EVALUACIÓN Y VERIFICACIÓN SOBRE LOS AVANCES Y MEJORAS OBTENIDAS EN EL MARCO DEL PROCESO DE LAS BASES DE DATOS

INFORME FINAL

Oficina de Control Interno
3 de Diciembre de 2024

Tabla de contenido

1. Objetivo de la auditoría:

Evaluar y verificar los avances y mejoras obtenidas en el marco del procedimiento de bases de datos.

2. Alcance de la auditoría:

En función del objetivo definido, se evaluarán los progresos y avances realizados en el marco del cumplimiento del procedimiento de bases de datos, de acuerdo con los resultados obtenidos en el informe de auditoría realizado en septiembre de 2023. A partir de los hallazgos y recomendaciones emitidos, se promoverá una mirada sobre el plan de mejoramiento por procesos que implica todos los sistemas de información contentivos de sus bases de datos del Ministerio de Justicia y del Derecho, en adelante (MJD).

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; Decreto 1377 de 2013; CONPES 3975 de 2019; Resolución 746 de 2022; Manual Operativo MIPG v5; ISO 27001:2022; Plan Estratégico De Tecnología De La Información (PETI) versión 1 de diciembre de 2023; Informe de auditoría “Evaluación y Verificación del cumplimiento del procedimiento de “Gestión, Administración y Mantenimiento de las Bases de Datos e Infraestructura que soportan el motor de Base de Datos” de septiembre de 2023.

4. Metodología:

La metodología empleada por la Oficina de Control Interno (en adelante OCI), se basó en el levantamiento de información por medio de un cuestionario con once (11) preguntas basadas en el Informe de auditoría “Evaluación y Verificación del procedimiento de base de datos” de septiembre de 2023, las cuales fueron enviadas con el plan específico bajo el memorando MJD-MEM24-0006670 y, posteriormente se enviaron tres preguntas adicionales basadas en el PETI; por otra parte, se utilizaron métodos de evaluación como la constatación de información y el análisis, a partir de los cuales se trazaron conclusiones que se presentan al final de este informe; 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 1° de Noviembre 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 y la auditora 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; adicionalmente, la DTGIJ y la STSI solicitaron el ajuste de algunas de las preguntas allegadas mediante el memorando anteriormente mencionado, quedando formuladas diez (10) en total con sus correspondientes respuestas y el ajuste del objetivo de la auditoria indicando que no existe un proceso de base de datos sino un procedimiento, sobre tal particular.

5. Desarrollo de la Auditoría

5.1. Antecedentes

En la vigencia 2023, la Oficina de Control Interno (OCI) realizó el informe de la auditoria denominada Evaluación y Verificación del procedimiento de base de datos, el cual es tomado como insumo para esta auditoría, cuyo objetivo señalaba: "*Evaluar y verificar del cumplimiento del procedimiento de "Gestión, Administración y Mantenimiento de las Bases de Datos (en adelante BD) e Infraestructura que soportan el motor de Base de Datos*[1]".

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

"Existe un procedimiento actualmente documentado; el cual, no toma en cuenta las actividades ejecutadas por los distintos actores que intervienen en el mismo, no involucra al oficial de seguridad y al de datos personales en cuanto a la definición de controles en las BD y solapa las actividades correctivas y preventivas realizadas en las bases de datos por el DBA.

Cabe resaltar que no se encuentra alineado en cuanto al establecimiento, documentación e implementación de procesos, procedimientos y controles para asegurar el nivel de continuidad y, de esa manera, fortalecer la seguridad de la información y de los datos personales durante una situación adversa[2]*".*

Se realizaron las siguientes recomendaciones:

"La OCI recomienda replantear el contenido del procedimiento, en cuanto a:

1. *El nombre del procedimiento, considerando que no está alineado con las actividades que se realizan en el mismo; teniendo en cuenta que el documento no menciona las acciones realizadas en cuanto a gestión, administración y mantenimiento de la infraestructura que soporta el motor de las Bases de Datos.*

2. *El objetivo no se encuentra ajustado al contenido del procedimiento, ya que no se mencionan las actividades, acciones operativas y/o de mantenimiento para propender los modelos relacionales, los esquemas de intercambio de información y de seguridad de la información.*

3. *Alinear las políticas de operación del procedimiento de acuerdo a lo manifestado en Política de seguridad de la información actualmente vigente en el SIG, en cuanto a "Los componentes tecnológicos estarán bajo la administración de los líderes de infraestructura y de sistemas de información de la STSI. Lo anterior sin perjuicio de la responsabilidad de la Subdirección de Tecnologías y Sistemas de Información, de aplicar los controles de seguridad informática definidos en las políticas de: seguridad de la información, tratamiento y protección de datos personales, tecnologías y gestión de la información, así como en los planes de tratamiento de riesgos que permiten hacer un uso responsable de los accesos privilegiados a los sistemas de información y los datos. Se pueden presentar casos en los cuales los activos de información como las bases de datos de sistemas de información y portales sean custodiadas técnicamente por parte de dicha Subdirección, lo cual implica la prestación de los servicios tecnológicos de administración, soporte, mantenimiento y copias de respaldo de las bases de datos.*

[1] Auditoría Evaluación y Verificación del procedimiento de base de datos; ítem 1. Objetivo de la auditoria; pág. 3; OCI MINJUSTICIA, septiembre de 2023; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2023/EvaluacionIndependiente/Informe-final-Procedimiento-de-Gestion-de-BD.pdf

[2] Auditoría Evaluación y Verificación del procedimiento de base de datos; ítem 6. Conclusiones, hallazgos y/ recomendaciones; pág. 12; OCI MINJUSTICIA, septiembre de 2023; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2023/EvaluacionIndependiente/Informe-final-Procedimiento-de-Gestion-de-BD.pdf

Sin embargo, la calidad de la información será responsabilidad de la(s) dependencia(s) que, de acuerdo con sus funciones, deba(n) gestionarla".

- *Determinar claramente las acciones relacionadas con la gestión, administración y mantenimiento de las Bases de datos.*
- *Discriminar las labores preventivas y correctivas realizadas sobre las BD.*
- *Contemplar todos los posibles responsables en las actividades definidas en el procedimiento.*
- *Incluir las verificaciones que se deben realizar para garantizar que los tiempos de respuesta de las bases de datos de los sistemas de información afectados hayan mejorado, en los casos generados por la herramienta de mesa de servicio.*
- *Incluir las verificaciones que se deben realizar para probar que los incidentes reportados en una BD hayan sido solucionados, en los casos generados por la herramienta de mesa de servicio.*
- *Añadir las labores de afinamiento dentro de los servidores.*[3]".

5.2. Gestión de las Bases de Datos

En la auditoría de base de datos realizada en la vigencia 2023, se analizó el procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos e Infraestructura que soporta el Motor de Base de Datos" con código: P-TI-05 en su versión 4 del 30 de junio de 2020, el cual a la fecha de la actual auditoria sigue vigente en el SIG.

En el marco de la auditoría realizada en el año 2023 se identificó el siguiente inventario de Bases de Datos (en adelante BD):

- 10 Bases de datos que se encuentran en SQL Server versión 2012, que corresponden a sistemas de información del MJD.
- 21 Bases de datos que se encuentran en SQL Server versión 2019, que corresponden a los sistemas de información del MJD.
- 3 Bases de datos que se encuentran en SQL Server versión 2012, que corresponden al software base[4] (configuración).
- 8 Bases de datos que se encuentran en SQL Server versión 2019, que corresponden al software base (configuración).

Con sujeción a la información aportada por el área de tecnología, se realiza comparación entre la información del inventario de base datos de las vigencias 2023 y 2024, identificando las siguientes coincidencias:

- 21 Bases de datos que se encuentran en SQL Server versión 2022, que corresponden a sistemas de información del MJD reportados en la vigencia 2023
- 3 Bases de datos que se encuentra en SQL Server versión 2022, que corresponden al software base (configuración).

[3] Auditoría Evaluación y Verificación del procedimiento de base de datos; ítem 6. Conclusiones, hallazgos y/ recomendaciones; pág. 17 y 18; OCI MINJUSTICIA, septiembre de 2023; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2023/EvaluacionIndependiente/Informe-final-Procedimiento-de-Gestion-de-BD.pdf

[4] El software de base o **software base** es el programa principal del dispositivo informático que controla completamente el dispositivo, como una computadora, un teléfono celular o una tableta. Se considera "base" porque es la plataforma donde el resto del software se apoya para ejecutarse.

En la vigencia 2023 encontramos que el MJD contaba con 42 BD de las cuales 31 soportaban sistemas de información y 11 soportaban software base. Con relación a la información allegada para la vigencia 2024 encontramos 24 BD de las cuales 21 BD soportan sistemas de información y 3 BD que soportan software base. En el ejercicio de la auditoria se encuentra una diferencia de 18 BD, las cuales presentaron novedades en el inventario de BD de la vigencia 2024, las cuales se describirán a continuación:

- 5 Bases de datos que pertenecían a sistemas de información (portales), fueron migrados a SharePoint[5]
- 6 Bases de datos salieron de producción (4 relacionadas con software base y 2 de sistemas de información correspondientes a SIGOB y SIGMINJUSTICIA)
- 7 Bases de datos fueron dadas de baja (5 relacionadas con software base y 2 de sistemas de información correspondientes a DS_MINJUS y DW_MINJUS)

Adicionalmente, el área de tecnología reporta las siguientes BD, las cuales no fueron incluidas en la auditoria de base de datos realizada en 2023:

- 1 Base de datos que se encuentran en Oracle versión 10G.
- 1 Base de datos correspondiente al sistema SICOC.
- 4 Bases de datos que se encuentran en SQL Server versión 2022, que corresponden a sistemas de información del MJD, los cuales ingresaron al inventario en esta vigencia (3 relacionados con bodega de datos y 1 con Sisgestion).

Con respecto a lo anterior, se resalta la labor del área de tecnología al realizar la estandarización de la versión del motor de base datos (2022) en SQL SERVER en las distintas bases de datos del MJD, y se insta a evaluar la actualización de la versión de la BD en Oracle ya que esta es obsoleta y puede provocar incidentes de seguridad al carecer de parches de seguridad recientes, lo que la hace vulnerables a ataques y brechas de seguridad; adicionalmente, en cuanto al inventario de BD este no mantiene un histórico de las diferentes novedades ocurridas con las BD de la Entidad, lo cual dificulta realizar trazabilidad en los mismos.

En cuanto al mantenimiento a las Bases de Datos, la STSI en cabeza del Administrador de Base de Datos (en adelante DBA[6]) habilita la opción de escaneo automático en el momento de la instalación de la BD; el cual consiste en la detección de lentitud y posibles fallas en planes de ejecución en tiempos de respuesta, evaluación del problema y aplicación de correctivos de forma autónoma y automática, y así evitar que se puedan presentar fallas que afecten la disponibilidad de las bases de datos.

Respecto a la disponibilidad[7] de la información de las BD de los sistemas de Información de la Entidad, estas se encuentran disponibles 7 x 24, para el acceso de los diferentes usuarios, tanto a nivel privado como público; adicionalmente, el acceso es restringido con el uso de perfiles (roles) de usuarios, los cuales son asignados por el administrador funcional del sistema, el cual

[5] **SharePoint** es una plataforma de colaboración empresarial desarrollada por Microsoft. Se utiliza para crear sitios web donde las organizaciones pueden almacenar, organizar y compartir información de manera segura desde cualquier dispositivo.
[6] Un **DBA, o Database Administrator** (Administrador de Bases de Datos), es un profesional responsable de la gestión, mantenimiento y operación de bases de datos.
7 La **disponibilidad** se refiere a la capacidad de acceder y utilizar la información y los sistemas de tratamiento de esta, por parte de individuos, entidades o procesos autorizados cuando lo requieran.

pertenece al área propietaria del mismo, manteniendo así la confidencialidad de la información[8], y por último para garantizar la integridad[9] de la información tienen definida la integridad de dominio[10] de entidad[11] y referencial[12] en las BD; es de resaltar que, estas actividades no se encuentran formalizadas en ningún documento; por lo anterior, la OCI sugiere a la DTGIJ y la STSI definir e implementar las medidas correspondientes.

5.3. Seguimiento y control al Plan de Mejoramiento vigente al 30 de septiembre de 2024

A través del informe de la auditoria denominada "Evaluación y Verificación del procedimiento de base de datos" realizado en septiembre de 2023, la OCI identifico varias problemáticas críticas que resultaron en los siguientes hallazgos:

Hallazgo 1: Se evidencia incumplimiento en la identificación de las bases de datos que contienen datos personales y/o sensibles; lo anterior, de acuerdo a lo mencionado en la Política de Seguridad de la información en el ítem 4.2. Organización de la Seguridad de la Información - Oficial de Protección de Datos Personales "*Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo*" y la ISO: IEC 27001 en el ítem A.8.2 Clasificación de la Información "*asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización*".

Hallazgo 2: Se evidencia incumplimiento, en la documentación de los lineamientos para el tratamiento, manejo y seguimiento a los riesgos relacionados con las bases de datos que contienen datos personales y/o sensibles y sus controles asociados (matriz de riesgos); de acuerdo a lo mencionado en la Ley 1581 de 2012 en el principio rector de seguridad "*La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"* y la ISO: IEC 27001 en el ítem 6.1.2 Evaluación de riesgos de la seguridad de la información - inciso C " *Identifique los riesgos: 1. Aplicar el proceso de evaluación de riesgos para su identificación; asociados con la pérdida de la confidencialidad, de la integridad y de la disponibilidad de la información dentro del alcance; 2. Identificar a los dueños de los riesgos*".

Ante estos hallazgos, y de acuerdo al procedimiento de auditoria interna con Código: P-SE- 01 versión 5 del 8 de noviembre de 2022, el cual en la actividad 12 menciona que se debe: "*Formular acciones u oportunidades de mejora*" lo cual implica que el responsable o líder del proceso debe "*Formular las acciones respectivas analizando las causas raíz que dieron origen al hallazgo y/o no conformidades. Una vez se definidas (SIC) deberán registrarse ante la Oficina Asesora de Planeación para*

[8] La **confidencialidad** se refiere a la propiedad de que la información no se ponga a disposición ni se revele a individuos, entidades o procesos no autorizados.
[9] La **integridad** se refiere a la propiedad de mantener la exactitud y completitud de la información y sus métodos de procesamiento.
[10] La **integridad de dominio** es un principio en bases de datos que asegura que los valores almacenados en una columna específica cumplen con un conjunto de reglas predefinidas. Estas reglas pueden incluir restricciones sobre el tipo de datos, el formato y el rango de valores permitidos.
[11] La **integridad de entidad** es un principio fundamental en bases de datos relacionales que asegura que cada registro en una tabla sea único y fácilmente identificable.
[12] La **integridad referencial** es un principio fundamental en bases de datos relacionales que asegura que las relaciones entre tablas se mantengan coherentes.

su respectivo monitoreo de acuerdo con el procedimiento de mejora integral de la gestión institucional [13]". La Dirección de Tecnologías y Gestión de Información en Justicia (DTGIJ) asumió el liderazgo en la implementación del plan de mejoramiento, en colaboración con la Subdirección de Tecnologías y Sistemas de Información (STSI).

En la matriz del Plan de Mejoramiento por Procesos (PMP[14]) , se encuentran identificados con el consecutivo interno 10-23 y 11-23, respectivamente; es de agregar que las acciones para dar cumplimiento al plan para ambos hallazgos iniciaron el 1° de abril de 2024 y finalizan el 15 de diciembre de 2024.

Imagen 1. Plan de Mejoramiento por Procesos vigente para los hallazgos 10-23 y 11-23

CONSECUTIVO INTERNO	DESCRIPCIÓN HALLAZGO (No más de 50 palabras)	ACCIÓN DE MEJORAMIENTO	DESCRIPCIÓN DE METAS	FECHA INICIACIÓN METAS	FECHA TERMINACIÓN METAS
10-23	Se evidencia incumplimiento en la identificación de las bases de datos que contienen datos personales y/o sensibles; lo anterior, de acuerdo a lo mencionado en la Política de Seguridad de la información en el ítem 4.2. Organización de la Seguridad de la información - Oficial de Protección de Datos Personales "Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo" y la ISO: IEC 27001 en el ítem A.8.2 Clasificación de la Información "asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización".	1. Revisión y actualización de la política de protección de datos. 2. Socialización de la política de protección de datos. 3. Revisión y actualización del procedimiento P-TI-05 gestión de bases de datos 4.Socialización del procedimiento P-TI-05 gestión de bases de datos.	1. Una política actualizada 2. Socialización de la política 3. procedimiento actualizado 4. socialización del procedimiento	1/04/2024	15/12/2024
11-23	Se evidencia incumplimiento, en la documentación de los lineamientos para el tratamiento, manejo y seguimiento a los riesgos relacionados con las bases de datos que contienen datos personales y/o sensibles y sus controles asociados (matriz de riesgos); de acuerdo a lo mencionado en la Ley 1581 de 2012 en el principio rector de seguridad "La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento" y la ISO: IEC 27001 en el ítem 6.1.2 Evaluación de riesgos de la seguridad de la información - inciso C " Identifique los riesgos: 1. Aplicar el proceso de evaluación de riesgos para su identificación; asociados con la pérdida de la confidencialidad, de la integridad y de la disponibilidad de la información dentro del alcance; 2. Identificar a los dueños de los riesgos".	1. Establecer el lineamiento documentado en alineación con la Política de protección de datos personales y de la Seguridad de la información. 2. Socializar el lineamiento.	1. Lineamiento documentado 2. lineamiento socializado	1/04/2024	15/12/2024

Fuente: Matriz de PMP tecnología vigencia 2024

Estos planes fueron evaluados por la OCI en el mes de octubre de 2024 con corte realizado a 30 de septiembre de 2024, encontrando lo siguiente:

Hallazgo 1: De acuerdo con las evidencias allegadas por la dependencia responsable, se encuentran la siguiente documentación relacionada a las metas:

1. Borrador de actualización del procedimiento de afinamiento de base de datos.
2. Borrador de actualización de la Política de tratamiento de datos personales y sus formatos asociados (aviso de privacidad, autorización de tratamiento de datos personales y el programa integral de gestión de datos personales).

Si bien es cierto, que la OCI evidencia un importante avance en la documentación del proceso, es de agregar que en cuanto a la política de datos personales no se encuentran lineamientos que definan como se van a identificar las bases de datos que contienen datos personales y/o sensibles, cómo se van a organizar y clasificar según su tipo; adicionalmente, no menciona las

[13] Procedimiento de auditoria interna; Código: P-SE- 01; versión 5 del 8 de noviembre de 2022; ítem 7. Desarrollo; pág.10.

[14] Plan de Mejoramiento por Procesos (**PMP**): Elemento de Control, que permite el mejoramiento continuo y el cumplimiento de los objetivos institucionales de la entidad. Integra las acciones de mejoramiento que a nivel de sus procesos y de los objetivos estratégicos.

medidas técnicas de seguridad que serán implementadas para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado y si a su vez estas estarán alineadas con el procedimiento de gestión de base datos, tampoco define si el administrador de las bases de datos realizara procedimientos adicionales sobre estas; es de resaltar, que la evidencia presentada corresponde a documentos que aún no se encuentran aprobados ni socializados ante la MJD.

Por lo anterior la OCI asigna avance del 20% y recomienda continuar con las gestiones tendientes para dar por superada la causa que dio origen al hallazgo; realizando REPROGRAMACIÓN.

Hallazgo 2: De acuerdo con las evidencias allegadas por la dependencia responsable, se encuentran la siguiente documentación relacionada a las metas:

1. Borrador de actualización del procedimiento de afinamiento de base de datos
2. Borrador de actualización de la Política de tratamiento de datos personales y sus formatos asociados (aviso de privacidad, autorización de tratamiento de datos personales y el programa integral de gestión de datos personales)

En cuanto a la política de datos personales se resalta la inclusión del “tratamiento y finalidades al cual serán sometidos los datos” y “deberes del responsable de tratamiento” aunque no es claro quién es el responsable de dicho tratamiento; la política no define como se regulará la transferencia de datos personales a terceros, asegurando que se realice conforme a la ley y con el consentimiento del titular; no indica como otorgará seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; adicionalmente, no se encuentra alineación con la política de seguridad de la información y el procedimiento de afinamiento de base de datos y no define los lineamientos para el tratamiento, manejo y seguimiento a los riesgos relacionados con las bases de datos que contienen datos personales y/o sensibles y sus controles asociados (matriz de riesgos) y quién será el responsable de dicha actividad. Es de resaltar, que la evidencia presentada corresponde a documentos que aún no se encuentran aprobados ni socializados ante la MJD y allegan la misma documentación generada para el hallazgo 10-23.

Por lo anterior la OCI asigna avance del 10% y recomienda continuar con las gestiones tendientes para dar por superada la causa que dio origen al hallazgo; realizando REPROGRAMACIÓN y REFORMULACIÓN.

En síntesis, aunque se reconocen los avances en las acciones propuestas para los dos hallazgos mencionados, la OCI considera que no se puede declarar la efectividad de los planes de mejoramiento en su estado actual. Las acciones implementadas no abordan completamente los problemas estructurales identificados en los hallazgos; por lo tanto, es esencial identificar las bases de datos que contienen datos personales y/o sensibles, definir claramente los responsables, implementar medidas de seguridad adecuadas y alinear las políticas con los procedimientos de gestión de bases de datos para garantizar la protección de los datos personales.

Se insta al área de tecnología a tener en cuenta que la falta de identificación de las bases de datos que contienen datos personales y/o sensibles dificulta la implementación de medidas de seguridad adecuadas, lo que aumenta el riesgo de accesos no autorizados y posibles filtraciones de datos. Además, la falta de medidas técnicas de seguridad incrementa el riesgo de alteración,

pérdida, tratamiento o acceso no autorizado a los datos personales, lo que puede resultar en brechas de seguridad y pérdida de confianza por parte de los stakeholders[15].

No definir claramente los responsables del tratamiento de datos y las medidas de seguridad puede afectar la transparencia y la rendición de cuentas dentro de la organización, además del posible incumplimiento de la Ley de Protección de Datos Personales en Colombia (Ley 1581 de 2012).

La falta de alineación entre las políticas de datos personales y los procedimientos de gestión de bases de datos, pueden generar ineficiencias operativas y dificultades en la implementación de controles efectivos.

5.4. Plan Estratégico de Tecnología de la Información (PETI)

El MJD suscribió el contrato de consultoría 1093 de 2023 para la elaboración del Plan Estratégico de Tecnología de la Información (en adelante PETI[16]) con el siguiente objeto: "*Diseño, formulación y definición del plan estratégico de tecnología de la información (PETI) del Ministerio de Justicia y del Derecho, de acuerdo con los lineamientos definidos en la política de gobierno digital vigente y visión de arquitectura empresarial, para el periodo 2024-2026*"; es de agregar que, el documento en mención actualmente se encuentra publicado en la página web del MJD.

A continuación, se mencionarán los lineamientos que, de acuerdo al criterio de la auditora, están relacionados con la gestión de base de datos:

- En el numeral 3.5.6.1.2.3 mencionan el procedimiento de administración y mantenimiento de bases de datos e infraestructura que soporta el motor de base de datos, e indican que "*Una vez analizada la situación actual anteriormente descrita respecto a los procesos y procedimientos que definen la operación de los servicios e infraestructura tecnológica, se sugiere continuar con la definición de los siguientes procesos y procedimientos:*

    - *La inclusión y actualización de nuevos servicios de TI en el catálogo de servicios.*
    - *Procedimiento de control de cambios tecnológicos (no solo cambios a los Sistemas de Información).*
    - *Fortalecer el procedimiento de gestión de incidentes, ya que el actual está enfocado principalmente en la gestión de incidentes de seguridad de la información.*
    - *Definir un procedimiento de monitoreo y control de la disponibilidad de la infraestructura tecnológica*[17]".

Acorde con lo expresado anteriormente, la OCI reitera lo indicado en el informe de auditoría del procedimiento de base de datos realizada en la vigencia 2023 en cuanto a que: "*Existe un*

[15] **Stakeholder** o parte interesada se refiere a cualquier persona u organización que puede afectar, verse afectada o percibirse como afectada por las decisiones o actividades de una organización. Esto incluye a clientes, proveedores, empleados, accionistas, comunidades locales, y cualquier otro grupo que tenga un interés en las operaciones de la organización.

[16] El Plan Estratégico de Tecnologías de la Información (**PETI**) es una herramienta clave para alinear la tecnología con los objetivos estratégicos de una organización. Su propósito principal es definir una hoja de ruta para implementar proyectos tecnológicos que apoyen las metas y objetivos de la entidad.

[17] Plan Estratégico de Tecnología de la Información; numeral 3.5.6.1.2.3 procedimiento de administración y mantenimiento de bases de datos e infraestructura que soporta el motor de base de datos; pág. 180 y 181; MINJUSTICIA - Dirección de Tecnologías y Gestión de Información en Justicia, 2023; https://www.minjusticia.gov.co/transparencia/Documents/PETI-MJD-2024-2026-V1.pdf

procedimiento actualmente documentado; el cual, no toma en cuenta las actividades ejecutadas por los distintos actores que intervienen en el mismo, no involucra al oficial de seguridad y al de datos personales en cuanto a la definición de controles en las BD y solapa las actividades correctivas y preventivas realizadas en las bases de datos por el DBA. Cabe resaltar que no se encuentra alineado en cuanto al establecimiento, documentación e implementación de procesos, procedimientos y controles para asegurar el nivel de continuidad y, de esa manera, fortalecer la seguridad de la información y de los datos personales durante una situación adversa. [18]"

- En el numeral 3.5.6.2 Administración señalan "La administración de los Servicios de TI tiene como propósito, asegurar que "*El Ministerio dispone de un procedimiento de administración de bases de datos y su infraestructura, pero no se evidencia documentación respecto a la administración de los demás componentes que hacen parte de la infraestructura tecnológica, cómo servidores, servicios de conectividad, telefonía, nube, centros de cómputo, almacenamiento [19]*".

En cuanto al procedimiento de base de datos evaluado por la OCI en la vigencia 2023, se reitera que: "*No se determinan claramente las acciones relacionadas con la gestión, administración y mantenimiento de las BD; No están discriminadas las labores preventivas y correctivas realizadas sobre las BD; El DBA tiene configuradas labores preventivas realizadas por el motor de base de datos para brindar afinamiento a la base de datos y realiza algunas actividades de forma manual, las cuales no están definidas en el procedimiento*" y lo mencionado en el informe de auditoría de evaluación y verificación del procedimiento de respaldo y restauración de los sistemas de información "*Existe un procedimiento actualmente documentado, el cual no toma en cuenta el respaldo de los componentes del sistema de información, diferentes a las bases de datos, tales como capa de negocio, capa de aplicación, y los requisitos de la información de la entidad y no establece un diferenciamiento en cuanto a la periodicidad de las copias de los distintos sistemas de información. Adicionalmente, no se encuentra alineado en cuanto al establecimiento, documentación e implementación de procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa[20].*"

Frente a los numerales mencionados es importante resaltar que la administración de los servicios de TI tiene como objetivo asegurar una gestión eficiente y segura de todos los componentes tecnológicos del MJD. Sin embargo, se ha identificado que, aunque existe un procedimiento documentado para la administración de bases de datos, no se ha evidenciado documentación similar para otros componentes esenciales como servidores, servicios de conectividad, telefonía, nube, centros de cómputo y almacenamiento. Por lo anterior, la OCI insta al área de tecnología a identificar, documentar y fortalecer sus procedimientos para estos componentes y realizar los correspondientes planes de mejoramiento interno con el fin de suplir estas falencias; estas acciones son fundamentales para mejorar la eficiencia operativa, la resiliencia y la capacidad de respuesta de la infraestructura tecnológica.

Dado lo anterior, la auditora valida cuáles son las acciones definidas por el área de tecnología para abordar el PETI e indican que "*la DTGIJ, la STSI y la SGIJ han adelantado acciones en varios*

[18] Auditoria de Evaluación y Verificación del procedimiento de base de datos; numeral 7.1. Conclusiones; pág. 12; MJD - OCI, 28 de sept 2023; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2023/EvaluacionIndependiente/Informe-final-Procedimiento-de-Gestion-de-BD.pdf

[19] Plan Estratégico de Tecnología de la Información; numeral 3.5.6.2 Administración; pág. 181; MINJUSTICIA - Dirección de Tecnologías y Gestión de Información en Justicia, 2023; https://www.minjusticia.gov.co/transparencia/Documents/PETI-MJD-2024-2026-V1.pdf

[20] Auditoria de auditoría de evaluación y verificación del procedimiento de respaldo y restauración de los sistemas de información; numeral 7.1. Conclusiones; pág. 13; MJD - OCI, junio de 2023; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2023/EvaluacionIndependiente/Informe%20final%20auditoria%20Evaluaci%C3%B3n%20y%20verificaci%C3%B3n%20de%20estrategia%20de%20respaldo.pdf

frentes en colinealidad con lo descrito en el PETI como: Procesos y procedimientos – Servicios; La inclusión y actualización de nuevos servicios de TI en el catálogo de servicios; Procedimiento de control de cambios tecnológicos (no solo cambios a los Sistemas de Información); Fortalecer el procedimiento de gestión de incidentes, ya que el actual está enfocado principalmente en la gestión de incidentes de seguridad de la información; Definir un procedimiento de monitoreo y control de la disponibilidad de la infraestructura tecnológica".

- Por último en el numeral 3.7.2.7 Protección de datos señala que "*En el Registro Nacional de Bases de Datos (RNBD) de la SIC, se encuentran registradas 18 bases de datos que la entidad ha identificado con datos personales*[21]".

Con respecto a este numeral, el área de tecnología adjunta 18 constancias de radicación ante la Superintendencia de Industria y Comercio (en adelante SIC) del trámite de registro de las bases de datos con información personal, cumpliendo lo dispuesto en el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015, el cual establece el plazo para que los responsables del tratamiento inscriban sus bases de datos en el Registro Nacional de Bases de Datos (RNBD), de acuerdo con las instrucciones que para el efecto imparta la SIC.

6. Análisis de Riesgo

El área de tecnología allega matriz de riesgos de gestión, la cual tiene identificado un riesgo con sus causas y controles asociados, los cuales serán descritos a continuación:

Tabla 1. Matriz de riesgos de gestión

PROCESO	RIESGO	CAUSA	DESCRIPCIÓN DEL CONTROL
Gestión de las Tecnologías y la Información	Deficiencias en la gestión o demoras en los procesos por la pérdida de información contenida en medio electrónico, al no contar con la seguridad necesaria para salvaguardar la información o los backups requeridos.	Fallas de los dispositivos que salvaguardan la información.	1. El profesional designado como supervisor y los que hacen parte del equipo de trabajo cada vez que se presente un evento contingente (falla, indisponibilidad, intermitencia) de los servicios tecnológicos que soportan al Ministerio, evalúa el evento y determina si activa el plan de Contingencia del componente afectado. Evidencia: Documentación de activación de contingencia por parte del líder de Plan de recuperación de Desastres- DRP.

[21] Plan Estratégico de Tecnología de la Información; numeral 3.7.2.7 Protección de datos; pág. 220; MINJUSTICIA - Dirección de Tecnologías y Gestión de Información en Justicia, 2023; https://www.minjusticia.gov.co/transparencia/Documents/PETI-MJD-2024-2026-V1.pdf

PROCESO	RIESGO	CAUSA	DESCRIPCIÓN DEL CONTROL
Gestión de las Tecnologías y la Información	Deficiencias en la gestión o demoras en los procesos por la pérdida de información contenida en medio electrónico, al no contar con la seguridad necesaria para salvaguardar la información o los backups requeridos	Perdida de información por ataques cibernéticos a los servicios tecnológicos del Ministerio	2.El profesional designado y los que hacen parte del equipo de trabajo a fin de salvaguardar la información y evitar ataques cibernéticos a los servicios tecnológicos del Ministerio, ejecutara tareas como análisis de vulnerabilidades, ingeniera social, procedimientos de ethical hacking, implementación de equipos de seguridad perimetral, Simulación de ataques cibernéticos, reporte a la autoridad competente, remediación, entre otros. Evidencia : 1. Plan de análisis de vulnerabilidades, Resultados de los análisis de vulnerabilidades, Resultados de la remediación, retest para verificación de la corrección de las vulnerabilidades. 2. Reporte de ingeniería social , y capacitaciones de seguridad

Fuente: Área de tecnología

La OCI sugiere al área de tecnología validar la clase del 1er control el cual está definido en la matriz de riesgo como preventivo[22]: "*El profesional designado como supervisor y los que hacen parte del equipo de trabajo cada vez que se presente un evento contingente (falla, indisponibilidad, intermitencia) de los servicios tecnológicos que soportan al Ministerio, evalúa el evento y determina si activa el plan de Contingencia del componente afectado* "; lo anterior, teniendo en cuenta que las actividades descritas en el control serán realizadas una vez se presente una falla, intermitencia y/o indisponibilidad de los servicios tecnológicos utilizando el plan de recuperación de desastres (DRP[23]), lo cual por definición estaría más relacionado con controles de tipo correctivo[24].

Adicionalmente, se recomienda contemplar la inclusión de riesgos de corrupción asociados a accesos no autorizados, manipulación de datos y riesgos de seguridad de la información asociados a las 18 BD que contienen datos personales, contemplando la fuga de información; lo anterior, teniendo en cuenta que dentro de la evidencia presentada no allegan información que indique que la entidad cuente con herramientas tecnológicas que permita prevenir la pérdida o fuga de datos críticos, lo cual está documentado en el PETI en el numeral 3.7.2.7 Protección de datos[25].

[22] Control Preventivo: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
[23] Un DRP (Disaster Recovery Plan o Plan de Recuperación ante Desastres) es un conjunto documentado de estrategias, procesos y acciones que una organización implementa para recuperarse de un desastre que afecte a sus sistemas informáticos1. Este plan define los pasos a seguir para restaurar los datos, los sistemas y las aplicaciones críticas para el negocio en el menor tiempo posible
[24] Control Correctivo: aquellos que permiten el restablecimiento de la actividad, después de ser identificado un evento no deseable, también la modificación de las acciones que propiciaron su ocurrencia
[25] Plan Estratégico de Tecnología de la Información; numeral 3.7.2.7 Protección de datos; pág. 220; MINJUSTICIA - Dirección de Tecnologías y Gestión de Información en Justicia, 2023; https://www.minjusticia.gov.co/transparencia/Documents/PETI-MJD-2024-2026-V1.pdf

7. Conclusiones, hallazgos y/ recomendaciones

Se presentan las siguientes conclusiones y recomendaciones para la mejora del procedimiento de bases de datos del Ministerio de Justicia y del Derecho.

7.1. Conclusiones

Aún sigue vigente el procedimiento evaluado en la vigencia 2023, por lo cual se reitera la conclusión generada en el informe de BD de esa vigencia en cuanto a que: "*actualmente documentado; el cual, no toma en cuenta las actividades ejecutadas por los distintos actores que intervienen en el mismo, no involucra al oficial de seguridad y al de datos personales en cuanto a la definición de controles en las BD y solapa las actividades correctivas y preventivas realizadas en las bases de datos por el DBA*. *Cabe resaltar que no se encuentra alineado en cuanto al establecimiento, documentación e implementación de procesos, procedimientos y controles para asegurar el nivel de continuidad y, de esa manera, fortalecer la seguridad de la información y de los datos personales durante una situación adversa*[26]*"*.

Adicionalmente, aunque se reconoce el avance logrado en el establecimiento de acciones para subsanar la causa raíz de los dos hallazgos identificados por la auditoría de control interno, estas acciones no abordan completamente los problemas estructurales señalados en el informe realizado en la vigencia 2023; es esencial identificar las bases de datos que contienen datos personales y/o sensibles, definir claramente los responsables, implementar medidas de seguridad adecuadas y alinear las políticas con los procedimientos de gestión de bases de datos para garantizar la protección de los datos personales. Por esta razón, la OCI considera que el plan carece de vocación de efectividad en su estado actual.

7.2. Recomendaciones

La OCI realiza las siguientes recomendaciones, en cuanto a:

- Evaluar la actualización de la versión de la BD en Oracle ya que esta es obsoleta y puede provocar incidentes de seguridad al carecer de parches de seguridad recientes, lo que la hace vulnerables a ataques y brechas de seguridad.
- Mantener un histórico de las diferentes novedades ocurridas con las BD de la Entidad.
- Ingresar en la política de datos personales lineamientos que definan como se van a identificar las bases de datos que contienen datos personales y/o sensibles, cómo se van a organizar y clasificar según su tipo.
- Documentar las medidas técnicas de seguridad que serán implementadas para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado y si a su vez estas estarán alineadas con el procedimiento de gestión de base datos.

[26] Auditoria de Evaluación y Verificación del procedimiento de base de datos; numeral 7.1. Conclusiones; pág. 12; MJD - OCI, 28 de sept 2023; https://www.minjusticia.gov.co/ministerio/Documents/ControlInterno/Auditorias2023/EvaluacionIndependiente/Informe-final-Procedimiento-de-Gestion-de-BD.pdf

- Definir en la política de datos personales como se regulará la transferencia de datos personales a terceros, asegurando que se realice conforme a la ley y con el consentimiento del titular.
- Indicar en la política de datos personales como se otorgará seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Alinear la política de seguridad de la información y el procedimiento de base de datos.
- Definir los lineamientos para el tratamiento, manejo y seguimiento a los riesgos relacionados con las bases de datos que contienen datos personales y/o sensibles y sus controles asociados (matriz de riesgos) y quién será el responsable de dicha actividad.
- Definir claramente los responsables del tratamiento de datos y de las correspondientes medidas de seguridad asociadas.
- Documentar los lineamientos y/o procedimientos para componentes esenciales como servidores, servicios de conectividad, telefonía, nube, centros de cómputo y almacenamiento.
- Contemplar la inclusión de riesgos de corrupción asociados a accesos no autorizados, manipulación de datos y riesgos de seguridad de la información asociados a las 18 BD que contienen datos personales, contemplando la fuga de información

Mediante memorando MJD-MEM24-0007216 del día 27 de noviembre de 2024, se remite informe preliminar de esta auditoría, a la Dirección Técnica de Tecnologías y Gestión de Información en Justicia y la Subdirección de Tecnologías y Sistemas de Información, 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.

Es de agregar que el área de tecnología no envía comentarios o solicita reunión de socialización; por lo anterior el informe y sus respectivas recomendaciones se mantienen.

Con un muy cordial saludo,

_____	_____
Cristina Alarcón Tapiero	Diego Orlando Bustos Forero
Profesional OCI	Jefe Oficina de Control Interno
Auditor Líder	