EVALUACIÓN Y VERIFICACIÓN DEL PROCEDIMIENTO DE GESTIÓN DE BASE DE DATOS

INFORME FINAL

Oficina de Control Interno
28 de Septiembre de 2023

Tabla de contenido

1. Objetivo de la auditoría:

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”.

2. Alcance de la auditoría:

En el marco del objetivo definido, se evaluará la vigencia comprendida entre junio 2022 a junio de 2023, definiendo acciones relacionadas con:

- Soporte y Mantenimiento.
- Notificaciones recibidas por memoria, almacenamiento y procesador.
- Incidentes reportados a la mesa de ayuda.
- Acciones de Seguridad de la información relacionadas con las Bases de Datos.

3. Criterios de auditoría o parámetros normativos:

Para el desarrollo de la presente auditoría, se tendrán en cuenta los siguientes criterios: procedimiento de Gestión, Administración y Mantenimiento de las Bases de Datos e Infraestructura que soportan el motor de Base de Datos, con código P-TI-05, versión 04 y vigencia del 30 de junio de 2020; Política de seguridad de la información, con Código: G-IC-14, versión 03 y vigencia 19 de diciembre de 2022; Ley 1581 de 2012; CONPES 3975 de 2019; Manual Operativo MIPG v5; ISO 27001:2013; Guía Técnica de Principios MinTIC, versión 1.0.

4. Metodología:

La metodología empleada por la Oficina de Control Interno (en adelante OCI), se basó en un levantamiento de información por medio de un cuestionario con treinta y nueve (39) preguntas; por otra parte, se utilizaron métodos de evaluación tales como la constatación de información y análisis sobre la misma; adicionalmente, se realizaron visitas de campo y se estableció comunicación con el área de tecnología, para resolver las inquietudes que se iban presentando en el desarrollo de la auditoria.

La apertura de la auditoría se realizó mediante reunión virtual el día 3 de Agosto de 2023 con el Director Técnico de Tecnologías y Gestión de Información en Justicia, el Subdirector de Tecnologías y Sistemas de Información, los profesionales encargados de atender la auditoría, la jefe de la Oficina de Control Interno(e) 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.

5. Desarrollo de la Auditoría

5.1. Generalidades

La Gestión de Bases de Datos[1] en el Ministerio de Justicia y del Derecho (MJD) está soportada en 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, siendo el responsable del procedimiento el Subdirector de Tecnologías y Sistemas de Información (STSI).

La STSI realiza mantenimiento a las Bases de Datos (BD) de forma automática, con una periodicidad semanal y mensual, el cual se encuentra soportado en un plan de mantenimiento por cada BD. Para garantizar que dichos planes se ejecutan SQL[2] envía un correo electrónico al terminar cada tarea del plan de forma satisfactoria; dentro de las labores realizadas se encuentran: el mantenimiento de Índices[3], reducción de registros[4], truncamiento de registros[5] y limpieza de temporales[6].

Esta auditoría pudo detectar, con sujeción a la información aportada por el área de tecnología, que se encuentran identificadas en el marco del inventario de las Bases de Datos vigentes, las siguientes, a saber:

- 10 Bases de datos que se encuentran en SQL Server versión 2012, que corresponden a sistemas de información del MJD.
- 3 Bases de datos que se encuentran en SQL Server versión 2012, que corresponden al software base[7] (configuración).
- 21 Bases de datos que se encuentran en SQL Server versión 2019, que corresponden a los sistemas de información del MJD.
- 8 Bases de datos que se encuentran en SQL Server versión 2019, que corresponden al software base (configuración).

---

[1] B**ase de datos** es una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

[2] **El lenguaje de consulta estructurada (SQL**) es un lenguaje de programación para almacenar y procesar información en una base de datos relacional. Una base de datos relacional almacena información en forma de tabla, con filas y columnas que representan diferentes atributos de datos y las diversas relaciones entre los valores de datos. Puede usar las instrucciones SQL para almacenar, actualizar, eliminar, buscar y recuperar información de la base de datos.

[3] **El mantenimiento de índices** es el proceso de optimizar el rendimiento y la eficiencia de las consultas en una base de datos mediante la creación, organización y reconstrucción de los índices. Los índices son estructuras que facilitan la búsqueda y el acceso a los datos en las tablas. El mantenimiento de índices implica evaluar el estado de los índices, identificar los índices faltantes o innecesarios, eliminar la fragmentación de los índices y ajustar los parámetros de los índices según las necesidades.

[4] **La reducción de registros** en una base de datos es el proceso de eliminar o comprimir los datos que ocupan espacio innecesario o que son redundantes.

[5] **El truncamiento de registros** en una base de datos es una operación que elimina los registros inactivos o confirmados del registro de transacciones lógico, lo cual libera espacio en el registro físico.

[6] La limpieza de temporales en una base de datos es el proceso de borrar algunos archivos y directorios que no se usan o que ocupan mucho espacio en el disco. Estos archivos pueden ser generados por el sistema operativo, el motor de la base de datos o las aplicaciones que acceden a ella.

[7] 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 tableta12345. Se considera "base" porque es la plataforma donde el resto del software se apoya para ejecutarse

Dado que los nombres de las bases de datos del MJD pueden considerarse como información reservada, la auditora prefiere no relacionar sus nombres.

Es de agregar que, en la información de las BD, no se aprecia la identificación de las bases que contienen datos sensibles[8] y/o privados, lo cual incumple lo mencionado en la política de seguridad de la información "*Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo*[9]".

Adicionalmente, el DBA[10] menciona que no tiene conocimiento del tipo de información que reside en las bases de datos, lo cual permite ver que no existe una comunicación activa entre el DBA y el oficial de datos personales quien debería informar al DBA de la correspondiente identificación de las BD y trabajar en conjunto para implementar los controles del Programa Integral de Gestión de Datos Personales[11] a que dieran lugar.

"La STSI debe asegurar que el software de antivirus, antimalware, antispyware y antispam cuente con las licencias de uso requeridas, certificando su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor de servicios[12], para cumplir lo anterior el área en mención contempló que las BD deben ser migradas dentro del contrato firmado el 31 de agosto de 2023 con la Fábrica de Software.

5.2. Procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos

El procedimiento mencionado anteriormente, tiene como objetivo "*: Definir, implementar, hacer control y seguimiento a las actividades y acciones operativas y de mantenimiento, que propendan por la optimización, aseguramiento de la calidad, integralidad y seguridad de información, de las bases de datos, modelos relacionales y esquemas de intercambio de información, así como, la infraestructura que soporta el motor de la base de datos; permitiendo un acceso seguro, efectivo y poniendo a disponibilidad la información residente en las bases de datos para que pueda ser accedida por los sistemas de información de la entidad de manera oportuna y en tiempos óptimos*[13]".

---

[8] Se entiende por **datos sensibles** aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

[9] Política de seguridad de la información; Código: G-IC-14; Versión: 03 del 19 de diciembre de 2022; pág. 8; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/73234aa5-2d8e-45b8-8f13-d19eb8723b7c.pdf

[10] **El administrador de bases de datos (DBA**) es el profesional que administra las tecnologías de la información y la comunicación, siendo responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios y legales de bases de datos.

[11] El Programa Integral de Gestión de Datos Personales (PIGDP) es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales. Este programa funciona de forma cíclica, y después de implementado lo que se busca es la constante mejora continua, brindado de esta forma seguridad al ciudadano, en cuanto al uso y manejo que se da a sus datos personales

[12] Política de seguridad de la información; Código: G-IC-14; Versión: 03 del 19 de diciembre de 2022; pág. 20; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/73234aa5-2d8e-45b8-8f13-d19eb8723b7c.pdf

[13] Procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos e Infraestructura que Soporta el Motor de Base de Datos; código P-TI-05; versión 4 del 30 de junio de 2020; Pág. 1; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/39c245c1-0f5c-4f57-a660-ed1aa48e765c.pdf

El alcance es: "*Inicia con el seguimiento continuo a las alertas emitidas por las tareas programadas y los incidentes reportados por la mesa de ayuda y termina con la solución implementada con el cierre del incidente después de la aplicación de ajustes, modificaciones o tareas necesarias para mejorar el desempeño de las mismas y confirmación de los usuarios, administrando las cuentas. Este procedimiento aplica para todas las Bases de Datos que se encuentran implementadas dentro de los lineamientos de la Dirección de Tecnologías y Gestión de Información*[14]".

De acuerdo a lo anterior, la OCI insta a 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[15], 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**. *Sin embargo, la calidad de la información será responsabilidad de la(s) dependencia(s) que, de acuerdo con sus funciones, deba(n) gestionarla*[16]".

Dentro de las políticas de operación referidas en el procedimiento, se encuentran:

- *"Todo incidente reportado de BD o demoras en los tiempos de respuesta de los sistemas de información para consultar los log, deben ingresar por mesa de ayuda, según lo establecido en el*

[14] Procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos e Infraestructura que Soporta el Motor de Base de Datos; código P-TI-05; versión 4 del 30 de junio de 2020; Pág. 1; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/39c245c1-0f5c-4f57-a660-ed1aa48e765c.pdf

[15] Un **modelo relacional** es una forma de representar los datos y las relaciones entre ellos mediante un conjunto de tablas, cada una con un nombre único y un conjunto de atributos. Cada tabla tiene una clave primaria que identifica de forma única a cada fila, y puede tener una o más claves foráneas que hacen referencia a otras tablas.

[16] Política de seguridad de la información; Código: G-IC-14; versión 3 del 19 de diciembre de 2022; pág. 11 y 12; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/73234aa5-2d8e-45b8-8f13-d19eb8723b7c.pdf

procedimiento de Soporte a usuarios P-TI-02-01"[17]. Es de agregar que durante la vigencia comprendida entre junio 2022 a junio 2023 no fueron reportados incidentes en la mesa de servicio por estos ítems.

- "*Revisar la disponibilidad de la base datos: subir todos los archivos y componentes de las bases de datos, garantizar la consistencia y fiabilidad de los datos*[18]". Para examinar la disponibilidad de las BD se ingresa al SSMS[19], para validar el acceso al motor de BD; de no ser posible, se revisa los servicios (Componentes[20]), se realizan las tareas de configuración que sean necesarias, posteriormente se ingresa y se prueba la accesibilidad de forma aleatoria a las bases, y para garantizar la consistencia de los datos, el motor de bases de datos se encarga de realizar el proceso de revisión de estos ítems, de no cumplir, genera error y no permite la implementación de estos.

- *"Se debe brindar soporte y mantenimiento continuo, necesario para mantener un óptimo desempeño del motor de la base de datos, por medio del monitoreo periódico de los ambientes de producción y pruebas, los cuales deben propender por minimizar los tiempos en aplicación de los mismos*". Dentro de las labores de monitoreo realizadas por el DBA en los ambientes de pruebas[21] y producción se encuentran: Disk Usage[22], Index Usage Statistics[23], Procesador, Memoria, disco, red

- *"Se debe brindar soporte y mantenimiento continuo, necesario para mantener un óptimo desempeño del motor de la base de datos, por medio del monitoreo periódico de los ambientes de producción y pruebas, los cuales deben propender por minimizar los tiempos en aplicación de estos".* Al presentarse una advertencia o error el Motor de base de datos mediante los procesos o tareas programadas, se genera un envío de correo al administrador (DBA); en este caso, el administrador de base de datos realiza un análisis del evento y genera los correctivos del caso.

[17] Procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos e Infraestructura que Soporta el Motor de Base de Datos; código P-TI-05; versión 4 del 30 de junio de 2020; Pág. 2; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/39c245c1-0f5c-4f57-a660-ed1aa48e765c.pdf
[18] Procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos e Infraestructura que Soporta el Motor de Base de Datos; código P-TI-05; versión 4 del 30 de junio de 2020; Pág. 2; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/39c245c1-0f5c-4f57-a660-ed1aa48e765c.pdf
[19] SQL Server Management Studio (**SSMS** para abreviar) es un entorno de desarrollo integrado para administrar cualquier infraestructura SQL. Se utiliza para acceder, administrar, configurar y desarrollar todos los componentes de SQL Server y SQL Database.
[20] Un motor de base de datos o **SGBD** suele estar formado por una serie de componentes123. Los componentes comunes incluyen: Motor de almacenamiento de datos, Procesador de consultas, Capa de acceso a los datos, Interfaz de usuario.
[21] Un **ambiente de pruebas de software** es un entorno cerrado que se utiliza para evaluar y verificar que un producto o aplicación de software funciona correctamente antes de ser lanzado al público1. Estos ambientes permiten a los desarrolladores y probadores realizar pruebas en un entorno controlado, sin afectar el entorno de producción.
[22] **Disk Usage** es una herramienta que muestra las estadísticas de uso del disco y ayuda a limpiar el espacio en disco en varias versiones de Microsoft Windows
[23] Los **Index Usage Statistics** son estadísticas que proporcionan información sobre el uso de los índices en una base de datos. Estas estadísticas pueden ayudar a los administradores de bases de datos a identificar qué índices se utilizan con frecuencia y cuáles no se utilizan en absoluto12. También pueden ayudar a determinar si hay índices innecesarios que podrían eliminarse para mejorar el rendimiento

- *"El MJD se hace responsable de las Bases de Datos que están implementadas de acuerdo a los lineamientos establecidos en las políticas de implementación de bases de datos. Si por algún motivo las bases de datos a implementar se encuentran implementadas en otros motores, estas deben ser migradas a la plataforma establecida por el Ministerio[24]".* Cabe resaltar que la OCI solicita las políticas mencionadas y el área de Tecnología allega el procedimiento "Puesta en Producción de Software", con código P-TI-03, en versión 4 del 30 de junio de 2022, en el ítem Desarrollo se indican los pasos para la implementación de una nueva base de datos. De acuerdo a lo anterior, se solicita la revisión y ajuste del ítem en mención, ya que el lineamiento no está contenido en una política.

5.2.1. Desarrollo del Procedimiento

A continuación, se mencionan las actividades definidas en el procedimiento ya mencionado:

Tabla 1. Relación de actividades del procedimiento de BD

N°	Actividad	Descripción de la actividad	Observación OCI
1	Revisar las notificaciones.	Revisar las notificaciones que envían los procesos automáticos del motor de las advertencias en los umbrales en los dispositivos (memoria, almacenamiento y procesador).	Al presentarse una advertencia o error, el Motor de BD mediante los procesos o tareas programadas genera un correo de notificación al Administrador de Base de Datos (DBA).
2	Realizar ajustes de acuerdo con la revisión y análisis realizado.	Analizar los resultados del monitoreo y establecer dentro de las opciones de afinamiento el proceso más adecuado a ser aplicado que permita mitigar la materialización del riesgo reportado en las notificaciones. Realizar las validaciones y acciones necesarias que permitan establecer que las medidas aplicadas mitigaron evitaron que le riesgo se materializara.	Esta actividad, según el procedimiento, está a cargo solamente del DBA, sin tener en cuenta al oficial de seguridad de la información con el fin de realizar una revisión conjunta en cuanto a la respectiva mitigación del riesgo y al oficial de datos personales cuando las BD incluyan datos sensibles y/o privados.
3	Asignar responsable.	Determinar quién debe ejecutar el ajuste requerido asignando un responsable de acuerdo a las	El personal encargado de Mesa de Ayuda asigna en la correspondiente herramienta

[24] Procedimiento de Gestión, Administración y Mantenimiento de Bases de Datos e Infraestructura que Soporta el Motor de Base de Datos; código P-TI-05; versión 4 del 30 de junio de 2020; Pág. 2; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/39c245c1-0f5c-4f57-a660-ed1aa48e765c.pdf

N°	Actividad	Descripción de la actividad	Observación OCI
		funciones de los niveles de servicio establecidos y la naturaleza del incidente.	al DBA, los casos relacionados a incidentes reportado de BD o demoras en los tiempos de respuesta de los sistemas de información para consultar los log.
		Hacer análisis de acuerdo al reporte para establecer el origen de la falla informada. Establecer la política más conveniente a ser aplicada para dar solución al inconveniente.	De acuerdo al procedimiento el responsable de estas actividades es el personal encargado de mesa de ayuda. Es de agregar que las labores de análisis y corrección del DBA, no se mencionan en el procedimiento. En la validación realizada por la auditoria, se encuentra que el personal de mesa de ayuda no tiene injerencia en estas actividades; sus labores se reducen a realizar una verificación del tiempo dado para atender el caso; adicionalmente, validan que el estado del caso se encuentre en “solucionado”, que exista la aprobación por parte del funcionario que solicitó el caso y que, por último, aquel diligencie la encuesta de satisfacción, para así dar por finalizado el caso.
		Aplicar los correctivos que permitan restablecer el desempeño de las Bases de Datos y/o servidores.	
4	Efectuar las pruebas requeridas.	Realizar pruebas de verificación para verificar que la situación presentada ya fue solucionada, se evalúa si el incidente fue solucionado y recibir el Visto Bueno de quien reportó el incidente.	
5	Cerrar el incidente	Una vez recibido el VoBo de las pruebas realizadas se finaliza el incidente en la mesa de ayuda, cerrando el caso.	En el procedimiento esta actividad se encuentra a cargo del personal encargado Mesa de Ayuda. Cabe agregar, que no se menciona quien debe enviar el VoBo de las pruebas realizadas, o por cual medio se deben remitir.
6	Administrar Cuentas de usuario	Se recibe la solicitud de mesa de ayuda, para la creación de cuentas para acceder a determinada base	A través de la herramienta de mesa de ayuda, el jefe del área debe registrar el caso

N°	Actividad	Descripción de la actividad	Observación OCI
		de datos, la cual debe venir aprobada por el Jefe del Área.	indicando los siguientes datos: • Nombre de la persona a la que se le va a dar acceso. • Nombre del sistema de información al que se le va a dar acceso en la BD. • Perfil o permisos requeridos. Esta actividad en el documento se encuentra a cargo del DBA; por lo anteriormente expuesto, se debe corregir la responsabilidad de dicha labor; adicionalmente, no menciona los datos mínimos que debe contener la solicitud o indica el procedimiento con el cual tiene relación.
		Se crea la cuenta se da acceso a la base y se asigna el rol de acuerdo a lo requerido.	Esta actividad la realiza el DBA, de acuerdo a la información consignada en el caso.
		Se informa al solicitante para que realice las pruebas pertinentes. Una vez recibido el visto bueno se cierra el caso.	Esta labor, no menciona el canal por el cual se le informa al solicitante que realice las pruebas pertinentes o cuales son dichas pruebas.

Elaboración Propia

Frente a lo expuesto en el contenido de la tabla y de acuerdo a lo evidenciado en la visita de campo, podemos inferir que:

1. No se determinan claramente las acciones relacionadas con la gestión, administración y mantenimiento de las BD.
2. No están discriminadas las labores preventivas y correctivas realizadas sobre las BD.
3. Se determinan 3 actividades (Revisión de notificaciones, caso por mesa de servicio, creación de usuario) que se realizan en momentos y por causas diferentes, las cuales se encuentran definidas en orden consecutivo, lo cual confunde al lector.

4. No se contemplan todos los posibles responsables en determinadas actividades. como por ejemplo la labor número 3, donde indican que la labor de análisis y generación de correctivos en la BD es responsabilidad de mesa de ayuda, sin describir las acciones realizadas por el DBA.
5. Dentro del procedimiento no se mencionan las actividades realizadas por el DBA para dar solución a los casos ingresados por mesa de ayuda relacionados a incidentes reportados de BD o demoras en los tiempos de respuesta de los sistemas de información.
6. El procedimiento adolece de 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.
7. El procedimiento adolece de 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.
8. En algunas ocasiones, para dar respuesta a casos de mesa de ayuda, el DBA trabaja en conjunto con los funcionarios responsables de los sistemas de información.
9. Cuando el caso de mesa de ayuda está mal direccionado, el DBA lo devuelve a la mesa.
10. Dentro de las pruebas de verificación del rendimiento realizadas por el DBA para dar solución a los casos ingresados por mesa de ayuda se encuentra la revisión del rendimiento del procesador, memoria, tarjeta de red y Disco duro.
11. 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.
12. El DBA realiza labores de afinamiento dentro de los servidores, las cuales no se encuentran mencionadas en el procedimiento.
13. En la vigencia comprendida entre junio 2022 a junio 2023, no ingresaron casos a mesa de servicio referentes a inconsistencias en las BD.
14. En la vigencia comprendida entre junio 2022 a junio 2023, no ingresaron casos a mesa de servicio referentes a solicitudes de creación de acceso a BD.

Por medio de la generación de caso en la mesa de ayuda, se puede solicitar la creación de cuenta de usuario para el motor de una base de datos en específico, para lo cual se cuenta con roles definidos de la siguiente manera:

Tabla 2. Relación de roles bases de datos

Rol	Características
db_accessadmin	Administrador base de datos
db_backupoperator	Operador de backups
db_datareader	Acceso de lectura
db_datawriter	Acceso de escritura
db_ddladmin	Administrador de lenguaje de definición

Rol	Características
db_denydatareader	Denegación de lectura
db_denydatawriter	Denegación de escritura
db_owner	Propietario
db_securityadmin	Administrador de seguridad
public	Acceso sin privilegios

Elaboración Propia

6. Análisis de Riesgo:

La STSI indica que el procedimiento no cuenta con matriz de riesgos; por lo anterior, cabe resaltar la importancia de identificar los riesgos asociados y sus respectivos controles con el fin de que la información contenida en las bases de datos que contengan información sensible y/o privada cuente 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. La OCI recomienda identificar y valorar dichos riesgos, y detallar los controles que deban ejercerse periódicamente para garantizar el principio de seguridad contemplado en la Ley 1581 de 2012, dentro de sus principios rectores.

Este posible riesgo puede provocar un presunto daño a la reputación de la entidad por la exposición o modificación parcial o total de datos sensibles y/o privados; adicionalmente, de implicar una posible multa o sanción por parte de la Superintendencia de Industria y Comercio (SIC).

7. Conclusiones, hallazgos y/ recomendaciones

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

7.1. Conclusiones

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.

7.2. Socialización del informe de auditoria

Mediante memorando MJD-MEM23-0006374 del día 22 de septiembre de 2023, se remite informe preliminar de esta auditoría, a la Dirección y Subdirección a cargo, mediante el cual se informa que pueden remitir sus comentarios o promover una reunión de socialización con la OCI, dentro de los tres (3) días siguientes a la recepción de este informe, conforme lo dispone el procedimiento de Auditoría Interna.

La DTGIJ, genera comunicación radicada bajo el número MJD-MEM23-0006473 del 26 de septiembre de 2023, a través de la cual envían respuesta frente a los hallazgos evidenciados en el informe.

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

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
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*".	Dentro del alcance del procedimiento P-TI-05 "Inicia con el seguimiento continuo a las alertas emitidas por las tareas programadas y los incidentes reportados por la mesa de ayuda y termina con la solución implementada con el cierre del incidente después de la aplicación de ajustes, modificaciones o tareas necesarias para mejorar el desempeño de las mismas y confirmación de los usuarios, administrando las cuentas. Este procedimiento aplica para todas las Bases de Datos que se encuentran implementadas dentro de los lineamientos de la Dirección de Tecnologías y Gestión de Información.", no contempla el tipo de información residente en las bases de datos puesto que esta es responsabilidad del área usuaria del sistema de información. En este sentido la Subdirección de Tecnologías y Sistemas de Información es responsable de la custodia de las bases de datos y archivos de copias de seguridad.	De acuerdo con lo mencionado por el área auditada, **nos permitimos confirmar el hallazgo**, teniendo en cuenta lo siguiente: • Dentro del objetivo del procedimiento P-TI-05 se indica: "*Definir, implementar, hacer control y seguimiento a las actividades y acciones operativas y de mantenimiento, que propendan por la optimización, aseguramiento de la calidad, integralidad y seguridad de información, de las bases de datos."* Para realizar las actividades de definición, implementación, control y seguimiento, se deben tener identificadas las BD a las cuales se les realizará dichas labores en primera instancia, lo cual debería estar alineado con lo mencionado en la política de seguridad de la información actualmente vigente en el MJD, la cual hace referencia a las labores del Oficial de Datos "*Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo*". • Dentro del alcance del procedimiento auditado, se indica que "*Este procedimiento aplica para todas las Bases de Datos que se encuentran implementadas dentro de los lineamientos de la Dirección de*

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
	Adicionalmente, las tareas y alcance del procedimiento están encaminadas a que los tiempos de respuesta en el acceso de los datos residentes y la atención a incidentes sean los óptimos. De otra parte, la entidad realiza la identificación y clasificación de los activos de información (la cual se actualiza anualmente) bajo el liderazgo del Oficial de Seguridad de la Información, con la participación de todas las dependencias, lo cual se encuentra estipulado en el procedimiento P-IC-06 Gestión de Activos de Información, vigente. Cada uno de los responsables o dueños de los activos (coordinadores, jefes, subdirectores, directores, etc) debe mantener el inventario de activos aprobado y actualizado, determinar los controles necesarios para asegurar su confidencialidad, integridad y disponibilidad, y mantener ese seguimiento y control a través de los custodios de cada activo. Adicionalmente, quien ejerza el rol o cargo de Oficial de Protección de Datos Personales lidera en el Ministerio la implementación de la Política de Protección de Datos Personales y así mismo, la identificación y reporte de las bases de datos personales gestionadas en la entidad, a la Superintendencia de Industria y Comercio. Este reporte fue realizado, en cumplimiento de la normatividad. En conclusión, La Subdirección de Tecnologías y Sistemas de Información está cumpliendo en función del procedimiento P-TI-05, objeto de la auditoria,	*Tecnologías y Gestión de Información*"; lo cual, incluye las BD con información personal y/o sensible. Si bien es cierto que tecnología no es responsable del tipo de información residente en las bases de datos, no exime al área de la responsabilidad de tener identificada y alineada la información del inventario de las bases de datos que contienen información personal y/o sensible con los diferentes actores que manejan, técnicamente, las bases de datos; en este caso el DBA, y el oficial de datos personales máxime si ambos funcionarios pertenecen a la Dirección de tecnología. • La política de seguridad de la información contempla que el oficial de datos personales debe ""*Servir de enlace y coordinador con las demás áreas de la organización para la implementación transversal del Programa Integral de Gestión de Datos Personales";* lo cual, implica que el oficial de datos personales, debería informar de la identificación de las BD con información sensible al DBA, para realizar unificación del inventario y así realizar las medidas técnicas necesarias para cumplir con el Programa Integral de Gestión de Datos Personales y así "*propender la optimización, aseguramiento de la calidad, integralidad y seguridad de información, de las bases de datos"*, lo cual está contemplado dentro del objetivo del procedimiento en mención. • Cabe resaltar que, en las distintas labores realizadas por la auditoria, no se vio reflejada la alineación de la información entre el DBA y el oficial de datos personales, teniendo en cuenta las evidencias aportadas, la visita de campo y la respuesta de la pregunta allegada por la auditoria "*Se encuentran identificadas las BD que contienen datos personales*" indicando que "*como DBA no tengo acceso ni conocimiento del tipo de información que reside en las bases de datos*"; lo cual reitera que los distintos actores que intervienen en el proceso de las BD no interactúan entre sí,

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
	aplicando los controles de seguridad sobre las bases de datos de la entidad. La auditoría no se extendió a temas de activos de información e inventario de las bases de datos personales, lo cual demanda una serie de soportes, procesos y actores que no fueron indagados, se entiende así que el hallazgo no corresponde a lo observado en el ejercicio de la auditoría.	provocando desinformación y en este caso la no identificación de las BD con datos personales y/o sensibles por parte del DBA. En conclusión, se mantiene el hallazgo y se recomienda a la Subdirección de Tecnologías y Sistemas de Información (STSI), en cabeza de la Dirección de tecnología, alinear la información de los diferentes procesos, guías, políticas y procedimientos del área, para evitar desinformación y unificar el inventario de BD con los diferentes actores que deban conocer dicha información identificando las que tienen datos personales y/o sensibles.
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*".	Dentro del alcance del procedimiento P-TI-05 "Inicia con el seguimiento continuo a las alertas emitidas por las tareas programadas y los incidentes reportados por la mesa de ayuda y termina con la solución implementada con el cierre del incidente después de la aplicación de ajustes, modificaciones o tareas necesarias para mejorar el desempeño de las mismas y confirmación de los usuarios, administrando las cuentas. Este procedimiento aplica para todas las Bases de Datos que se encuentran implementadas dentro de los lineamientos de la Dirección de Tecnologías y Gestión de Información.", no contempla la documentación de los riesgos relacionados con las bases de datos que contienen datos personales y/o sensibles y sus controles asociados (matriz de riesgos). En este sentido la Subdirección de Tecnologías y Sistemas de Información es responsable de la custodia de las bases de datos y archivos de copias de seguridad. Adicionalmente, las tareas y	En el memorando MJD-MEM23-0004902 correspondiente a la apertura de la auditoria, se realizó la solicitud de la matriz de riesgos asociada al procedimiento, lo cual se reiteró por medio de solicitud por correo institucional con fecha del 15 de agosto de 2023, obteniendo respuesta por parte del DBA vía correo electrónico con fecha del día 15 de agosto de 2023 que indica "*El procedimiento no tiene matriz de riesgo asociado*"; adicionalmente, todos los informes de auditoría independiente manejan un capítulo dedicado a riesgos, como es el caso del presente informe. En el objetivo del procedimiento se menciona "*implementar, hacer control y seguimiento a las actividades y acciones operativas y de mantenimiento, que propendan por la optimización, aseguramiento de la calidad, integralidad y seguridad de información, de las bases de datos".* Al mencionar optimización y aseguramiento de la seguridad de la información se incluye el estudio y gestión de los riesgos a la seguridad de la información, los cuales hacen parte de la matriz de riesgos. Si bien es cierto que la Dirección de tecnología, en cabeza del oficial de seguridad, lidera la identificación y valoración de los riesgos de seguridad de la información, en conjunto con las

HALLAZGO	RESPUESTA DTGIJ	RESPUESTA OCI
	alcance del procedimiento están encaminadas a que los tiempos de respuesta en el acceso de los datos residentes y la atención a incidentes sean los óptimos. La entidad realiza la gestión de los riesgos de seguridad de la información, relacionados con los activos de cada proceso, de acuerdo con lo establecido en la Guía de Administración de Riesgos G-MC-04. El rol de Oficial de Seguridad de la Información lidera la identificación y valoración de los riesgos de seguridad, así como la definición de los controles requeridos para su mitigación. Sin embargo, los dueños de los riesgos son los líderes de cada proceso; quienes se deben responsabilizar por la gestión de dichos riesgos y la implementación de los controles aplicables, es decir 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". En conclusión, el Ministerio de Justicia y del Derecho identifica y hace gestión sobre riesgos al margen del procedimiento P-TI-05, objeto de la auditoria. La auditoría no se extendió a temas de gestión de riesgos de seguridad, lo cual demanda una serie de soportes, procesos y actores que no fueron indagados; se entiende así que el hallazgo no corresponde a lo observado en el ejercicio de la auditoría.	áreas del MJD; de acuerdo a la política de seguridad de la información actualmente vigente en el MJD, dentro de las labores del oficial de datos personales se encuentra: "*Implementar buenas prácticas de gestión de datos personales dentro del MJD. El oficial de privacidad tendrá la labor de estructurar, diseñar y administrar el programa que permita a la entidad cumplir el marco regulatorio sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente*". Al referirse en el lineamiento de la política lo relacionado a establecer, evaluar y revisar los controles, hacen referencia a la respectiva matriz de riesgo. Adicionalmente, la política contempla "*Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales",* dado lo anterior, dicha labor está en cabeza de la Subdirección de tecnología de la cual hace parte el oficial de datos personales, según la resolución 0164 del 08 de febrero de 2023. Teniendo en cuenta lo anteriormente descrito, **se mantiene el hallazgo**.

Elaboración propia

7.3. 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*".

7.4. 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**. 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.

Con un muy cordial saludo,

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