la OCI le preocupa la coherencia en lo mencionado en la cláusula 8 en cuanto a "… *Una vez culminadas las obligaciones contractuales, en caso de no cumplir EL CONTRATISTA con lo pactado, se hará exigible la cláusula penal pactada en el contrato"*.

Por lo anterior la OCI valida la correlación entre el contenido del acuerdo de confidencialidad de proveedores y sus respectivos contratos, encontrando que en la cláusula 4. Alcance del acuerdo menciona "*Este documento es desarrollo de lo estipulado en la cláusula de obligaciones Generales del Contratista, numeral 6 del contrato No. -----, como se expresa a continuación …"* y en la cláusula 3. Obligaciones generales del contrato indica "*Guardar la confidencialidad y la reserva de toda información o documentación que le haya sigo asignada en desarrollo de sus obligaciones contractuales*". La OCI sugiere hacer mención del acuerdo de confidencialidad en el contrato ya sea como anexo de este o incluirlo tácitamente en la cláusula 3.

En otros escenarios, la oficina de Control Interno ha sugerido la introducción de cláusulas en el contrato que hagan alusión a las multas, como mecanismo correctivo y ejemplarizante de eventuales incumplimientos parciales, porque se hace necesario realizarlo de manera expresa en la minuta contractual con sujeción a las consideraciones realizadas en la sentencia del Consejo de Estado sobre dicha situación. También 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.

5.2.6. Acuerdos de confidencialidad o de no divulgación

Según el anexo A de la ISO/IEC 27001:2022, los controles para los acuerdos de confidencialidad tienen como objetivo "*Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados regularmente por el personal y otras partes interesadas pertinentes".*

En la versión 3 de la política de seguridad de la información, los lineamientos se encuentran definidos en el ítem "4.8. Política de seguridad en las comunicaciones / Acuerdos de

confidencialidad o de no divulgación". La OCI realiza validación de la política y de la evidencia allegada encontrando lo siguiente:

- El Grupo de Gestión Contractual asegura la firma del Formato de confidencialidad para los contratistas y proveedores; el formato firmado se debe guardar con el contrato o acuerdo en su respectiva carpeta, antes de iniciar actividades. Dentro de las evidencias allegadas, anexan 22 formatos diligenciados para contratistas del área de tecnología, encontrando 3 formatos con campos en blanco en los ítems 4,5,7,8 y 10 referentes a: datos del contratista, datos del supervisor, número del contrato y numeral del contrato, con lo cual incumplen el principio de integridad[28] de la información; adicionalmente, adjuntan 3 formatos diligenciados para proveedores diligenciados en su totalidad.

- El Grupo de Gestión Humana garantiza la firma del Formato de confidencialidad para los funcionarios. Este documento firmado debe ser guardado en la respectiva carpeta de hoja de vida del funcionario. Dentro de las evidencias allegadas, anexan 17 formatos diligenciados para funcionarios de tecnología, encontrando 2 formatos con campos en blanco en los ítems 4 y 10 en cuanto a: fecha de diligenciamiento, nombre, número de cedula de ciudadanía, cargo y dependencia del jefe directo, incumpliendo el principio de integridad de la información en cuanto a la completitud de la información se refiere.

- En 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.

- Dentro de los controles de la política, no se contempló mencionar quien es el responsable de la validación de la calidad de la información, diligenciada en los formatos de confidencialidad.

- En la política no se menciona, quien debe hacer la validación en las respectivas carpetas para evidenciar que se encuentren alojados en su contenido los formatos de confidencialidad.

- En los lineamientos de la política no se menciona en qué casos se debe de volver a firmar el formato de confidencialidad.

Por lo anterior, se reitera lo mencionado en el informe de Auditoría Evaluación y Verificación al Proceso de seguridad de la información de la vigencia 2022 "*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*[29]" lo cual en su momento genero un hallazgo.

[28] Integridad: Propiedad de la información relativa a su exactitud y completitud.

[29] Auditoría Evaluación y Verificación al Proceso de seguridad de la información; ítem 5. Desarrollo de la Auditoría / Acuerdos de confidencialidad o de no divulgación; pág. 14; OCI MINJUSTICIA, noviembre de 2022; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2022/Informe%20Final%20seguridad%20de%20la%20inf%202022%20(1).pdf

5.3. Gestión de incidentes de la seguridad digital

Según la ISO/IEC 27000:2022, la Gestión de Incidentes de Seguridad de la información tiene como objetivo "*La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información*" y "*Los conocimientos obtenidos de los incidentes de seguridad de la información deben utilizarse para reforzar y mejorar los controles de seguridad de la información*" .

En la versión 3 de la política de seguridad de la información, los lineamientos se encuentran definidos en el ítem "4.12. Política de Gestión de Incidentes de Seguridad". La OCI realiza validación de la política y de la evidencia allegada encontrando lo siguiente:

- Los lineamientos detallados para el manejo de incidentes de seguridad se encuentran en el Procedimiento Gestión de Incidentes de seguridad, el cual será abordado más adelante.

- El reporte de eventos e incidentes de seguridad se debe realizar a través de la Mesa de Ayuda.

- Para la vigencia 2023, se reportaron 58 incidentes de seguridad de los cuales 12 fueron reportados directamente en la oficina de mesa de ayuda y 41 fueron ingresados por la herramienta Aranda; los cuales se encuentran discriminados de la siguiente manera:

Descripción	Cantidad
Correo sospechoso	43
Revisión de PC	8
Solicitud de Copia de seguridad	2
Recuperación de archivos	2
URL sospechosa	2
Solicitud de Permisos de acceso	1
Total	58

Fuente: Elaboración propia

  De acuerdo con lo anterior podemos inferir que, de los 58 incidentes de seguridad de la información, el 74,14% fueron por correo sospechoso, el 13,79% fueron por solicitud de revisión del computador empresarial; el 3,45% respectivamente por solicitud de copia de seguridad, recuperación de archivos y URL sospechosa; por último, el 1,72% fue por solicitud de permisos de acceso. Es de agregar que varios de estos ítems fueron tratados como incidentes de seguridad sin serlo, como, por ejemplo, la solicitud de permisos de acceso o las solicitudes de copia de seguridad; por lo cual, se sugiere la posibilidad de reclasificación de la categoría en la herramienta Aranda.

- El documento no menciona en qué casos se debe escalar el incidente de seguridad de la información a entidades tales como COLCERT[30] o CSirt[31]; adicionalmente, el documento no indica donde se encuentran los números telefónicos, direcciones de correo electrónico, o nombres de los funcionarios para realizar dicha notificación.

[30] COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia
[31] CSIRT-CCIT: Centro de Coordinación Seguridad Informática Colombia.

- Al realizar la validación de las evidencias allegadas en cuanto a las lecciones aprendidas, se encuentran socializaciones y publicaciones en diversos temas relacionados con seguridad de la información, que dan cuenta de actividades de uso y apropiación de las distintas herramientas con las que cuenta el MJD para evitar incidentes de seguridad; pero no se encuentra evidencia de la documentación de las lecciones aprendidas o de bases de conocimiento.

Dado lo anterior, la OCI sugiere robustecer la política de gestión de incidentes y la documentación completaría (procedimientos, guías).

5.3.1. Procedimiento de Gestión de Incidentes

La Gestión de Incidentes de seguridad en el Ministerio de Justicia y del Derecho (MJD) está soportada en el "Procedimiento Gestión de Incidentes de seguridad" con código: P-IC-04 en su versión 1 del 11 de mayo de 2021, siendo el responsable del procedimiento la Subdirección de Tecnologías y Sistemas de Información (STSI).

El procedimiento mencionado anteriormente, tiene como objetivo "*Administrar la seguridad de la información con el fin de proteger la integridad, disponibilidad y confidencialidad de ésta y minimizar el impacto en el negocio de los riesgos y amenazas a los cuales se encuentra expuesta. (Objetivo del procedimiento, debe responder el qué, cómo y para qué del procedimiento*[32]*)*".

El alcance es "*Aplica para los contratistas, funcionarios y terceros que gestionen información del Ministerio de Justicia y del Derecho y que puedan afectar su disponibilidad, integridad y/o confidencialidad. Inicia con la recepción de la notificación por mesa de ayuda y finaliza con el cierre del ticket*.[33]**"**

La OCI revisa el contenido del procedimiento e insta a replantear su contenido, en cuanto a:

- El responsable del procedimiento no coincide en su totalidad con el mencionado en la política de seguridad de la información, en donde se menciona que los responsables del procedimiento son la STSI y el Oficial de seguridad de la información y no se encuentra alineado con la política de seguridad de la información.

- El procedimiento no plantea reclasificar el evento en el caso que, al realizar el análisis de este no sea considerado un incidente que afecte la seguridad de la información.

- El documento no menciona las actividades que se deben realizar en la detección, reporte, análisis, monitoreo y resolución de incidentes de seguridad de la información.

- En el documento no se contempla las distintas criticidades que se pueden presentar en un incidente; adicionalmente, no define los lineamientos a seguir en los diferentes escenarios contemplados para un incidente de seguridad de la información.

[32] Procedimiento Gestión de Incidentes de seguridad; Código: P-IC-04 versión 1 del 11 de mayo de 2021; ítem 3. Objetivo del procedimiento; Pág. 2

[33] Procedimiento Gestión de Incidentes de seguridad; Código: P-IC-04 versión 1 del 11 de mayo de 2021; ítem 3. Objetivo del procedimiento; Pág. 2

- El documento solo menciona las interacciones entre mesa de ayuda y el oficial de seguridad, pero no contempla las interacciones con los grupos de respuesta de acuerdo con el vector del incidente.

- El documento no contiene los lineamientos para reportar y gestionar un incidente de seguridad que provenga de un proveedor de servicios, no indica 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 no se contempla las sanciones o multas que esto implicaría para el proveedor.

- El procedimiento adolece de las verificaciones que se deben realizar para probar que los incidentes reportados por la herramienta de mesa de servicio hayan sido solucionados de manera satisfactoria.

Dado lo anterior, la OCI recomienda la generación de una guía complementaria que permita definir los lineamientos para detectar, reportar, analizar y resolver incidentes de seguridad, así como para recuperarse de ellos.

5.4. 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 [34]".

En la medición con fecha de evaluación diciembre de 2023, 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 el total de dominios de acuerdo con la ISO/IEC 27001:2013 y su anexo A:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	85	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	95	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	97	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	81	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	94	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	90	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	EFECTIVO
A.18	CUMPLIMIENTO	91	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		89	100	OPTIMIZADO

Fuente: Instrumento de evaluación MSPI vigencia 2023, elaborado por tecnología

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

Con base a la información de la tabla; podemos deducir que, de 14 dominios, el 85,72% posee controles con un grado optimizado (Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua), el 7,14% posee controles con grado gestionado (Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente) y por ultimo el 7,14% posee controles con grado efectivo (Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicado) ; con un promedio de evaluacion de los controles del 89%.

Con respeto a la Calificación Frente a Mejores Prácticas en ciberseguridad (NIST), la cual "muestra una tabla con los resultados de comparar la calificación de acuerdo a la escala de evaluación de los controles existentes en la entidad frente a la mejor práctica en Ciberseguridad definida por NIST[35]".

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

Fuente: Instrumento de evaluación MSPI vigencia 2023, elaborado por tecnología

Al validar la información en la tabla y contrastarla con la del Instrumento de evaluación MSPI generado para la vigencia 2021, no se encuentra ningún cambio en los valores registrados en la calificación de la entidad para la vigencia 2023; dado lo anterior, se insta al área de tecnología a validar la formulación en las correspondientes celdas y realizar la respectiva corrección de ser necesario.

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 "DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN", 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".

- Administrativas, Técnicas: Se sugiere 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.

[35] 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

6. Análisis de Riesgo:

Para realizar el análisis de riesgos de seguridad de la información, la OCI revisa la matriz que consolida estos riesgos evidenciando con corte 31 de diciembre de 2023 se han identificado 40 riesgos, encontrando lo siguiente:

- Se observa que, para ese periodo, la Dirección de Tecnologías y Gestión de Información en Justicia actualizó la matriz de riesgos, contemplando los activos críticos para cada proceso. Esta actualización incluye la definición de riesgos, la identificación de causas y la construcción de los controles correspondientes.

- En cuanto a la implementación de controles, solo se cuenta con evidencias de los controles de los riesgos del proceso de Gestión de las Tecnologías y la Información. Este proceso es el responsable del monitoreo y revisión de la gestión de los riesgos de todo el Ministerio, según la Guía de administración de riesgos de la Entidad. Por lo anterior, no se evidencia la implementación de los demás controles de los otros procesos contemplados en la matriz, y la DTGIJ no ha verificado dicha implementación, a pesar de la actualización que realizó a la matriz de riesgos durante la vigencia. Además, se observa que la dependencia no realiza un seguimiento semestral (dos veces al año) de la implementación de los controles para la mitigación de los riesgos de seguridad de la información como función de segunda línea de defensa. Aunque se actualizó la matriz, no se contempló la revisión de las evidencias de los controles, por lo cual se presume un incumplimiento en la Guía de administración de riesgos de la Entidad.

- Si bien la dependencia realiza reuniones con los procesos para la actualización de los riesgos -cuando aplique-, no se dejan evidencias de los ajustes realizados ni de las nuevas formulaciones de los riesgos y/o controles. Por tanto, no es posible verificar la efectividad de estos ni determinar si los controles funcionan correctamente; esto, puede llevar a desconocer la posible materialización de un riesgo de seguridad digital y a no identificar la disminución del riesgo inherente (riesgo residual). Esta situación se debe a la falta de un monitoreo permanente por parte de la primera línea de defensa y a la ausencia de un análisis, seguimiento y verificación del cumplimiento de los lineamientos y controles definidos para el tratamiento de los riesgos por parte de la DTGIJ, que desarrolla la función de segunda línea de defensa. Esta problemática ha sido señalada desde la auditoría realizada en 2022, denominada "Evaluación y Verificación al Proceso de Seguridad de la Información", llevada a cabo por este despacho.

- Se evidencia que existen deficiencias en la formulación de los planes de tratamiento, ya que no cumplen con su objetivo principal de fortalecer el control. En muchos de los casos actuales, estos planes están formulados como actividades que se desarrollan dentro de la implementación del control. Además, los planes de tratamiento relacionados en la matriz no están vigentes para el periodo de evaluación, ya que todas sus actividades inician en febrero de 2024 y se está evaluando la vigencia de 2023.

Con base en lo expuesto anteriormente, se sugiere que la DTGIJ reformule los controles establecidos, ya que los que se encuentran diseñados actualmente no son competencia directa de los procesos y dependen de otros. Es necesario contar con controles cuya verificación de cumplimiento esté a cargo de la dependencia en cuyo proceso se presenta el riesgo. Asimismo,

se insta a la DTGIJ, como segunda línea de defensa, a realizar seguimientos adecuados a la implementación de los controles, recopilando las evidencias correspondientes para mantener la trazabilidad y preservar la gestión del conocimiento. De igual forma, todas las actualizaciones relacionadas con los riesgos de seguridad de la información deben ser registradas y conservadas adecuadamente en la misma matriz para facilitar el acceso a esta información y a la gestión de cambios que se ha realizado al respecto.

Con relación al plan de tratamiento de riesgos del área de tecnología, la OCI pudo evidenciar que no guarda relación con los planes de tratamiento que se encuentran planteados en la matriz de riesgos de seguridad de la información, por lo cual se recomienda unificar y alinear los planes de tratamiento y sus actividades, guardando la finalidad de creación de un plan de tratamiento que es fortalecer los controles establecidos para la mitigación del riesgo.

7. Conclusiones, hallazgos y/ recomendaciones

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

7.1. Conclusiones

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 .

7.2. Socialización del informe de auditoria

Mediante memorando MJD-MEM24-0004195 del día 27 de junio de 2024, se remite informe preliminar de esta auditoría, a la Dirección de tecnología, 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.

La DTGIJ, genera comunicación radicada bajo el número MJD-MEM24-0004286 del día 03 de julio de 2024, 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 DTGIJ	RESPUESTA OCI
1a: Se evidencia incumplimiento en la propiedad asociada a la integridad de la información en cuanto a la completitud del diligenciamiento de los campos de los formatos F-TI-02-01 Versión 4 del 16 de agosto de 2023 “Planilla de control de acceso” en cuanto a “Nombre del visitante”, “Entidad y/o dependencia”, “Objeto ingresado”, “Funcionario que autoriza”, “Firma de quien autoriza”,” Trabajo realizado”, “Hora de salida” y “Firma visitante”. **1b**:En cuanto a los acuerdos de confidencialidad para contratistas formato con Código: F-IC-G14-02 del 19 de diciembre de 2022 con campos en blanco en los ítems 4,5,7,8 y 10 referentes a datos del contratista, datos del supervisor, número del contrato y numeral del contrato y acuerdo de confidencialidad para funcionarios formato con Código: F-IC-G14-01 del 19 de diciembre de 2022 con campos en blanco en los ítems 4 y 10 en cuanto a: fecha de diligenciamiento, nombre, número de cedula de ciudadanía, cargo y dependencia del jefe directo; lo anterior de acuerdo a la definición mencionada en la ISO/IEC 27000:2017 y conforme a la definición citada en la política de seguridad de la información del MJD “*Integridad: Propiedad de la información relativa a su exactitud y completitud*”.	***1a**: En cuanto al hallazgo reportado, se entiende la necesidad de contar con el control de acceso, y que este debe ser registrado y llevado de manera formal, en el entendido que este hallazgo tiene mucho de forma y adicionalmente es la primera vez que se observa; por lo que se somete a su consideración elevarlo a la categoría de recomendación y desde la Dirección se tomaran las medidas correctivas que den cuenta de dicha recomendación.* *Un plan de mejoramiento en este sentido no atacaría un tema de fondo sino de forma, toda vez que ya existe un control y que es necesario continuar con él.* ***1b:** La Dirección de tecnología previendo las dificultades del manejo de este formato en la etapa de ejecución contractual y con propósito de dar alcance de fondo, adelantó mesas de trabajo tanto con el grupo de Gestión Humana como con el grupo de Gestión Contractual con el fin de lograr la firma de estos acuerdos en las etapas previncular y precontractual respectivamente para cualquier vinculación al Ministerio de Justicia. Esta medida tuvo por objeto asignar la adecuada responsabilidad del diligenciamiento y revisión como prerrequisito para ser parte del Ministerio de Justicia en calidad de funcionario público. Esta medida debe garantizar la integridad del formato, toda vez que lo somete a una rigurosa verificación por parte del responsable en virtud de los procedimientos que se establecen en el sistema integrado de gestión. Es de anotar que este es un proceso concertado y formalizado a través del Comité Institucional de Gestión y Desempeño adelantado*	De acuerdo con lo mencionado por el área auditada, **nos permitimos confirmar el hallazgo**, teniendo en cuenta lo siguiente: **1a:** Si bien cierto que puede ser “*la primera vez que se observa”* de 9 formatos allegados de la Planilla de control de acceso, 7 presentan inconsistencias en la completitud de la información diligenciada, como campos en blanco o comillas en los respectivos campos, por lo cual claramente se debe de fortalecer el control incorporando la responsabilidad de revisión al registro. Dada la respuesta la DTGIJ surgen varios cuestionamientos en cuanto a: si tecnología implementa un control físico que busca asegurar la protección de los activos tangibles de la entidad, en este caso los elementos propios del Datacenter; no se requiere fortalecer un control que en caso de un incidente permitirá rastrear quiénes ingresaron al Datacenter. Con el registro de las cámaras puedo identificar a las personas que accedieron al Datacenter, las cámaras registran los rostros de las personas que acceden, si no se registró el nombre del visitante en la planilla como puedo encontrar sus datos. Adicionalmente, la OCI no comparte la premisa mencionada por tecnología en cuanto a “*Un plan de mejoramiento en este sentido no atacaría un tema de fondo sino de forma, toda vez que ya existe un control y que es necesario continuar con él*”, ya que se puede fortalecer el control definiendo políticas claras sobre quiénes pueden acceder al Datacenter, cuándo y por qué, establecer procedimientos para solicitar acceso y autorizaciones especiales, validar la posible inclusión de nuevos campos en el formato como por ejemplo “empresa a la que pertenece el visitante” “observaciones (campo que permitiría ingresar detalles sobre el propósito de la visita o cualquier incidente relevante). **1b**: Es de aclarar que la OCI no está solicitando bajo ninguna circunstancia “*recomponer formatos de contratos ya finalizados y posiblemente liquidados*” como

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
	el pasado 12 de diciembre de 2023. *Así las cosas, teniendo en cuenta que el alcance de la auditoria fue para la vigencia 2023, año durante el cual contábamos con el formato de la política de seguridad F-IC-G14-02 del 19 de diciembre de 2022, donde se hacía un llamado a los acuerdos de confidencialidad y se encontraban bajo la gestión de la DTGIJ, no encontramos procedente recomponer formatos de contratos ya finalizados y posiblemente liquidados.* *Encontramos procedente y es la expectativa que la modificación de procesos y procedimientos antes mencionada, de como fruto el control efectivo al cual el presunto hallazgo hace referencia.* *En este mismo sentido se informa que, actualmente se cuenta con una nueva versión de la política de seguridad con fecha del 26 de diciembre de 2023, la cual asigna al grupo de gestión humana y al grupo de gestión contractual la responsabilidad de diligenciar, revisar y aprobar el formato de acuerdo de confidencialidad, previa a una vinculación de un funcionario público (funcionarios y contratistas). A continuación, se presenta el extracto correspondiente al ítem 4.4.1 de la política de seguridad de la información del 26 de diciembre de 2023 en su versión nro. 4.* *"4.4.1 SELECCIÓN E INGRESO DEL PERSONAL, ACUERDOS DE CONFIDENCIALIDAD* *El Grupo de Gestión Humana, así como el Grupo de Gestión Contractual, antes de realizar la vinculación, deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada en la*	lo mencionan en la respuesta otorgada por tecnología; el hallazgo busca que se genere un plan de mejoramiento que garantice la completitud de la información de los formatos establecidos, para este caso los formatos de acuerdos de confidencialidad; antes de ser enviados a los Grupos de Gestión Contractual y/o Gestión Humana, realizando validación del diligenciamiento de dichos formatos por parte del supervisor del contrato (Dirección o subdirección de tecnología) o del enlace delegado para tal fin, teniendo en cuenta que los formatos allegados a la auditoria son de tecnología. Lo anterior teniendo en cuenta lo mencionado en el actúal Manual de contratación con código M-GC-01 versión 5 del 2 de agosto de 2022, en el ítem 3.8.3 Concurso de méritos/ Desarrollo del proceso "*La documentación deberá estar legajada, de acuerdo con las listas de chequeo diseñadas para cada modalidad de selección y que se encuentran publicadas en el link de documentación del Sistema Integrado de Gestión SIG, de la página web del ministerio. Las solicitudes incompletas, o que no cumplan con lo aquí dispuesto, serán devueltas sin tramitar, para que sean subsanadas por el área solicitante*" y en el ítem 3.8.4 Contratación directa/ Desarrollo de la contratación directa "*Mediante memorando dirigido al Coordinador del Grupo de Gestión Contractual, por parte del Director, Subdirector, Jefe de Oficina Asesor o Coordinador, según sea el caso, en la forma prevista en el procedimiento P-GC-04, remitirá la solicitud para adelantar a contratación directa … Recibida la solicitud por parte del Grupo de Gestión Contractual, y una vez subsanadas la posibles inconsistencias, se procederá a la elaboración de la minuta respectiva en el SECOP II, junto con el acto de justificación directa cuando aplique".* Adicionalmente, en el Procedimiento de Solicitud y Tramite de Procesos de Gestión con código P-GC-04 versión 10 del 24 de febrero de 2024 en el parágrafo 7 del ítem 6. Políticas de operación "*Los estudios y documentos previos deberán ser suscritos y remitidos mediante memorando por el*

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
	hoja de vida del candidato y verificar los antecedentes penales de los candidatos seleccionados para hacer parte de la entidad. *El Grupo de Gestión Humana debe garantizar que los funcionarios firmen el F-TH-01-13 Formato Declaración de Títulos Académicos, Certificación de Políticas, uso y Autorización de Tratamiento De Datos Personales. el cual incluye el compromiso con el cumplimiento de la normatividad en cuanto al tratamiento de los datos personales (Ley 1581 de 2012) y la aceptación de Políticas de Seguridad de la Información. Este documento firmado debe ser guardado en la respectiva carpeta de hoja de vida del funcionario.* *En el caso de los contratistas, proveedores y aliados, el Grupo de Gestión Contractual asegura la firma del F-GC-04-44 Formato Compromiso de Confidencialidad de Información - Contratistas el cual incluye el cumplimiento de la normatividad en el tratamiento de los datos personales (Ley 1581 de 2012) y la aceptación de Políticas de Seguridad de la Información. El formato firmado se debe guardar con el contrato o acuerdo en su respectiva carpeta, antes de iniciar sus actividades".* *Por lo anterior se solicita que el segundo párrafo del hallazgo 1(b), no haga parte del hallazgo toda vez que es un tema que ya se venía trabajando por parte de la Dirección, como ejercicio de la autogestión en busca de la mejoramiento continua, y adicionalmente no habrá forma de elaborar un plan de mejoramiento que corrija de fondo lo señalado en el párrafo 2 del hallazgo 1, por las condiciones antes expresadas.*	*Director, Subdirector, Jefe de Oficina Asesor o Coordinador, según corresponda, dirigido a la Coordinación del Grupo de Gestión Contractual a través del Sistema de Gestión de Documentos"* lo cual es reiterado en el parágrafo 5 del ítem 7.3. Desarrollo de concurso de méritos, para el caso de los funcionarios de carrera y el ítem 7.5 Desarrollo de la contratación directa por prestación de servicios profesionales o apoyo a la gestión en el caso de los contratistas. Es de aclarar que, si bien es cierto que la nueva versión de la Política de seguridad con fecha del 26 de diciembre de 2023, le asigna "*al grupo de gestión humana y al grupo de gestión contractual la responsabilidad de diligenciar, revisar y aprobar el formato de acuerdo de confidencialidad, previa a una vinculación de un funcionario público (funcionarios y contratistas)*", no es procedente lo solicitado por tecnología en cuanto a "*Por lo anterior se solicita que el segundo párrafo del hallazgo 1(b), no haga parte del hallazgo toda vez que es un tema que ya se venía trabajando por parte de la Dirección*", ya que en el marco de la auditoria, no fue remitida evidencia del envío de los acuerdos de confidencialidad a los grupos ya mencionados, por lo cual no se puede contemplar un incumplimiento por parte de los Grupos de Gestión Humana y Gestión Contractual y no se considera dejar de lado el incumplimiento detectado en cuanto a la completitud de la información teniendo en cuenta que, el área solicitante de la vinculación, en este caso tecnología, es el primer actor que interviene en el procedimiento, remitiendo la correspondiente documentación; por lo cual desde el área, se debe generar un control que permita allegar la documentación garantizando la completitud de la misma. Es de agregar que este hallazgo también surgió en la auditoria al proceso de seguridad de la información realizada en noviembre de 2022; a la fecha con el respectivo plan de mejoramiento en estado "Cumplido – no efectivo", dado que las actividades definidas aún no tienen vocación de efectividad, por lo cual se debe reformular y reprogramar.

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
2: Se evidencia incumplimiento en la documentación de las lecciones aprendidas o de bases de conocimiento de los incidentes de seguridad; lo anterior de acuerdo con lo mencionado en la Política de seguridad de la información en el ítem 4.12. Política de Gestión de Incidentes de Seguridad versión 3 del 19 de diciembre de 2022 "La STSI debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento" y en la ISO/IEC 27001:2022 en el anexo A "Aprendizaje de los incidentes de seguridad de la información: Los conocimientos obtenidos de los incidentes de seguridad de la información deben utilizarse para reforzar y mejorar los controles de seguridad de la información".	*La evidencia entregada da cuenta de las acciones tomadas producto de analizar la base de conocimiento que contiene los incidentes y eventos reportados en la herramienta de gestión ARANDA, conforme lo insinúa el hallazgo.* *Por esta razón es importante aclarar que la herramienta ARANDA, brinda una base de datos de conocimiento de incidentes, entre ellos de seguridad, ya que cuenta con la identificación del incidente y la resolución del mismo.* *La base de conocimiento permitió al ministerio de justicia tomar acciones, muchas de carácter preventivo y otras de carácter correctivo, donde el documento entregado da cuenta de lo adelantado desde la estrategia de uso y apropiación en relación con los temas de seguridad para la agenda 2023.* *Por lo anterior se solicita reconsiderar el hallazgo como parte del informe preliminar, toda vez que habría evidencia suficiente para dar cuenta de la existencia de una base de conocimiento como se acaba de mencionar. En este sentido sugerimos sea entendida esta como una recomendación donde el alcance de la misma sea que la estrategia de uso y apropiación documente la forma como se usó la base de conocimiento para trazar la estrategia en cada vigencia.*	En cuanto a la respuesta otorgada, la evidencia no "da cuenta de las acciones tomadas producto de analizar la base de conocimiento que contiene los incidentes y eventos reportados en la herramienta de gestión ARANDA" ya que es un documento en Word que relaciona prints de pantalla de tips y relaciona capacitaciones de uso y apropiación en temas tecnológicos y de seguridad de la información. Si bien es cierto que la herramienta ARANDA genera un registro y trazabilidad del incidente reportado hasta su solución (el cual es conocido por la auditora y no fue allegado para este caso en específico), en la evidencia aportada para el caso el "Resumen Ejecutivo - LECCIONES APRENDIDAS", no da cuenta del análisis realizado sobre los incidentes, no se describe la lección: ¿Qué se aprendió? ¿Fue positivo o negativo?, ¿Cuál fue la situación, el problema o el logro?, ¿Qué se puede mejorar o replicar en el futuro?, ¿Qué cambios o mejoras se pueden implementar?, ¿Cómo evitar o aprovechar esta lección en un próximo incidente?, ¿Qué cambios o mejoras se pueden implementar? Por lo cual el reporte generado por la herramienta ya mencionada se considera como un insumo y no como "base de conocimiento" por las razones anteriormente expuestas la OCI confirma el Hallazgo.
3: Se evidencia incumplimiento en la Guía de administración de riesgos de la Entidad con código G-MC-04 versión 7 del 14 de octubre de 2022, en el numeral 4.3.5 Monitoreo y revisión / riesgos de seguridad digital /	*La dirección de tecnología consiente de las dificultades que había en términos de calidad y alineación con los activos de información, promovió durante la vigencia 2023 la realización de un ejercicio de actualización de las*	Ante lo expuesto por la DTGIJ, la OCI mantiene su posición respecto al hallazgo 3, considerando que la Guía para la Administración del Riesgo del año 2022, vigente a la fecha de la auditoría, estableció lo siguiente en relación con los riesgos de seguridad digital:

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
segunda línea de defensa "*El oficial de seguridad, semestralmente debe analizar y verificar el cumplimiento de los lineamientos y de los controles definidos para el tratamiento de los riesgos de seguridad digital*" teniendo en cuenta que en la documentación allegada no se evidencia que el responsable del monitoreo realice un seguimiento semestral (dos veces al año) de la implementación de los controles para la mitigación de los riesgos de seguridad de la información como función de segunda línea de defensa.	*matrices y controles de riesgos, que facilitara el cumplimiento de la guía de administración de riesgos de la entidad, y para ello se apoyó en el oficial de seguridad quien coordino y generó como resultado una matrices y controles de riesgos para los diferentes procesos de la entidad conforme la establecido en la guía de administración de riesgos.* *En consecuencia, con lo anterior no se llevó a cabo un proceso especifico de seguimiento toda vez que no se podía actualizar y hacer seguimiento de manera simultánea.* *Sin embargo, para el periodo 2024 se está ejecutando el seguimiento, análisis, verificación y cumplimiento de los lineamientos y de los controles definidos para el tratamiento de los riesgos de seguridad digital, con una periodicidad de una vez (1) por periodo en la vigencia.* *Lo cual está establecido en la guía de administración de riesgos publicado en el SIG. Por lo anterior se sugiere eliminar el hallazgo toda vez que no existe un seguimiento en el periodo 2023 por las razones antes expuestas y en este sentido se entiende el ejercicio de seguimiento como una recomendación para el periodo 2024, y tal como se anunció, es lo que se tiene planeado para esta vigencia.*	"*Para riesgos de Seguridad digital:* *(…)* *Segunda línea de defensa: El oficial de seguridad, semestralmente debe analizar y verificar el cumplimiento de los lineamientos y de los controles definidos para el tratamiento de los riesgos de seguridad digital*. (…)" Subrayado fuera de texto Por lo tanto, la DTGIJ debió realizar una adecuada planeación que no solo involucrara la actualización de los activos de información, sino que además garantizara el seguimiento a la implementación de los controles, como lo exige la guía. En consecuencia, al no haberse realizado el seguimiento de forma semestral, se originó el incumplimiento al criterio establecido en dicho documento; adicionalmente, la respuesta otorgada por tecnología reconoce que no se realizó el proceso que dio origen al hallazgo, por lo anterior **la OCI confirma el hallazgo**.

Elaboración propia

7.3. Hallazgos

Hallazgo 1: Se evidencia incumplimiento en la propiedad asociada a la integridad de la información en cuanto a la completitud del diligenciamiento de los campos de los formatos F-TI-02-01 Versión 4 del 16 de agosto de 2023 "Planilla de control de acceso" en cuanto a "Nombre

del visitante", "Entidad y/o dependencia", "Objeto ingresado", "Funcionario que autoriza", "Firma de quien autoriza"," Trabajo realizado", "Hora de salida" y "Firma visitante".

En cuanto a los acuerdos de confidencialidad para contratistas formato con Código: F-IC-G14-02 del 19 de diciembre de 2022 con campos en blanco en los ítems 4,5,7,8 y 10 referentes a datos del contratista, datos del supervisor, número del contrato y numeral del contrato y acuerdo de confidencialidad para funcionarios formato con Código: F-IC-G14-01 del 19 de diciembre de 2022 con campos en blanco en los ítems 4 y 10 en cuanto a: fecha de diligenciamiento, nombre, número de cedula de ciudadanía, cargo y dependencia del jefe directo; lo anterior de acuerdo a la definición mencionada en la ISO/IEC 27000:2017 y conforme a la definición citada en la política de seguridad de la información del MJD "*Integridad: Propiedad de la información relativa a su exactitud y completitud*".

Hallazgo 2: Se evidencia incumplimiento en la documentación de las lecciones aprendidas o de bases de conocimiento de los incidentes de seguridad; lo anterior de acuerdo con lo mencionado en la Política de seguridad de la información en el ítem 4.12. Política de Gestión de Incidentes de Seguridad versión 3 del 19 de diciembre de 2022 "*La STSI debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento*[36]" y en la ISO/IEC 27001:2022 en el anexo A "Aprendizaje de los incidentes de seguridad de la información: *Los conocimientos obtenidos de los incidentes de seguridad de la información deben utilizarse para reforzar y mejorar los controles de seguridad de la información*".

Hallazgo 3: Se evidencia incumplimiento en la Guía de administración de riesgos de la Entidad con código G-MC-04 versión 7 del 14 de octubre de 2022, en el numeral 4.3.5 Monitoreo y revisión / riesgos de seguridad digital / segunda línea de defensa "*El oficial de seguridad, semestralmente debe analizar y verificar el cumplimiento de los lineamientos y de los controles definidos para el tratamiento de los riesgos de seguridad digital*" teniendo en cuenta que en la documentación allegada no se evidencia que el responsable del monitoreo realice un seguimiento semestral (dos veces al año) de la implementación de los controles para la mitigación de los riesgos de seguridad de la información como función de segunda línea de defensa.

7.4. 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*

[36] Política de seguridad de la información; Código: G-IC-14 versión 3 del 19 de diciembre de 2022; ítem 4.12. Política de Gestión de Incidentes de Seguridad; Pág. 34.

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.

- 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.

- Documentar el proceso de seguimiento de los controles y de actualización de la matriz de riesgo, explicando por qué ocurrió la materialización del riesgo, en lugar de simplemente generar un caso en la mesa de ayuda, como se hace actualmente.
- Se recomienda unificar y alinear los planes de tratamiento y sus actividades, guardando la finalidad de creación de un plan de tratamiento que es fortalecer los controles establecidos para la mitigación del riesgo.

Con un muy cordial saludo,

_____	_____
Cristina Alarcón Tapiero Profesional OCI Auditor Líder	Lilian Stefanny Diaz Ortiz Profesional OCI Auditor de Apoyo

---

Diego Orlando Bustos Forero
Jefe Oficina de Control Interno