OFICINA DE CONTROL INTERNO

INFORME DE EVALUACIÓN

TIPO DE INFORME

Preliminar [ ] **Definitivo** [x]

Evaluación interna de la calidad a las bases de datos que hacen parte de la operación estadística de los Grupos de Investigación Reconocidos y Medidos por el Ministerio de Ciencia, Tecnología e Innovación, e Investigadores Reconocidos por el Ministerio de Ciencia, Tecnología e Innovación, que serán evaluados por el DANE bajo la Norma Técnica de Calidad del Proceso Estadístico NTC PE 1000-2020.

AÑO	EVALUACIÓN No.	PROCESO, PROCEDIMIENTO O ACTIVIDAD	ÁREA RESPONSABLE
2023	E-01	Base Datos Operación Estadística Grupos de Investigación reconocidos y medidos por el Ministerio de Ciencia, Tecnología e Innovación e Investigadores reconocidos por el Ministerio de Ciencia, Tecnología e Innovación	Dirección de Ciencia (Equipo Técnico Operaciones Estadística) - Oficina de Tecnologías y Sistemas de Información.

PERIODO AUDITADO O EVALUADO	FECHA INFORME PRELIMINAR	FECHA INFORME DEFINITIVO
Año 2022 hasta el 30 de marzo de 2023	11/05/2023	16/05/2023

Informe elaborado por:
Javier Herrera – Greecy Rivera
Oficina de Control Interno

Contenido

INTRODUCCION

Las actividades de la Evaluación de la Base de Datos de la Operación Estadística de los Grupos de Investigación Reconocidos y Medidos por el Ministerio de Ciencia, Tecnología e Innovación, e Investigadores Reconocidos por el Ministerio de Ciencia, Tecnología e Innovación, se desarrollan en el marco del Plan de Evaluación definido por la Oficina de Control Interno, el cual tiene como propósito evaluar el cumplimiento de los requisitos la Norma Técnica de la Calidad del Proceso Estadístico NTC PE 1000:2020 para la generación de Estadísticas, para verificar el cumplimiento de las disposiciones establecidas en el desarrollo de la Base Datos de la Operación Estadística y así, comprobar que las actividades de han desarrollado y se mantienen de manera eficaz, llevando controles adecuados teniendo en cuenta los riesgos identificados dentro de la Entidad.

Al finalizar se habrán encontrado las desviaciones que es necesario corregir para lograr elevar el cumplimiento en las actividades desarrolladas y así permitir que la Operación Estadística se desarrollen eficazmente en cumplimiento de las directrices dadas.

1. OBJETIVOS

Los objetivos propuestos para el desarrollo de la presente **Evaluación** apuntan a:

Llevar a cabo la evaluación interna de la calidad a las bases de datos que hacen parte de la operación estadística de los Grupos de Investigación Reconocidos y Medidos por el Ministerio de Ciencia, Tecnología e Innovación, e Investigadores Reconocidos por el Ministerio de Ciencia, Tecnología e Innovación, que será evaluado por el DANE bajo la Norma Técnica de Calidad del Proceso Estadístico NTC PE 1000-2020.

2. ALCANCE

Aplica a los procesos definidos en el Mapa de Procesos de Minciencias relacionado con las bases de datos que hacen parte de las operaciones estadísticas de los Grupos de Investigación Reconocidos y Medidos e Investigadores Reconocidos por el Ministerio de Ciencia, Tecnología e Innovación, desarrollada en el año 2022 hasta el 30 de marzo de 2023.

3. METODOLOGÍA

La Metodología empleada para desarrollar la presente Evaluación se soporta en la verificación y análisis de documentos y/o registros físicos y virtuales, la consulta en sistemas de información, página web, revisión de respuestas a solicitudes de información escrita y verbal, pruebas selectivas, pruebas de observación, visitas de inspección, entrevistas, encuestas, mesas de trabajo con los servidores públicos y contratistas que lideran y apoyan el Equipo Técnico de Minciencias: responsables técnicos de la Operación Estadística y los responsables en la OTSI, con el fin de valorar su estado y nivel de cumplimiento frente a los requisitos técnicos, de oportunidad y legales que le aplican.

4. MUESTRA

La Muestra empleada para desarrollar la presente Evaluación se fundamenta en muestreo aleatorio simple revisando la información relevante del proceso y con la que se puede demostrar cumplimiento.

5. RIESGOS EVALUADOS

Se identificaron que los siguientes riesgos potenciales a los que se ve expuesta la Entidad en el desarrollo de las actividades relacionadas con la presente Evaluación y que no están contemplados en el Mapa de Riesgos vigente para la entidad son:

RIESGOS POTENCIALES IDENTIFICADOS
1. Riesgo de presentación no apropiada de resultados en casos de prueba al no incluir las evidencias de cumplimiento obtenidos en cada uno de los pasos establecidos en los casos de pruebas.
2. Riesgo de Ataques de malware y phishing de credenciales.
3. Riesgo de Falta de segregación de funciones.
4. Riesgo de Acceso no autorizado a la información.
5. Riesgo de Aprovechamiento de vulnerabilidades de seguridad.

6. Riesgo de Pérdida de disponibilidad de la información.
7. Riesgo de Intercambio inseguro de información con terceros.
8. Riesgo de Pérdida de confidencialidad de datos sensibles o robo de contraseñas por debilidad en controles de infraestructura con acceso a Internet.
9. Riesgo de Errores en el análisis de los datos.

6. RESULTADOS DE AUDITORIA

6.1 FORTALEZAS

1. La definición de controles en el manejo de la base de datos permite obtener resultados adecuados y cumplir con los requisitos de cumplimiento a las operaciones de Gestión Estadística.
2. Las actividades de Diseño y Desarrollo se mantienen controladas permitiendo controlar la materialización de riesgos.
3. Se mantienen controladas las relaciones con los proveedores externos, actividades que favorecen los buenos resultados de la administración de la Base de Datos para las Operaciones Estadísticas.

6.2 HALLAZGOS

Hallazgo ***No. 1: Debilidades en la definición y configuración de cuentas de usuario de terceros***	
Riesgo Potencial: Ataques de malware y phishing de credenciales. **Causa:** • Ausencia de adecuadas directrices de seguridad implementadas para la gestión de cuentas de usuario y contraseñas.	**Nivel de riesgo Alto** 
USO DE NOMBRES DE CUENTA GENÉRICOS PARA LA ASIGNACIÓN DE USUARIOS Las cuentas de usuario genéricas son el principal objetivo en los ataques de malware y phishing de credenciales, casi un 30% se dirigen a alias de cuentas de usuario genéricas y no a aquellas cuentas que claramente pertenecen a un individuo en concreto. Estos alias de grupo suelen ser particularmente atractivos para los atacantes, porque, por un lado, a través de ellos pueden alcanzar un mayor número de objetivos dentro de una misma organización y, además, son más difíciles de proteger con una autenticación multifactor. Con el propósito de ***evaluar directrices de seguridad implementadas para la gestión de cuentas de usuario y contraseñas***, solicitamos a la Oficina de Tecnologías y Sistemas de Información, el listado de usuarios con sus roles, privilegios, permisos, dueño/propietario de cada ID de usuario (Nombre, cargo, cédula, dependencia, entidad) y alcance funcional, con acceso a las bases de datos (objeto de estudio) y que soportan las actividades de operación de las bases de datos, incluidos los usuarios que consultan información de las bases de datos (producción, desarrollo, réplica, pruebas, etc.) mediante, por ejemplo, la ejecución de comandos SQL.	

Al respecto nos fue remitida la relación de los 237 usuarios creados con accesos a con acceso a las bases de datos (objeto de estudio) y que soportan las actividades de operación de estas.

A partir de los archivos remitidos, realizamos revisión del **100%** de estos registros.

Con base en las entrevistas sostenidas con cada uno de los involucrados al proceso, pruebas realizadas, y análisis de la información remitida, procedimos a seleccionar las cuentas cuyo nombre fuera de interpretación Genérica, es decir que no se identificará responsable o propietario directo y personalizado de la cuenta, evidenciando aspectos susceptibles a mejorar relacionados con la asignación de 237 cuentas con nombres genéricos, de las cuales algunas corresponden a cuenta de tipo "Administración", lo que puede representar una pérdida de integridad de la información, debido a que las cuentas genéricas en usuarios administradores o de altos privilegios son utilizados mediante accesos que pueden ser efectuados desde múltiples equipos y distintas ubicaciones.

Existen cuentas de usuario genéricas que son utilizadas por el equipo de desarrollo, soporte de aplicaciones, gestión de la configuración y DBA, con privilegios de amplio alcance funcional, situación que se constituye en un alto índice de complejidad en el análisis a la trazabilidad de la información, al no poder identificar específicamente que usuario realmente utilizaba la cuenta objeto de alguna investigación.

Con base en los procesos de observación realizados, identificamos que existen usuarios a los que se les ha otorgado el privilegio del sistema CREATE USER, quienes pueden crear cuentas de usuario, incluidas las cuentas de usuario que se utilizarán como usuarios proxy. Debido a que el privilegio del sistema CREATE USER es un privilegio poderoso, un administrador de base de datos o un administrador de seguridad suele ser el único usuario que tiene este privilegio del sistema.

En conclusión, parte fundamental de los controles de acceso, es la adecuada gestión de privilegios, perfilamiento de usuarios y trazabilidad, por lo que en cuanto a la gestión de usuarios, tener usuarios genéricos se constituye en una muy mala práctica de seguridad porque bajo la asignación de un usuario ADMINFUNCIONAL, ADMINTECNICO, BNP, etc. al momento en que se cometa un fraude o un uso no autorizado de la cuenta no se tendrían las herramientas para imputar responsabilidad (ante una instancia por ejemplo legal) debido que, tal y como esta creado el usuario, no habría forma de corroborar que específicamente ese usuario genérico corresponde a determinada persona, justificando que así como se utilizó por X persona, se pudo haber utilizado por Y persona, así se cuente con un acta en donde formalmente se haya asignado el usuario a determinada persona, ante un juicio, no habría lugar, adicionalmente se presta para que haya uso compartido de esos accesos, mientras que si se individualizan los usuarios de alguna manera se le da la responsabilidad del uso y manejo específicamente al usuario al que se le asignó, esta labor de individualización de responsabilidad es fundamental, lo que adicionalmente facilita las gestiones de trazabilidad y seguimiento, hoy en día una de las buenas prácticas como parte del monitoreo de accesos que debe realizarse de manera periódica.

Recomendación

- Fortalecer el proceso de gestión de cuentas privilegiadas a partir de la creación de una política general que incluya la especificación que permita contar con un estándar centralizado que establezca el nivel de control que debe existir sobre las cuentas privilegiadas de la entidad, sus mecanismos de monitoreo, así como incluir el inventario existente que administra el área de TI por cada una de las plataformas y aplicaciones utilizadas por la entidad y de otra parte conforme al nivel de riesgo y la evaluación correspondiente de la gestión de cuentas y/o usuarios privilegiados en la entidad, se sugiere ampliar la cobertura a otros sistemas de información o plataformas, todo lo anterior con base en un marco documentado y estandarizado para la gestión de cuentas privilegiadas en la entidad y la existencia de herramientas especializadas como PASSWORD MANAGER.

- Analizar la posibilidad de que los usuarios con altos privilegios y administradores solo usen cuentas con identificador personal, con el fin que este identificador no indique sus privilegios y sean fácilmente rastreadas ante cualquier análisis a la trazabilidad de la información por cada cuenta objeto de alguna investigación.

- Para cuentas de usuario genéricas que son utilizadas por el equipo de desarrollo, soporte de aplicaciones, gestión de la configuración y DBA, las cuales, en algunos casos, se pueden ver expuestas a compartirse, se debe establecer privilegios de solo

consulta a las bases de datos.

- Implementar adecuadas directrices para la gestión de cuentas de usuario, tales como:
  - No promueva el uso compartido de cuentas de usuario. Siempre se debe crear una cuenta separada para cada usuario de Oracle. Oracle admite como máximo 10 cuentas de usuario locales. Si está gestionando un sitio más grande y requiere más de 10 cuentas de usuario, debe considerar utilizar un servicio de autenticación de usuarios de terceros, como LDAP o AD.
  - Seleccione nombres que cumplan con los requisitos para las cuentas de usuario locales. Cuando elija una contraseña para la cuenta de usuario de Oracle local, la contraseña debe cumplir con, al menos, lo siguiente: Debe ser siempre una contraseña segura que contenga una longitud máxima de dieciséis caracteres, debe contener una combinación de caracteres en minúscula y mayúscula, además de uno o dos caracteres especiales para crear una contraseña compleja y segura, no debe tener espacios, punto (.) ni dos puntos (:), debe cumplir con la política de gestión de contraseñas de la empresa, entre otros.
  - Limite los privilegios de cuenta de usuario basados en el rol del puesto (principios de menor privilegio). El principio del menor privilegio indica que, para una buena práctica de seguridad, se le debe dar al usuario la menor cantidad posible de privilegios para hacer su trabajo. El otorgamiento excesivamente ambicioso de responsabilidades, roles, etc. (en especial, al comienzo del ciclo de vida de una organización), puede dejar vulnerable un sistema. Revise los privilegios de usuarios con regularidad para determinar la relevancia con las responsabilidades actuales de los puestos de cada usuario. Oracle brinda la posibilidad de controlar los privilegios de usuario de cada usuario. Asegúrese de que se asignen los permisos de rol de usuario adecuados a cada cuenta de usuario, según el rol del puesto.
- Implementar adecuadas directrices para la gestión de contraseñas, tales como:
  - Cambie la contraseña por defecto root Password (changeme) inmediatamente después del primer inicio de sesión. Para activar el primer inicio de sesión y acceder a Oracle, se proporciona una cuenta root de administrador local con el sistema. Para crear un entorno seguro, debe cambiar la contraseña de administrador (changeme) después del primer inicio de sesión en Oracle. La obtención de acceso no autorizado a la cuenta root de administrador proporciona al usuario acceso libre a todas las funciones de Oracle. Por lo tanto, es importante especificar una contraseña segura.
  - Cambie todas las contraseñas de la cuenta de Oracle con regularidad. Para evitar la actividad maliciosa y garantizar que las contraseñas se ajusten a las políticas de contraseñas actuales, debe cambiar todas las contraseñas de Oracle regularmente.
  - Aplique prácticas comunes para la creación de contraseñas complejas y seguras, tales como:
    - No cree una contraseña de menos de dieciséis caracteres de longitud.
    - No cree una contraseña que contenga el nombre de usuario, el nombre del empleado o el nombre de un miembro de su familia.
    - No elija contraseñas que se adivinen fácilmente.
    - No cree contraseñas que contengan una cadena consecutiva de números, como 12345.
    - No cree contraseñas que contengan una palabra o cadena que se pueda descubrir fácilmente mediante una simple búsqueda por Internet.
    - No permita que los usuarios vuelvan a utilizar la misma contraseña en varios sistemas.
    - No permita que los usuarios vuelvan a utilizar contraseñas anteriores. Maneje históricos.

- Para obtener la máxima seguridad, siempre enmascare las nuevas entradas de contraseña.
- Establecer restricciones de política de contraseña para usuarios locales. Aplique una política de contraseñas para todas las cuentas de usuarios locales.

- Consulte con el responsable de seguridad de TI para conocer las políticas de gestión de contraseñas.

- Realice campañas de sensibilización periódicamente para promover cumplimiento a las directrices para la gestión de cuentas de usuario y contraseñas.

Hallazgo No. 2: Perfiles asignados que no corresponden conforme a las funciones del cargo

Riesgo Potencial: Falta de segregación de funciones.

Causa:

- Alcance funcional otorgado a los usuarios mediante perfil asignado que no corresponde a sus funciones.

Nivel de riesgo Medio

2

PERFIL ASIGNADO CONFORME A FUNCIONES

La segregación de funciones es una herramienta de control interno que se utiliza para prevenir riesgos de fraudes o errores operativos en las empresas u organizaciones. Consiste básicamente en separar las funciones o tareas críticas, que sean incompatibles entre sí, para que no recaigan en una sola persona. Segregar funciones significa por ejemplo que la misma persona que emite un cheque no sea quien lo apruebe, para evitar riesgos de que haga fraudes con pagos indebidos.

Con el propósito de ***evaluar cumplimiento al principio de segregación de funciones***, solicitamos a la Oficina de Tecnologías y Sistemas de Información, confirmación del usuario nombrado en sus funciones u obligaciones contractuales con responsabilidades de gestión o administración de las aplicaciones (y a la vez de sus componentes, como bases de datos).

Al respecto nos fue remitida la siguiente respuesta *"(…) A nivel de contratistas para el apoyo de las funciones de la Oficina de Tecnologías, es importante señalar que se tiene identificado y se requiere contemplar la contratación de los siguientes perfiles:*

- *Líder funcional del sistema misional SCIENTI.*
- *Líder técnico del sistema misional SCIENTI.*
- *Administrador de bases de datos.*

En la actualidad se cuenta con el apoyo de los profesionales:

- *Nidia Janneth León Cabeza, contrato 198 de 2023*
- *Gabriel Bustos Quiroga, contrato 206 de 2023 (…)".*

A partir de los archivos remitidos, realizamos revisión del **100%** de estos registros.

Con base en las entrevistas sostenidas con cada uno de los involucrados al proceso, pruebas realizadas, y análisis de la información remitida, identificamos que revisado el Manual_especifico_de_funciones_y_competencias_laborales_minciencias_2020.pdf, existe dentro de la Planta de Personal del Ministerio de Ciencia, Tecnología e Innovación el cargo de profesional especializado 2028-17, ubicado en la oficina de tecnologías y sistemas de información, el cual a la fecha de esta evaluación se encuentra vacante. (página 134)

Entre las funciones esenciales se encuentran las siguientes:

- Ejecutar proyectos de tecnologías de la información de acuerdo con las necesidades y requerimientos del Ministerio.
- Desarrollar los proyectos o soluciones informáticas que requiera la Entidad, de acuerdo con las políticas de Tecnologías de la Información y las Comunicaciones.
- Desarrollar actividades para la implementación, actualización y mantenimiento del Sistema de Seguridad de la Información del Ministerio, siguiendo las políticas internas.
- Participar en el diseño e implementación de la arquitectura empresarial del Ministerio, de acuerdo con las necesidades de la Entidad y los lineamientos de gobierno Nacional.
- Desarrollar las operaciones de mantenimiento y soporte a la plataforma tecnológica del Ministerio, para la continuidad en la prestación de los servicios informáticos, y de acuerdo con las políticas establecidas y los recursos asignados.

- Mantener actualizada la información para la instalación, configuración y operación de las soluciones tecnológicas bajo su responsabilidad.
- Diseñar y administrar los esquemas y estructuras de las bases de datos del Ministerio, de acuerdo con los procedimientos de la entidad.
- Coordinar y adelantar asuntos relacionados con la planeación, ejecución y seguimiento de actividades para los procesos de apoyo que requiera la operación de la dependencia.
- Elaborar documentos, conceptos e informes que le sean requeridos.
- Desempeñar las demás funciones que le sean asignadas por la autoridad competente, de acuerdo con el área de desempeño, el nivel jerárquico y la naturaleza del empleo.

Con los siguientes requisitos de formación académica y experiencia:

- Ingeniero de sistemas/electrónica con postgrado en la modalidad de especialización.
- Tarjeta profesional en los casos reglamentados por la ley.
- Veintidós (22) meses de experiencia profesional relacionada. Con postgrado.
- Cuarenta y seis (46) meses de experiencia profesional relacionada. Con Tarjeta profesional.

Conforme a lo indicado anteriormente, en la actualidad se cuenta con el apoyo de los siguientes profesionales para apoyar esta gestión:

- Nidia Janneth León Cabeza - Contrato 198 de 2023.
- Gabriel Bustos Quiroga - Contrato 206 de 2023.

Con base en los procesos de observación realizados a los contratos de estos profesionales, identificamos que:

Contrato 198 de 2023

- El profesional no cuenta con obligaciones que permitan dar cumplimiento a las funciones esenciales solicitadas para el cargo de profesional especializado 2028-17.
- El profesional no cuenta con la formación académica y experiencia según lo indicado en el cargo de el cargo de profesional especializado 2028-17 y sus equivalencias.

Contrato 206 de 2023

- El profesional cuenta con obligaciones que permiten dar cumplimiento a las funciones esenciales solicitadas para el cargo de profesional especializado 2028-17.
- El profesional cuenta con la formación académica y experiencia según lo indicado en el cargo de el cargo de profesional especializado 2028-17 y sus equivalencias.
- El profesional actualmente ejerce el rol de DBA, y a la vez funciones del gestor de accesos a la BD, líder funcional, líder técnico, arquitecto de bases de datos, analista de base de datos, entre otras por lo que no se identifica una adecuada segregación de funciones.

En conclusión, se requiere fortalecer la planta de personal del MinCiencia en lo relacionado a la gestión de seguridad, administración, operación, mantenimiento y monitoreo de las bases de datos, teniendo en cuenta que el Ing. Bustos (uno de los profesionales que se encuentra apoyando la gestión) es quien ejerce actualmente la responsabilidad de DBA, gestor de accesos a la BD, líder funcional, líder técnico, arquitecto de bases de datos, analista de base de datos, entre otras.

Por principio de segregación de funciones es prioritario que la capa de datos se encuentre bajo la gestión de un empleado diferente a quien administre la capa de aplicación.

Adicionalmente, se realizan solicitudes de tipo auditoría, y esta opción recae por demanda expresamente sobre el Ing. Bustos, actualmente

a cargo de las responsabilidades de un DBA. Generalmente este puesto requiere, además de la creación de las tablas, la codificación manual de los triggers y otros objetos que contienen todo el DML[1] necesario para registrar las pistas de auditoría. En este punto debe de tenerse muy clara la segregación de funciones, el sistema de auditoría de base de datos no puede ser administrado por los DBA del área de IT.

Recomendación

- Se deben establecer procesos de revisión de los accesos otorgados a los servicios y componentes de infraestructura, con base en el principio de segregación de funciones, teniendo en cuenta las cadenas de autorización y control enfocadas a evitar la existencia de una única persona a cargo de toda la operación como captura o preparación y de la aprobación o rechazo de operaciones. Desde el punto de vista formal, los dueños de los procesos y dueños de los activos de información, deben definir los niveles de protección de los activos de información del respectivo proceso, mantener actualizados los activos de información, autorizar y monitorear los permisos de acceso a los activos de información, evaluando y segregando las atribuciones y funciones principales entre los diferentes usuarios a su cargo, que permita reducir el riesgo de error, mal uso, fraude, abuso, reproceso y otras irregularidades. Esto incluye separar las responsabilidades para autorizar transacciones, procesarlas y registrarlas, revisar las transacciones y manejar cualquier activo relacionado, de manera que ningún usuario controle todos los aspectos clave de una transacción o evento.

- Adelantar los procesos de contratación del cargo de profesional especializado 2028-17 y los que sean requeridos a fin de garantizar cumplimiento al principio de segregación de funciones en todo el ciclo de vida de la operación de las bases de datos (en lo relacionado a la gestión de seguridad, administración, operación, mantenimiento y monitoreo de las bases de datos).

- Garantizar cumplimiento con lo establecido por MinTic en cuanto a los roles y responsabilidades en términos de la seguridad y privacidad de la información, respecto de *"(…) En el momento de asumir un rol, un individuo tiene la responsabilidad de alcanzar ciertos objetivos trazados conforme a unas determinadas funciones y capacidades descritas para ello, es así como el establecer los roles y la asignación de un responsable para cada acción definida dentro de la planeación de seguridad de la información en cada entidad es un aspecto clave para el correcto funcionamiento del Modelo de Seguridad de la Información (en adelante MSPI), de esta manera se busca asegurar que siempre se tenga el panorama claro respecto a la ejecución de las actividades definidas, teniendo un responsable al cual solicitar información sobre la ejecución y funcionamiento de las mismas. Las responsabilidades determinadas para cada rol dependerán de las metas establecidas para las diferentes actividades, pues éstas van a permitir detallar los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a la implementación del MSPI, por otro lado, para elegir de forma más fácil y adecuada un responsable, debe generarse un análisis de las funciones de cada rol comparándolas con el personal de la entidad. Teniendo en cuenta lo anterior, una de las preocupaciones de este ejercicio es que, en el momento de la asignación de las tareas, se genere un sobredimensionamiento de las actividades, es por eso que se debe garantizar primero en cada una de las asignaciones la preparación para el cargo, así como el análisis juicioso para la definición de sus funciones e independiente de quien sería el encargado de asumir cierto rol. Otro aspecto a contemplar en esta definición de roles y responsabilidades es la de hacer una segregación de funciones ya que permite detectar errores involuntarios, y sobre todo evitar fraude interno en el momento en el cual un solo personaje no tiene la capacidad operacional por asignación de privilegios, para generar todas las fases de una transacción. De esta forma, es necesario que las responsabilidades asignadas en el desarrollo del proyecto del MSPI para cada perfil, sean incorporadas a los manuales de funciones de cada entidad de acuerdo al cargo que desempeñan (...)".*

[1] (Data Manipulation Language, DML) es un idioma proporcionado por los sistemas gestores de bases de datos que permite a los usuarios de la misma llevar a cabo las tareas de consulta o modificación de los datos contenidos en las Bases de Datos del Sistema Gestor de Bases de Datos.

Hallazgo No. 3: Políticas y procedimientos de gestión de accesos	
Riesgo Potencial: Acceso no autorizado a la información. **Causa:** • Ausencia de políticas y procedimientos documentados, dirigidos a administrar y monitorear en forma controlada y segura la creación, inactivación y eliminación de las cuentas de usuario en los sistemas de información. • Ausencia de proceso formal para la revisión de los derechos de acceso.	**Nivel de riesgo Medio** 2

Diseñar controles de acceso adecuados y ajustados a las necesidades de explotación de los datos por parte de usuarios y herramientas, es fundamental para reducir los riesgos de exfiltración[2] o accesos no autorizados. La mayoría de las amenazas se engloban en esta categoría y se minimizan o directamente se eliminan manteniendo unos controles estrictos. El acceso a una instancia o a una base de datos requiere que el usuario se autentique. Oracle proporciona distintos protocolos de autenticación. Se recomienda hacer uso de mecanismos robustos de autenticación como SERVER, LDAP o Kerberos y evitar hacer uso de autenticación CLIENT, sobre todo en aquellos entornos donde no se puede garantizar la seguridad del usuario. Se recomienda seguir el principio de mínimo nivel de privilegios, donde solo se permita a los usuarios acceder a la información y hacer las acciones que realmente necesitan, minimizando la superficie de exposición.

Teniendo en cuenta la importancia de los controles de seguridad lógicos los cuales restringen las capacidades de acceso de los usuarios del sistema y evitan que usuarios no autorizados accedan a este, pueden existir controles de seguridad lógicos dentro del sistema operativo, el sistema de administración de la base de datos, el programa de aplicación, entre otros, por lo que las contraseñas y los perfiles de usuario resultan siendo un enfoque importante para restringir el acceso, asegurando que solo el personal autorizado pueda acceder a los sistemas clave, como los servidores.

En virtud de lo anterior, y con el propósito de ***evaluar la implementación de lineamientos establecidos formalmente en relación con la gestión de accesos***, solicitamos a la Oficina de Tecnologías y Sistemas de Información, las políticas y procedimientos documentados, dirigidos a administrar y monitorear en forma controlada y segura la creación, inactivación y eliminación de las cuentas de usuario en los sistemas de información (asociados a las bases de datos en cuestión. (Centro de contacto).

Al respecto nos fue remitida documentación soporte respecto de las políticas de seguridad de la información, inventario de activos de información, manual de usuario del Centro de contacto, procedimientos de gestión de solicitudes y formatos que los soportan.

A partir de los archivos remitidos, realizamos revisión del **100%** de estos registros.

Con base en las entrevistas sostenidas con cada uno de los involucrados al proceso, pruebas realizadas, y análisis de la información remitida, identificamos que se tienen políticas y procedimientos de seguridad asociadas a la operación y acceso a las bases de datos (objeto de estudio), los cuales se contemplan mediante los siguientes artefactos:

Manual de políticas de seguridad de la información D103M01, en los siguientes puntos:

- 6.4.2 GESTIÓN DE ACCESO DE USUARIOS La Oficina de Tecnología y sistemas de Información debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware, bases de datos y demás recursos tecnológicos.
- 6.9.3 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS La Oficina de Tecnologías y Sistemas de Información debe exigir toda la documentación de los repositorios y bases de datos de los sistemas de información a los proveedores externos
- 6.9.4 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE Los desarrolladores internos y externos deben certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.

[2] La exfiltración de datos ocurre cuando se incurre en la copia, transferencia o recuperación no autorizadas de datos de un servidor o el ordenador de un individuo.

Los desarrolladores deben implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

Manual de inventario de activos, clasificación y publicación de la información D103M02, donde se establece lineamientos para la identificación, clasificación, valoración y actualización de los activos tecnológicos de información del Ministerio de Ciencia Tecnología e Innovación, contando con el tipo de activo de Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

Matriz de inventarios de activos de información de TI D103M02F01: Listado de Activos de Información los cuales son la base para la gestión de riesgos de seguridad de la información y poder determinar los niveles de protección requeridos, incluyendo los activos de información – base de datos, en donde se evidenció lo siguiente:

MATRIZ DE INVENTARIOS DE ACTIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Nombre de Activo	Función /Propósito	Proceso	Nombre del Responsable de la Producción de la Información (Propietario del Activo)	Custodio del activo
ScienTI-GrupLAC	Aplicación Web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI-InstituLAC	Aplicación Web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI-Créditos condonables	Aplicación Web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI-Publindex	Aplicación Web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI-Ciencia	Aplicación Web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI- Convocatorias	web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI- Convocatorias Formacion	web	Gestión de Tecnologías y Sistemas de	Jefe Oficina de Tecnologías y Sistemas de Información	Oficina de Tecnologías y
ScienTI-CvLAC	Base de datos	Gestión del Conocimiento para la CTeI	Director de la Dirección de Generación del Conocimiento	Oficina de Tecnologías y
ScienTI-GrupLAC	Base de datos	Gestión del Conocimiento para la CTeI	Director de la Dirección de Generación del Conocimiento	Oficina de Tecnologías y
ScienTI-InstituLAC	Base de datos	Gestión del Conocimiento para la CTeI	Director de la Dirección de Generación del Conocimiento	Oficina de Tecnologías y

Información confidencial

El propietario de los activos de información relacionados con la información contenida en base de datos (objeto de estudio) es la Dirección de Ciencia.

El propietario de los activos de información relacionados con la infraestructura de las bases de datos (objeto de estudio) es la Oficina de Tecnologías y Sistemas de Información.

En el Ministerio se cuenta con el **Manual de inventario de activos, clasificación y publicación de la información** (Código: D103M02), el cual tiene como propósito establecer lineamientos para la identificación, clasificación, valoración, actualización de los activos tecnológicos de información y se detallan los campos que se establecen en el instrumento para realizar el levantamiento de activos de información a través de Matriz de Inventario de activos de Información de TI (Código: D103M02F01), algunos de los campos que contempla son: Propietario del Activo: Persona, dueña del activo. Custodio del activo: Responsable de la información almacenada en los activos de tecnologías de la información.

Registro de Activos de Información documental e índice de Información reservada y clasificada A204M01F01: La identificación y clasificación de los activos de información de tipo datos o información parte del reconocimiento de la producción documental de la entidad (documentos de archivo o registros) así como su clasificación en series (categorías de información), las cuales se incluyen en el Cuadro de Caracterización Documental que luego se articula y complementa para conformar el Registro de Activos de Información, en el cual se incluye el Índice de información clasificada y reservada.

Por otro lado, se identifica la existencia de un procedimiento de gestión de solicitudes, a través del cual se gestionan las solicitudes relacionadas a herramientas informáticas, servicios tecnológicos y sistemas de *información, realizadas por los usuarios del MinCiencia, a través del punto único de contacto Mesa de Servicios.*

En la herramienta de Mesa de servicio que tiene el MinCiencia que actúa como soporte tecnológico para la gestión de solicitudes, se tiene configurado un flujo de trabajo que incluye una tarea (en la cual, a partir de la validación del ticket y la dependencia), se define la acción para la creación de cuentas para la aplicación: **Centro Contacto Web**, especialmente para la dependencia "Equipo de Atención al ciudadano", quienes deben contar con este acceso para realizar las actividades de soporte de primer nivel al ciudadano para el sistema

SCIENTI. En el caso de la inactivación, se procede manualmente a la revisión de la existencia de usuario en la aplicación para realizar la inactivación y se solicita la creación de la tarea en CA para el registro de dicha inactivación.

La herramienta Centro Contacto Web cuenta con su respectivo manual de usuario que establece los tipos de usuarios y roles de acuerdo con la necesidad del área solicitante y la administración de la aplicación.

En cuanto a la documentación propia de las creaciones, activaciones e inactivaciones de usuarios, se cuenta con la "Cartilla para el diligenciamiento del formato de gestión de cuentas y servicios informáticos - D103PR01F01AN01". Para el formato de "Gestión de Cuentas y Servicios Informáticos - D103PR01F01", se estableció el campo "OBSERVACIONES", en el que el usuario diligencia la solicitud de esta creación y/o activación.

Sin embargo, no nos fue posible observar en dicho procedimiento el tratamiento especial que se le debe dar cuando las solicitudes corresponden a la creación, inactivación y eliminación de las cuentas de usuario para el acceso a las bases de datos, en donde se identificará específicamente las autorizaciones que se deben surtir una vez se solicita accesos con información altamente crítica como son las bases de datos, autorizaciones que deben ser otorgadas única y específicamente por la Dirección de Ciencia como propietario de los activos de información relacionados con la información contenida en base de datos (objeto de estudio).

Así mismo no nos fue posible obtener documentación soporte de los procedimientos implementados a cargo de la supervisión, auditoría o monitoreo de los accesos otorgados sobre estos activos de información.

Recomendación

- Considerar en el procedimiento de gestión de solicitudes el tratamiento especial que se le debe dar cuando las solicitudes corresponden a la creación, inactivación y eliminación de las cuentas de usuario para el acceso a las bases de datos, en donde se detalle específicamente las autorizaciones que se deben surtir una vez se solicita accesos con información altamente crítica como son las bases de datos, autorizaciones que deben ser otorgadas única y específicamente por la Dirección de Ciencia como propietario de los activos de información relacionados con la información contenida en base de datos (objeto de estudio).

  La autorización es el proceso de determinar si un usuario autenticado, dispone de acceso a la información y permisos que está solicitando. Este proceso se realiza íntegramente dentro de Oracle 19c, consultando los permisos asociados a una identidad concreta. En este sentido, existen distintos tipos de permisos que pueden ser otorgados.

  A continuación, se exponen recomendaciones de seguridad para Oracle según informe de buenas prácticas generado en mayo de 2022 por el Centro Criptológico Nacional - **CCN-CERT BP/22:**

  Permisos primarios: Aquellos que se otorgan directamente al identificador de autorización.
  Permisos secundarios: Aquellos que se otorgan a grupos y roles de los cuales es miembro un identificador de autorización.
  Permisos públicos: Aquellos que se otorgan a la entidad PUBLIC.
  Permisos basados en contexto: Aquellos que se otorgan a un rol de contexto de confianza.

  Estos permisos se pueden otorgar a los usuarios en varios niveles o categorías:

  Autorización a nivel de sistema: Son las autoridades que realizan labores de administración. Hay varios usuarios con roles diferenciados.
  - El usuario SYS es administrador de sistema. Su contraseña debe ser cambiada sobre la predeterminada del fabricante. No conviene crear objetos dentro de su esquema.
  - El usuario SYSTEM a cargo del control del sistema, éste posee el rol DBA y también debe cambiar su contraseña por defecto. En su esquema se pueden crear tablas y vistas de administración.
  - Los usuarios SYSBACKUP, SYSDG, SYSKM, y SYSRAC se crean automáticamente en la instalación para facilitar las labores de administración.
  - El usuario SYSBACKUP facilita las operaciones de copia de seguridad y recuperación de Oracle Recovery Manager (RMAN) ya sea desde RMAN o SQL * Plus.
  - El usuario SYSDG facilita las operaciones de Data Guard. El usuario puede realizar operaciones con Data Guard Broker o con

la interfaz de línea de comandos DGMGRL.

- El usuario SYSKM facilita las operaciones del almacén de claves de cifrado transparente de datos.
- El usuario SYSRAC facilita las operaciones de Oracle Real Application Clusters (Oracle RAC) al conectarse a la base de datos a través del agente Clusterware contra las utilidades de Oracle RAC como SRVCTL.
- El privilegio administrativo de SYSRAC no se puede otorgar a los usuarios de la base de datos y no se admite en un archivo de contraseña. El privilegio administrativo de SYSRAC solo lo usa el agente de Oracle de Oracle Clusterware para conectarse a la base de datos mediante la autenticación del sistema operativo.
- Los usuarios a los que se les ha otorgado el privilegio del sistema CREATE USER pueden crear cuentas de usuario, incluidas las cuentas de usuario que se utilizarán como usuarios proxy. Debido a que el privilegio del sistema CREATE USER es un privilegio poderoso, un administrador de base de datos o un administrador de seguridad suele ser el único usuario que tiene este privilegio del sistema. Si se desea crear usuarios que tengan el privilegio de crear usuarios, se puede incluir la cláusula WITH ADMIN OPTION en la declaración GRANT.
- **Autorización a nivel de base de datos:** Oracle 19c posee 79 roles predefinidos durante la instalación. Independientemente de éstos, se pueden generar otros roles, con la sentencia create role a los que posteriormente se le pueden asignar permisos específicos. Por ello, una auditoría de permisos en la base de datos debe ser dinámica y no restringirse únicamente a los roles y permisos generados en una instalación. El fabricante provee al menos 30 vistas de administración de roles para facilitar estas tareas. Las autoridades con permisos sobre grant and revoke privilege, pueden asignar y revocar los permisos a los usuarios y roles.
- **Autorización a nivel de objeto:** La autorización a nivel de objeto implica la verificación de privilegios cuando se realiza una operación concreta sobre un objeto específico.
- **Autorización basada en contenido:** Una forma de autorizar el acceso basado en contenido son las vistas. Las vistas permiten controlar qué columnas o filas de una tabla pueden ser leídas por usuarios específicos. Por otro lado, el fabricante Oracle a través Oracle Label Security, permite que el control de acceso llegue a filas específicas (etiquetadas) de una base de datos. Con Oracle Label Security implementado, los usuarios con diferentes niveles de privilegios tienen automáticamente (o están excluidos) el derecho a ver o modificar filas de datos etiquetadas. La Guía del administrador de Oracle Label Security describe cómo utilizar Oracle Label Security para proteger datos confidenciales. Explica los conceptos básicos detrás de la seguridad basada en etiquetas y proporciona ejemplos para mostrar cómo se usa.
- Otro componente importante a la hora de definir la seguridad de un gestor de bases de datos es el cifrado, tanto de los datos en tránsito como de los datos en reposo. Oracle 19c ofrece diferentes opciones de cifrado de los datos y de transporte.

- Definir, documentar, implementar y socializar procedimientos en relación con la supervisión, auditoría o monitoreo de los accesos otorgados sobre estos activos de información.

Hallazgo No. 4: Cierre de brechas de seguridad pendientes por gestionar

Riesgo Potencial: Aprovechamiento de vulnerabilidades de seguridad.

Causa:

- Cierre de brechas pendientes por gestionar.

Nivel de riesgo
Alto

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel sumamente importante, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

En virtud de lo anterior, y con el propósito de ***evaluar la gestión de vulnerabilidades***, solicitamos a la Oficina de Tecnologías y Sistemas de Información, los informes del resultado del escaneo de vulnerabilidades (infraestructura que soportan las bases de datos) realizado en los últimos dos (2) años y plan de acción para el cierre de brechas, especificando **el estado de cierre** de cada brecha identificada.

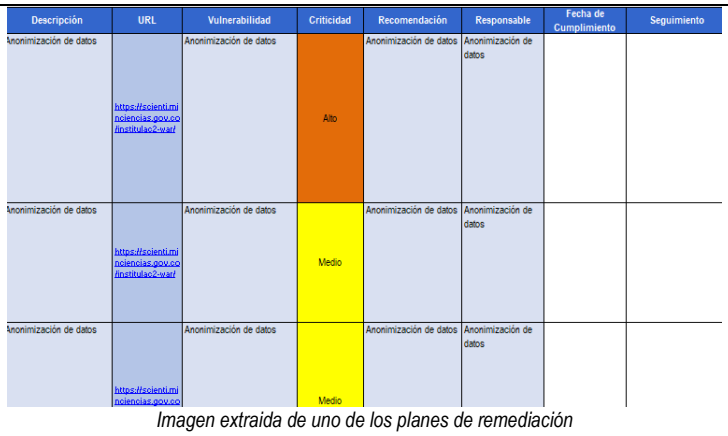
Al respecto nos fue remitida documentación soporte respecto de los resultados generados, producto de los escaneos realizados a las diferentes aplicaciones CVLAC, GrupLAC e InstituLAC.

A partir de los archivos remitidos, realizamos revisión del **100%** de estos registros.

Con base en las entrevistas sostenidas con cada uno de los involucrados al proceso, pruebas realizadas, y análisis de la información remitida, identificamos que se realiza análisis de vulnerabilidades a los componentes de plataforma tecnológica y aplicativos web que soporta el Sistema a través las pruebas de vulnerabilidades utilizando la solución de Tenable SC y Tenable IO y con base a las vulnerabilidades detectadas, se construye el plan de remediaciones, el cual posteriormente es enviado a los responsables, con el fin de que sean remediadas en el menor tiempo posible.

Para el caso de los informes debido a que se consideran como confidenciales, debido a que contiene información sensible, se adjunta plan de remediación, sin embargo, se anonimizan los datos de vulnerabilidad, descripción y remediación, ya que es información sensible para el MinCiencia, sin embargo, el Equipo Auditor solicitaba información respecto del plan de acción para el cierre de brechas, especificando el **estado de cierre** de cada brecha identificada, información que no fue compartida aun cuando se contaba con los acuerdos de confidencialidad debidamente firmados de cada uno de los auditores.

En virtud de lo anterior, observamos que, para las vulnerabilidades con nivel de severidad ALTA, no se han establecido planes de acción para el cierre de las mismas, teniendo en cuenta el impacto que puede representar para el negocio la materialización de dichas brechas de seguridad.



Descripción	URL	Vulnerabilidad	Criticidad	Recomendación	Responsable	Fecha de Cumplimiento	Seguimiento
Anonimización de datos	https://scienti.minciencias.gov.co/institulac2-war/	Anonimización de datos	Alto	Anonimización de datos	Anonimización de datos		
Anonimización de datos	https://scienti.minciencias.gov.co/institulac2-war/	Anonimización de datos	Medio	Anonimización de datos	Anonimización de datos		
Anonimización de datos	https://scienti.minciencias.gov.co	Anonimización de datos	Medio	Anonimización de datos	Anonimización de datos		

Imagen extraida de uno de los planes de remediación

Recomendación

- Emitir formal y periódicamente informe del seguimiento al cierre de las brechas detectadas, resultado del escaneo de vulnerabilidades (infraestructura que soportan las bases de datos) realizado anualmente, incluidas las vulnerabilidades técnicas excluidas del plan de remediación, teniendo en cuenta:

  - ✓ Aplicativo y/o servicio tecnológico afectado con la remediación de la vulnerabilidad.
  - ✓ Justificación técnica y económica de la exclusión.
  - ✓ Criticidad del activo en términos del impacto económico, legal, reputacional y/o de imagen que se pueda presentar con la materialización de los riesgos identificados.
  - ✓ El costo de implementar la recomendación.
  - ✓ El riesgo de no aplicar la remediación.
  - ✓ La seguridad alternativa del activo impactado.
  - ✓ Cualquier otra razón documentada que imposibilite la aplicación de la remediación.

- Realizar la implementación de los planes de acción, asegurando que las vulnerabilidades de criticidad alta, media y baja sean remediadas, toda vez se determine que el "Impacto" en términos de reputación, imagen, legal y económico, pueda ser más alto que el mismo costo de implementación del control o cierre de la brecha. Dicha determinación deberá quedar documentanda y socializada ante quienes correspondan, en donde se asuma formalmente el riesgo en la ejecución de la operación dado que la implementación del tratamiento es más costoso que el impacto que genera la materialización del riesgo.

Hallazgo No. 5: Procedimiento de gestión de copias de respaldo y restauración	
Riesgo Potencial: Pérdida de disponibilidad de la información. **Causa:** • Ausencia de políticas y procedimientos implementados, dirigidos a la realización, administración y monitoreo de las copias de respaldo y restauraciones.	**Nivel de riesgo** **Alto** 3

El backup y la recuperación son el proceso de creación y almacenamiento de copias de datos que se pueden utilizar para proteger a las organizaciones contra pérdidas de datos. A esto se le conoce a veces como **recuperación operativa**. Para recuperar un backup es necesario restaurar los datos en la ubicación original o en una ubicación alternativa, donde se podrán utilizar en lugar de los datos perdidos o dañados.

Una copia de seguridad correcta se almacena en un sistema o medio separado, como una cinta, de los datos primarios para protegerlos contra la posibilidad de pérdida de datos debido a un fallo del hardware o software primario.

El propósito de la copia de seguridad es crear una copia de los datos que se pueden recuperar en caso de que se produzca un error de datos primarios. Los fallos de datos primarios pueden ser el resultado de fallos de hardware o software, daños en los datos o un evento causado por el ser humano, como un ataque malicioso (virus o malware) o la eliminación accidental de datos. Las copias de seguridad permiten restaurar los datos desde un momento anterior para ayudar a la empresa a recuperarse de un evento no planificado.

El almacenamiento de la copia de los datos en un medio separado es fundamental para protegerse contra la pérdida de datos primarios o la corrupción. Este medio adicional puede ser tan sencillo como una unidad externa o una memoria USB, o algo más importante, como un sistema de almacenamiento en disco, un contenedor de almacenamiento en cloud o una unidad de cinta. El medio alternativo puede encontrarse en la misma ubicación que los datos principales o en una ubicación remota. La posibilidad de eventos relacionados con el clima puede justificar la existencia de copias de datos en ubicaciones remotas.

Para obtener mejores resultados, las copias de seguridad se realizan de forma constante y regular para minimizar la cantidad de datos perdidos entre los backups. Cuanto más tiempo transcurre entre las copias de backup, mayor será el potencial de pérdida de datos al recuperarse de una copia de seguridad. La retención de varias copias de datos proporciona el seguro y la flexibilidad para restaurar hasta un momento no afectado por daños en los datos o ataques malintencionados.

En virtud de lo anterior, y con el propósito de ***evaluar los procedimientos de gestión de copias de respaldo y restauraciones***, solicitamos a la Oficina de Tecnologías y Sistemas de Información, documentación respecto a los procedimientos de respaldo y restauraciones, así como documentación soporte, producto de la ejecución de estos ejercicios.

A partir de los archivos remitidos, realizamos revisión del **100%** de estos registros.

Con base en las entrevistas sostenidas con cada uno de los involucrados al proceso, pruebas realizadas, y análisis de la información remitida, identificamos que existe un documento GUÍA PARA LAS COPIAS DE RESPALDO DE INFORMACIÓN / ETIQUETADO Y MANEJO DE LA INFORMACIÓN, el cual tiene como objetivo de describir las actividades que se ejecutan en el Ministerio, bajo las cuales se realizan las copias de respaldo de la información misional y de apoyo, institucional de los usuarios, y de los servidores físicos y virtuales del Ministerio; para proteger la información en el evento de tener que recuperarse ante un eventual desastre, pérdida o daño. Actualmente el documento se encuentra en revisión por el equipo de infraestructura tecnológica.

Se evidencian los logs de ejecución de los backups realizados en el último mes y documentación de las restauraciones realizadas desde enero de 2022 a la fecha. Trazabilidad desde la solicitud hasta la entrega.

Las restauraciones realizadas a demanda durante el intervalo de tiempo indicado tienen que ver con:

a. 20221227 - Solicitud # 102949 - Publicar el proceso de homologación de revistas.

b. 20220525 - Solicitud # 93286 - Actualización del Servicio de Información de Evaluadores del SNCTeI.
c. 20220127 - Solicitud # 87237 - Publicación resultados convocatoria 894 de 2021.

Por otro lado, se confirma que las cintas de backup se encuentran ubicadas en la cintoteca dentro del centro de cómputo (Datacenter) de la entidad, estas luego de llegar a una cantidad específica, se relacionan en el Formato Único de Inventario Documental FUID para entrega a Gestión Documental quienes realizan entrega a un tercero para su almacenamiento fuera de la entidad.

Adicionalmente se observa que en el Plan Anual de Adquisición PAA formulado y aprobado que tiene el Ministerio para la vigencia 2023, se contempla contratar la arquitectura, diseño e implementación del Plan de Recuperación ante Desastres - DRP para la infraestructura tecnológica del Ministerio, con fecha estimada de inicio de selección para el mes de junio 2023.

En la ficha técnica del proceso se tiene contemplado el respaldo y continuidad de la operación que soportan las bases de datos.

Con base en los procesos de observación e inspección realizada sobre la documentación indicada anteriormente, evidenciamos que actualmente no existen formalmente establecidos procedimientos de restauración que sean ejecutados con una periodicidad fija establecida, los cuales se recomienda (incluidos los backups) cifrar independientemente del medio donde se almacenen. Adicionalmente se identifica que el almacenamiento de las cintas de respaldo se realiza en la misma ubicación física del servidor de producción (Datacenter principal).

Recomendación

- Definir, documentar, implementar y socializar procedimientos en relación con la gestión de copias de respaldo y restauración.
- Se recomienda garantizar que la restauración de cualquier copia de seguridad debe requerir un acceso controlado a la clave de cifrado y debe ser auditado, tanto el acceso como la propia restauración.
- Se deben mantener las prácticas recomendadas por el fabricante de copias de seguridad.
- Se recomienda realizar copias de seguridad periódicas. Al menos también debe generarse una copia de seguridad incremental semanal en domingo con conservación de cuatro semanas. También debe generarse una copia incremental cada día uno de mes, conservándose los doce últimos meses. También debe generarse una copia de seguridad anual, conservándose durante cinco años.
- Se deben almacenar copias de seguridad en lugares distintos a la ubicación física del servidor de producción.
- Se recomienda la ejecución de pruebas de recuperación periódicamente al igual que ejecutar periódicamente simulacros de recuperación frente a desastres.
- Debe generarse una copia de seguridad incremental diaria que debe conservarse durante siete días.

Hallazgo No. 6: Controles de intercambio de información.	
Riesgos Potenciales: • Intercambio inseguro de información con terceros. • Pérdida de confidencialidad de datos sensibles o robo de contraseñas por debilidad en controles de infraestructura con acceso a Internet. **Causas:** • Ausencia de mecanismos de autenticación mutua o basada en mensajería para proteger los flujos de datos entre los componentes de la infraestructura de MinCiencia y el primer hops (segmento de red) al que se conecten. • Hackers.	**Nivel de riesgo Medio** 2

CONFIGURACIÓN DE FIREWALLS

La administración del firewall sigue siendo la principal defensa de la red de una organización. Prácticamente, representa la actividad que más tiempo insume a los administradores de seguridad de redes en comparación con cualquier otra actividad. Mientras que el software antivirus protege el sistema de archivos de programas no deseados, el uso de firewalls impide que los atacantes o las amenazas externas accedan a nuestra infraestructura.

El firewall supervisa todo el tráfico de red y tiene permisos para identificar y bloquear el tráfico no deseado. Esto, adquiere fuerza por el solo hecho de que hoy en día la mayoría de los equipos estén conectados a Internet, lo que facilita a los atacantes un sinfín de víctimas potenciales. Los atacantes sondean otros equipos conectados a Internet para determinar si son vulnerables a varias clases de ataques. Cuando detectan una víctima propicia, pueden franquear sus sistemas de seguridad e infiltrarse en ese equipo. Llegados a este punto, el atacante puede obligar al equipo a efectuar prácticamente cualquier tarea que quiera. Los atacantes suelen intentar apropiarse de información personal para cometer fraudes, generalmente financieros.

En virtud de lo anterior, y con el propósito de ***evaluar controles de intercambio de información***, solicitamos a la Oficina de Tecnologías y Sistemas de Información, la relación de las máquinas que tienen tráfico habilitado a los servidores de la BD y políticas y procedimientos de seguridad asociadas a la operación y acceso a las bases de datos (objeto de estudio).

Al respecto nos fue remitido el reporte generado desde la solución de firewall que funciona en MinCiencias y Manual de políticas de seguridad de la información D103M01, en los siguientes puntos:

- GESTIÓN DE ACCESO DE USUARIOS La Oficina de Tecnología y sistemas de Información debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware, bases de datos y demás recursos tecnológicos.
- 6.9.3 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS La Oficina de Tecnologías y Sistemas de Información debe exigir toda la documentación de los repositorios y bases de datos de los sistemas de información a los proveedores externos
- 6.9.4 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE Los desarrolladores internos y externos deben certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.

A partir de los archivos remitidos, realizamos revisión del **100%** de estos registros.

Con base en las entrevistas sostenidas con cada uno de los involucrados al proceso, pruebas realizadas, y análisis de la información remitida, identificamos que el acceso a la BD está controlado por el dispositivo de seguridad Firewall, administrado por el equipo de infraestructura.

Respecto a la gestión de reglas de firewall el equipo de infraestructura cuenta con controles de tipo preventivo, que incluye el registro y trazabilidad de los casos así como la segregación de funciones que se instruyen desde Tecnología, sin embargo, debido a que no nos fue posible obtener documentación respecto a procedimientos o políticas de seguridad en relación a la gestión de reglas del firewall, se recomienda establecer un proceso de revisión independiente que permita realizar control periódico de las reglas de Firewall con el fin de

depurar aquellas reglas que han sido creadas y que ya no cubren ningún requerimiento operativo o funcional, así como aquellas creadas incluyendo sus objetos que puedan representar un riesgo para la entidad, como por ejemplo reglas creadas sin soporte o evidencia de autorización o el uso de protocolos inseguros y el riesgo que debe controlarse por ejemplo a través del uso de controles compensatorios entre otros, estos aspectos deben ser estrictamente vigilados no solo por el riesgo que puede suponer para la entidad el uso de reglas innecesarias o bajo servicios inseguros u obsoletos, sino por el esquema de administración que se encuentra bajo control de un tercero (en caso que aplique), lo cual debe ser vigilado a fin de prevenir cambios no autorizados y mantener pleno conocimiento de cualquier acción realizada sobre dicho elemento y su evidencia de autorización, toda vez que este tipo de activos se considera como uno de los más críticos siendo este la puerta de acceso de borde o perímetro, hacia la red interna de la entidad. Se recomienda que este control también cubra lo correspondiente al firewall de capa de aplicaciones (Web application firewall).

Recomendación

- Revisar el tipo de tráfico que pasa por las zonas configuradas con políticas de tipo All a All_Interface_IP y limitar el intercambio de información a los protocolos adecuados. Es importante tener en cuenta estas configuraciones durante procesos posteriores de migración a plataformas de seguridad o actualización, con el objetivo de asegurar que no se permita tráfico libre por ninguna de las zonas configuradas.

- Evaluar la configuración de los protocolos, realizando los cambios a las versiones seguras de éstos o a otros protocolos que ofrezcan mejores condiciones de seguridad. Es importante que se tenga en cuenta el uso de protocolos seguros para todas las políticas y reglas durante procesos posteriores de migración a plataformas de seguridad o actualizaciones, asegurando que los protocolos inseguros utilizados actualmente no sean migrados.

- Recomendamos documentar el procedimiento y las actividades que actualmente ejecuta la Oficina de Tecnologías y Sistemas de Información respecto a la gestión de cambios en el firewall, así como, cuál debería ser la evidencia del análisis realizado y los responsables del mismo. En cuanto a los cambios que afectan la disponibilidad del servicio es necesario documentar cada una de las etapas llevadas a cabo y cada una de las autorizaciones realizadas, garantizando que los formatos de control de cambios estén acordes con las actas del Comité de Cambios en los que fueron aprobados.

- Adicionalmente, analizar e implementar un control que permita garantizar que los cambios a través de un requerimiento GLPI se registre en su totalidad en la bitácora del firewall y viceversa.

- Adicional a los controles existentes de acuerdo con lo informado por el área de infraestructura, se recomienda establecer un proceso de revisión independiente que permita realizar control periódico de las reglas de Firewall con el fin de depurar aquellas reglas que han sido creadas y que ya no cubren ningún requerimiento operativo o funcional, así como aquellas creadas incluyendo sus objetos que puedan representar un riesgo para la entidad.

- Ampliar la vigilancia permanente de los eventos Web a la internet profunda para anticipar posibles ataques en gestación sobre la entidad, sumado a los ejercicios proactivos de revisión realizados por la entidad dentro de las pruebas efectuadas.

- Conforme a las mejores prácticas en cuanto a la administración de firewalls, se recomienda lo siguiente:

  1. Defina su plan de administración del cambio. Una autoridad de administración del firewall centralizada y un proceso documentado pueden ayudar a evitar cambios indeseados en la configuración actual de la red, al limitar los riesgos que perjudican la funcionalidad, dificultar los cambios futuros o abrir una brecha de seguridad en la red. Un plan de administración del cambio debe cumplir con lo siguiente:

     - Establecer un enfoque aceptado para solicitar cambios de política y estipular requisitos.
     - Implementar controles adecuados con identificación de las personas que pueden o no autorizar un cambio.
     - Centralizar la administración del firewall para crear, distribuir y cumplir con las políticas con eficiencia.
     - Describir los puntos de comunicación y coordinación necesarios para procesar adecuadamente cualquier cambio.
     - Crear una pista de auditoría para realizar el seguimiento de las solicitudes, las acciones y los resultados de un cambio de firewall.

2. Pruebe los cambios de firewall antes de implementarlos plenamente. De ser posible, cree un entorno de prueba que refleje los sistemas de producción. El hecho de no probar los cambios adecuadamente puede conllevar una interrupción del negocio, como problemas de latencia de red o cortes totales de suministro de red.

3. Tome una instantánea de la configuración antes de efectuar grandes cambios de firewall. Tenga implementado un sistema de revisión de cambios, con planes de recuperación y de conmutación por error, antes de que surja una necesidad imperiosa. Las instantáneas constantes del sistema pueden ahorrar tiempo y dinero si una migración se lleva a cabo incorrectamente o si falla un equipo de forma inesperada.

   Con el tiempo, estas instantáneas pueden generar un perfil de la actividad de la red. Este perfil puede ayudar a monitorear el uso de las características de la red, y a detectar los comportamientos irregulares, el exceso de suscripciones y los problemas de carga.

4. Monitoree el acceso de los usuarios a la configuración del firewall. Los registros de acceso de los usuarios pueden funcionar como un sistema de detección de intrusiones primario, que potencialmente puede revelar los intentos de acceso no autorizados desde dentro o fuera de la red. Los registros también pueden poner de manifiesto los cambios progresivos, incrementales e indeseados en la política de seguridad. Como bloqueo de una enorme brecha en la seguridad de su red, el firewall es un solo punto de entrada a la red y contiene elementos de prueba de conexiones no deseadas. El firewall puede exponer códigos malintencionados, troyanos y rootkits mediante alertas de conexiones denegadas o demasiadas conexiones permitidas.

5. Programe auditorías de políticas periódicas. Con el paso del tiempo, es posible que las reglas no coincidan con la política de seguridad, y que las reglas que no se usan bloqueen el tráfico y presenten una barrera a los cambios de red. La seguridad diferenciada también puede presentar riesgos legales. Revise su política de firewall con regularidad, actualícela según sea necesario y verifique su cumplimiento mediante la revisión de la configuración y las reglas del firewall. Revise la política en los siguientes casos:

   - Al introducir nuevas instancias de seguridad o firewall que alteren considerablemente las capacidades de la red.
   - Al introducir a la red nuevas aplicaciones compatibles con IP.
   - Al cambiar a un nuevo IPS (proveedor de servicios de Internet).
   - Al comenzar a compartir tráfico de red en colaboración con un socio empresarial.
   - Al atravesar un cambio empresarial u operativo importante.
   - Al sostener una rotación de personal significativa.

6.3 OPORTUNIDADES DE MEJORA

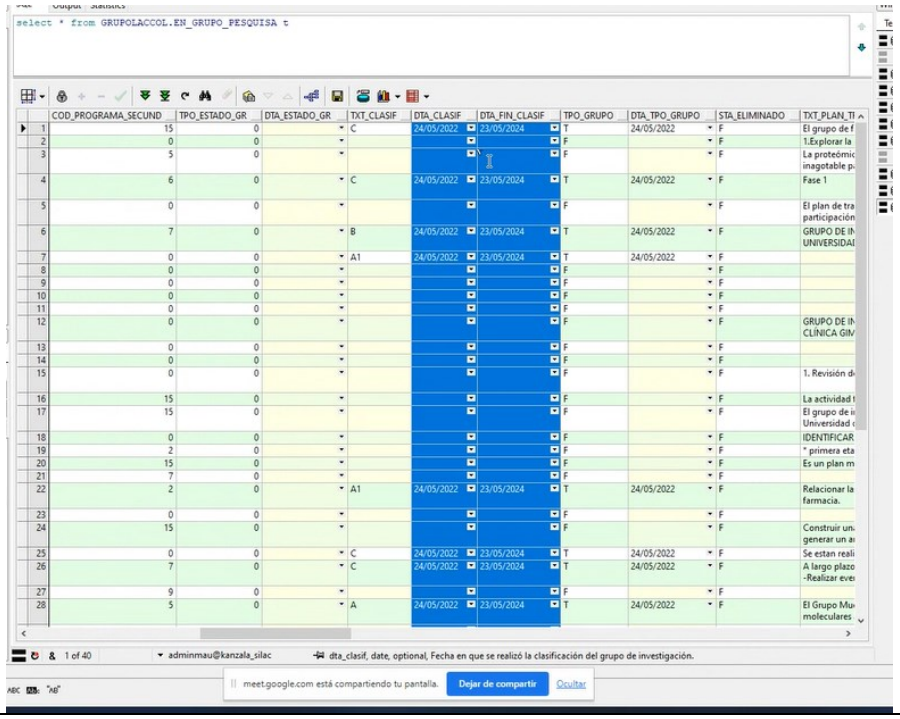
Oportunidad de mejora No. 1: Actualización de Diccionario de Datos.	
Riesgos Potenciales: • Errores en el análisis de los datos. **Causas:** • Desactualización del Diccionario de Datos.	**Nivel de riesgo Bajo** 1

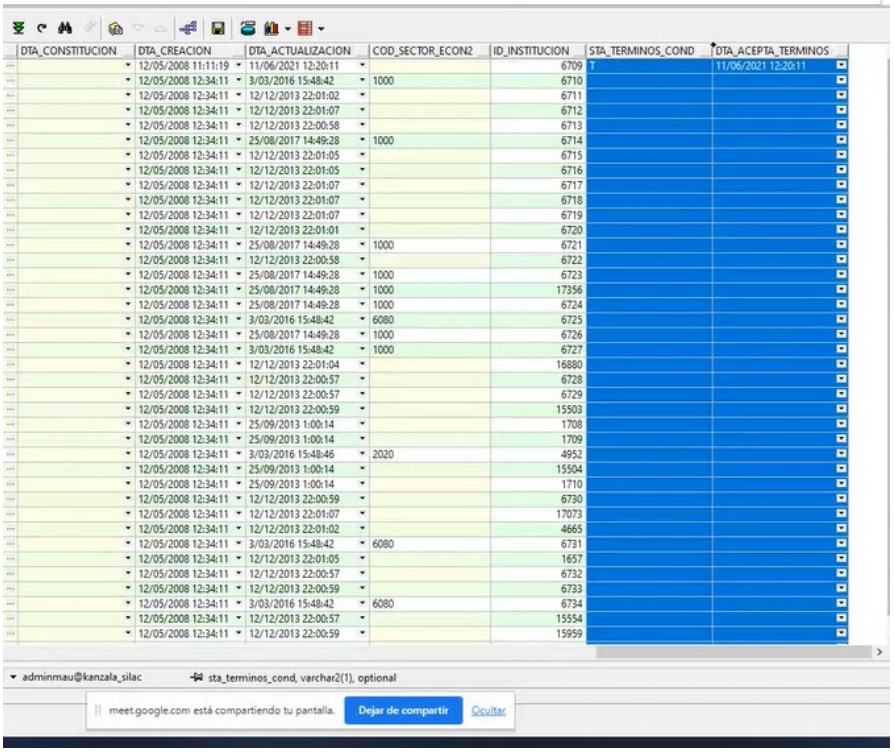
DICCIONARIO DE DATOS

Los diccionarios de datos ofrecen muchas ventajas a los usuarios, como la posibilidad de seguir los cambios, mejorar la calidad de los datos y reforzar la coherencia. Sin embargo, el uso de diccionarios de datos pasivos también puede presentar algunas desventajas. Uno de los inconvenientes es que su mantenimiento puede requerir un esfuerzo considerable, sobre todo si el conjunto de datos es extenso o se actualiza con frecuencia. En consecuencia, un diccionario de datos puede quedar obsoleto con el tiempo, lo que puede dar lugar a errores en el análisis de los datos.

La mala calidad de los datos es uno de los principales indicadores de proyectos fallidos y, a menudo, es identificada como la causa raíz de los fallos de procesos, siendo también la principal causante de las decisiones erróneas en una organización.

Durante sesión realizada el 04 de mayo de 2023 sostenida con el Equipo de la Dirección de Ciencias y Oficina de Tecnologías y Sistemas de Información donde se dio un recorrido completo del procedimiento de Gestión de la Información Estadística (Anexo No.1), mediante el cual se corroboran controles que garantizan la integridad de la información durante el flujo completo de información, se evidenciaron algunas desactualizaciones del Diccionario de Datos, las cuales tienen que ver con los siguientes objetos de las bases de datos (objeto de estudio):



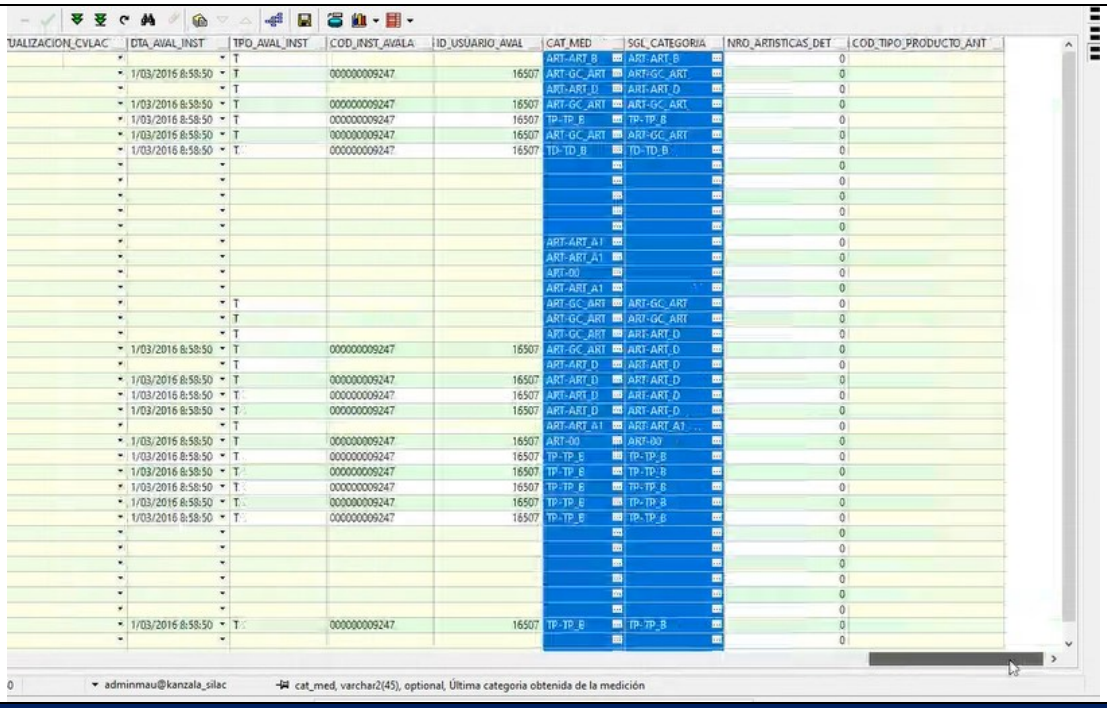


Objetos no observados en el Diccionario de Datos:

			educación superior.
DTA_CONSTITUCION		DATE	No se utiliza actualmente este campo en el aplicativo.
DTA_CREACION		DATE	Fecha de creación de la institución en el aplicativo InstituLAC.
DTA_ACTUALIZACION		DATE	Fecha de actualización de la información sobre la institución registrada en InstituLAC.
COD_SECTOR_ECON2		VARCHAR2(4)	Código interno para identificar otro sector económico de la institución.
ID_INSTITUCION		NUMBER	Almacena el ID de la institución del usuario de referencia.

17.3 LLAVES FORÁNEAS DE LA TABLA EN_INSTITUCION

Nombre	Llave foránea	Tabla padre
FK_EDR_EI FK_EI_ER	COD_INST ID_REPRESENTANTE; COD_INST	EN_INSTITUCION EN_REPRESENTANTE



Recomendación

- Garantizar actualización del Diccionario de Datos.

Oportunidad de mejora No. 2 Documentación Soporte.

Riesgos Potenciales:

- Presentación no apropiada de resultados en casos de prueba al no incluir las evidencias de cumplimiento obtenidos en cada uno de los pasos establecidos en los casos de pruebas.

Causas:

- Ausencia de documentación soporte respecto del resultado de las pruebas realizadas.

Nivel de riesgo Bajo

1

Al verificar las actividades desarrolladas en la Base de Datos de la Operación estadística Gestión Estadística y encontrar que en el formato caso de prueba MIC-DE-DS-CP-000 V1.0 10082018 de MIC System para publicaciones de contenido digital al usuario de prueba CVlac, la prueba se mantiene determinada por veintiún (21) pasos donde no se pueden evidenciar los resultados obtenidos en cada paso, generaría inconsistencias en la información presentada al no poder verificar si cada paso fue cumplido de acuerdo a las disposiciones planificadas.

Recomendación

- Garantizar documentación soporte de las pruebas realizadas.

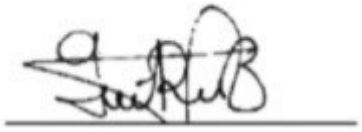
7. PLAN DE MEJORAMIENTO

Con base en este informe definitivo, se solicita a los Líderes de Proceso, deben elaborar un Plan de Mejoramiento, en el formato adjunto, que dé solución a los hallazgos identificadas y sea remitido a la Oficina de Control Interno para su aprobación, dentro de los ocho (8) días hábiles siguientes al recibo del presente informe.

Se recuerda que las acciones del Plan de Mejoramiento deben ser preventivas y/o correctivas, según el caso y requieren ser formuladas de manera efectiva para subsanar las debilidades encontradas.

Igualmente es necesario tener en cuenta que si en la ejecución de las acciones de mejora que se propongan se requiere la participación y responsabilidad de otras dependencias, la dependencia responsable del proceso auditado deberá coordinar con dichas dependencias la elaboración del Plan de Mejoramiento, antes de la presentación del Plan a la OCI.

Javier Herrera: _____
Firma del Auditor



Greecy Rivera: _____
Firma del Auditor

_____
GUILLERMO ALBA CARDENAS
JEFE OFICINA DE CONTROL INTERNO