



AS-AATIC-110-2022

27 de junio de 2022

Máster

Idannia Mata Serrano, 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

Eithel Giovanni Corea Baltodano, jefe CGI

GERENCIA DE PENSIONES - 9108

Estimados señores:

ASUNTO: Oficio de asesoría referente a la finalización del ciclo de vida para el soporte técnico del Internet Explorer.

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 para el soporte técnico del Internet Explorer 11.

Al respecto, el sitio oficial¹ de la empresa Microsoft indica que el aplicativo de escritorio llamado Internet Explorer 11, ha finalizado su soporte técnico, esto desde el pasado 15 de junio. Consecuentemente, la compañía recomienda la utilización de Microsoft Edge, citando lo siguiente:

¹ Enlace a publicación: <https://docs.microsoft.com/es-es/lifecycle/announcements/internet-explorer-11-end-of-support>



“Se recomienda a los clientes que cambien a Microsoft Edge, que proporciona soporte técnico para aplicaciones y sitios web heredados y modernos. Para las organizaciones que dependan de sitios y aplicaciones heredados basados en Internet Explorer, los sitios deberán configurarse para abrirse en Microsoft Edge mediante el modo Internet Explorer (IE).

El modo Internet Explorer en Microsoft Edge permite la compatibilidad con versiones anteriores y recibirá soporte técnico al menos hasta 2029. Además, Microsoft notificará con un año de antelación la retirada del modo IE. Haga clic aquí para obtener una lista de los sistemas operativos compatibles con Microsoft Edge.”

Bajo ese contexto, es significativo comunicar al conjunto de involucrados a nivel táctico y operativo sobre la condición tecnológica del Internet Explorer 11, así como definir formalmente el proceder en el tema de marras.

En ese sentido, valorando la necesidad de precisar las acciones orientadas a la desinstalación del aplicativo obsoleto, transición en la utilización del Microsoft Edge y/o estandarización de navegador web en la plataforma tecnológica de la CCSS, entre otras consideraciones que surjan con el objetivo de evitar comprometer el funcionamiento de los equipos computacionales, así como una posible afectación en el servicio brindado a los usuarios.

Además, evitando el incrementar la exposición a vulnerabilidades en el sistema operativo y sus aplicaciones, esto ante ataques informáticos por parte de hackers, virus u otro tipo de malware. 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.

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 (...).”



CAJA COSTARRICENSE DE SEGURO SOCIAL

Auditoría Interna

Teléfono: 2539-0821 ext. 2000-7468

Correo electrónico: auditoria_interna@ccss.sa.cr

Por lo tanto, este Órgano de Fiscalización previene sobre la situación planteada en el presente oficio, con el propósito que en apego al marco normativo vigente, considere las observaciones indicadas y de ser procedente, se establezca las acciones recomendadas 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

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/ghc

C. Auditoría