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

AD-ATIC-0069-2023
15 de junio de 2023

Máster
Eithel Geovanni Corea Baltodano, subgerente a.i
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Ingeniero
Alexander Solís Abarca, jefe CGI
GERENCIA FINANCIERA - 1103

Ingeniera
Giselle Tenorio Chacón, jefe CGI
GERENCIA ADMINISTRATIVA - 1104

Ingeniero
Roy Armando Ovares Valerio, jefe CGI
GERENCIA LOGÍSTICA - 1106

Ingeniero
Giovanni Campos Alvarado, jefe CGI
GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS – 1107

Ingeniero
Esteban Zúñiga Chacón, jefe CGI
GERENCIA MÉDICA - 2901

Ingeniero
Marco González Jimenez, jefe CGI
GERENCIA DE PENSIONES - 9108

Estimados señores:

ASUNTO:	**Oficio de Advertencia referente a finalización del ciclo de vida para el soporte de SQL Server 2012 & Windows Server 2012/2012 R2.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo de esta Auditoria para el período 2023, y de conformidad con las competencias establecidas en el artículo 22, inciso d) de la Ley General de Control Interno, a continuación se procede a informar y advertir a la Administración Activa, sobre la finalización del ciclo de vida para el soporte técnico de SQL Server 2012 & Windows Server 2012/2012 R2, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa Administración.

El 7 de junio de 2023, mediante oficio AS-ATIC-0047-2023, la Auditoría Interna informó a la Dirección de Tecnologías de Información y Comunicaciones y a los jefes de Centros de Gestión Informática de las respectivas Gerencias, establecer las prevenciones del caso sobre los productos de la empresa tecnológica Microsoft que finalizan soporte técnico en el período 2023.

Al respecto y considerando que son herramientas que se utilizan juntas, esta Auditoria constató[1] que el soporte para SQL Server 2012 finalizó el pasado 12 de julio de 2022 y para Windows Server 2012/2012 R2 finalizará el 10 de octubre de 2023, por lo que posterior a esa fecha, estos productos ya no recibirán actualizaciones de seguridad, ni de otro tipo, correcciones de errores y/o de soporte técnico. Bajo esa premisa, la corporación recomienda planificar y realizar la migración a Azure SQL Managed Instance o versiones más recientes como Windows Server 2019 o Windows Server 2022, a efectos de mantener la seguridad y el soporte continuo, según el detalle:

> *"Microsoft recomienda a los clientes migrar las aplicaciones y cargas de trabajo a Azure para que se ejecuten con seguridad. Azure SQL Managed Instance está totalmente administrado y siempre se actualiza (PaaS). Los clientes*

[1] Finalización del soporte de SQL Server 2012 y Windows Server 2012/2012 R2 - Microsoft Lifecycle | Microsoft Learn

también pueden migrar mediante lift-and-shift a Azure Virtual Machines, incluidos Azure Dedicated Host, Azure VMware Solution y Azure Stack (Hub, HCI, Edge), para obtener tres años adicionales de Actualizaciones de seguridad extendidas sin coste.

Los clientes que necesitan una solución local pueden actualizar a Windows Server 2022 y SQL Server 2019…".

Resulta significativo para este Órgano de Control y Fiscalización informar y señalar al ente rector en materia tecnológica, al nivel táctico y operativo de la institución, sobre la condición técnica de los productos señalados, así como concretar formalmente el proceder en el caso específico.

En esa misma línea y con el propósito de evitar comprometer el funcionamiento de los equipos computacionales, la continuidad de las operaciones, así como una posible afectación en el servicio que se brinda a los usuarios, es necesario se ratifiquen las acciones de planificación que conlleva este tipo de actividades o la migración de una versión de software a otra, dado que podría resultar complejo de no considerarse aspectos tales como: recursos, compatibilidad entre versiones, ambientes de pruebas, seguridad de los datos, monitoreo, entre otras.

Igualmente, es importante recordar que el uso de software sin soporte técnico del fabricante puede conllevar a riesgos significativos para la organización, entre los más comunes se pueden mencionar:

- Asistencia técnica: No se podrá acceder a la asistencia técnica oficial para resolver problemas y obtener orientación de parte del fabricante. Esto puede dificultar la resolución de problemas complejos y ralentizar el tiempo de respuesta ante incidencias.

- Vulnerabilidades de seguridad: El software sin soporte no recibirá actualizaciones de seguridad periódicas para abordar nuevas amenazas y vulnerabilidades. Esto deja al sistema expuesto a ataques informáticos por parte de ciberdelincuentes, virus u otro tipo de malware y puede resultar en brechas de seguridad y pérdida de datos.

- Cumplimiento normativo: En aras de garantizar la protección y privacidad de los datos, el uso de software sin soporte técnico podría presentar un incumplimiento regulatorio, en virtud de que el marco normativo de gobierno y gestión de las tecnologías de información en el sector público costarricense, precisa en la implementación de controles y mecanismos efectivos que minimicen el riesgo de vulnerabilidades a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información.

- Corrección de errores: Sin soporte técnico, no se proporcionarán actualizaciones ni correcciones de errores para el software. Esto puede llevar a problemas persistentes, fallas del sistema y errores funcionales que no se resolverán.

- Incompatibilidad con nuevas tecnologías: A medida que evolucionan las tecnologías y los sistemas operativos, el software descontinuado puede volverse incompatible y experimentar problemas de integración con otros componentes del sistema. Esto puede limitar la capacidad de la organización para adoptar nuevas tecnologías y mantenerse actualizada.

Las Normas técnicas para la gestión y el control de las tecnologías de información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), en el apartado "XI. SEGURIDAD Y CIBERSEGURIDAD", dispone:

> "La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.
>
> Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que 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 Institución, basada en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…).
>
> La Institución 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.

La institución debe implementar medidas de control asociadas a la administración del riesgo de seguridad de la información y ciberseguridad, que permitan el cumplimiento de los objetivos de los procesos, protegiendo la confidencialidad, autenticidad, privacidad e integridad de la información (…)".

En virtud de lo descrito, la institución deberá mantener su software actualizado y evitar el uso de versiones descontinuadas o sin soporte para garantizar la seguridad y la eficiencia de sus aplicativos, ya que como se ha mencionado en párrafos anteriores, utilizar software sin soporte técnico del fabricante aumenta significativamente la exposición a riesgos de seguridad, fallas del sistema y problemas operativos.

Por lo tanto, este Órgano de Fiscalización y Control, previene sobre la situación planteada en el presente oficio, con el propósito de que, en apego al marco normativo vigente, considere las observaciones indicadas y de ser procedente, se establezcan las acciones recomendadas para abordar los diferentes aspectos sometidos a su consideración. Lo anterior, con el fin de coadyuvar al cumplimiento de los objetivos institucionales, optimizando los procesos de trabajo e incrementando la calidad en la prestación de los servicios brindados por la Caja Costarricense de Seguro Social.

Al respecto, se deberá informar, a esta Auditoría Interna, sobre las acciones ejecutadas para la administración del riesgo y atención de la situación comunicada, en el plazo de **2 meses**, a partir del recibido de este documento

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2023.06.20 07:40:30 -06'00'

Msc. Olger Sánchez Carrillo
Auditor Interno

OSC/RJS/RAHM/OCHA/jfrc

C. Licenciada Vilma Campos Gómez, Gerente Administrativa - 1104
Auditoría

Referencia: ID-91468