La justicia es de todos

Minjusticia

# EVALUACIÓN Y VERIFICACIÓN AL PROCESO DE SEGURIDAD DE LA INFORMACIÓN CON ÉNFASIS EN LA FASE DE IMPLEMENTACIÓN

Oficina de Control Interno

2021

1. **Objetivo de la auditoría:**

   Evaluar y verificar el estado actual del Modelo de Seguridad y Privacidad de la Información en su fase de implementación.

2. **Alcance de la auditoría:**

   En el marco del objetivo definido, se evaluará el avance en la implementación del Modelo de Seguridad y Privacidad de la Información, hasta la fecha de presentación de este informe.

3. **Criterios de auditoría o parámetros normativos:**

   Para el desarrollo de la presente auditoría, se tomarán en cuenta los criterios de la Guía de Gestión de Riesgos, Guía Técnica de Sistemas de Información, Gestión de la Información y de las Comunicaciones, Guía de indicadores de gestión para la seguridad de la información, Gestión de Incidentes - MINTIC dentro de la estrategia de Gobierno en Línea, tanto como las siguientes normas: Ley 1581 de 2012; Ley 1712 de 2014 en su artículo 18; ISO 27001; ISO 27002 e ISO 27005.

4. **Metodología:**

   La metodología empleada por la Oficina de Control Interno se fundó en un levantamiento de información por medio de un cuestionario, basado en reunión previa a la generación del plan de auditoría, con el fin de indagar con el servidor encargado de la seguridad de la información del MJD, sobre el proceso de seguridad de la información con la implementación del Modelo de Seguridad y Privacidad de la Información (en adelante MSPI).

   A continuación, se relacionan las actividades realizadas en el marco de la auditoría.

   **Reunión previa a la planeación:** El 8 de octubre de 2021 se realizó una reunión con la oficial de seguridad de la información del MJD, con el fin de aclarar incertidumbres sobre el proceso, permitiendo concebir una planeación congruente.

   **Apertura de la auditoría:** En reunión del 19 de octubre de 2021, con el personal de Tecnología, se dio apertura a la auditoría, dándose a conocer el alcance y las fechas de las actividades principales, sin tener observación alguna por parte del auditado.

**Solicitud de información:** El 29 de octubre de 2021, se solicitó la información asociada al procedimiento de seguridad de la información y su avance en la implementación del Modelo de Seguridad y Privacidad de la Información, la cual fue recibida el 3 noviembre del mismo año. A continuación, se detalla la información que fue solicitada y recibida.

| N° | INFORMACIÓN SOLICITADA | RECIBIDA |
|---|---|---|
| 1 | Controles de seguridad de la información, para las diferentes aplicaciones del Ministerio de Justicia y del Derecho. | ✓ |
| 2 | Acuerdos de confidencialidad de terceros que manejen información del MJD. | ✓ |
| 3 | Gestión de riesgos de seguridad de la información | ✓ |
| 4 | Gestión de incidentes de la seguridad de la información | ✓ |
| 5 | Estrategia de Planificación y control operacional. | ✓ |
| 6 | Avance en la ejecución del plan de tratamiento de riesgos. | ✓ |
| 7 | Matrices de riesgos de seguridad de la información de la entidad. | ✓ |
| 8 | Indicadores de gestión del Modelo de Seguridad y Privacidad de la Información (MSPI). | ✓ |
| 9 | Implementación de planes de seguridad de la información 2021 | ✓ |

- **Reunión inquietudes sobre evidencias analizadas:** El 4 de noviembre de 2021 se realizó una reunión con la oficial de seguridad de la información del MJD, para aclarar algunas dudas que surgieron al realizar el análisis de las evidencias allegadas por el auditado, sin perjuicio de que durante el desarrollo de la auditoría se mantuvo un constante dialogo.

## 5. Desarrollo de la auditoría:

### Entendimiento.

Se llevó a cabo un entendimiento general del proceso de seguridad de la información mediante el modelo de seguridad y privacidad de la información del MJD (en adelante MSPI), con una reunión el 8 de octubre de 2021, con la oficial de seguridad de la información, para identificar incertidumbres con el proceso de seguridad de la información y el avance en la implementación del MSPI.

Teniendo bajo consideración el objetivo de la presente auditoría, se tomó como referencia para la evaluación del proceso el “Modelo de Seguridad y Privacidad de la Información” de MINTIC, por otra parte, la norma técnica colombiana NTC ISO/IEC 27001, normatividad establecida en los criterios para la presente

auditoría. Dicho proceso de implementación del modelo inicia con la fase de planificación y termina con la fase de mejora, dando lugar al ciclo de operación del MSPI.

Para la evaluación y verificación del proceso de seguridad de la información, se estableció en el alcance de la planeación, evaluar y verificar el proceso de seguridad de la información con énfasis en la fase de implementación del MSPI.

Teniendo en cuenta lo anterior, se desarrolló la auditoría con base en el desarrollo de las actividades determinadas en 7 capítulos que se discriminan así:

### 5.1 Seguridad de la información en las aplicaciones del Ministerio de Justicia y del Derecho.

La seguridad en las aplicaciones del MJD, hace referencia a aprobar medidas y características de seguridad, las cuales buscan que las aplicaciones sean más seguras al encontrar, corregir y mejorar su seguridad, para evitar vulnerabilidades de seguridad contra amenazas, tales como la modificación y el acceso no autorizado.

El MINTIC en su “Guía Técnica de Sistemas de Información” recomienda para la disponibilidad de la información en los sistemas de información, “*Asegurar el buen funcionamiento y disponibilidad de los componentes de software del Sistema de Información, que tienen por responsabilidad el registro de los logs, controlando la manipulación y el fallo seguro de los mismos cuando se presenten errores que interrumpan el registro de los eventos*”. El tener registros “logs” adecuadamente, permitirá identificar problemas operativos, incidentes de seguridad, entre otros eventos relevantes para la entidad, y recopilar información útil para la resolución de dichos problemas.

Para el análisis de este punto se solicitó la política de seguridad de la información, controles de la matriz de riesgos, validaciones de acceso a los sistemas de información del MJD (seleccionando una muestra), plan de seguridad y privacidad de la información y logs.

Los controles de seguridad de la información para las aplicaciones del MJD se encuentran establecidas en la política de seguridad de la información y la matriz de riesgos; a continuación, se realiza un análisis de cada control, luego de analizar las evidencias y entrevistar a los funcionarios de tecnología encargados de la seguridad de la información y las aplicaciones del MJD así:

| POLÍTICAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN RELACIONADAS A SISTEMAS DE INFORMACIÓN | | |
|---|---|---|
| **CAPITULO** | **CONTROL** | **OBSERVACIÓN OCI** |
| POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO A SISTEMAS INFORMACIÓN Y APLICATIVOS: | La STSI con el apoyo de las áreas funcionales de los sistemas de información y aplicaciones, debe velar por que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, así mismo debe ejecutar mecanismos para que los desarrolladores, tanto internos como externos, acojan las buenas prácticas de desarrollo seguro en los productos generados, con el fin de controlar el acceso lógico y evitar accesos no autorizados cuando estos estén en producción. | Se tienen definidas políticas y controles para el acceso a los sistemas de información; por otro lado, están los controles de la matriz de riesgos, observando que no se encuentran controles para todas las aplicaciones del MJD, hallando controles mal definidos, que no tienen que ver con el riesgo y la amenaza determinados, como es el caso del "Sistema de información de Drogas de Colombia", se debe reevaluar la matriz de riesgos.<br>Se valida el reporte de incidentes de seguridad de la información 2021 y no se observan casos reportados sobre acceso a aplicaciones. |
| | La STSI debe establecer un instructivo para la asignación de accesos a los sistemas de información y aplicativos de MINISTERIO DE JUSTICIA Y DEL DERECHO. | No se cuenta con el instructivo, pero cada sistema de información cuenta con los manuales y en ellos se contempla la parametrización de los accesos, la persona encargada del directorio activo, al crear usuarios y designar accesos tiene en cuenta las observaciones establecidas en la solicitud de acceso. |
| | Establecer ambientes separados a nivel físico y lógico para pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes | Se evidencia que se cuentan con los ambientes separados tanto de pruebas como de producción, en aplicaciones y en bases de datos. |
| | La STSI debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles, es decir que las personas responsables para los ambientes pruebas y no tengan acceso a producción y así mismo que los menús muestren los mensajes de identificación apropiados para reducir el riesgo de error. | Se encuentran definidos en el "Procedimiento Puesta en Producción de Software", en el cual se discrimina el acceso por roles, se valida el reporte de incidentes de seguridad 2021, en el que no se evidencian incidentes de este tipo. |
| | 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. | Se cuentan con los repositorios, se observa que se encuentran alojados en el servidor, una vez se valida su acceso, se evidencia que estos están restringidos, teniendo acceso el personal de infraestructura y el personal de sistemas de información. |
| | Los administradores y custodios de los servicios de información y aplicaciones deben autorizar el acceso a sus sistemas de información o aplicativos de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los | Se evidencia las solicitudes realizadas a mesa de ayuda por los líderes funcionales autorizando el acceso, cuyos controles se encuentran contemplados en el procedimiento "Gestión de acceso a recursos informáticos". |

| | | |
|---|---|---|
| | procedimientos establecidos. | |
| | Las áreas funcionales y el oficial de seguridad de la información deben monitorear periódicamente (cada cuatro meses) los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos. | A partir del segundo semestre del 2021 no se está realizando este monitoreo, debido a q no se llevó a cabo la contratación de la herramienta, la cual estaba implementada desde julio 2020 hasta julio del 2021. La no adquisición de la herramienta es analizada más adelante, en el capítulo “5.6 Implementación de planes de seguridad de la información 2021” |
| CONTROL CONTRA SOFTWARE MALICIOSO | El MINISTERIO DE JUSTICIA Y DEL DERECHO proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre los funcionarios públicos, colaboradores y terceros frente a los ataques de software malicioso. | Se tienen controles como antivirus, firewall, directorio activo, y los mantenimientos realizados a la infraestructura; la parte de ethical hacking no se realizó para esta vigencia ya que no se llevó a cabo la contratación (declarada desierta), por ende, no se realizó escaneo de vulnerabilidades a estos controles, para determinar su correcta funcionalidad, fortaleciendo la seguridad del MJD. Por otra parte, se observa la matriz de riesgos, validando el riesgo “Actos Vandálicos y/o terrorismo” encontrando que no tiene definido controles. Se validan los casos reportados sobre seguridad de la información, para la presente vigencia no se han materializado por contagio de software malicioso, sin embargo, en los reportes realizados por los usuarios del MJD a mesa de ayuda, se presenta un alto índice de correos maliciosos (Phishing), se recomienda validar el control, los filtros spam; se advierte una posible materialización del riesgo debido al alto reporte de correos phishing. |
| | STSI debe contar con herramientas tales como antivirus, antimalware, anti spam y antispyware que reduzcan el riesgo de contagio de software malicioso y respalden la Seguridad Digital contenida y administrada en la plataforma tecnológica | Se tienen las herramientas antivirus, antimalware, anti spam y antispyware; como se mencionó anteriormente, se necesita un análisis de vulnerabilidades ethical hacking, para determinar la efectividad de los controles que se tienen implementados a través de estas herramientas, para prevenir la materialización de riesgos y que se pueda bajar el índice de reportes de correos phishing. |
| | 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. | Se realizó escaneo por el antivirus Kaspersky al servidor “VMMJDSFMISI IP 192.168.8.106”, el cual arrojo como resultado 0 vulnerabilidades, 0 ataques y 0 virus detectados. |
| | STSI, a través de sus funcionarios públicos, colaboradores y/o terceros, debe asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, anti | Se ingresa al antivirus para intentar realizar modificaciones, evidenciando que este inhabilita las opciones de configuración; solo tienen acceso los usuarios establecidos con el rol de administrador. |

| | | |
|---|---|---|
| | spam y antimalware. | |
| | El software de antivirus, anti APT y demás controles de seguridad perimetral posea tengan las últimas actualizaciones, para mitigar las vulnerabilidades de la plataforma tecnológica. | Se evidencia que el antivirus para amenazas persistentes avanzadas, presenta en su consola el estado actualizado y activo. |
| | STSI, en cabeza de la Mesa de Servicios, debe mantener actualizada una lista del software autorizado dentro de la Entidad. | Se comprobó que se cuenta con la lista del software autorizado para actuar en el MJD, adicional la lista contiene el software que se tiene instalado por cada equipo. |
| | El Oficial de Seguridad de la Información, debe implementar y documentar lineamientos para verificar la información relacionada con el software malicioso, y asegurarse de emitir boletines de advertencia informativos. | Se detectó la campaña de sensibilización, en el que se envían boletines diarios por correo electrónico. Se evidenció sesiones de entrenamiento y sensibilización a todos los usuarios del sector justicia |
| | El Oficial de Seguridad de la Información y el personal de apoyo deberán de manera periódica concientizar a los funcionarios contratistas y terceros sobre las falsas alarmas que se pueden generar, y las acciones a tomar en caso de que se presenten. | En la misma campaña de sensibilización, se realizó la concientización de alarmas y acciones a tomar, sesiones hechas por la oficial de seguridad y por el proveedor externo de uso y apropiación. |
| | STSI, en cabeza del Oficial de Seguridad de la Información, tomará las acciones pertinentes para contener un incidente asociado a software malicioso en caso de que se presente con el fin de evitar impactos catastróficos. | El primer nivel (mesa de ayuda) que recibe el reporte, informa a la oficial de seguridad en todo lo relacionado con seguridad de la información, quien valida y dependiendo del impacto reportado involucra los demás niveles de soporte, de ser necesario. |
| | Los usuarios tienen prohibido la instalación de software en los equipos del MINISTERIO DE JUSTICIA Y DEL DERECHO, en caso de requerirlo, deben escalar la solicitud a la mesa de servicios de la entidad, quien validará, con el grupo de Seguridad de la Información, si el software requerido está o no autorizado para su uso sin que represente un riesgo de Seguridad Digital. | Se tiene la restricción para la instalación de software, al momento que un usuario intente realizar la instalación, le aparecerá una ventana solicitando el logueo de un usuario administrador, si no lo ingresa, el sistema no permitirá la instalación del Sw. |
| | Los usuarios de los servicios tecnológicos del MINISTERIO DE JUSTICIA Y DEL DERECHO no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware y anti spam definida por STSI; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios. | La configuración del antivirus permite a los usuarios realizar escaneo para la búsqueda de vulnerabilidades, pero no permite el acceso a configuraciones del sistema. |

| | | |
|---|---|---|
| REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN: | El MINISTERIO DE JUSTICIA Y DEL DERECHO realizará monitoreo permanente del uso que dan los funcionarios públicos, colaboradores y terceros, a los recursos de la plataforma tecnológica y los sistemas de información de la Entidad. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos por dichos registros. | Se está dando inicio a la parte de implementación del modelo de seguridad de la información, el monitoreo se realiza de forma manual; hasta ahora se está comenzando a entender el comportamiento de los usuarios, pero no se tiene un cubrimiento total al monitoreo, adicional, no se cuenta con un monitoreo automatizado, el cual permite un análisis más profundo sobre los eventos de interacción entre los sistemas de información y los usuarios, por otra parte, permite la custodia de los registros generados. |
| | STSI definirá la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la Entidad. El personal de apoyo de STSI se reunirá cada dos meses para analizar los resultados del monitoreo efectuado. | El monitoreo se está realizando mensual, no es un análisis profundo que permita identificar vulnerabilidades, posibles fallas que permitan el mejoramiento operativo y de seguridad en los sistemas de información.; adicional, los eventos que presentan los registros carecen de información; no se cuenta con un monitoreo automatizado debido a que no se llevó a cabo el contrato de ethical hacking, el cual se puntualizara más adelante. |
| | STSI, en cabeza del Oficial de Seguridad de la Información, el personal de apoyo de Infraestructura Tecnológica y el personal de apoyo de Sistemas de Información, debe determinar los eventos que generan registros de auditoría en los recursos tecnológicos y los sistemas de información de MINISTERIO DE JUSTICIA Y DEL DERECHO. | Se analizan los registros solicitados para el análisis de esta auditoría y los registros no tienen habilitado o configurado eventos relevantes que generen registros de auditoría, como se analiza más adelante sobre los registros (logs). |
| | STSI, en cabeza del Oficial de Seguridad de la Información, el personal de apoyo de Infraestructura Tecnológica y el personal de apoyo de Sistemas de Información debe definir de manera mensual cuál monitoreo se realizará a los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la Entidad. Así mismo, deben reunirse para analizar los resultados del monitoreo realizado. | Como se mencionó anteriormente, los registros no contemplan eventos que permitan un análisis de los registros generados por los diferentes sistemas de información. |
| | STSI debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información del MINISTERIO DE JUSTICIA Y DEL DERECHO. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado. | Se encuentran en onedrive con acceso restringido; el acceso lo tiene el personal encargado de los de sistemas de información y la oficial de seguridad. |

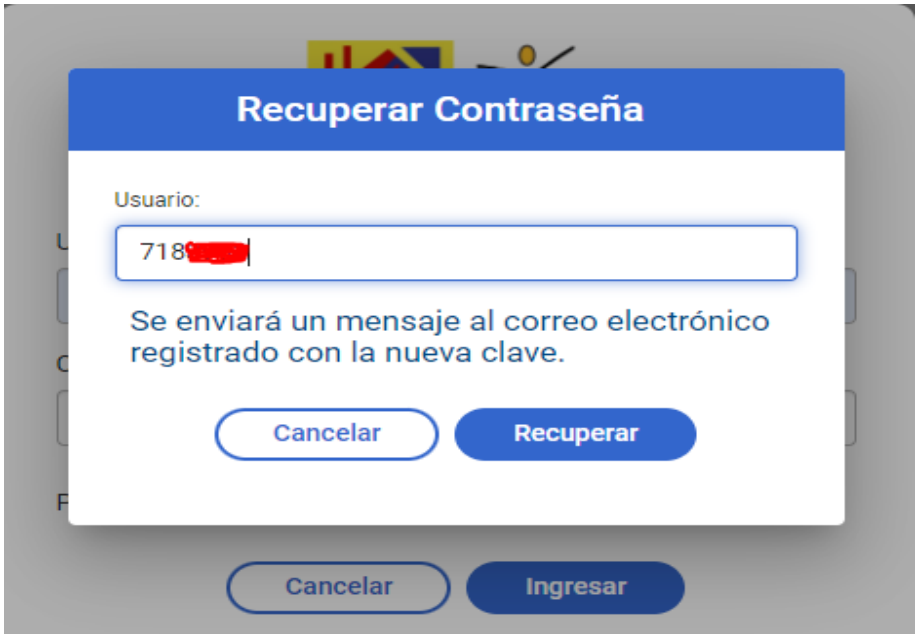
| | | |
|---|---|---|
| | STSI en cabeza del personal de apoyo de Sistemas de Información, debe garantizar que los desarrolladores (internos y externos), generen registros (Log) de auditoria de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros. | Como se viene mencionando, existen los registros, pero no cumplen con la habilitación de eventos que permitan su análisis; su integridad es protegida con acceso restringido como se comentó anteriormente. |
| | Los desarrolladores (internos y externos) deben habilitar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por STSI. | Estos eventos son los que se vienen manifestando que no se encuentran habilitados en los registros, lo cual se detalla más adelante. |
| CONTROL DE TRANSFERENCIA DE LA INFORMACIÓN | MINISTERIO DE JUSTICIA Y DEL DERECHO busca la protección de la información en el momento de ser transferida o intercambiada con las otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información. | Se establecen políticas y controles para el intercambio de información; pero se han materializado vulnerabilidades en la perdida de información con correos electrónicos hacia otras entidades, la OCI ha tenido conocimiento de estos sucesos; validando la matriz 2021 de casos reportados en seguridad de la información, estos no se encuentran reportados, por lo cual, se debe validar si los usuarios del MJD, tienen el conocimiento necesario para el reporte de casos de seguridad de la información, y si el plan de sensibilización está siendo captado por todos los usuarios del MJD. |
| | Los Funcionarios, Contratistas y Terceros con accesos a la información del Ministerio de Justicia y del Derecho deben tener en cuenta la “Política de tratamiento y protección de datos personales”, el “Procedimiento de seguridad de la información” de La Dirección de Tecnologías y Gestión de Información antes del intercambio de información con internos y externos a la Entidad, así mismo, se deben utilizar los medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de esta. | Se evidencia que se tienen proyectados formatos de acuerdos de confidencialidad, pero aún no han sido implementados, por consiguiente, funcionarios y contratistas vienen desarrollando funciones de intercambio de información, sin tener presente las políticas y procedimientos, lo que conlleva a presentar vulnerabilidades en el cumplimiento de las normas sobre protección de datos personales. Se utilizan los medios autorizados por el MJD para el intercambio de información, pero como se mencionó anteriormente, se han presentado casos de perdida de información en correos electrónicos hacia otras entidades. |
| | Los propietarios de los activos de la información deben asegurarse que el intercambio de información Digital solamente se realice mediante la herramienta autorizada por la STSI | Se evidencia que los propietarios de activos como coordinadores, jefes de oficina y directores, emplean las herramientas autorizadas por la STSI, a su vez, se validaron los eventos reportados en seguridad de la |

| | | |
|---|---|---|
| | | información, observando que no se registraron casos de perdida de información o alteración por utilizar herramientas inapropiadas. |
| | El Oficial de Seguridad de la información debe verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el propósito por el cual fue enviada. | En los formatos de acuerdos de confidencialidad que se están implementando, se encuentra una clausula sobre disposición final de la información, pero hasta el momento no se cuenta con evidencias de destrucción de información por terceros, de igual forma estos formatos están en proceso de aprobación. Por lo anterior, se evidencia vulnerabilidad en la confidencialidad e integridad de la información. |
| | La STSI, debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas. | La OCI durante sus informes de seguimiento y evaluación, ha refutado la no interoperabilidad entre los diferentes sistemas de información del MJD, que permitan el intercambio de información generando transformación de datos; es por esto que en el informe de “Evaluación y verificación a Hw, Sw e infraestructura tecnológica” se obtuvo un hallazgo de interoperabilidad en los sistemas de información. Aún se sigue manifestando esta necesidad, claro ejemplo es el módulo de auditoría que se viene desarrollando para la OCI, en el que la STSI confirmó que, para la puesta en producción, este no será interoperable con ningún sistema de información del MJD, siendo la interoperabilidad una de las solicitudes que la OCI diligenció en el documento de requerimientos. |
| | Los usuarios no deben realizar intercambio de información de MINISTERIO DE JUSTICIA Y DEL DERECHO por medios diferentes a los establecidos por la Dirección de Tecnologías y Gestión de Información. | No se evidencia el reporte de algún caso debido a la no utilización de medios autorizados; por otra parte, no se puede realizar monitoreo a este control debido a que no se contó con la contratación de la herramienta de vulnerabilidades de ethical hacking y de los registros (logs) ya que no cuentan con los eventos necesarios para la identificación de este tipo de vulnerabilidades ocasionadas por los usuarios finales. |
| MENSAJERÍA ELECTRÓNICA | La STSI debe implementar controles que eviten el acceso no autorizado a los servicios de mensajería autorizados por la Entidad (Correo institucional, Proveedor Drive Institucional y FTP autorizados) con el fin de evitar cualquier modificación o denegación del servicio. | Se evidencia la realización de sesiones con Microsoft para las configuraciones de las herramientas adquiridas con ellos, se recibió la documentación de las políticas implementadas para el acceso a estas herramientas. Sin embargo, como se mencionó anteriormente, se debe validar el alto índice de correos con phishing, ya que alguno de estos puede llegar a materializarse. |

| | | |
|---|---|---|
| | La STSI debe velar por que los controles de autenticación desde redes públicas hacia los servicios de la entidad sean fuertes y en lo posible, contar con doble factor de autenticación. | Estas configuraciones fueron realizadas bajo el respaldo de Microsoft, de igual manera el proveedor entrego la documentación de los controles realizados en diferentes sesiones con el equipo de infraestructura y oficial de seguridad, la cual es confidencial entre las partes involucradas. |
| | El equipo de seguridad de la información debe velar por la implementación de mecanismos que permitan garantizar la integridad y no repudio de la información, mediante el uso de firmas digitales. | Se evidencia en la matriz de reportes de seguridad de la información que no se han realizado reportes de integridad en firmas digitales, sin embargo se realizó un control de análisis de vulnerabilidades a la herramienta EPX, el cual arrojo 0 vulnerabilidades. |
| REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN | Todos los sistemas de información o desarrollos de software deben tener un área funcional responsable de la administración y la STSI será el responsable de la custodia dentro de la Entidad. | Se cuenta con un catálogo de sistemas de información, en el que se contempla la historia del sistema de información, detallando el responsable funcional y el responsable técnico; este catálogo reposa en los archivos digitales de la Dirección de Tecnología el cual fue visualizado por el auditor, pero no entregado como evidencia. |
| | La STSI debe velar porque la entrega de los ambientes de pruebas y producción estén libres de vulnerabilidades en sus sistemas operativos. | Se evidenció que para la entrega del sistema de información misional, se realizó análisis de vulnerabilidades con la herramienta “SonarQube” por el proveedor The Factory. |
| | La STSI debe velar porque los proveedores de los servicios de desarrollo de Sistemas Información realicen y certifiquen pruebas de vulnerabilidades al producto de software entregado, éste deberá contar con todas las vulnerabilidades remediadas. | Como se comentó anteriormente, se llevó a cabo las pruebas de vulnerabilidades para el sistema de información misional, el cual arrojo 0 vulnerabilidades en todos sus sistemas de información. |
| | La STSI debe velar porque todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas, soportadas, actualizadas y reconocidas en el mercado. | Dentro de los estudios previos se menciona la plataforma tecnológica q maneja el MJD la cual está licenciada; por otra parte, le fue solicitado al proveedor el ambiente de desarrollo por parte de ellos contenga los mismos ambientes del MJD y las mismas versiones. |
| | La STSI debe exigir toda la documentación requerida para uso y administración de los sistemas de información a los proveedores externos. | Cada sistema de información cuenta con una carpeta, cada una contiene una lista de chequeo con la documentación que debe tener cada sistema de información; esta se encuentra con acceso restringido. |

Adicional a lo mencionado anteriormente en el análisis de controles de la política de seguridad, se selecciona una muestra de los sistemas de información, para probar el acceso al Sistema de Información de la Conciliación en Equidad SICEQ, y a los atribuidos a Asuntos Internacionales, Casas de Justicia y Centros de Convivencia Ciudadana; inicialmente, se probó el acceso con un usuario que se encuentra inactivo, para comprobar que el sistema no permita el acceso de usuarios que se encuentren en ese estado, al tratar de ingresar con las credenciales de dicho usuario, el sistema arroja un mensaje de error en inicio de sesión, como se observa en la siguiente imagen.


Se comprueba que el control de accesos temporales y la inactividad de usuarios se desempeña efectivamente. Por otra parte, si bien no permite el acceso por que el usuario se encuentra inactivo, el sistema ofrece la opción de recuperar contraseña enviando un mensaje al correo electrónico registrado, luego de lo cual se procede a realizar la prueba de recuperación de contraseña, como se ilustra en la siguiente imagen (se oculta el usuario por seguridad ya que son datos personales del auditor).



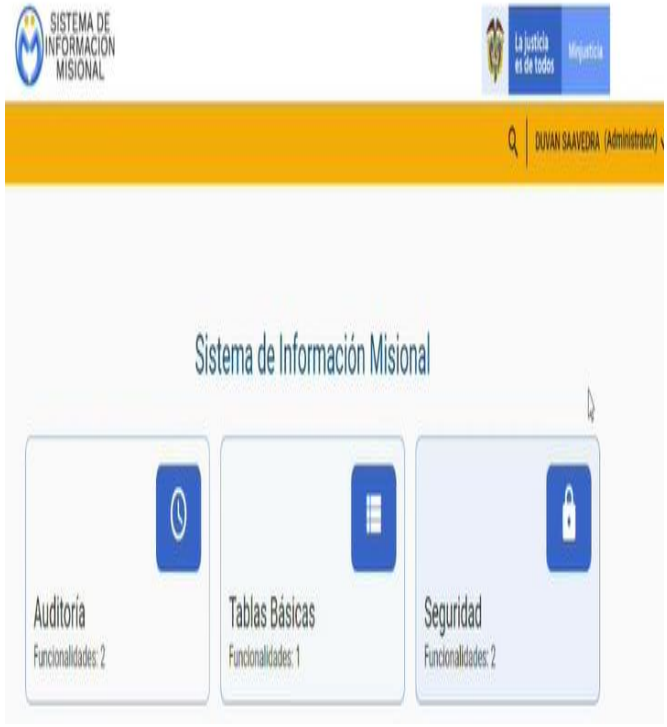

Al ingresar los datos de usuario y darle en la opción recuperar, el sistema arroja el mensaje “Proceso Exitoso”, como se evidencia en la siguiente imagen.


Si bien el sistema informa que el proceso fue exitoso, el correo para recuperar la contraseña no se recibió. Debido a lo anterior, pueden ocurrir varias posibilidades; una de ellas es que el sistema no envió el correo por tratarse de un usuario inactivo, pero no debería informar un proceso exitoso cuando no lo

es; la otra posible situación es que la opción de recuperación de contraseña no está funcionando, por ende, no envía los correos para el proceso de recuperación de contraseña.

Se recomienda realizar una validación a este proceso de recuperación de contraseña que ofrecen los diferentes sistemas de información del SIM, en el que se valide el correcto funcionamiento y los mensajes que arroja para que sean coherentes con su funcionalidad.

Se realiza prueba de acceso con el usuario administrador el cual ingresa sin inconvenientes, como se ilustra en las siguientes imágenes.


Al intentar ingresar con una contraseña diferente arroja error, como se observa en las siguientes imágenes.



Una forma de realizar un análisis más profundo es la validación de “logs”, los cuales nos manifiestan el comportamiento de los sistemas o programas; esta información no es visible para los usuarios, pero sí suele estar relacionada con su actividad (es decir, estado actual de programas, seguridad, accesos, conectividad de redes, etc.). La Norma Técnica NTC-ISO-IEC 27001, en su anexo A.12.4 “Registro y seguimiento” tiene como objetivo el registrar eventos y generar evidencias, para el control de las actividades de los usuarios, sistemas de información y la protección de la información. A su vez, el MINTIC en su fortalecimiento con la gestión de las tecnologías de la información, expone a las entidades del estado la “Guía Técnica de Sistemas de Información - Trazabilidad” para que las entidades cuenten con directrices referentes al manejo de los registros de errores, eventos y trazabilidad de sus Sistemas de Información.

Es por esto que, para realizar un análisis más profundo sobre los diferentes eventos de los sistemas de información con los usuarios, en los que se pueda validar la gestión y control de la información, amenazas de red o virus, fugas de información o comportamientos inadecuados que causen errores, de la muestra seleccionada para los sistemas de información del Ministerio de Justicia y del Derecho, se realizó la solicitud de logs para su análisis. Los cuales fueron recibidos en archivo Excel, extraídos de los sistemas de información solicitados; dicha matriz Excel cuenta con más de 227.000 registros, solo para el mes de junio del 2021. Al validar los campos de la matriz de logs, se evidencia que esta extrae o exhibe datos como: el id de usuario, rol, fecha de ingreso, aplicación

que se está consultando, módulo de la aplicación y acción, como se ilustra en la siguiente imagen.

| | | | | | |
|---|---|---|---|---|---|
| Fecha inicio | 1/6/2021 | | | | |
| Fecha fin | 30/6/2021 | | | | |
| Fecha generación | 27/10/2021 | | | | |
| | | | | | |
| **Usuario** | **Rol** | **Fecha Ingreso** | **Aplicación** | **Módulo** | **Accion** |
| 25156167 | CRI | 1/6/2021 07:04 | Casas de justicia | Casos Asignados | Adicionar |
| 25156167 | CRI | 1/6/2021 07:04 | Casas de justicia | CRI | Adicionar |
| 25156167 | CRI | 1/6/2021 07:05 | Casas de justicia | CRI | Adicionar |
| 25156167 | CRI | 1/6/2021 07:05 | Casas de justicia | Casos Asignados | Adicionar |
| 1077877363 | CRI | 1/6/2021 07:06 | Casas de justicia | CRI | Adicionar |
| 1077877363 | CRI | 1/6/2021 07:06 | Casas de justicia | CRI | Adicionar |
| 1077877363 | CRI | 1/6/2021 07:06 | Casas de justicia | Casos Asignados | Adicionar |

Una vez analizados los registros, como se mencionó en el análisis de políticas y controles, se halló que estos carecen de información para lograr realizar un análisis sobre los diferentes eventos que puede presentar un sistema de información, ya que no se observan datos como: su ubicación/IP, eventos como actividades del sistema, registros de intentos de acceso al sistema exitosos y rechazados, registros de datos exitosos y rechazados y otros intentos de acceso a recursos, archivos a los que se tuvo acceso y el tipo de acceso, direcciones y protocolos de red, alarmas accionadas por el sistema de control de acceso, entre otros.

Por lo anterior, se determina que los registros (logs) referentes a los sistemas de información no presentan una configuración o habilitación adecuada que permita el análisis de los diferentes eventos de los sistemas de información; se debe establecer el alcance de controles para la habilitación de la información necesaria para el análisis de eventos, definiendo las actividades que deben ser registradas, información relevante que debe ser incluida en el registro y formato de la información registrada. Se recomienda tener en cuenta los lineamientos que revela la “Guía Técnica de Sistemas de Información” del MINTIC, la cual ilustra la estructura que se debe tener para el registro de mensajes, tipos de mensajes, eventos del sistema de información, eventos de seguridad de la información, entre otros. Lo anterior evidencia que se infringe la política de “*Registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información*”, incluida dentro de la política de seguridad de la información del

MJD, debido a que los registros de eventos (logs) actuales no ostentan la información propicia para realizar un análisis de los eventos presentados en los sistemas de información, ni para ser utilizada en caso dado de presentarse un incidente en el que se necesite validar esta información. A su vez, se incumple con el control del anexo A.12.4 "*Registro y seguimiento*" de la ISO 27001.

Se concluye que, una vez analizadas las evidencias allegadas por el auditado, se evidenció que el Ministerio de Justicia y del Derecho, cuenta con la definición de políticas, lineamientos y controles en seguridad de la información para sus diferentes Sistemas de Información, sin embargo, al validar su efectividad, se evidenció que aún no se cuenta con la implementación del Modelo de Seguridad y Privacidad de la Información, se detectan incumplimientos en sus políticas y controles; la matriz de riesgos debe ser revalidada, al identificarse definiciones inapropiadas en riesgos, amenazas y controles; no se fortaleció la seguridad de la información con la adquisición de ethical hacking, a su vez, el incumplimiento de la política de "*Registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información*", lo cual genera vulnerabilidad al no contar con monitoreo de registros, análisis de vulnerabilidades que permitan el fortalecimiento de controles.

**5.2 Intercambio de Información.**

La norma ISO 27001, estándar internacional para la seguridad de la información, menciona que se debe "*mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa"*; a su vez, el Modelo de Seguridad y Privacidad de la Información establecido por MINTIC, instaura el lineamiento de acuerdos de intercambio de información "*La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer los Acuerdos de Nivel de Servicio (ANS) con las dependencias o instituciones para el intercambio de la información de calidad, que contemplen las características de oportunidad, disponibilidad y seguridad que requieran los Componentes de información."*

Se valida si el MJD cuenta con lineamientos políticas y controles para el intercambio de información, encontrando que: dentro de la política de seguridad de la información, numeral 4.9 "*Política de Seguridad en las Comunicaciones*", a su vez, en el mismo numeral se establecen acuerdos de transferencia de información; y en el Sistema Integrado de Gestión reposa el procedimiento para el intercambio de información.

Se observa que los documentos mencionados, tienen en común el mismo lineamiento; "INTEROPERABILIDAD", la OCI desde vigencias pasadas ha venido manifestando en sus diferentes informes de Seguimiento y Evaluación, no

solo con los procesos que tienen que ver con Tecnologías, si no, con los demás procesos como misionales, estratégicos y de apoyo que involucren sistemas de información: La falta de interoperabilidad en el Ministerio de Justicia y del Derecho ha llevado a dificultades en la realización de trámites y gastos en tiempos y recursos, la OCI desde sus primeros informes identifico que las dependencias se encontraban en islas informáticas, razón por la cual se ha reiterado informe tras informe, solicitando el replanteamiento en la adquisición de software, en el que se deje atrás la falta de visión sistémica y surja la optimización de procesos para el intercambio de información dentro y fuera de la Entidad, con el propósito de facilitar la interlocución con el ciudadano brindándosele información de calidad, y por consiguiente estar a nivel de las grandes entidades del estado Colombiano. Si bien, la Dirección de Tecnología y Sistemas de Información, ha hecho el esfuerzo de seguir las recomendaciones del Marco de Interoperabilidad para Gobierno Digital, aún no se reflejan los resultados, no obstante, se tenía la expectativa con la adquisición del módulo de auditoría, en el que se siguió manifestando la necesidad de un software interoperable con los diferentes Sistemas de Información de la Entidad, permitiendo la transformación de datos, que hasta la vigencia actual no se tendrá. Por lo anterior, se puede afirmar que se cuenta con los lineamientos y políticas para el intercambio de información; pero los sistemas de información con los que se cuenta no permiten el tratamiento de datos. Adicional, como se comentó anteriormente en el cuadro de análisis a los controles de la política de seguridad de la información, la OCI tuvo conocimiento sobre la perdida de información al enviar información por medio del correo electrónico hacia otra entidad; si bien este caso no se encontró en los reportes a mesa de ayuda sobre seguridad de la información, se recomienda validar si el plan de sensibilización y el conocimiento al procedimiento de reportes a fallas en la seguridad de la información, es claro para todos los funcionarios y contratistas del MJD.

Por otra parte, al validar la información allegada por el auditado, se identifican 4 formatos de acuerdos de confidencialidad para: proveedores, funcionarios, convenios y contratistas, los cuales se encuentran en proceso de aprobación, por lo cual, dichos formatos no cuentan con codificación. Se validó que la Dirección de Tecnología cuenta con los acuerdos de nivel de servicio, y que estos se encuentren contemplados dentro de la política de seguridad de la información.

A continuación, se selecciona de la matriz de riesgos el activo “Modelo de gestión de información en justicia - Acuerdos de Intercambio de información” para su análisis ya que se encuentra dentro del proceso “Proveer información oportuna, confiable, veraz y accesible a clientes internos y Externos del Ministerio de justicia y del derecho”

| Proceso | Proveer información oportuna, confiable, veraz y accesible a clientes internos y Externos del Ministerio de justicia y del derecho | Observación OCI |
|---|---|---|
| Riesgo | Pérdida de información debido a errores en la ejecución del procedimiento de backup, fallas en el software de backup. | Aunque el riesgo se encuentra identificado, se observa que está incompleto, ya que la única perdida de información no es el backup; se debe tener en cuenta la perdida de información debida a desastres naturales; Perdida de información. por Fraude y robo de información. Se debe revalidar los riesgos asociados al proceso. |

El riesgo analizado se encuentra evaluado como inherente bajo, el cual no cuenta con controles, se realizan validaciones observando que el riesgo se encuentra incompleto. Se recomienda contemplar otros riesgos que permitan la protección del activo.

Se concluye que el MJD tiene definido acuerdos para el nivel de servicio, lineamentos, políticas, controles y procedimiento para el intercambio de información; pero no cuenta con una herramienta que permita el tratamiento de datos institucional, que conciba en el intercambio de información de calidad para el MJD.

### 5.3 Gestión de incidentes de la seguridad de la información

Para este punto del informe, se realiza un contexto de la documentación con la que cuenta el Ministerio de Justicia y del Derecho, siendo uno de ellos el procedimiento "*Gestión de Incidentes*" para el proceso de "*Gestión de la Información y de las Comunicaciones*", cuyo responsable del procedimiento es la Subdirección de Tecnologías y Sistemas de Información STSI, dicho procedimiento está basado en la guía "*Gestión de Incidentes*" del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC.

Para el análisis de este punto, se realizó la solicitud de información respecto a los incidentes presentados durante la vigencia 2021; dicha información fue solicitada a mesa de ayuda por la oficial de seguridad del MJD; la evidencia es allegada en una matriz Excel, en la que se identifican 30 registros correspondientes a incidentes de seguridad presentados durante la actual vigencia; donde la mayoría corresponden a reportes por recibimiento de correos electrónicos con phishing.

Se validan los registros de incidentes, encontrando que la matriz cuenta con un parámetro llamado urgencia, observando que, durante lo que va de la vigencia 2021, se han presentado de los 30 registros de incidentes, dos incidentes que se materializaron, uno relacionado con la disponibilidad de la página web y el otro con la disponibilidad de información en la intranet para el Grupo de Servicio al Ciudadano; los demás están calificados como bajos. Se inspeccionan los dos incidentes encontrando lo siguiente:

El primer incidente materializado se presentó el 7 de mayo del 2021 a las 10 pm (Según el registro de la matriz de incidentes de mesa de ayuda), catalogado como incidente crítico, el cual se trata de la afectación de la disponibilidad de la página Web del MJD. Mesa de ayuda contacta al proveedor de la infraestructura (BEXT); a su vez, mesa de ayuda involucra a la oficial de seguridad de la información del MJD para su gestión. La afectación se llevó a cabo hasta el 11 de mayo de 2021 a las 8:36 pm, hora en la que se encuentra cerrado el incidente. Al indagar, se observó que este riesgo nunca se había materializado, el cual se encontraba contemplado en la matriz de riesgos, pero al ser un riesgo bajo no contaba con controles. Una vez, materializado el incidente que, al parecer, fue un ataque de denegación de servicios por la comunidad de Ciberactivismo y Hacktivismo “Anonymous”, afectando la disponibilidad del servicio; las medidas que se tomaron para controlarlo fueron las siguientes: Se modificó el direccionamiento del dominio minjusticia.gov.co al firewall del Ministerio de Defensa, luego se cambiaron las IP´s relacionadas al sitio web para dejar de recibir ataques masivos desde diferentes partes del mundo, puesto que ya había un descubrimiento por parte de los ciberatacantes, lo cual provocaba la caída del servicio cada vez que se reestablecía. La OCI evidenció que, una vez solucionado el incidente, se actualizó la matriz de riesgos, cambiando la criticidad del riesgo inherente a alto y definiendo el control (Controles de red.), El cual es evaluado en el informe de “Evaluación y verificación al proceso de modelación del riesgo en el Ministerio de Justicia y del Derecho”.

El segundo incidente que conllevó a la materialización del riesgo, fue registrado el 14 de julio del 2021, a las 8:46 am, afectando la disponibilidad de información en la intranet; la Subdirección de Tecnología y Sistemas de información llevó a cabo las siguientes medidas para controlar el incidente: se informó al profesional especializado de la mesa de ayuda; por otro lado, se informó al área funcional afectada; se decide realizar copias de respaldo en un sharepoint, para el acceso a los documentos, descargándolos y dejando copias físicas, por último, junto con mesa de ayuda y la STSI se realizó seguimiento hasta el restablecimiento del servicio; el incidente fue solucionado, pero no fue registrado el cómo fue solucionado en la matriz de incidentes. Luego, como en el anterior incidente, se relacionó en la matriz de riesgos para establecer el control (Revisión de los derechos de acceso de los usuarios), el cual se analizó de la siguiente manera:

| Proceso | Gestión de la Relación con los Grupos de Interés | | Observación OCI |
|---|---|---|---|
| Riesgo | Indisponibilidad del servicio por gestión de cambio (plataforma o portales). | | Se evidencia que el riesgo es muy ambiguo, no se identifica que servicio está afectando, se considera que el riesgo puede ser "Indisponibilidad de la información que afecta la disponibilidad de los "Informes de balance de participación en ferias" |
| **Causa** | **Descripción del control** | **Clase de control** | **Observación OCI** |
| No disponibilidad de la información. | El coordinador de la dependencia GSC, anualmente, para garantizar la seguridad de la información, designará un servidor como encargado de la administración y custodia de dichos documentos en archivo físico, digital y virtual, incluyendo los backup del SharePoint. En caso de no hacerlo, dicho rol será asumido por el mismo coordinador (a). Evidencia: correo electrónico de asignación del rol y accesos privilegiados en OneDrive otorgados. | Preventivo | La causa: no se encuentra bien definida, se aconseja como causa "las actividades de mantenimiento y gestión de cambio programadas en horario hábil que afecta la disponibilidad de la información de la infraestructura que soporta la intranet", otra podría ser "Errores en las actividades de gestión de cambio".<br><br>Control: el control "Revisión de los derechos de acceso de los usuarios", no hace referencia a la descripción del control, ya que el control no habla de un respaldo de la información en un medio distinto que es la intranet, de ser así, se tendría que modificar el riesgo, el cual involucre la validación de accesos, para que no sea visto por personas no autorizadas.<br>Por otra parte, la descripción del control menciona el correo electrónico como evidencia, pero el correo no garantiza que esa persona lo vaya hacer, se debe fortalecer la evidencia con pantallazos, imágenes o logs que acrediten que esa persona realizó la copia de seguridad. |

Dado lo anterior se concluye que, se tomaron las medidas necesarias para la solución de los incidentes presentados, a pesar que en el primer incidente el tiempo de disponibilidad afectado fue alta, estos no contaban con controles definidos para estos tipos de incidentes; si bien estos incidentes no se habían presentado, es de reiterar que hoy en día las amenazas informáticas son latentes en toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema, por ende, no se puede esperar a que se materialicen los riesgos para pensar en medidas de control. Por otra parte, se debe reevaluar la definición de riesgos y controles, debido a las observaciones hechas en la

verificación del riesgo y control definido para el segundo incidente, ya que el control del primer incidente es evaluado en el informe “Evaluación y verificación al proceso de modelación del riesgo en el Ministerio de Justicia y del Derecho”, lo cual puede indicar que otros riesgos y controles presenten las observaciones ya señaladas.

**5.4 Estrategia de Planificación y control operacional.**

El Ministerio de Justicia y del Derecho debe planificar, implementar y controlar los procesos necesarios para dar cumplimiento con las exigencias que implica la seguridad y privacidad de la información, las cuales permitan implementar las acciones determinadas en el plan de tratamiento de riesgos, a su turno; debe contar con información documentada que permita confidencialidad en los procesos que se hayan llevado a cabo.

Una vez analizadas las evidencias, la OCI encuentra que, para la estrategia de planificación y control operacional, se cuenta con el documento “*Plan de Seguridad y Privacidad de la Información*”; dicho documento, cuenta con cinco (5) estrategias: liderazgo de seguridad de la información, gestión de riesgos, gestión de incidentes, implementación de controles y concientización.

Se observó que el documento para la planificación cuenta con una serie de planes como lo son el plan de activos de información, plan de riesgos de seguridad de la información y plan de uso y apropiación para la seguridad de la información.

Para llevar el control operacional, se evidenció en el documento que este contiene una serie de proyectos que permitirán el control operacional y que estos se encuentran alineados con las estrategias. Los proyectos son: identificar, valorar y clasificar los riesgos asociados a los activos de información; establecer desde el inicio de cada año la planeación de sensibilización para todo el año; realizar jornadas de sensibilización a todo el personal; realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas; sensibilizar al sector Justicia; contar con una metodología de gestión de incidentes e implementación de la gestión de incidentes a través de la mesa de ayuda. A su vez, se evidenció que el documento fue socializado con el secretario general, en reunión cuyo objetivo fue abordar la seguridad de la información.

Se verificó que dicho documento se encuentra estructurado con la misión y visión de la entidad; política y objetivos de seguridad de la información; el plan de seguridad y privacidad de la información tienen definido el objetivo, el cual enmarca los pilares fundamentales de la seguridad de la información; cada

estrategia definida cuenta con su objetivo; los proyectos se encuentran alineados con las estrategias y definen sus productos; el tiempo de las metas está establecido entre el 2021 hasta el 2023, definiendo costos de inversión para cada vigencia; Se establecen los responsables en el plan de activos y riesgos de seguridad de la información, definiendo sus actividades y fechas de ejecución. Se observa que se debe corregir la fecha en el capítulo de “mapa de ruta” en la definición del plan de acción correctivo, ya que se tiene como fecha la vigencia 2020 y las fases son para el 2021. Una vez validado el documento de Plan de Seguridad y Privacidad de la Información, se evidencia que cuenta con las variables pertinentes y su planificación con los proyectos, los cuales se encuentran bien concebidos y alineados a las estrategias. Se espera el éxito de su implementación para fortalecer la seguridad de la información en el MJD.

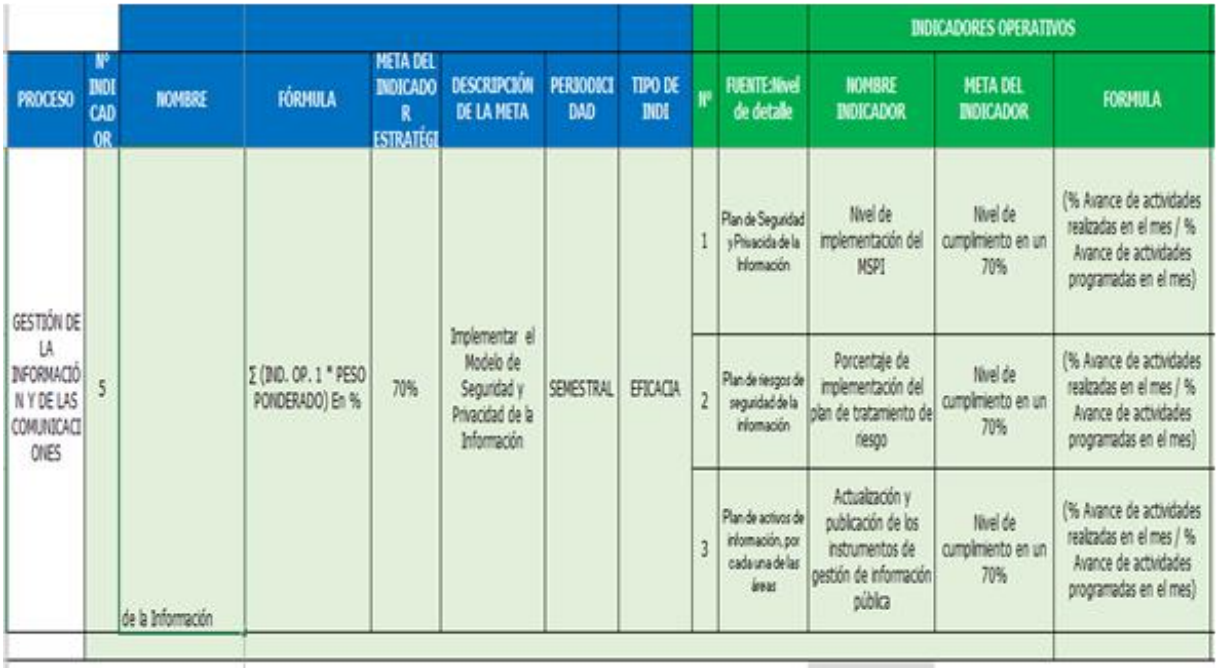
**5.5 Indicadores de gestión del MSPI.**

Los indicadores de gestión para la seguridad de la información son fundamentales para medir la efectividad, eficacia y eficiencia dentro del Ministerio de Justicia y del Derecho, los cuales serán materia para la mejora continua.

Se valida la información entregada por el auditado que, para este punto, valora evidencias como el: “Acta 01-2021 correspondiente al Comité Institucional de Gestión y Desempeño -Planes TI; también se obtiene un documento con la presentación llamada “Indicadores” y un archivo Excel llamado “indicadores DTGIJ octubre”.

En este sentido, se evidenció la presentación y aprobación de los indicadores para el Sistema de Gestión de Seguridad de la Información, en el Comité Institucional de Gestión y Desempeño, realizado por sesión virtual el 30 de septiembre de 2021, el cual se encontraba en el numeral 6 del orden del día como “Presentación y Aprobación de los Indicadores SGSI – Seguridad de la Información”.

Se analiza la evidencia del archivo Excel “indicadores DTGIJ octubre”, en el cual se observa una matriz con la formulación de indicadores, evidenciando que tiene definido un proceso “*GESTIÓN DE LA INFORMACIÓN Y DE LAS COMUNICACIONES*”, el cual contempla 3 indicadores para el “Nivel de implementación del Modelo de Seguridad y Privacidad de la Información”, con una periodicidad semestral y teniendo un solo tipo de indicador (Eficacia), como se ilustra en la siguiente imagen.



| | | | | | | | | INDICADORES OPERATIVOS | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO | Nº INDICADOR | NOMBRE | FÓRMULA | META DEL INDICADOR ESTRATÉGI | DESCRIPCIÓN DE LA META | PERIODICIDAD | TIPO DE INDI | Nº | FUENTE-Nivel de detalle | NOMBRE INDICADOR | META DEL INDICADOR | FORMULA |
| GESTIÓN DE LA INFORMACIÓN Y DE LAS COMUNICACIONES | 5 | de la Información | Σ (IND. OP. 1 * PESO PONDERADO) En % | 70% | Implementar el Modelo de Seguridad y Privacidad de la Información | SEMESTRAL | EFICACIA | 1 | Plan de Seguridad y Privacidad de la Información | Nivel de implementación del MSPI | Nivel de cumplimiento en un 70% | (% Avance de actividades realizadas en el mes / % Avance de actividades programadas en el mes) |
| | | | | | | | | 2 | Plan de riesgos de seguridad de la información | Porcentaje de implementación del plan de tratamiento de riesgo | Nivel de cumplimiento en un 70% | (% Avance de actividades realizadas en el mes / % Avance de actividades programadas en el mes) |
| | | | | | | | | 3 | Plan de activos de información, por cada una de las áreas | Actualización y publicación de los instrumentos de gestión de información pública | Nivel de cumplimiento en un 70% | (% Avance de actividades realizadas en el mes / % Avance de actividades programadas en el mes) |

**Imagen tomada – Matriz "2021 indicadores DTGIJ-octubre"**

Dado lo anterior, se observó que la matriz de indicadores carece de indicadores para abarcar la medición de efectividad, eficacia y eficiencia en la seguridad de la información.

Se recomienda ampliar la medición de indicadores, como: el indicador porcentaje de implementación de controles, plan de sensibilización (fundamental para identificar si los usuarios MJD tienen claro las políticas lineamientos, controles y reporte de ocurrencias de seguridad de la información), ataques informáticos a la entidad, aseguramiento en la adquisición y mantenimiento de software, identificación de lineamientos de seguridad de la entidad, entre otros, como los aconsejados por la "*Guía de indicadores de gestión para la seguridad de la información*" del MINTIC. Lo anterior, con el fin de incrementar el alcance de la medición, la cual sea más amplia, teniendo en cuenta la efectividad de la implementación de los controles de seguridad y la eficiencia del Modelo de Seguridad y Privacidad de la Información MSPI.

### 5.6 Implementación de planes de seguridad de la información 2021

Se evidenció que, dentro del PLAN ANUAL DE ADQUISICIONES –2021 (PAA), el plan de acción, PETI y plan de seguridad de la información, se proyectó la adquisición de las herramientas y el servicio de seguridad informática para "fortalecer la disponibilidad, integridad y confidencialidad de la información, al igual que la operación de las aplicaciones críticas y misionales, dada la

importancia y criticidad de estos servicios, mediante la adquisición de las herramientas y servicios de protección especializados, que permitan mitigar los riesgos tecnológicos a los que puedan estar expuestos dichos servicios".

Por consiguiente, la Dirección de Tecnología busca obtener estas herramientas por medio de la contratación de subasta inversa. Lo anterior descrito en el ítem 1. "DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD ESTATAL PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN SIE No. 11 DE 2021 SEGURIDAD INFORMÁTICA", con objeto "Implementación y puesta en marcha de herramientas y servicios de ciberseguridad y seguridad informática que genere el fortalecimiento del modelo de seguridad y privacidad del Ministerio de Justicia y del Derecho", publicado en la plataforma de Colombia Compra Eficiente SECOP II. Este proceso mencionado anteriormente, se declara desierto el 23 de septiembre de 2021, mediante la Resolución 1455, la cual fue firmada por el doctor Camilo Rojas Secretario General; por lo cual, se denota lo establecido en la siguiente resolución: *"Que siendo claro que, las ofertas presentadas al proceso, al no cumplir con los requisitos habilitantes técnicos, no era posible continuar con la siguiente etapa, esto es, a la verificación de la oferta económica, publicación de oferentes que participarían en la subasta, y posterior inicio de la subasta, 'por lo que la evaluación de las propuestas en efecto, al poder ser verificadas en su integridad, arrojó el resultado de ser declaradas NO HÁBILES. Que, de acuerdo con lo anterior, los miembros del Comité Evaluador, en lo de su competencia, recomiendan al Ordenador del Gasto, declarar desierta la Selección Abreviada con Subasta Inversa No, 11 de 2021, teniendo en cuenta que ninguno de los proponentes, se encuentra habilitado para continuar en el proceso de selección, ARTÍCULO PRIMERO. - Declarar desierto la Selección Abreviada con subasta Inversa No, 11 de 2021.*

Debido a que este proyecto, concebido para el plan de seguridad de la información, no se llevó a cabo, la entidad no fortaleció la disponibilidad, integridad y confidencialidad de la información, pues al no contar con estas herramientas, se debilita la seguridad de la información del MJD ya que, no se realizaron pruebas de vulnerabilidades y hacking ético para la búsqueda de amenazas, monitoreo de seguridad, pentesting o test de penetración, siendo estas unas de las mejores formas de evaluar los sistemas de seguridad del MJD y la seguridad de infraestructura de TI, las cuales son útiles por diferentes razones; en primer lugar, porque determinan qué posibilidad de éxito podría tener un ciberataque, qué vulnerabilidades de mayor y menor riesgo tiene el MJD, cuáles de ellas pueden poner en riesgo a la entidad y cuáles son casi imposibles de detectar. También comprueban la capacidad y la eficiencia de los informáticos a la hora de responder a posibles ataques; y más aún, cuando la entidad ya fue víctima de ataques, lo que conllevó a la materialización del riesgo. Por lo cual, se está incumpliendo con la política de seguridad de la información

del MJD, en su política "*Gestión de Vulnerabilidades - El Líder de Seguridad Informática con el apoyo del Oficial de Seguridad, deben adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas*". A su vez, se incurre en una omisión asociada a la norma NTC-ISO-IEC 27001, en su anexo A.12.6.1: "*Gestión de las vulnerabilidades técnicas – Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado."*

Por otra parte, se observó que, en la Política de Seguridad de la Información, en el capítulo "*4.2 Organización de la Seguridad de la Información - Oficial de Protección de datos personales*", se establecen las funciones del Oficial de Protección de Datos Personales, el cual tiene como objetivo implementar las buenas prácticas de gestión de datos personales dentro del MJD. Por lo anterior, se indagó sobre las actividades que dicho Oficial desempeña, evidenciando que la Subdirección de Gestión de Información en Justicia no cuenta con el recurso para elaborar dichas funciones. Como lo menciona la Política de Seguridad de la información. Se recomienda validar si dicha labor puede ser desarrollada por el oficial de seguridad; de ser así, se debe actualizar la política definiendo estás funciones al Oficial de Seguridad o adquirir el recurso como lo menciona la política.

## 6. Análisis de Riesgo:

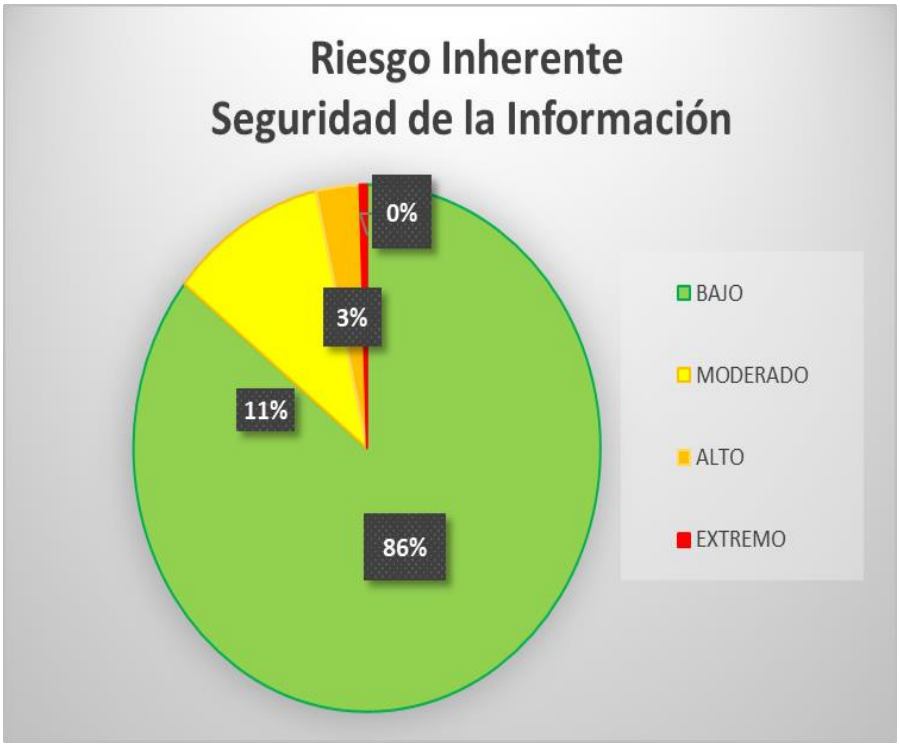
La información que hace parte del Ministerio de Justicia y del Derecho, es crucial para su correcto desempeño dentro de la política pública y su correspondencia con el ciudadano, la cual es parte primordial en el cumplimiento de sus Objetivos, por consiguiente, es muy importante proteger todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, que puedan afectar el normal desarrollo de las actividades del MJD.

Dentro del Modelo de Seguridad y Privacidad de la información MSPI, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones, es importante resaltar que para la evaluación de riesgos en seguridad de la información la guía de "*Gestión de Riesgos*" establecida por el MINTIC, resalta que un insumo vital es "*la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad se encuentren clasificados*".

Dado lo anterior, se procedió a verificar la gestión de riesgos para el MJD, validando los activos de información con los que cuenta la institución y la gestión de riesgos aplicada para este, encontrando que:

La Subdirección de Gestión de Información en Justicia SGIJ, en el mes de febrero del 2021, realizó una solicitud a cada jefe de dependencia por medio del MJD-MEM21-0001499-SGIJ-1600, para que este delegara un líder de transparencia, el cual representara a su dependencia en el proceso actualización de inventarios de activos de información, adicional, se realizaron reuniones con la Dirección de Tecnología y Gestión de Información en Justicia, con la Oficina Asesora de Planeación, para así, al final consolidar la matriz de activos del MJD 2021. Como se detalla en las evidencias, la OCI observó que la SGIJ para este proceso estableció un cronograma entre los meses de mayo a julio del 2021, definiendo para cada día una dependencia para realizar una asesoría y acompañamiento a los líderes de transparencia para facilitar el diligenciamiento de las matrices tanto de activos de información como la de riesgos.

Como resultado de la actualización de riesgos de seguridad de la información, se discriminaron teniendo en cuenta el riesgo inherente, quedando de la siguiente manera: 342 presentan un riesgo inherente bajo; 43 presentan riesgo inherente moderado; 12 presentan riesgo inherente alto; 2 presentan riesgo inherente extremo; generando la siguiente grafica para una mejor interpretación.



Cabe resaltar que, de los riesgos de seguridad de la información mencionados anteriormente, existen en realidad quince (15) riesgos, ya que se repiten con diferente activo.

Para la validación de riesgos y controles, se selecciona de la matriz el activo “Sistema de Información Interinstitucional de Justicia Transicional (SIIJT).”, el cual presenta un riesgo con diferentes causas, analizado de la siguiente manera:

| **Proceso** | **Gestión contra la Criminalidad y la Reincidencia** | | |
|---|---|---|---|
| **Riesgo** | Pérdida de información debido a errores en la ejecución del procedimiento de backup, fallas en el software de backup. | | Se establece un solo riesgo para el sistema de información SIIJT. Se considera que pueden existir otros riesgos como:<br><br>- Desarrollo de software seguro.<br><br>- Falta de planificación de continuidad de negocio.<br><br>-Manipulación u operación indebida del sistema de información. |
| **Causa** | **Descripción del control** | **Clase de control** | **Observación OCI** |
| Dependencia de proveedores. | 1. Diligenciamiento del formato de confidencialidad de la información con los datos del usuario, el cual va dirigido a la Red Nacional de Información, el cual va firmado por el líder funcional del SIIJT y por la Dirección de Justicia Transicional<br><br>2. Una vez aprobado el rol del usuario, se crea en el sistema SIIJT y se la asigna usuario y contraseña.<br><br>Se tiene implementada una política de bloqueo de sesión en el SIIJT, menor o igual a 10 minutos. | Preventivo | Como se mencionó en este informe en el capítulo 5.2 Intercambio de información. Los formatos de acuerdos de confidencialidad se encuentran en proceso de aprobación, por lo tanto, este control aún no es efectivo.<br><br>Para el segundo control se observa que el control debe redactarse adecuadamente, ya que se percibe como la actividad de “Creación de Usuario”. |

Dado lo anterior se concluye que, se realizó el proceso de actualización de activos y riesgos de seguridad de la información para todas las dependencias del MJD. Sin embargo, la matriz de riesgos se ha venido analizando desde el primer capítulo de este informe, encontrando que se presentan inconsistencias en sus definiciones, redacción inapropiada, amenazas que no concuerdan con los riesgos establecidos o insuficiencia de riesgos y causas como se evidenció para el Sistema de Información Interinstitucional de Justicia Transicional (SIIJT). Se identifica que se está adoptando la metodología, pero es necesario reevaluar la matriz de riesgos de seguridad de la información; por consiguiente, con los controles, debido a que se evidenciaron problemas en la redacción del control.

**6.1 Avance en la ejecución del plan de tratamiento de riesgos.**

El Plan de Tratamiento de Riesgos se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes. El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

El Plan de Tratamiento de Riesgos del MINTIC, contempla la definición de las actividades a desarrollar con el fin de mitigar los riesgos sobre los activos, por lo cual recomienda que las actividades se estructuren de la siguiente manera: Gestión – Actividad – Tarea – Responsable – fecha de Inicio – Fecha Fin.

Teniendo en cuenta las recomendaciones del MINTIC, se validó el plan de tratamiento de riesgos para el MJD, encontrando que; este se encuentra inmerso al final de las columnas de la matriz de riesgos de seguridad de la información.

Como se mencionó en el capítulo anterior, se identificaron 14 riesgos inherentes evaluados entre alto y extremo; por lo cual, 12 presentan riesgo inherente alto y 2 presentan riesgo inherente extremo. Dado lo anterior, se evidenció que, de los 14 riesgos inherentes evaluados entre alto y extremo, 5 cuentan con Plan de Tratamiento de Riesgos.

Para realizar un análisis al Plan de Tratamiento de Riesgos, se seleccionó el activo Fortalecimiento Étnico (Subsitio Web), el cual tiene definido como riesgo "*Pérdida de información debido a errores en la ejecución del procedimiento de backup, fallas en el software de backup*." Y como amenaza "*Error en el uso (de equipos, medios, información, sistemas o servicios de información)",* analizando el plan de tratamiento de riesgos así:

| META | INICIO | DURACIÓN | ACCION SI SE MATERIALIZA |
|---|---|---|---|
| 2 Capacitaciones para incrementar el nivel de concientización:<br>1. Seguridad de la información<br>2. Herramientas colaborativas Microsoft- OneDrive | 1/06/2021 | anualmente | 1. informar a seguridad de la información la materialización del riesgo, para activar el procedimiento de gestión de incidentes.<br>2. designación de la persona que se encargará del levantamiento de la información.<br>3. generación y publicación de la información |
| **OBSERVACIÓN OCI** | En la matriz de riesgos en el campo de consecuencias, aluden otro tipo de amenazas como: ataques al sistema; errores de transmisión o almacenamiento; y ya en el plan de tratamiento en la "META Y ACCIÓN SI SE MATERIALIZA", están enfocados a la falta de conocimiento y concientización por parte del usuario y no a la falla en el procedimiento de backup, por lo cual, el plan de tratamiento se encuentra desenfocado frente al riesgo establecido. | | |

Una vez analizado los lineamientos de la guía administración del riesgo, y los recomendados por MINTIC; se evidencia que el formato para el plan de tratamiento de riesgos, inmerso en la matriz de riesgos de seguridad de la información, obtiene las variables necesarias para su diligenciamiento, sin embargo, se evidencia que hasta ahora se está apropiando la metodología, ya que contempla la definición de las actividades a desarrollar para el plan de tratamiento; se debe tener en cuenta las 5 fases del desarrollo metodológico para el tratamiento de riesgos (Análisis de la información, Desarrollo de los proyectos, Análisis de los proyectos, Definición del organigrama de responsabilidad y el Ciclo de vida del tratamiento de riesgos PHVA), recomendado por MINTIC. Se recomienda reevaluar y completar los planes de tratamientos de riesgos para los que hacen falta; ya que si se llegan a materializar no se obtendrá una reacción inmediata para superarlo.

## 7. Conclusiones, hallazgos y/ recomendaciones

### 7.1 Conclusiones

- EL MJD cuenta con la definición políticas, lineamientos y controles en seguridad de la información, sin embargo, incurre en el incumplimiento de algunas de sus políticas y controles mencionados en el desarrollo del informe afectando la integridad, confidencialidad y disponibilidad de los activos de información.

- La entidad fue víctima de ataques por la comunidad de Ciberactivismo y Hacktivismo "Anonymous", afectando la disponibilidad del portal web de la entidad.

- El MJD cuenta con un documento de estrategia y planificación de la seguridad de la información, el cual cuenta con las variables propias de una planificación bien concebida, la cual inicia en la actual vigencia y finalizará en el 2023.

- Se evidenció que los indicadores para el Sistema de Gestión de Seguridad de la Información, fueron presentados en el Comité Institucional de Gestión y Desempeño.

- Para la actual vigencia, el MJD no contó con la realización de pruebas de vulnerabilidades y hacking ético, por este motivo no se fortaleció la disponibilidad, integridad y confidencialidad de la información.

- El MJD no cuenta con un Oficial de Protección de Datos Personales para la implementación de buenas prácticas en la gestión de datos personales.

- Se actualizaron los activos y riesgos para todas las dependencias del MJD, generando una sola matriz de riesgos de seguridad de la información.

- Se identificó que la matriz de riesgos posee inconsistencias como las mencionadas en el desarrollo del informe, por consiguiente, se debe reevaluar la matriz de riesgos ya que afecta la integridad, confidencialidad y disponibilidad de los activos de información.

- Se debe validar las grandes inversiones presupuestales que se tienen programadas en seguridad de la información, cuando los Sistemas de Información del MJD presentan grandes deficiencias en interoperabilidad y transformación de datos.

## 7.2 Hallazgos

### Hallazgo 1

Los logs solicitados para la validación a los sistemas de información no presentan una configuración o habilitación adecuada sobre las actividades que deben ser registradas o información relevante que debe ser incluida en los registros, ya que no ostentan información propicia para realizar un análisis detallado de los diferentes eventos en los sistemas de información del MJD, incumpliendo presuntamente la política de Seguridad de la Información del MJD "*Registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información*", incumpliendo a su vez, la norma NTC-ISO-IEC 27001 anexo

A.12.4.1 "*Registro de eventos – Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información*", predicable a la luz de lo dispuesto en los criterios establecidos en el Modelo Estándar de Control Interno a la altura del numeral 10.3.

**Hallazgo 2**

Para la actual vigencia no se realizaron pruebas de vulnerabilidades y hacking ético, lo cual deja a la entidad vulnerable en la disponibilidad, integridad y confidencialidad de la información, incumpliendo presuntamente con la política de seguridad de la información "*Gestión de Vulnerabilidades - El Líder de Seguridad Informática con el apoyo del Oficial de Seguridad, deben adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas*". A su vez, se incurre en omisión en relación con la norma NTC-ISO-IEC 27001 en su anexo A.12.6.1 "*Gestión de las vulnerabilidades técnicas – Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado",* predicable a la luz de lo dispuesto en los criterios establecidos en el Modelo Estándar de Control Interno a la altura del numeral 10.3.

**7.3 Recomendaciones**

**Recomendación 1 (frente al hallazgo 1)**

Se debe realizar la habilitación o configuración de los "Logs" para los sistemas de información, estableciendo la información mínima básica que debe registrarse para la identificación adecuada de los eventos y excepciones generadas por los Sistemas de Información de la entidad, como: su ubicación/IP; actividades del sistema; registros de intentos de acceso al sistema exitosos y rechazados; registros de datos exitosos, rechazados y otros intentos de acceso a recursos; archivos a los que se tuvo acceso y el tipo de acceso; direcciones y protocolos de red; alarmas accionadas por el sistema de control de acceso entre otros. Por otra parte, se debe validar la clasificación de los diferentes tipos de mensajes de error y trazabilidad que deben registrar los Sistemas de Información, con el fin de facilitar la identificación, selección y priorización de la información necesaria para los procesos de monitoreo, gestión de incidentes e identificación de mejoras.

**Recomendación 2 (frente al hallazgo 2)**

Ya que para la actual vigencia no se llevó a cabo la adquisición de las herramientas de fortalecimiento de la Seguridad de la Información, se recomienda en la siguiente vigencia dar prioridad a la adquisición de estas herramientas, para fortalecer la disponibilidad, integridad y confidencialidad de la información del MJD; se realiza un monitoreo de registros manual, pero no es comparable con el escaneo de vulnerabilidades y monitoreo que brinda estas herramientas, ya que se debe contar oportunamente con información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, como lo recomienda la NTC-ISO-IEC 27001 en su anexo A.12.6.1.

### 7.4 Recomendaciones Generales

- Se recomienda tener en cuenta los indicadores mencionados en el capítulo 5.5 del presente informe, para ampliar la medición de efectividad

- Se recomienda dar pronta aprobación a los formatos de “Acuerdos de Confidencialidad”, para el aseguramiento de la información.

- Se recomienda validar si labor del “Oficial de Protección de Datos Personales” puede ser desarrollada por el Oficial de Seguridad; de ser así, se debe actualizar la política de seguridad de la información en su capítulo “*4.2. Organización de la Seguridad de la Información – Oficial de protección de Datos Personales*”.

- Se recomienda finalizar el ciclo PHVA con la mejora continua, ya que la próxima auditoría de Seguridad de la Información, se llevará a cabo en noviembre del 2022, evaluando la evaluación del desempeño y mejora continua del MSPI.

- Se recomienda para la matriz consolidada de riesgos de seguridad de la información, organizar o agrupar los procesos y no que estos se encuentren dispersos por toda la matriz.

- Realizar la reevaluación de la matriz de riesgos, ya que presenta inconsistencias como las mencionadas en el desarrollo del informe, ya que afecta la integridad, confidencialidad y disponibilidad de los activos de información.

- Validar el proceso de recuperación de contraseña que ofrecen los diferentes sistemas de información del SIM, en el que se valide el correcto

funcionamiento y los mensajes que arroja para que sean coherentes con su funcionalidad.

- Definir el plan de tratamiento para los demás riesgos inherentes que se encuentran en la matriz, evaluados como “Altos y Extremos”, ya que de materializarse no se podrá actuar de manera inmediata, ocasionando daños y afectaciones a los activos del MJD.

- Se recomienda remediar las inconsistencias ostentadas en el presente informe, antes de continuar con las siguientes fases de implementación del MSPI, para evitar que las subsiguientes se vean afectadas por daños colaterales de su primera fase de implementación.

El presente informe se emite en Bogotá D.C., a los treinta (30) días de noviembre de 2021.

Elaboró: Aprobó:

**WILMAN FERNANDO MORENO YANQUÉN**
Profesional OCI

**DIEGO ORLANDO BUSTOS FORERO**
Jefe Oficina de Control Interno