CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

AS-AATIC-137-2022
11 de julio de 2022

Ingeniero
Esteban Zúñiga Chacón, jefe
Centro de Gestión Informática
GERENCIA MÉDICA - 2901

Ingeniero
Alexánder Solís Abarca, jefe
Centro de Gestión Informática
GERENCIA FINANCIERA – 1103

Ingeniera
Guiselle Tenorio Chacón, jefe
Centro de Gestión Informática
GERENCIA ADMINISTRATIVA - 1104

Ingeniero
Roy Ovares Valerio, jefe
Centro de Gestión Informática
GERENCIA DE LOGÍSTICA - 1106

Ingeniero
Giovanni Campos Alvarado, jefe
Centro de Gestión Informática
GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS- 1107

Ingeniero
Marco Vinicio González Jiménez, jefe.
Centro de Gestión Informática
GERENCIA DE PENSIONES - 9108

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimados(as) señores(as):

ASUNTO:	**Oficio de Asesoría relacionado con la gestión de Bases de Datos y sus mecanismos de seguridad.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno específicamente en su rol de asesor, esta Auditoría informa sobre la importancia de implementar acciones preventivas y correctivas en la gestión de bases de datos en la institución, así como mecanismos de seguridad de estos, considerando el restablecimiento de las diferentes fuentes de datos Institucionales, una vez transcurrido la emergencia por el ciberataque del pasado 31 de mayo.

Al respecto, considerando las amenazas por ciberataques que ha tenido el país en los últimos meses, donde la Caja se vio afectada directamente, generando impactos negativos en la atención de los servicios, así como en su propia gestión administrativa, es que resulta importante que la Institución esté informada de las amenazas y vulnerabilidades asociadas al uso de las tecnologías, especialmente de las emergentes, permitiendo conocer el riesgo inherente en este campo, e implementar así con garantía, las medidas, tanto procedimentales, como técnicas y organizativas que permitan un entorno seguro y confiable.

Las Bases de Datos al contener en su mayoría información sensible e importante para las organizaciones, es que se convierten en uno de los principales objetivos de ataque de los cibercriminales, por lo que es recomendable la implantación de directrices de seguridad, manteniendo el cumplimiento de la normativa en materia de seguridad y privacidad de los datos, por lo que es adecuado observar las recomendaciones que emiten los expertos en esta materia, con el fin de preservar la seguridad de la información y la integridad de las bases de datos ante un ataque cibernético.

En relación con lo anterior, independientemente de la tecnología del producto de la Base de Datos implementada como lo es Oracle, MySQL, SQL Server, DB2 entre otros, es importante considerar las diversas recomendaciones, de tal forma que preserven la seguridad de la información y la integridad en las Bases de Datos ante un incidente de seguridad, es por esta razón que se enlistan algunas de ellas, producto del análisis e indagación por parte de este órgano control y fiscalización:

1. **Sobre la implementación de las Bases de Datos**

a) En el proceso de instalación de las bases de datos, se crean identificadores de usuario, un grupo y una contraseña cuyos valores se implementan por defecto, por lo que se recomienda modificarlos en el tanto la tecnología lo permita.

b) Es recomendable especificar requisitos robustos de autenticación a nivel del sistema operativo, ante la utilización de mecanismos propios de autenticación por parte de los gestores de datos.

c) Revisar y modificar los privilegios predeterminados que se han otorgado a los usuarios durante la instalación, asimismo, crear identificadores de usuarios propietarios de instancias específicos para cada instancia, añadiéndolo solo como miembro de grupo propietario de la instancia y no usarlo en ningún otro grupo, con el objetivo de tener un mayor control en el número de usuarios y grupos que pueden modificar una instancia.

d) Durante la instalación de los gestores de bases de datos, se recomienda hacer uso de contraseñas robustas que cumplan las directivas de seguridad implementadas por la Institución.

2. **Sobre la configuración de las Bases de Datos**

a) Efectuar una adecuada configuración de control de acceso a las bases de datos, con medidas de seguridad centradas en permisos precisos ajustados a las necesidades de explotación de datos por parte de los usuarios, con el fin de controlar el tipo de información que estos acceden, disminuyendo el riesgo de ingresos no autorizados y fugas de información, para esto se efectúan las siguientes recomendaciones:

- ✓ Existir un mecanismo de comprobación de las peticiones de acceso mediante operaciones y datos solicitados y usuarios solicitantes según las reglas de seguridad.
- ✓ Tener la capacidad de reconocer el origen de una petición usuario para decidir qué reglas de seguridad son aplicables a cierta petición.
- ✓ Es recomendable que únicamente los administradores de las bases de datos creen las cuentas de acceso a las bases de datos, conceder y cancelar privilegios a las cuentas de usuario, así como asignar cuentas de usuario a niveles de seguridad o acreditación

b) Cuando existan sistemas interconectados se recomienda aplicar las medidas necesarias para delimitar la responsabilidad en cada sistema donde la identificación se produzca en diferentes dominios de seguridad.

c) Garantizar los controles de acceso mediante autenticación, ya sea a través de los mecanismos habilitados por el sistema operativo o de los propios del gestor de la base de datos.

d) Fortalecer el control de las cuentas de usuario, cumpliendo con criterios de seguridad para minimizar la exposición y posible explotación de la información, especialmente de las cuentas predeterminadas, por cuanto estas son un vector de ataque, por lo que se recomienda cumplir con aspectos como:

- ✓ Segregación de privilegios y mínima exposición, es decir, dar permisos únicamente a los objetos a los que se deba tener acceso.
- ✓ Debido cuidado en el otorgamiento de privilegios, asignando únicamente los necesarios.
- ✓ Crear identificadores de usuarios propietarios de instancias específicos para cada instancia, añadiéndolo solo como miembro del grupo propietario de la instancia y no usarlo en ningún otro grupo.
- ✓ Implementar las pautas de seguridad de contraseñas de las cuentas de usuario definido por la Institución.
- ✓ Configurar parámetros de bloqueo de cuentas como número permitido de intentos fallidos de inicio de sesión, número de días de bloqueo de cuenta posterior a los intentos fallidos, límite de tiempo de sesión activo para todas las cuentas del servidor de aplicaciones, número limitado de sesiones por usuario para cuentas no pertenecientes al servidor de bases de datos, definición de tiempo de cierre de sesión por inactividad para cuentas no pertenecientes al servidor de aplicación.
- ✓ Configurar cuentas de usuario específicas para los servidores de aplicaciones, por lo que no deben usarse cuentas genéricas asociadas a los distintos roles sino cuentas que identifiquen inequívocamente al autor de cualquier cambio.
- ✓ En los casos que aplique es recomendable establecer un doble factor de autentificación al motor de base de datos.

e) Implementación de roles y grupos de cuentas de usuario, donde se controlen los privilegios predeterminados durante la instalación del gestor de base de datos, se revoque el privilegio de crear bases de datos a todos los usuarios, excepto el usuario DBA, revisar los permisos de usuarios o grupos que no necesiten el acceso, verificar que no se otorgue accesos públicos a ninguna base de datos que contenga información sensible, por lo que se debe de controlar el acceso a los datos sensibles a nivel de registro, fila o celda, y analizar la pertinencia del acceso basado en etiquetas. Por lo anterior se recomienda que como mínimo se consideren la implementación de los siguientes roles:

- ✓ Usuarios habituales de la base de datos que están restringidos a las tablas, vistas, índices y procedimientos almacenados que solo les compete.
- ✓ Cuentas de aplicaciones quienes normalmente se utilizan para la ejecución de aplicaciones propias y de terceros.
- ✓ Administradores de las aplicaciones quienes administran y corrigen vulnerabilidades y realizan actualizaciones.
- ✓ Los analistas de datos o usuarios de inteligencia del negocio quienes por su naturaleza suelen tener solamente acceso de lectura.
- ✓ Administradores de Bases de Datos, siendo los responsables de la gestión del rendimiento, el diagnóstico y el ajuste, la actualización y la corrección de vulnerabilidades, el inicio de la base de datos y apagado, y respaldo de estas.
- ✓ Administradores de seguridad quienes verifican la seguridad en la gestión de cuentas de usuario, la gestión de claves de cifrado y gestión de auditoría.

f) Implementación de mecanismos de auditoría donde se proporcione un registro histórico de la actividad de los sistemas de base de datos, permitiendo que se audite a nivel de instancia como a nivel de base de datos individual, para esto se recomienda generar directivas de auditoría que registren los fallos y/o los aciertos, asimismo contemplar la creación del rol auditor en el que se le otorguen los privilegios necesarios para leer y administrar los eventos de auditoría.

g) Se recomienda implementar aquellas medidas de protección de la información, tanto las que se configuran e implementan en el entorno del servidor de las bases de datos, como en el entorno del sistema operativo que ejecuta el servidor.

h) En los casos que se considere necesario, se recomienda diseñar y hacer uso de políticas de acceso basado en filas y columnas (RCAC) en aquellos entornos donde existan una regulaciones o normativas que cumplir y el acceso a los datos tenga que realizarse según el contexto de quien lo solicita.

i) La implementación de control de acceso basado en etiquetas (LBAC) el cual permite tener el registro sobre quién puede acceder a los datos, aumentando el control sobre quién puede leer o consultar y quién puede modificar la información de las filas y columnas.

j) Implementar el enmascaramiento de datos dinámicos donde se anonimiza y ocultan datos limitando el acceso a los usuarios sin privilegios a la información sensible, ocultando el acceso a datos confidenciales, para lo anterior se recomienda disponer de una directiva o política de control de acceso adecuada.

k) Necesariamente implementar políticas de respaldos o back up de las bases de datos que permita recuperar la información existente en estas en caso de fallo o evento que no permita acceder a los datos, para esto se recomienda:

- ✓ Cifrar todos los ficheros de back up e imágenes de archivo, independientemente del medio donde se almacenen.
- ✓ 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.
- ✓ Mantener las prácticas recomendadas por el fabricante en cuanto a copias de seguridad.
- ✓ Realizar copias de seguridad periódicas donde se considere generar una copia de seguridad incremental diaria conservándose al menos durante siete días, una incremental semanal conservando la copia durante al menos cuatro semanas, una copia incremental cada mes conservándose los doce últimos meses y una anual conservándose durante cinco años.
- ✓ Para lo anterior se recomienda almacenar las copias de seguridad en lugares distintos a la ubicación física del servidor de producción y en sistemas de discos redundantes.
- ✓ Efectuar pruebas de recuperación periódicamente.

l) Una vez instalado el producto y sus actualizaciones, se recomienda revisar el estado de la solución periódicamente, para mantener la versión del motor de datos actualizada, mantener las versiones de cualquier software dependiente del motor actualizado, configurar alarmas de consumo y uso del motor de la base de datos, documentar todos los cambios en el motor de la base de datos y tareas de administración, revisar las vulnerabilidades de cada componente perteneciente a la instalación, en caso de que se publiquen vulnerabilidades y no hayan sido corregidas por el fabricante se debe reportar a los responsables superiores de seguridad y finalmente limpiar los ficheros temporales después de la instalación del producto, actualización o corrección de vulnerabilidades.

Aunado a lo anterior, considera esta Auditoría que es importante que la Administración Activa, valore a futuro la implementación de nuevas tendencias en la gestión de datos, como parte de sus actividades de reforzamiento de la plataforma tecnológica y sus mecanismos de seguridad, siempre dentro del marco de sus competencias y en el tanto los recursos lo permitan. Al respecto, entre las tendencias que se observan en el mercado entre otras se encuentran las siguientes:

- ✓ Implementación del modelo de base de datos como servicio DBaaS (Database-as-a-Service), permitiendo hacer cambios en cuanto a autoservicio, pago por uso, dinamismo, seguridad, automatización y mayor aprovechamiento de los recursos, así como agregar un nivel de complejidad a la estructura de seguridad mediante la gestión proactiva de los entornos.
- ✓ Implementación de plataformas de base de datos autónoma (Self-Driving Database Platform, SDDP) donde se tenga capacidad de auto conducción permitiendo que las bases de datos tomen decisiones y realizan optimizaciones de forma independiente con el fin de generar un servicio continuo.
- ✓ Gestión de Datos aumentada (ADM) el cual utiliza el aprendizaje automático y la inteligencia artificial para automatizar las tareas de gestión de datos, como detectar anomalías en grandes cantidades de datos y resolver problemas de calidad de datos.
- ✓ La virtualización de datos como solución para el aprovechamiento de la cantidad de información como la implementación de arquitecturas “data mesh”, tejidos de datos e inteligencia de datos.

Esta Auditoría considera que lo anteriormente mencionado, resulta importante se analice ante la afectación sufrida tanto en la encriptación de datos como en la interrupción de servicios, producto del hackeo del pasado 31 de mayo, y determinar si es necesario realizar una revisión o valoración general para definir una estrategia orientada a minimizar los riesgos e impacto institucional ante posibles ataques de ciberseguridad en el futuro, y se realice además en apego a lo establecido en las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, en el punto V. lo correspondiente a la “Arquitectura Empresarial”, a saber:

> *“La entidad debe contar con un modelo de arquitectura que permita visualizar adecuadamente la estructura de procesos institucionales y la relación de uso de recursos instalados (sistemas de información, infraestructura tecnológica) para gestionar los datos e información requeridos en la operativa. El órgano rector de Gobernanza en TI tiene la responsabilidad de establecer el modelo de arquitectura empresarial.*
>
> *La institución debe disponer de un modelo de clasificación de datos e información, según criterios y requisitos legales, de valor, según el nivel de criticidad y susceptibilidad a divulgación o modificación no autorizada. La Unidad de TI se basará en este modelo para establecer las directrices de seguridad y protección de los datos e información institucionales”.*

Asimismo, en el punto XI. “Seguridad y Ciberseguridad”, establece:

> *“La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*
>
> *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información. (…)”.*

Y en el punto XII. "Administración infraestructura tecnológica" de la citada norma señala:

> *"(…) La Unidad de TI debe establecer prácticas formales para la gestión de la entrega de servicios a través de los recursos tecnológicos instalados en la institución, administrados interna y externamente, gestionando la configuración y mantenimiento del desempeño y capacidad de los activos de TI, de manera que a través de monitoreos y actualizaciones se mantenga el uso óptimo de los recursos y brinden una garantía razonable sobre la continuidad de las operaciones institucionales, establecidos a través de niveles de operación y sostenibilidad para brindar los servicios requeridos. (…)".*

Al respecto, esta Auditoría informa sobre lo descrito con el objetivo de que la Dirección de Tecnologías y Comunicaciones en su rol de rector y direccionamiento tecnológico y en acompañamiento de los diferentes Centros de Gestión Informática y aquellas unidades que administran bases de datos, valoren dentro de sus estrategias la información expuesta y se profundice en el tema de así requerirlo, reforzando los mecanismos de ciberseguridad en estas, una vez que se hayan reestablecido los servicios tecnológicos institucionales, reduciendo la posibilidad de que se vuelvan a materializar riesgos que afecten las actividades sustantivas de la institución y teniendo un efecto directo en la atención de la población que hace uso de los servicios institucionales.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.13 14:36:24 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General –1100.
Doctor Randal Álvarez Juárez, gerente, Gerencia Médica -2901.
Licenciado Luis Fernando Campos Montes, gerente, Gerencia Administrativa –1104.
Licenciado Gustavo Picado Chacón, gerente, Gerencia Financiera –1103.
Ingeniero Jorge Granados Soto, gerente, Gerencia de Infraestructura y Tecnologías –1107.
Doctor Esteban Vega de la O, gerente, Gerencia de Logística -1106.
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia de Pensiones -9108.
Auditoría.