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

AS-AATIC-160-2022
26 de julio de 2022

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

Ingeniero
Alexander Solís Abarca, jefe
Centro de Gestión Informática
GERENCIA FINANCIERA - 1103

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

Ingeniero
Roy Armando Ovares Valerio, jefe
Centro de Gestión Informática
GERENCIA 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 referente a la finalización del ciclo de vida del software de desarrollo SQL Server 2012**

Esta Auditoría 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, emite la siguiente asesoría sobre la finalización del ciclo de vida del software de desarrollo SQL Server 2012.

Al respecto, el sitio oficial[1] de la empresa Microsoft indica que el aplicativo "Microsoft SQL Server 2012" finalizó su ciclo de vida el pasado 12 de julio. Consecuentemente, la compañía recomienda accionar los planes de migración o modernización.

Es decir, el fin del soporte significa que ya no se proporcionarán actualizaciones de seguridad periódicas al software supracitado. Bajo ese contexto, es significativo comunicar al conjunto de usuarios sobre la condición tecnológica de esa solución.

Lo anterior, al considerar que los ataques cibernéticos cada vez son más sofisticados y frecuentes; por ende, la ejecución de aplicaciones y datos en versiones no compatibles puede crear importantes riesgos de seguridad y cumplimiento.

En ese sentido, resulta necesario definir formalmente el proceder en el tema de marras, por ejemplo al desinstalar el aplicativo obsoleto; actualizarse a versiones soportadas del software (actualización on-premise); adquirir actualizaciones de seguridad extendida (retrasar el cambio); migrar al Cloud; capacitación sobre la nueva herramienta a utilizar; entre otras valoraciones a efectuar y que eviten comprometer el funcionamiento de los equipos y/o aplicativos, así como una eventual afectación en el servicio brindado a los usuarios.

Todo lo anterior, en apego a lo indicado 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, lo correspondiente a la "Seguridad y Ciberseguridad", a saber:

> *"XI. SEGURIDAD Y CIBERSEGURIDAD*
>
> *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.*
>
> *La Unidad de TI, basado 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 (…).*
>
> *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.*

[1] https://docs.microsoft.com/es-es/lifecycle/products/?terms=sql%20server%202012.

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 (…)".

Por lo tanto, este Órgano de Fiscalización 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 establezca las acciones pertinentes y así 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.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.27 12:56:23 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C. Auditoría