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

ATIC-0025-2025
25 de junio de 2025

RESUMEN EJECUTIVO

El presente estudio fue realizado de acuerdo con el Plan Anual Operativo 2025 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar la gestión efectuada por la administración activa para el desarrollo de aplicaciones y/o sistemas de información mediante software libre y/o lenguaje de código abierto en la CCSS.

Esta auditoría efectuó una revisión del Catálogo Institucional de Aplicaciones Informáticas (CIAI), con el fin de establecer la existencia de aplicaciones y/o sistemas cuyo entorno de programación se hubiese efectuado mediante herramientas de software libre y/o lenguaje de código abierto, sin embargo, en los datos consignados, no se identificaron registros que fueran concordantes con este tipo de desarrollos.

Asimismo, los resultados del estudio permitieron identificar aplicaciones y/o sistemas de información realizados mediante la utilización de software libre y/o lenguaje de código abierto en la institución; no obstante, la Dirección de Tecnologías de Información y Comunicaciones y los Centros de Gestión Informática Gerenciales carecen de información donde se establezca -de manera veraz y confiable- la cantidad total de estos desarrollos, los entornos de programación utilizados, su versión y funcionamiento actual en la red institucional.

Por otra parte, de conformidad con los datos suministrados a esta auditoría, se determinó que, en la institución no se ha emitido lineamientos o directrices específicos en torno al desarrollo de sistemas o aplicaciones con software libre y/o lenguaje de código abierto.

Aunado a lo anterior, en revisión efectuada por esta auditoría el 20 de febrero de 2025, se constató la existencia de un sitio (https://intranet.ccss.sa.cr/sitios/TIC/SA/SitePages/Descargas.aspx) para la descarga de software libre habilitado en la intranet por la Dirección de Tecnologías de Información y Comunicaciones, el cual podía ser accesado por cualquier funcionario o unidad que requiera hacer uso de esas herramientas.

Asimismo, se determinó que, el análisis de vulnerabilidades del software libre para el desarrollo de aplicaciones -a la ejecución del presente estudio- se realiza como uno de los procedimientos establecidos por la Comisión de Validación de Software Libre y el Comité de Control de Cambios de la DTIC, para brindar el aval para su utilización a nivel institucional, estas pruebas se efectúan únicamente a la versión especifica indicada en la solicitud de aval; posterior a su autorización, tanto el análisis de vulnerabilidades (de versiones que se descarguen o apliquen posteriormente), como la actualización a nuevas versiones de estas herramientas, queda a valoración y solicitud de los funcionarios o unidades que descargaron y utilizaron el software libre.

En relación con lo anterior, según lo indicado por funcionarios del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, al 28 de febrero de 2025, se encontraba en proceso un replanteamiento del procedimiento de aval para las nuevas solicitudes de utilización de software libre a nivel institucional, donde por medio de la firma de un acuerdo de uso, la persona responsable se compromete a mantener el software actualizado, no realizarle modificaciones (sin previa autorización de la DTIC) ni compartirlo; sin embargo, anteriormente estas responsabilidades no se tenían delimitadas o establecidas formalmente, quedando a criterio de los funcionarios, su adecuada utilización; situación que causa incertidumbre o preocupación respecto a los componentes que previamente habían sido descargados y utilizados sin haberse efectuado ningún acuerdo.

Aunado a lo anterior, preocupa a esta auditoría que la planificación o establecimiento de la hoja de ruta de los análisis de vulnerabilidades, a nivel institucional, se realice según demanda y que no es un tema exclusivo de sistemas (de conformidad con lo indicado por la Subárea de Seguridad en Tecnologías de Información), ya que esta situación disminuye, aún más, las posibilidades de detectar cualquier vulnerabilidad existente en las

versiones de servicio de las herramientas de software libre y/o lenguaje de código abierto utilizadas en el desarrollo de sistemas.

En virtud de lo expuesto, este Órgano de Fiscalización emitió conclusiones y 1 recomendación dirigida a la Dirección de Tecnologías de Información y Comunicaciones (como unidad rectora de TI) con la integración de un equipo de trabajo conformado por representantes de los Centros de Gestión Informática Gerenciales y las instancias que se estimen pertinentes -según sus competencias-, tendiente a establecer un plan de acción orientado a atender las oportunidades de mejora determinadas en la gestión de aval, utilización y administración de software libre para el desarrollo de aplicaciones y/o sistemas de información en la institución.

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

ATIC-0025-2025
25 de junio de 2025

ÁREA AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE EL DESARROLLO DE APLICACIONES Y/O SISTEMAS DE INFORMACIÓN MEDIANTE SOFTWARE LIBRE Y/O LENGUAJE DE CÓDIGO ABIERTO EN LA CAJA COSTARRICENSE DE SEGURO SOCIAL.

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención a las actividades especiales del Plan Anual Operativo 2025 para el Área de Auditoría de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión efectuada por la administración activa para el desarrollo de aplicaciones y/o sistemas de información mediante software libre y/o lenguaje de código abierto en la CCSS.

OBJETIVOS ESPECÍFICOS

- Determinar la utilización de software libre en el desarrollo de aplicaciones y/o sistemas de información en la Caja Costarricense de Seguro Social.
- Identificar la existencia de un marco normativo o lineamiento en torno al desarrollo de aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto.
- Verificar que el desarrollo de aplicaciones y/o sistemas de información con software libre cumple con el marco normativo y regulaciones aplicables.
- Determinar los mecanismos de control implementados para la detección y atención de vulnerabilidades, errores y riesgos de seguridad propios del desarrollo de aplicaciones y/o sistemas de información con software libre.

NATURALEZA Y ALCANCE

El estudio comprendió la revisión del Catálogo Institucional de Aplicaciones Informáticas (CIAI) y otras fuentes de información, con el fin de establecer el desarrollo de aplicaciones y/o sistemas de información mediante software libre en la CCSS; la verificación de la existencia de un marco normativo o lineamiento que regule dicha materia. Además, se evaluaron los mecanismos de control implementados para el aval, utilización, comunicación a los usuarios de vulnerabilidades y administración (soporte técnico, análisis y atención de vulnerabilidades, seguimiento y actualización de nuevas versiones y resolución de incidencias, etc.) del software libre para el desarrollo de aplicaciones y sistemas de información en la plataforma institucional.

El periodo de evaluación incluye desde enero del 2024 a febrero del 2025, ampliándose en los casos donde se consideró necesario.

La evaluación se efectuó de acuerdo con lo dispuesto en las Normas Generales de Auditoría para el Sector Público y Normas para el Ejercicio de la Auditoría Sector Público, divulgadas a través de la Resolución R-DC064-2014 de la Contraloría General de la República, publicadas en La Gaceta 184 del 25 de setiembre 2014, vigentes a partir del 1º de enero 2015 y demás normativa aplicable.

LIMITACIONES

Esta Auditoría mediante mensajes enviados por la plataforma TEAMS los días 12 y 13 de febrero del presente año, solicitó al Ing. Roy Ovares Valerio, jefe del Centro de Gestión Informática de la Gerencia de Logística, espacio para realizar entrevista y aplicar el "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" mediante la herramienta FORMS, lo anterior, de conformidad al oficio de comunicación de inicio de estudio AI-0255-2025 del 5 de febrero de 2025; no obstante, a la fecha de conclusión de la aplicación de los procedimientos que sustentan este estudio, no se obtuvo respuesta por parte del citado funcionario.

Asimismo, los resultados evidenciados en el presente estudio no representan la totalidad de la información solicitada a los Centros de Gestión Informática (Regionales (médica y financiera), locales y de hospitales nacionales y especializados) de la institución, mediante la herramienta desarrollada en FORMS "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre", ya que no todos cumplieron en tiempo y forma con lo requerido por esta auditoría, situación que limitó establecer la situación real en materia de desarrollo de aplicaciones mediante software libre y/o lenguaje de código abierto en la institución.

METODOLOGÍA

Con el propósito de alcanzar los objetivos propuestos, se desarrollaron los siguientes procedimientos metodológicos:

- Aplicación de entrevistas y de la herramienta desarrollada en FORMS "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" a los Centros de Gestión Informática de las gerencias administrativa, financiera, médica, pensiones y de infraestructura y tecnologías.

- Aplicación de la herramienta desarrollada en FORMS "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" a 69 Centros de Gestión Informática (Regionales (médica y financiera), locales y de hospitales nacionales y especializados).

- Entrevistas, reuniones y solicitud de información a los siguientes funcionarios:

  - Ing. Danilo Hernández Monge, jefe, Área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones.
  - Ing. Daniel Berrocal Zuñiga, jefe del Área de Seguridad y Calidad de la Dirección de Tecnologías de Información y Comunicaciones.
  - Ing. Laura Paz Morales, jefe, Subárea Sistema Automatizado en Recursos Humanos, Dirección de Administración y Gestión de Personal.
  - Ing. Marlon Delgado Álvarez, jefe a.i y el Ing. Luis Angel Gómez Alfaro, coordinador de la Comisión de Validación de Software Libre, ambos funcionarios del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones.
  - Ing. Erick David Vindas Umaña, jefe a.i. Subárea de Seguridad en Tecnologías de Información.
  - Ing. George Aguilar Prieto, encargado de la unidad de desarrollo de software del Centro de Gestión Informática del Hospital San Vicente de Paúl.

- Revisión del Catálogo Institucional de Aplicaciones Informáticas (CIAI), con el fin de establecer la existencia de aplicaciones y/o sistemas cuyo entorno de programación se hubiese efectuado mediante herramientas de software libre y/o lenguaje de código abierto.

- Revisión del sitio (https://intranet.ccss.sa.cr/sitios/TIC/SA/SitePages/Descargas.aspx) para la descarga de software libre, habilitado en la intranet por la Dirección de Tecnologías de Información y Comunicaciones.

- Revisión de informes de análisis de vulnerabilidades, con el fin de verificar la inclusión de aspectos asociados a posibles vulnerabilidades en software libre: S.467 Informe de Análisis de vulnerabilidades Sitio Web CCSS (febrero 2023), Informe de Análisis de vulnerabilidades a rrhh.ccss.sa.cr (enero 2023), Informe Análisis de Vulnerabilidades Web SIPE (diciembre 2023) e Informe de Análisis de vulnerabilidades a rrhh.ccss.sa.cr (febrero 2023), Informe Análisis de Vulnerabilidades Bitzú (enero 2025) e Informe de Análisis de Vulnerabilidades Internas al Sistema de Información de Sostenibilidad Ambiental (noviembre 2023).

MARCO NORMATIVO

- Ley General de Control Interno, No. 8292, julio 2002.
- Normas de Control Interno para el Sector Público de la Contraloría General de la República, febrero 2009.
- Normas Generales de Auditoría para el Sector Público, Resolución R-DC-064-2014, setiembre 2014.
- Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, 2021.
- Normas Institucionales en Tecnologías de Información y Comunicaciones, abril 2012.
- Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, octubre 2012.
- Modelo de Organización de los Centros de Gestión Informática, octubre 2013.

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría informa y previene al Jerarca y a los titulares subordinados acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37, 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"(…) Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)".*

ANTECEDENTES

I. SOFTWARE LIBRE Y/O LENGUAJE DE CÓDIGO ABIERTO PARA EL DESARROLLO DE APLICACIONES

El término código abierto se refiere a programas cuyo código fuente está disponible para su uso o modificación según lo consideren oportuno los usuarios u otros desarrolladores. A diferencia del software propietario, el software de código abierto es un programa informático puesto a disposición del público de forma gratuita.

El código abierto contrasta con las aplicaciones de software propietarias o de código cerrado, el creador o el titular de los derechos de autor vende el software propietario o de código cerrado a los usuarios finales, a los que no se les permite editar, mejorar o redistribuir el producto excepto según lo especifique el titular de los derechos de autor.

El término "código abierto" también hace referencia de manera más general a un enfoque basado en la comunidad para crear cualquier propiedad intelectual, como el software, a través de la colaboración abierta, la inclusión, la transparencia y las actualizaciones públicas frecuentes.

A continuación, se indican algunos conceptos claves:

1. **Código Abierto (Open Source):** Significa que el código fuente del software está disponible públicamente. Los desarrolladores pueden ver, modificar y mejorar el código según sus necesidades.
2. **Licencias de Código Abierto:** El software de código abierto se distribuye bajo licencias específicas que definen cómo puede ser utilizado, modificado y redistribuido.
3. **Colaboración y Comunidad:** El desarrollo de software de código abierto a menudo implica la colaboración de una comunidad global de desarrolladores. Esta colaboración permite mejoras continuas, corrección de errores y la adición de nuevas funcionalidades.
4. **Flexibilidad y Personalización:** Los desarrolladores tienen la libertad de adaptar el software a sus necesidades específicas. Esto es especialmente útil para organizaciones que requieren soluciones personalizadas.

En relación con lo anterior, a continuación, se mencionan algunos ejemplos de herramientas y frameworks[1] de código abierto:

- **Python y Django:** Para el desarrollo de aplicaciones web y scripts.
- **PHP y Laravel:** Para el desarrollo de sitios y aplicaciones web.
- **Node.js y Express:** Para crear aplicaciones web rápidas y escalables.
- **React y Angular:** Librerías y frameworks de JavaScript para el desarrollo de interfaces de usuario dinámicas.
- **MySQL y PostgreSQL:** Sistemas de gestión de bases de datos relacionales.
- **Git:** Sistema de control de versiones para gestionar el código fuente.

Actualmente, el software de código abierto se utiliza en una amplia variedad de áreas, desde aplicaciones web hasta sistemas operativos y herramientas de desarrollo.

A través de los años, distintos órganos y especialistas nacionales e internacionales han destacado oportunidades estratégicas y beneficios financieros que podrían generar la adopción de software libre en la Caja Costarricense de Seguro Social, señalándose posibles ventajas significativas en distintos ámbitos.

El 29 de setiembre del 2011, se emitió el Informe del equipo de especialistas nacionales nombrado para el análisis de la situación del seguro de salud de la CCSS, documento en el que se genera las “Recomendaciones para restablecer la sostenibilidad financiera del seguro de salud”, de las cuales se derivó la recomendación número 50, según se detalla a continuación:

> *“R.50. Migrar a software libre en un plazo máximo de dos años.*
>
> *Entre los años 2008 y 2010 la CCSS pagó más de 5.000 millones de colones por concepto de licencias de software, incluyendo software ofimático, soporte de aplicaciones web, soporte de bases de datos, software de seguridad (antivirus, filtros de contenido, certificados de seguridad) y otros. Para los años 2012 a 2016 la Dirección de Tecnologías de Información y Comunicaciones estima que un gasto por este concepto de 9.642 millones, de los cuales cerca de la mitad corresponde a licenciamiento de software ofimático y de productividad, es decir, las aplicaciones de escritorio (procesadores de texto, correo, acceso, navegación, antivirus, etc. de todas las computadoras institucionales del país. Dado que para la mayoría de esas aplicaciones existe software libre, gratuito, se recomienda iniciar un proceso de migración hacia ese tipo de software, de forma que en un máximo de dos años se hayan sustituido la mayor parte de los sistemas operativos y de las aplicaciones de escritorio.*
>
> *Esta migración es posible, y hay experiencias muy avanzadas en el país, como la del Poder Judicial, que deben ser tomadas en cuenta a nivel institucional”.*

[1] Un framework o marco de trabajo, es una estructura o conjunto de herramientas y componentes que nos proporciona una base para desarrollar aplicaciones o crear páginas web de una manera más organizada, robusta y escalable.

En relación con el tema de la utilización del software libre en la Caja Costarricense de Seguro Social, esta auditoria desde el 29 de agosto del 2011 emitió el informe ATIC-287-2011 "Gestión del Licenciamiento Adquirido a Nivel Institucional", en el cual, se estableció la siguiente recomendación:

> *"(…) A LA GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS*
> *1. En coordinación con la Dirección de Tecnologías de Información y Comunicaciones, establecer un equipo de trabajo, el cual se encargue de elaborar un análisis situacional respecto a la oportunidad, viabilidad, efectividad y valor agregado que puedan ofrecer alternativas de solución tales como herramientas de software libre, cómputo en la nube, entre otros; como alternativa a componentes de software propietario. Este análisis deberá contemplar como mínimo la factibilidad de la iniciativa, la funcionalidad de las herramientas (ofimática, seguridad, monitoreo, entre otros), sus posibles usuarios finales por herramienta, la capacitación necesaria para su utilización, mantenimiento y soporte, la curva de aprendizaje a nivel institucional y los costos asociados.*

En relación con lo anterior, en marzo del 2017 esta auditoría estableció el cumplimiento de dicha recomendación, ya que, se evidenció que la administración activa llevó a cabo el "Estudio Preliminar y de Factibilidad del Proyecto Implementación gradual Software Libre en la CCSS"; no obstante, se les indicó la responsabilidad de gestionar ante las autoridades superiores, la oficialización y aval para procurar la participación activa de los profesionales, áreas y servicios de las diferentes unidades involucrados en el proyecto.

Por otra parte, mediante oficio No. 17.827 del 5 de febrero del 2013, remitido por la Licda. Emma Zúñiga Valverde, Secretaria de Junta Directiva, a la comisión de Tecnologías y Ambiente de la Institución, se consigna lo dispuesto en la sesión No. 8621 del 31 de enero del 2013, artículo 6, referente a la posibilidad de migrar hacia software libre e implementar los correspondientes cambios como alternativa para el fortalecimiento e innovación de la plataforma tecnológica institucional, indicándose, los tres acuerdos alcanzados la Junta Directiva:

> *"(…) 1. Dar por recibido el informe de análisis y resultados elaborado por los expertos del PNUD con el apoyo logístico de la Gerencia de Infraestructura y Tecnologías y brindar un agradecimiento especial al equipo de expertos del PNUD por la colaboración brindada en este tema.*
> *2. Trasladar a la Comisión de Tecnologías y Ambiente de la Junta Directiva el informe elaborado por la Gerencia de Infraestructura y Tecnologías contenido en el oficio número GIT- 0117-20143, de fecha 19 de enero del año en curso, firmado por la señora Gerente de infraestructura y tecnologías, para que lo incorpore como insumo en el proceso de análisis, previo a las decisiones que tome esta Junta Directiva.*
> *3. Someter a consideración de la Comisión de Tecnologías y Ambiente de la Junta Directiva las propuestas planteadas en el informe presentado por los expertos del PNUD, para procurar una decisión de implementación a nivel institucional y en términos parciales, según corresponda. En un plazo no mayor a treinta días dicha Comisión deberá presentar ante esta Junta Directiva los resultados del análisis realizado."*

En las actas de la sesión No. 8633 de Junta Directiva del 04 de abril del 2013, ese máximo órgano decisor acordó:

> *"(…) 1. Dar por recibido el informe TIC-R50-0001-2013, anexo a GIT-0351-2013, relativo al análisis y recomendaciones del "Diagnóstico sobre la Factibilidad de Implementar R50 en la Caja Costarricense de Seguro Social", como parte del proceso de seguimiento a la implementación de las recomendaciones del "Informe del equipo de especialistas nacionales nombrado para el análisis de la situación del Seguro de Salud".*
>
> *2.Instruir a la Gerencia de Infraestructura y Tecnologías la conformación de un equipo de proyecto, adscrito a la Dirección de Tecnologías de Información y Comunicaciones, que conduzca y ejecute las acciones necesarias para la implementación gradual del software libre en la Caja, de acuerdo con las posibilidades institucionales y una adecuada evaluación de los beneficios y riesgos esperados. La conformación de dicho equipo es de orden funcional y no implica cambios en la estructura*

organizacional. Dicho equipo debe estar conformado por funcionarios de las diferentes Gerencias con el perfil requerido por el Proyecto y deben presentar a la Junta Directiva en el plazo de dos meses el plan de trabajo que contenga plazos, responsables, actividades, metas y sus respe (sic) indicadores de avance. Asimismo, de conformidad con las posibilidades institucionales se designarán recursos financieros para darle viabilidad a la implementación del software libre en las áreas que corresponda, según el plan de trabajo correspondiente, el cual, previamente, será aprobado por Junta Directiva.

3.Instruir a las Gerencias de Pensiones, Administrativa, Médica, de Logística y Financiera, para que designen en un plazo no mayor a dos semanas, un representante con conocimiento y experiencia en el uso de software libre aplicable a las áreas de competencia de cada Gerencia. Instruir a la Presidencia Ejecutiva, para que, en el marco de la cooperación brindada por el PNUD, se gestione la continuidad del acompañamiento de dicho Organismo, en la implementación de la recomendación R 50".

No obstante, también se han establecido diversos riesgos asociados con el uso de software libre o lenguaje de código abierto para el desarrollo de aplicaciones.

Mediante oficio GG-0011-2023 del 09 de enero del 2023 el Ing. Josué Guillermo Zuñiga Hernandez, en ese momento funcionario de la Gerencia General, indicó a los miembros del Consejo Tecnológico de la CCSS, lo siguiente:

"Reciban un cordial saludo. Con el propósito de brindar atención al acuerdo segundo consignado en la sesión de Junta Directiva No. 9270, efectuada el 11 de agosto del 2022; en el cual se consignó el acuerdo segundo de versa de la siguiente manera:

"Instruir al Consejo Tecnológico para que replantee la estrategia de utilización de software libre a nivel institucional considerando los riesgos evidenciados durante el Ciberataque del 31 de mayo de 2022"

Así las cosas, esta Gerencia General procede a informar al Consejo Tecnológico lo siguiente respecto a la adopción del Software Libre en la Caja Costarricense de Seguro Social (…)

Propuesta de Acuerdo:

Conocidos los antecedentes presentados por la Gerencia General respecto a la adopción del Software Libre en la Caja Costarricense de Seguro Social, se instruye a la Dirección de Tecnologías de Información para que, en conjunto con los Centros de Gestión Informática Gerenciales y la Dirección de Planificación Institucional, realicen un análisis sobre la gestión institucional del software libre, con el propósito de determinar la estrategia institucional para la adecuada gestión, control y monitoreo de las herramientas de software libre implementadas a nivel institucional: Lo anterior deberá ser presentado ante este consejo tecnológico el lunes 6 de marzo del 2023".

En relación con lo anterior, mediante oficio AD-ATIC-0120-2023 del 2 de noviembre de 2023, esta auditoría le informó al Consejo Tecnológico y la Dirección de Tecnologías de información y Comunicación, sobre el estado de las acciones efectuadas por las autoridades institucionales para la valoración del uso e implementación de software libre en la Caja Costarricense de Seguro Social, señalándose que, si bien las autoridades institucionales habían ejecutado diversas acciones orientadas a la implementación gradual de software libre en la CCSS (en atención a lo indicado en la recomendación 50 del informe del equipo de especialistas nacionales nombrado para el análisis de la situación del seguro de salud de la CCSS, lo señalado en el informe presentado por los expertos del PNUD, acuerdos de Junta Directiva y los productos emitidos por este órgano de fiscalización), preocupaba a este órgano de fiscalización que, a la fecha de emisión del citado oficio, todavía se encontraba en proceso la atención de lo solicitado por Junta Directiva (posterior al ciberataque del 31 de mayo de 2023), lo cual, aumentaba el riesgo de que los niveles estratégicos no pudieran realizar una adecuada toma de decisiones en relación con las estrategias a seguir para la implementación de estas tecnologías de formato abierto.

En relación con lo anterior, mediante el oficio GG-DTIC-7464-2023 del 07 de noviembre de 2023 se le trasladó al equipo conformado por la Dirección de Tecnologías de Información y Comunicaciones el oficio GG-DTIC-6393-2023, donde se les solicitó valorar el diseño del proceso de gestión de software libre dentro de la estrategia solicitada por Junta Directiva.

Posteriormente, el citado equipo remitió al Máster Robert Picado Mora, subgerente de la Dirección de Tecnologías de Información y Comunicaciones el oficio GG-DTIC-8248-2023 del 11 de diciembre de 2023, donde se adjuntó el *"Plan de trabajo"* y se describió las actividades que se estarían ejecutando para la atención de la estrategia, la cual, posteriormente sería presentada ante el Consejo Tecnológico; sin embargo, no se informó a esta auditoría los resultados de dicha presentación o posteriores acciones efectuadas por la administración activa en relación a dicho tema.

Por otra parte, en relación con lo anterior con la información anteriormente citada y según datos extraídos del sitio web www.cobalt.io a continuación, se indican algunos riesgos asociados con el uso de software código abierto:

- **Vulnerabilidades:** Como cualquier software, el software de código abierto puede contener vulnerabilidades que los atacantes pueden explotar. Es fundamental mantener el software de código abierto actualizado con los últimos parches de seguridad y seguir las mejores prácticas para una configuración y un uso seguros.
- **Falta de soporte:** algunos programas de código abierto pueden tener un nivel de soporte diferente al del software propietario, lo que hace que sea más difícil obtener ayuda con problemas de seguridad u otros problemas.
- **Dependencias:** El software de código abierto suele depender de otras bibliotecas y componentes de código abierto, lo que puede suponer riesgos de seguridad adicionales si dichas dependencias presentan vulnerabilidades. Es importante gestionar cuidadosamente las dependencias y mantenerlas actualizadas para reducir el riesgo de vulnerabilidades.
- **Compromiso de paquetes legítimos:** Existe el riesgo de que los paquetes de código abierto utilizados en proyectos sean comprometidos, ya sea por un ataque directo a los desarrolladores o a través de vulnerabilidades en los sistemas de distribución.
- **Software obsoleto:** Utilizar componentes de código abierto que no se actualizan regularmente puede llevar a problemas de compatibilidad y seguridad.
- **Riesgos operativos:** Los componentes de código abierto pueden introducir riesgos operativos que comprometan la disponibilidad y el rendimiento de la aplicación.

Además, es importante mencionar que, según datos extraídos de los sitios web www.cybersecuritydive.com y www.greynoise.io, el 10 de marzo 2025, se indica la existencia de una vulnerabilidad asociada con el uso de software de código abierto PHP:

> *"(...) Resumen de la inmersión:*
>
> *CVE-2024-4577, una vulnerabilidad crítica de inyección de argumentos que afecta a las instalaciones de PHP en sistemas Windows, ha sido objeto de explotación generalizada en varios países como Estados Unidos y el Reino Unido, dijo GreyNoise en una publicación de blog el viernes.*
>
> *La vulnerabilidad de PHP se reveló por primera vez en junio pasado y rápidamente fue atacada por una variedad de actores de amenazas y campañas de malware, incluido el ransomware TellYourPass, según un informe de Censys.*
>
> *La semana pasada, Cisco Talos informó sobre ataques recientes a CVE-2024-4577 por parte de un actor de amenazas desconocido contra objetivos en Japón. Sin embargo, GreyNoise afirmó que la vulnerabilidad ha sido explotada masivamente en varios países.*
>
> *Información sobre la inmersión:*

La explotación de CVE-2024-4577, que afecta a todas las versiones de instalaciones de PHP para dispositivos Windows, puede permitir la ejecución remota de código en sistemas específicos. Si bien los ataques recientes a la vulnerabilidad de PHP parecieron limitarse inicialmente a Japón, GreyNoise afirmó que no es así (...)".

Para mitigar estos riesgos, es necesario establecer prácticas robustas de gestión de seguridad, mantener actualizadas las dependencias, realizar análisis regulares de vulnerabilidades e implementar un plan de contingencia para abordar posibles problemas técnicos y operativos que puedan surgir.

II. RESPECTO AL MODELO DE LA INFRAESTRUCTURA TECNOLÓGICA SOBRE EL DESARROLLO DE SISTEMAS CON SOFTWARE LIBRE

El Modelo de la Infraestructura Tecnológica TIC-MIT-0001 en el apartado de "i. Presentación", señala el modelo de infraestructura tecnológica de la Caja Costarricense de Seguro Social, misma que soporta y provee una serie de servicios informáticos para el continuo desarrollo de gestiones de trabajo a lo interno de la institución, indicándose, además, como uno de sus objetivos específicos: "b. Servir de documento base para la planificación, desarrollo e implementación de proyectos de infraestructura tecnológica tanto de nivel central como a desconcentrado".

Este mismo marco normativo, en el apartado 8.14 Capa de Servicios Informáticos, indica:

"El acelerado crecimiento tecnológico bajo el que se ha visto inmerso la CCSS ha hecho que se adopten nuevas formas para poder competir y responder adecuadamente en los distintos campos de acción. Así mismo debemos estar capacitados para utilizar las nuevas tecnologías que nacen a ritmo acelerado con el propósito de brindar un servicio de primera línea (...)

b. La tendencia en los últimos años ha sido el desarrollo Web, dada las ventajas que este ambiente presenta, como tener un mayor alcance que cualquier otro tipo de arquitectura, utilizar un protocolo estándar como http (https), la no necesidad de distribuirse o instalarse en los clientes, brinda la capacidad de estar siempre disponible en cualquier lugar y en cualquier momento, sin importar barreras físicas o geográficas. Ya que la aplicación y su información es permanente y está siempre disponible para ser utilizada de manera instantánea, esta puede llegar mediante un explorador de internet en cuestión de segundos desde el servidor a cualquier lugar que posea acceso a Internet, permitiendo ampliar la cobertura nacional e inclusive internacional de ser requerida.

c. Estas aplicaciones Web han sido desarrolladas en diversas tecnologías como .Net, que se ejecuta en servidores Intel y Sistemas operativos Microsoft; también podemos encontrar aplicaciones Java (j2ee) que se ejecutan en servidores de aplicaciones Java (Oracle y Bea), corriendo en diversos tipos de hardware (Spark, x86, x64, Itanium) y en variedad de sistemas operativos (Windows, Linux, Solaris, HP-UX), y en menor medida podemos encontrar desarrollos en PHP (...)".

III. INTERFACES Y WEBSERVICES

Las interfaces y los webs services son mecanismos de comunicación en software, pero con diferentes enfoques.

Las interfaces, especialmente las API (Interfaz de Programación de Aplicaciones), son conjuntos de reglas y protocolos que permiten que diferentes aplicaciones o sistemas se comuniquen, por otro lado, los webs services son un tipo específico de API que facilitan la comunicación entre aplicaciones a través de la web, utilizando protocolos como HTTP, SOAP o REST.

Interfaces (API):

- Son mecanismos que definen cómo dos o más componentes de software se comunican.
- Pueden ser utilizadas tanto en sistemas locales como en redes, sin requerir necesariamente la web.

Ejemplos: una biblioteca de funciones que permite a un programador realizar ciertas operaciones, o una API que permite a una aplicación web acceder a los datos de una base de datos.

Web Services:

- Son un tipo de API que se basa en protocolos web (HTTP, SOAP, etc.) para facilitar la comunicación entre aplicaciones a través de Internet.
- Permiten que aplicaciones diferentes, incluso en diferentes plataformas, se comuniquen y compartan datos y funcionalidades.
- Son fundamentales para la construcción de aplicaciones web y la interconexión de sistemas en la nube.

Ejemplos: un servicio que permite a una aplicación obtener información del clima, o un servicio de pago en línea.

En resumen, los webs services son un tipo de API que utiliza protocolos web para la comunicación en red, mientras que las API son un concepto más general que se refiere a la comunicación entre cualquier componente de software.

HALLAZGOS

1. RESPECTO AL REGISTRO Y ACTUALIZACIÓN DE CARACTERISTICAS DE LAS APLICACIONES DESARROLLADAS MEDIANTE SOFTWARE LIBRE O LENGUAJE DE CÓDIGO ABIERTO EN EL CATALOGO INSTITUCIONAL (CIAI)

En revisión del Catálogo Institucional de Aplicaciones Informáticas (CIAI), realizada por esta auditoría, se determinó la carencia de registros donde se consignen sistemas informáticos que su entorno de programación se hubiese efectuado mediante herramientas de software libre y/o lenguaje de código abierto; no obstante, según se muestra en el hallazgo 2 del presente estudio, en la institución actualmente existen aplicaciones efectuadas mediante estas herramientas de desarrollo.

Las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE, en el artículo 5.6 “Calidad de la información”, estipula:

> *“El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo.*
> *Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad.*
> ***5.6.1 Confiabilidad** La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente.*
> ***5.6.2 Oportunidad** Las actividades de recopilar, procesar y generar información, deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales.*
> ***5.6.3 Utilidad** La información debe poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario (…)”.*

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en su apartado “*X. Desarrollo, implementación y mantenimiento de sistema de información”*, señala:

"(…) La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones (…)".

En ese mismo marco normativo, en el apartado "*XI. Seguridad y ciberseguridad"*, cita:

"(…) 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 (…)

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 (…)".

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, en el numeral 5.7 Responsabilidades de los niveles organizacionales y funciones sustantivas, para el Área de Ingeniería de Sistemas, entre otros aspectos señala:

" 5.7.3. Nivel Área de Ingeniería de Sistemas.

Es responsables del desarrollo de los sistemas de información institucionales, del mantenimiento preventivo y correctivo de los mismos, de las modificaciones requeridas por el software, de suministrar los servicios a los usuarios, del soporte técnico a las actividades de Telesalud y la automatización de los sistemas en el área Financiera-Administrativa y Salud (…)

Esta Área de Trabajo debe asesorar, colaborar y apoyar técnicamente para que los Centros de Gestión Informática, a los cuales el Consejo de Presidencia y de Gerentes o la Dirección de Tecnologías de Información y Comunicaciones le asigne, como estrategia operacional, el desarrollo de sistemas de ámbito global del sistema de salud, de pensiones, financiero, administrativo, bienes y servicios, entre otros, cumplan en forma efectiva con la solicitud específica. (…)

Mantener un registro actualizado de las aplicaciones disponibles y sus características, de conformidad con las políticas vigentes, con el fin de contar con información oportuna y veraz (…)

Suministrar en forma oportuna la información solicitada por las autoridades superiores, a partir de los requerimientos específicos, para que se cumplan efectivamente las acciones de fiscalización, seguimiento, control y evaluación de la gestión (…)".

En el Modelo de Organización de los Centros de Gestión Informática en el numeral 5.6.1 Modelo Tipo A: Centros de Gestión Informática Gerenciales, apartado de Responsabilidades del nivel organizacional y funciones sustantivas, se indica:

"(…) ***Conceptualización del Área***
Área: Centro de Gestión Informática Gerencial (…)
Gestión Técnica:

(…) Desarrolla e implementa, previa autorización de Dirección de Tecnologías de Información y Comunicaciones, sistemas de información y aplicaciones, con el fin de automatizar los procesos operativos específicos y define una cartera de proyectos a nivel gerencial en coordinación con los centros de gestión informática de su ámbito de acción (…)

Aplica la regulación, la normativa técnica y las metodologías de trabajo que permitan la eficiente y eficaz utilización de los recursos, con el fin de garantizar la confiabilidad y continuidad de las operaciones que se realizan (…)

Establecer mecanismos de control que permitan el auditoraje de los sistemas de información, a partir de las técnicas aceptadas y los manuales respectivos, para facilitar la evaluación de la gestión.

Documentar los cambios que se produzcan en los sistemas y aplicaciones, en su ámbito de competencia, de acuerdo con las políticas y la normativa vigente, con el objeto de mantener un registro interno e institucional actualizado de aplicaciones.

Realizar pruebas de los sistemas de información y las aplicaciones, con base en las metodologías de trabajo establecidas y la normativa vigente, con el fin de lograr el desarrollo efectivo de la gestión.

Comunicar el desarrollo e implementación de los sistemas y las aplicaciones a la Dirección de Tecnologías de Información y Comunicaciones, con el fundamento en la normativa vigente, con el objetivo de que éstos se incorporen oportunamente al Registro Institucional de Aplicaciones.

Desarrollar acciones que permitan proteger los recursos de tecnologías de información, con base en las políticas vigentes y el análisis de los riesgos, con el objeto de lograr un ambiente seguro y controlado (…)"

Asimismo, en el citado marco normativo, en el numeral 5.6.1 Modelo Tipo B: Centros de Gestión Informática Regionales y Locales, se señala:

"(…) Para el desarrollo de los programas y aplicaciones en su ámbito de competencia, requiere de la autorización previa de la Dirección de Tecnologías de Información y Comunicaciones (…)"

Las Normas Institucionales en Tecnologías de Información y Comunicaciones, en el numeral 3.2 Implementación de Software, se establece:

"(…) Toda Área de trabajo debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

- *Acatar lo dispuesto en el punto 3.1 de este documento.*
- *Aplicar lo establecido en la Metodología de Desarrollo de Software, que considera la definición*
- *de requerimientos, los estudios de viabilidad, la elaboración de diseños, la programación y*
- *pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción,*
- *así como también la evaluación post-implantación de la satisfacción de los requerimientos.*
- *Aplicar lo establecido en la Metodología de Modelación de Datos Institucional.*
- *Contar con la debida Certificación de Cumplimiento con el Modelo de Datos Institucional que otorga la Dirección de Tecnologías de Información y Comunicaciones, con el propósito de integrar el modelo de datos la arquitectura de información de la Institución (…)".*

En relación con lo anterior, mediante entrevistas realizadas al Ing. Danilo Hernández Monge, jefe, Área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones, respecto a la disponibilidad en la Dirección de Tecnologías de Información y Comunicaciones de un registro o catálogo donde se consigne la totalidad de aplicaciones y/o sistemas de información desarrollados con software libre o lenguaje de código abierto en la Caja Costarricense de Seguro Social, este indicó:

"Nosotros disponemos desde hace algún tiempo de un catálogo, que se ha denominado catálogo institucional de aplicaciones informáticas (CIAI), en ese catálogo tenemos el registro de las aplicaciones y como parte de la información que recopilamos de cada una de las aplicaciones que capturamos o

documentamos hay alguna data relacionada con lenguaje desarrollo, motor de base de datos, sistema operativo y la parte de servidores aplicativos (…) no es un catálogo exclusivo de desarrollo basados en componentes de software libre, si no, es un catálogo donde están todos los desarrollos y como parte de los ítems de información se consignan aquellas herramientas o componentes de software libre que son parte de la arquitectura de cada aplicativo".

Asimismo, al consultarle si los Centros de Gestión informática (Gerenciales, Regionales y Locales) reportan o solicitan autorización a la Dirección de Tecnologías de Información y Comunicaciones para realizar el desarrollo de aplicaciones y/o sistemas de información con software libre y/o lenguaje de código abierto, el ingeniero Hernández Monge, indicó:

"La respuesta es que, salvo una que otra excepción, eso no está sucediendo, no estamos recibiendo la mayoría de las solicitudes de aval o criterio que deberían de estarse remitiendo a la DTIC y al Área de Ingeniería de Sistemas (como instancia especializada en temas de desarrollo de software), esto no ha estado sucediendo, quizás es una de las áreas de mejora importante. Ya en el pasado, con base a distintos informes y recomendaciones de Auditoría, se hicieron recordatorios a los CGI, no solo de reportar las aplicaciones sino de recordar todo el tema de la coordinación que debería realizarse con la DTIC para efectuar desarrollos de sistemas (…)

Seguimos todavía, hoy en día, con un importante desconocimiento sobre los desarrollos que se hacen fuera de la DTIC y que, de alguna manera, eso se ve reflejado en el contenido de lo que hoy tenemos registrado en el catálogo de aplicaciones CIAI.

La respuesta categórica es que sigue siendo un tema de incumplimiento por parte de los que estén haciendo desarrollos, nosotros no tenemos conocimiento, no tenemos en el mapa qué desarrollos están haciendo instancias fuera de la DTIC dado que no se están solicitando a la DTIC los avales y autorizaciones respectivos".

Además, respecto a un posible incumplimiento normativo por parte de las unidades que están desarrollando sistemas o aplicaciones con herramientas que no cumplen con esos estándares establecidos por la dirección de Tecnologías de Información y Comunicaciones y sin haber solicitado la autorización o criterio correspondiente, el Ing. Danilo Hernández Monge, señaló:

"A pesar de todos los esfuerzos que la DTIC ha realizado, actualmente, nosotros no tenemos la totalidad de aplicaciones o sistemas registrados en el catálogo que nos hagan conocer la magnitud real de la utilización de herramientas de software libre o lenguaje de código abierto en el desarrollo de aplicaciones, no obstante, se mantiene criterio de la DTIC en cuanto a promover que todas las unidades que realicen desarrollos, deban primero coordinar con la DTIC, más aún, se presume que hay esfuerzos que nos han sido ni tan siquiera informados, por lo tanto, es altamente probable que hay incumplimientos en ese sentido, así como, en lo referente a la utilización de los estándares definidos por la dirección de tecnologías para los entornos de desarrollo".

En relación con lo anterior, según lo externado por el Ing. Danilo Hernández Monge, la mayoría de los desarrollos con software libre o lenguaje de código abierto, se realizan sin haberse realizado los procedimientos de notificación o actualización de características, así como, de la solicitud formal de aval a la Dirección de Tecnologías de Información y Comunicaciones, establecidos normativamente; lo cual, imposibilita de manera significativa su identificación.

Al respecto, la Ing. Laura Paz Morales, jefe, Subárea Sistema Automatizado en Recursos Humanos, Dirección de Administración y Gestión de Personal, al consultarle sobre qué parámetros se utilizaron para tomar la decisión de utilizar herramientas de lenguaje de código abierto, como PHP, para el desarrollo de estas aplicaciones, indicó:

"Esa decisión no fue tomada por mí, eso fue en el 2008 cuando Don Luis Rivera estaba como jefe de área y el director era Don Gustavo Picado, donde había necesidades de sistemas en materia de recursos humanos y la de DTIC no tenía la capacidad que se necesitaba para el desarrollo de esos sistemas, ellos mantenían lo que era el SPL que era el sistema de pago, pero no existía ningún otro sistema. Con los avances del internet y con más de 130 oficinas en el país, que necesitaban agilizar sus procesos, se inició con desarrollos, unos de los primeros fueron: Evaluación del Desempeño y uno de curriculum -ya no existe-.

Básicamente el parámetro utilizado era que, había una unidad en la DAGP con puestos de analistas en sistemas -que tenían conocimiento en el desarrollo de PHP- y existía una necesidad de sistemas que la DTIC no podía satisfacer, entonces se tomó la decisión de hacer uso de los recursos que tenía la DAGP -en ese momento- para poder responder a las necesidades de tramitología que tenían las oficinas. Además, no se necesitaba comprar licencias ni hacer incurrir a la institución en ningún gasto, porque es PHP contra el motor de base de datos Oracle -que de este ya existían licencias y se podía utilizar sin problema-, entonces no se necesitaba hacer ningún proceso de compra y se tenía el recurso humano necesario".

Asimismo, respecto a si se efectuó alguna notificación o coordinación con la DTIC para tomar la decisión de utilizar estas herramientas de código abierto, la ingeniera respondió:

"En el 2014 fue que se llevó a cabo el proceso para que PHP fuera autorizado como un lenguaje que se podía utilizar a nivel institucional y antes de eso las reuniones que sostuvo en Don Luis pero no sé si se hicieron minutas, dónde él sí informaba que iban a iniciar con el desarrollo de sistemas en PHP, dada la necesidad que se tenía y la falta de capacidad de DTIC para responder a esas necesidades, en esas reuniones se solicitaba que ellos nos dieran alojamiento en los servidores, entonces la instalación de PHP en los servidores, nosotros no la hicimos, la hizo soporte técnico".

"Algunos de esos proyectos fueron desarrollados desde el 2008, sí se comunicaron, el que era antes el jefe de área de información, Don Luis Rivera, hizo reuniones con la DTIC, con tal de que ellos nos dieran alojamiento en los servidores institucionales, los sistemas actualmente están alojados en servidores institucionales y el área de soporte institucional es el que nos da el mantenimiento de dichos servidores, entonces en esa medida la DTIC sí tenía conocimiento y posteriormente los últimos sistemas que se han desarrollado han sido bajo el marco del proyecto SIPE, donde pasan por un proceso de aprobación de las puestas en producción y es la DTIC la que aprueba eso; entonces, ellos sí están enterados del lenguaje y de los sistemas desarrollados".

"(…) También muchos de los sistemas están registrados como activos, eso lo maneja cada usuario líder, inclusive en la página de inicio tienen la placa de activo Institucional, nosotros mandamos a revisar todos los desarrollos al MDI (Modelo de Datos Institucionales) del Área Ingeniería de Sistemas, Dirección Tecnologías de Información y Comunicaciones.

Además, todo lo que se ha desarrollado en PHP dentro del marco de desarrollo del SIPE es de conocimiento de la DTIC, inclusive Don Danilo forma parte del comité de gestión de SIPE, él tal vez no tiene mapeados todos los desarrollos desde el 2008, pero él sabe que nosotros desarrollamos en PHP".

De conformidad con lo anterior, se puede observar que, la Ing. Laura Paz Morales menciona que para estos desarrollos se efectuaron, en su momento, coordinaciones y comunicaciones previas con la Dirección de Tecnologías de Información y Comunicaciones, lo cual, difiere -en algunos aspectos- con lo indicado por el Ing. Danilo Hernández Monge; además, se señala que la utilización de estas herramientas de software libre y/o lenguaje de código abierto se originó como respuesta a las necesidades existentes de aplicativos en materia de recursos humanos (que la DTIC no podía satisfacer), su utilización gratuita (al no tener que incurrir en gastos de licenciamiento por la institución) y a la disponibilidad de personal con conocimientos en desarrollo con PHP en la Subárea Sistema Automatizado en Recursos Humanos.

Asimismo, respecto a si se efectuó la solicitud de autorización y notificación del entorno de programación a la Dirección de Tecnologías de Información y Comunicaciones, el Ing. George Aguilar Prieto, encargado de la unidad de desarrollo de software del Centro de Gestión Informática del Hospital San Vicente de Paúl, indicó:

> *"No, considerando que a nivel del Hospital la filosofía de trabajo es distinta a la que sigue tradicionalmente, buscando agregar valor al negocio desde otros stack de tecnologías, además las aplicaciones desarrolladas se planificaron con un alcance local, no obstante, las aplicaciones se exportaron a nivel nacional, hito que pone sobre la mesa otras prácticas y tecnologías".*

La situación descrita, referente a la carencia de información en el Catálogo Institucional de Aplicaciones Informáticas sobre los desarrollos realizados -fuera de la DTIC- con software libre y/o lenguaje de código abierto, permite evidenciar la necesidad de fortalecer la gestión de control y seguimiento por parte del Área de Ingeniería de Sistemas en su rectoría del tema por parte de la DTIC a nivel institucional, así como, al incumplimientos de las regulaciones normativas existentes respecto a la obligatoriedad –de los CGI Gerenciales, regionales y locales- de notificar y solicitar autorización a la Dirección de Tecnologías de Información y Comunicaciones, para realizar estas aplicaciones o sistemas de información; esta situación genera un debilitamiento del sistema de control interno e imposibilita a las autoridades institucionales y órganos de fiscalización poder disponer de información confiable para un eventual análisis y toma de decisiones, en dicha materia.

2. RESPECTO A LAS APLICACIONES DESARROLLADAS MEDIANTE LA UTILIZACIÓN DE SOFTWARE LIBRE A NIVEL INSTITUCIONAL

De conformidad con los datos suministrados a esta auditoría, se identificó el desarrollo de aplicaciones y/o sistemas de información realizados mediante la utilización de software libre y/o lenguaje de código abierto en la institución, no obstante, la Dirección de Tecnologías de Información y Comunicaciones y los Centros de Gestión Informática Gerenciales carecen de información donde se establezca -de manera veraz y confiable- la cantidad total de estos desarrollos, los entornos de programación utilizados, su versión y funcionamiento actual en la red institucional.

Dentro de los sistemas y/o aplicativos desarrollados con software libre y/o lenguaje de código abierto, señalados por los Centros de Gestión Informática (gerenciales, regionales, locales y de hospitales nacionales y especializados), la Subárea Sistema Automatizado en Recursos Humanos y la Dirección de Tecnologías de Información y Comunicaciones, se indican los siguientes:

- Sistema de Información para la Sostenibilidad Ambiental (SISA).
- "Herramienta para repositorio de información para la DRIPSSPC".
- "C# pequeño aplicativo que procesa varios Excel de enfermería para consolidar una estadística, no usa BD" (Hospital William Allen Taylor).
- Aplicativos ARCA:
  - **Arca SINU:** Gestiona los procesos del servicio de Nutrición.
  - **Arca Patología:** Gestiona los procesos del servicio de Patología. Aplica solo los módulos: Fallecidos, Biopsias, Medula Ósea.
  - **Arca Hospitalización**: Gestiona los procesos del servicio de Hospitalización y Quirúrgico. Aplica solo los módulos: Solicitud de sinónimos, Gestión préstamos salas, Control de tiempos, Administrador cirugías, Suspender Cirugías Nota Operatoria, Monitor de cirugías, Gestor Camas Covid, Mantenimiento camas y Mantenimiento salones.

  Las herramientas y lenguajes son:
  - **MongoDB** como motor de base de datos. Versión: 5.x.
  - **ExpressJS** como framework estándar de aplicación web de back-end para NodeJS. Versión: 4.17.3.
  - **Angular** como framework de JavaScript y TypeScript para construir aplicaciones web complejas y escalables. Versión: 13.x.

  - **NodeJS** como entorno de ejecución JavaScript del lado del servidor o back-end que permite crear y ejecutar aplicaciones web de red escalables. Versión: 14.x.
  - **Pentaho** como generador de reportes. Versión: 9.1.
- En la Dirección de Administración y Gestión de Personal:
  - Portal de recursos humanos.
  - SIPE Concursos.
  - Sistema de control y evaluación de la nómina.
  - Sistema de requerimientos estadísticos.
  - La red de recursos humanos.
  - Sistema de remuneración salarial.
  - Módulo de ingreso de talento humano.
  - Sistema manejo de proyectos.
  - Sistema de evaluación del desempeño.
  - Base de datos de políticas y normas.

Las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE, en el artículo 5.6 “Calidad de la información”, estipula:

> *“El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo.*
> *Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad.*
> *5.6.1 Confiabilidad La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente.*
> *5.6.2 Oportunidad Las actividades de recopilar, procesar y generar información, deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales.*
> *5.6.3 Utilidad La información debe poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario (…)”.*

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en su apartado “*X. Desarrollo, implementación y mantenimiento de sistema de información”*, señala:

> *“(…) La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones (…)”.*

En ese mismo marco normativo, en el apartado “*XI. Seguridad y ciberseguridad”*, cita:

> *“(…) 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 (…)*
>
> *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 (…)”.*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, en el numeral 5.7 Responsabilidades de los niveles organizacionales y funciones sustantivas, para el Área de Ingeniería de Sistemas, entre otros aspectos señala:

> *" 5.7.3. Nivel Área de Ingeniería de Sistemas.*
>
> *Es responsables del desarrollo de los sistemas de información institucionales, del mantenimiento preventivo y correctivo de los mismos, de las modificaciones requeridas por el software, de suministrar los servicios a los usuarios, del soporte técnico a las actividades de Telesalud y la automatización de los sistemas en el área Financiera-Administrativa y Salud (…)*
>
> *Esta Área de Trabajo debe asesorar, colaborar y apoyar técnicamente para que los Centros de Gestión Informática, a los cuales el Consejo de Presidencia y de Gerentes o la Dirección de Tecnologías de Información y Comunicaciones le asigne, como estrategia operacional, el desarrollo de sistemas de ámbito global del sistema de salud, de pensiones, financiero, administrativo, bienes y servicios, entre otros, cumplan en forma efectiva con la solicitud específica. (…)*
>
> *Mantener un registro actualizado de las aplicaciones disponibles y sus características, de conformidad con las políticas vigentes, con el fin de contar con información oportuna y veraz (…)*
>
> *Suministrar en forma oportuna la información solicitada por las autoridades superiores, a partir de los requerimientos específicos, para que se cumplan efectivamente las acciones de fiscalización, seguimiento, control y evaluación de la gestión (…)".*

En el Modelo de Organización de los Centros de Gestión Informática en el numeral 5.6.1 Modelo Tipo A: Centros de Gestión Informática Gerenciales, apartado de Responsabilidades del nivel organizacional y funciones sustantivas, se indica:

> *"(…) Conceptualización del Área*
> *Área: Centro de Gestión Informática Gerencial (…)*
> *Gestión Técnica:*
>
> *(…) Desarrolla e implementa, previa autorización de Dirección de Tecnologías de Información y Comunicaciones, sistemas de información y aplicaciones, con el fin de automatizar los procesos operativos específicos y define una cartera de proyectos a nivel gerencial en coordinación con los centros de gestión informática de su ámbito de acción (…)*
>
> *Establecer mecanismos de control que permitan el auditoraje de los sistemas de información, a partir de las técnicas aceptadas y los manuales respectivos, para facilitar la evaluación de la gestión.*
>
> *Documentar los cambios que se produzcan en los sistemas y aplicaciones, en su ámbito de competencia, de acuerdo con las políticas y la normativa vigente, con el objeto de mantener un registro interno e institucional actualizado de aplicaciones.*
>
> *Realizar pruebas de los sistemas de información y las aplicaciones, con base en las metodologías de trabajo establecidas y la normativa vigente, con el fin de lograr el desarrollo efectivo de la gestión.*
>
> *Comunicar el desarrollo e implementación de los sistemas y las aplicaciones a la Dirección de Tecnologías de Información y Comunicaciones, con el fundamento en la normativa vigente, con el objetivo de que éstos se incorporen oportunamente al Registro Institucional de Aplicaciones.*

Desarrollar acciones que permitan proteger los recursos de tecnologías de información, con base en las políticas vigentes y el análisis de los riesgos, con el objeto de lograr un ambiente seguro y controlado (…)"

Mediante la aplicación de entrevistas y la herramienta desarrollada en FORMS *"Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre"* a los Centros de Gestión Informática de las gerencias administrativa, financiera, médica, pensiones y de infraestructura y tecnologías, se recabó información sobre las aplicaciones y/o sistemas institucionales desarrollados mediante software libre y/o lenguaje de código abierto en la institución, según se detalla a continuación:

Según los datos suministrados por los Centros de Gestión Informática gerenciales, anteriormente citados, se indica el desarrollo de aplicaciones y/o sistemas de información con herramientas de software libre o lenguaje de código abierto en las gerencias de pensiones, administrativa y de infraestructura y tecnología, lo anterior, mediante la utilización de herramientas como PHP[2], Apache[3], JavaScript[4] y React[5]. Asimismo, se indica la realización de estos desarrollos en la Subárea de Información de Recursos Humanos (Concursos, Evaluación de Desempeño y la sitio de RRHH) y en la Dirección de Administración de Proyectos Especiales (sistema SISA); en la Gerencia de Pensiones se indicó la utilización de bibliotecas de código abierto, pero no se detallaron las aplicaciones desarrolladas (**Ver tabla 1**).

Tabla 1
Principales resultados del "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" aplicado a los CGI Gerenciales
febrero 2025

Centro de Gestión Informática	Respuesta
Consulta: ¿En el Centro de Gestión Informática o alguna unidad adscrita a la gerencia se han desarrollado aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto?	
CGI Gerencia Administrativa:	sí (en una unidad adscrita a la gerencia)
CGI Gerencia de Pensiones	sí (en el CGI)
CGI Gerencia Financiera	no
CGI Gerencia de Infraestructura y Tecnología	sí (en una unidad adscrita a la gerencia)
CGI Gerencia Médica	no
Consulta: ¿Qué aplicaciones y/o sistemas se han desarrollado mediante estas herramientas (indique el nombre del software libre o lenguaje de código abierto que se utilizó y la unidad que lo desarrolló (CGI o nombre de la unidad adscrita))?	
CGI Gerencia Administrativa:	PHP y apache, Subárea de Información de Recursos Humanos, Concursos, Evaluación de Desempeño y la sitio de rrhh.(…)
CGI Gerencia de Pensiones	Hemos utilizado algunas herramientas de Java Script, React y otras para integrarlas dentro de las aplicaciones, estas bibliotecas de código abierto están en continua revisión por parte de comunidades a nivel mundial y son altamente utilizadas en el desarrollo de aplicaciones.
CGI Gerencia Financiera	No aplica
CGI Gerencia de Infraestructura y Tecnología	Se hizo una contratación por parte de la Dirección de Administración de Proyectos Especiales para la realización del sistema SISA en el lenguaje de programación en Java. Las coordinaciones se hicieron con la DTIC para el desarrollo del sistema, usando una metodología de desarrollo Scrum. EL CGI-GIT brinda acompañamiento técnico a la unidad de la GIT.
CGI Gerencia Médica	No aplica

Fuente: Elaboración propia de auditoría, con datos del "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" aplicado a los CGI Gerenciales mediante la herramienta Forms.

2 PHP (Hypertext Preprocessor): Es un lenguaje de código abierto destinado para el desarrollo web
3 Apache: Es un servidor web de código abierto que maneja solicitudes HTTP.
4JavaScript: En sí no es de código abierto, ya que es un lenguaje de programación estandarizado mantenido por una organización llamada ECMA International.
5 React (también llamada React. js o ReactJS): Es una biblioteca Javascript de código abierto diseñada para crear interfaces de usuario con el objetivo de facilitar el desarrollo de aplicaciones en una sola página.

Por otra parte, se remitió a los Centros de Gestión Informática (Regionales (médica y financiera), locales y de hospitales nacionales y especializados) el citado *"Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre"* obteniéndose de ellos, la siguiente información:

De los 69 Centros de Gestión Informática que respondieron el citado cuestionario, únicamente 2 de ellos (la Dirección de Red Integrada Prestación de Servicios de Salud Región Pacifico Central y el Hospital William Allen Taylor) indicaron haber realizado desarrollos con software libre y/o lenguaje de código libre, indicando las siguientes aplicaciones:

- "Herramienta para repositorio de información para la DRIPSSPC".
- "C# pequeño aplicativo que procesa varios Excel de enfermería para consolidar una estadística, no usa BD".

De conformidad con lo anterior, el Ing. Danilo Hernández Monge, jefe, Área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones, respecto al conocimiento de aplicaciones y/o sistemas que se hayan desarrollado con software libre o lenguaje de código abierto en la institución, indicó:

> *"Varios de los desarrollos que llevamos a cabo, actualmente, los tenemos con lenguaje Java en su versión gratuita. Java es una tecnología que hace algún tiempo nació como Código Libre, esta fue adquirida por Oracle, pero en esa adquisición Oracle, en realidad no eliminó la versión libre de Java, lo que sí hizo fue desarrollar una versión licenciada a partir del CORE gratuito que existía.*
>
> *(…) Entonces sí tenemos desarrollo y conocemos otros fuera de la Dirección de Tecnologías que han utilizado también componentes de software libre como PHP y toda la arquitectura llamada MEAN, que es una mezcla de herramientas de código abierto, que se han hecho particularmente en el hospital de Heredia (aplicativos ARCA) y entiendo que el BITZU tiene algunos elementos (es una solución complementaria dentro de la implementación del RPP del proyecto del plan de innovación). Estos son los que ahorita tengo presentes, que se desarrollaron fuera de la DTIC.*
>
> *También el sitio o página web de la Caja Costarricense de Seguro Social teníamos conocimiento que había sido desarrollada con lenguaje de código abierto (PHP), la cual está a cargo la Dirección de Comunicación Organizacional".*

Además, referente a la existencia de algunos sistemas o aplicaciones que se desarrollaron en la Dirección de Administración y Gestión de Personal con el lenguaje de código abierto PHP, mencionados en la entrevista a los CGI Gerenciales, señaló:

> *"Sí, sí tenemos conocimiento de esos desarrollos y particularmente en toda la planificación que se ha trabajado en la Dirección de Tecnologías en conjunto con las DAGP, enmarcadas en el proyecto SIPE, dentro del cual, en todo el mapeo, la estrategia y lo que se ha definido en el proyecto SIPE, efectivamente conocemos y tenemos noción de los desarrollos en PHP. Particularmente, estos desarrollos con componentes de recursos humanos.*
>
> *Hemos conocido y sabemos que hay componentes, por ejemplo, Evaluación de Desempeño que, de hecho, dentro del alcance de desarrollo que hizo el equipo de la DAGP en PHP había un módulo SIPE GESTIÓN que ya la Dirección de Tecnologías hicimos una migración a Java, dentro del contexto del marco del Proyecto SIPE.*
>
> *Ahorita pierdo un poquito la noción de dónde está adscrita la DAGP, pero ya en el pasado, con la intención de mantener actualizado el catálogo de aplicaciones, se hicieron peticiones y recordatorios a los CGI para que reportaran las aplicaciones desarrolladas a lo interno de cada gerencia, pero, durante el tiempo que la DAGP estuvo adscrita a la gerencia administrativa, no recuerdo haber recibido un*

reporte de Guiselle, en el sentido de reconocimiento o de la identificación de los desarrollos que venía haciendo el equipo de la DAGP, porque en la buena teoría, mientras la DAGP estuvo en la gerencia Administrativa, está debió haber sido parte para la información suministrada por el CGI de la Gerencia Administrativa a la DTIC, por lo tanto, debió haber sido conocedora".

Según lo indicado por el ingeniero Hernández Monge, la Dirección de Tecnologías de Información y Comunicaciones tiene conocimiento de algunas aplicaciones con componentes de software libre como PHP y toda la arquitectura llamada MEAN en el hospital de Heredia (aplicativos ARCA) y el BITZU (una solución complementaria dentro de la implementación del RPP del proyecto del plan de innovación); además, indicó conocer algunos desarrollos realizados por la Dirección de Administración y Gestión de Personal con el lenguaje de código abierto PHP.

En relación con lo anterior, la Ing. Laura Paz Morales, jefe, Subárea Sistema Automatizado en Recursos Humanos, Dirección de Administración y Gestión de Personal, respecto al desarrollo de aplicaciones o sistemas de información mediante herramientas de software libre o lenguaje de código abierto, señaló:

"Sí, correcto. Están en PHP actualmente y sí son varios sistemas: El portal de recursos humanos, SIPE concursos, el sistema de control y evaluación de la nómina, el sistema requerimientos estadísticos, la red de recursos humanos, el sistema de remuneración salarial, el módulo de ingreso de talento humano, el sistema manejo de proyectos, el sistema de evaluación del desempeño y la base de datos de políticas y normas.

Nosotros tenemos desarrolladores propios y el Sistema de Concursos fue con una contratación externa en PHP (Licitación Abreviada N° 2019LA-000011-1150, por concepto de "Servicios Profesionales de Apoyo en Desarrollos en Lenguaje PHP") esta fue llevada por la DTIC".

Según la información suministrada por la Ing. Paz Morales, se indica en la Dirección de Administración y Gestión de Personal, el desarrollo de las siguientes aplicaciones con software libre y/o lenguaje de código abierto:

- Portal de recursos humanos.
- SIPE Concursos.
- Sistema de control y evaluación de la nómina.
- Sistema de requerimientos estadísticos.
- La red de recursos humanos.
- Sistema de remuneración salarial.
- Módulo de ingreso de talento humano.
- Sistema manejo de proyectos.
- Sistema de evaluación del desempeño.
- Base de datos de políticas y normas.

De conformidad con lo anterior, respecto al desarrollo de aplicaciones o sistemas de información mediante herramientas de software libre o lenguaje de código abierto, el Ing. George Aguilar Prieto, encargado de la unidad de desarrollo de software del Centro de Gestión Informática del Hospital San Vicente de Paúl, señaló:

"Las aplicaciones desarrolladas son:

- ***Arca SINU**: Gestiona los procesos del servicio de Nutrición.*
- ***Arca Patología**: Gestiona los procesos del servicio de Patología. Aplica solo los módulos: Fallecidos, Biopsias, Medula Ósea.*
- ***Arca Hospitalización**: Gestiona los procesos del servicio de Hospitalización y Quirúrgico. Aplica solo los módulos: Solicitud de sinónimos, Gestión préstamos salas, Control de tiempos, Administrador cirugías, Suspender Cirugías Nota Operatoria, Monitor de cirugías, Gestor Camas Covid, Mantenimiento camas y Mantenimiento salones.*

Las herramientas y lenguajes son:

- ***MongoDB*** *como motor de base de datos. Versión: 5.x.*
- ***ExpressJS*** *como framework estándar de aplicación web de back-end para NodeJS. Versión: 4.17.3.*
- ***Angular*** *como framework de JavaScript y TypeScript para construir aplicaciones web complejas y escalables. Versión: 13.x.*
- ***NodeJS*** *como entorno de ejecución JavaScript del lado del servidor o back-end que permite crear y ejecutar aplicaciones web de red escalables. Versión: 14.x.*
- ***Pentaho*** *como generador de reportes. Versión: 9.1.*

Es importante tener presente que, si bien los lenguajes indicados (…) se consideran lenguajes de programación abiertos, los lenguajes actuales oficiales indicados por la DTIC como C# en .NET o Java entran en la misma categoría, esto para que no se quiera de alguna manera satanizar el tema (…)".

Los aspectos anteriormente señalados responden a oportunidades de mejora en el monitoreo y control a desarrollos de sistemas en las diversas unidades institucionales, mismos que se encuentran en funcionamiento dentro de la red institucional, sin registro oficial en mecanismos establecidos para tales efectos, como es el caso del CIAI y SCBM, que permiten a nivel estratégico y táctico, no solo identificarlos, sino además mantener un monitoreo de los aplicativos existentes para la toma de decisiones.

Preocupa a esta auditoría, que institucionalmente se desconozca -de manera real- la totalidad de aplicaciones desarrolladas con software libre y/o lenguaje de código abierto y que, a su vez, estos se encuentren funcionando actualmente en la CCSS, sin los adecuados mecanismos de monitoreo y control; máxime al considerar el aumento de riesgos asociados a vulnerabilidades que podrían afectar la continuidad de servicios brindados al usuario debido a la materialización de irrupciones en la plataforma tecnológica y la información que en ella se resguardan, situación que expone a la Institución a posibles repercusiones en el ámbito administrativo o legal.

3. REFERENTE A LINEAMIENTOS O DIRECTRICES EN MATERIA DE DESARROLLO DE SISTEMAS CON SOFTWARE LIBRE Y/O LENGUAJE DE CÓDIGO ABIERTO

Se determinó que, en la institución no se ha emitido lineamientos o directrices específicos en torno al desarrollo de sistemas o aplicaciones con software libre y/o lenguaje de código abierto.

De los datos suministrados a esta auditoría, se determinó que, la mayoría de los Centros de Gestión de Informática consultados señalaron no tener conocimiento sobre un marco normativo (institucional, nacional o extranjero) establecido en torno al desarrollo de aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto, así mismo, indicaron no haber recibido comunicado oficial alguno o rectoría por parte de la Dirección de Tecnologías de Información y Comunicaciones en dicha materia.

Esta auditoría efectuó entrevistas y la aplicación de la herramienta en FORMS *"Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre"* a los Centros de Gestión Informática (CGI) de las gerencias administrativa, financiera, médica, pensiones y de infraestructura y tecnologías respectivamente, con el fin de recabar información sobre el conocimiento de un marco normativo o regulaciones (institucionales, nacionales o extranjeras) con relación al desarrollo de aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto, generándose los siguientes resultados:

1. De los 5 CGI un 80% (4) de ellos no tienen conocimiento sobre marco normativo o regulaciones (institucionales, nacionales o extranjeras) con relación al desarrollo de aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto. Solamente el Centro de Gestión Informática de la Gerencia de Infraestructura y Tecnologías respondió de manera afirmativa, indicando la metodología de SCRUM como marco normativo.

2. Asimismo, el 100% (5) de ellos indicaron que no han recibido algún comunicado oficial o rectoría por parte de la Dirección de Tecnologías de Información y Comunicaciones, respecto al desarrollo de aplicaciones y/o sistemas desarrollados con software libre o lenguaje de código abierto.

Por otra parte, se remitió a los Centros de Gestión Informática (Regionales (médica y financiera), locales y de hospitales nacionales y especializados) el citado *"Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre"*, obteniéndose de la siguiente información:

1. De los 69 CGI un 87% (60) de ellos no tienen conocimiento sobre marco normativo o regulaciones (institucionales, nacionales o extranjeras) con relación al desarrollo de aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto y 13% (9) de ellos respondieron de forma afirmativa.
2. Asimismo, en la tabla 2 se muestra las normas indicadas por los 9 CGI, cuya respuesta fue afirmativa en la consulta anterior.

Tabla 2
Principales resultados del "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" aplicado a los CGI regionales (médica y financiera), locales y de hospitales nacionales y especializados
febrero 2025

Centro de Gestión Informática	Respuesta
Consulta: Indique el nombre del marco normativo o regulaciones (institucionales, nacionales o extranjeras) que conoce.	
CGI de la Dirección de Red Integrada Prestación de Servicios de Salud Región Pacifico Central	Para la Bases de Datos se utilizó "Metodología para el modelo de bases de datos institucional MDI" y también "TIC-MDI-0006 Estándares de Nomenclatura, Representación Gráfica y Documentación para el Diseño de Bases de Datos"
CGI de la Dirección Regional Central de Sucursales	Sin datos
CGI del Área de Salud Coronado	Metodología de desarrollo de Software, Metodología de modelación de datos institucional, Marco metodológico de desarrollo de sistemas de información
CGI de la Dirección Regional de Sucursales Huetar Atlántica	Manual de los Centros de Gestión Informática. Lista Oficial Software Libre
CGI del Área de Salud del Guarco	ISO/IEC 27001
CGI de la Dirección Red Integrada de Prestación de Servicios de Salud Huetar Atlántica	A nivel institucional: LEY N 17 Ley Constitutiva de la CCSS y a nivel Nacional la Ley N9416.
CGI del Área de Salud Zarcero	Decreto Ejecutivo 37859-Artículo 48-Sistema Costarricense de Información Jurídica. Free Software Foundation Europe.
CGI del Área de Salud Poás	Ministerio de Hacienda fomenta el uso de software libre y estándares abiertos en los sectores públicos.
CGI del Hospital México	Utilización del software libre en las instituciones del estado

Fuente: Elaboración propia de auditoría, con datos del "Cuestionario sobre desarrollo de aplicaciones y/o sistemas con software libre" aplicado a los CGI regionales (médica y financiera), locales y de hospitales nacionales y especializados, mediante la herramienta Forms.

Además, 71% (49) de los 69 CGI consultados, indicaron no haber recibido algún comunicado oficial o rectoría por parte de la Dirección de Tecnologías de Información y Comunicaciones, respecto al desarrollo de aplicaciones y/o sistemas desarrollados con software libre o lenguaje de código abierto, mientras un 29% (20) de ellos indicaron que sí.

La Ley 8292: Ley General de Control Interno, artículo 15. Actividades de control, indican lo siguiente:

> *"Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
> *a)* ***Documentar, mantener actualizados y divulgar internamente****, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.*

> *b)* ***Documentar, mantener actualizados y divulgar internamente*** *tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
> *i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.*
> *ii. La protección y conservación de todos los activos institucionales.*
> *iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.*
> *iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.*
> *v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación"* ***El resaltado no pertenece al original.***

Las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE, en el inciso 1.4 "Responsabilidad del jerarca y los titulares subordinados sobre el SCI" indica:

> *"La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.*
> *En el cumplimiento de esa responsabilidad las autoridades citadas deben dar especial énfasis a áreas consideradas relevantes con base en criterios tales como su materialidad, el riesgo asociado y su impacto en la consecución de los fines institucionales, incluyendo lo relativo a la desconcentración de competencias y la contratación de servicios de apoyo. Como parte de ello, deben contemplar, entre otros asuntos, los siguientes: (…)*
> *c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y* ***actualizados****, y sean divulgados y puestos a disposición para su consulta."* ***El resaltado no pertenece al original.***

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, en el numeral 5.7 Responsabilidades de los niveles organizacionales y funciones sustantivas, para el Área de Ingeniería de Sistemas, entre otros aspectos señala:

> *" 5.7.3. Nivel Área de Ingeniería de Sistemas.*
>
> *(…) Formular, actualizar y evaluar la regulación, la normativa técnica, los protocolos y los estándares relacionados con su ámbito de acción, en respuesta a la normativa aprobada por el Consejo de Presidencia y de Gerentes, la tecnología en uso y los procesos de investigación, a efecto de lograr la uniformidad en los sistemas y la maximización de los recursos institucionales (…)*
>
> *Actualizar la documentación técnica en su ámbito de competencia, con base en los requerimientos de la organización, la normativa aprobada por el Consejo de Presidencia y de Gerentes, las políticas y estrategias vigentes, con el objeto de lograr la operación efectiva del hardware y software institucional (…)"*

De conformidad con lo anterior, el Ing. Danilo Hernández Monge, jefe, Área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones, respecto a la existencia de un marco normativo o regulaciones para el desarrollo de aplicaciones y/o sistemas de información con software libre -a nivel institucional-, indicó:

> *"La gestión de software libre es un proceso conducido desde el Área de Soporte Técnico, de igual manera desde el Área de Seguridad y Calidad se gestiona toda la recopilación de los aspectos normativos en TIC, por lo que, es importante conocer desde esas instancias los detalles, sobre el marco*

normativo vigente. Desde la perspectiva del proceso de desarrollo de software, se tiene enmarcado en un solo proceso, indistintamente de la tecnología o herramienta que se utilice, sean estas licenciadas, de software libre, gratis o combinaciones de ellas.

Sobre el proceso que tiene a cargo el Área de Soporte Técnico, se conoce que, si alguien tiene la intención de utilizar alguno de estos componentes de software libre, debe hacer una solicitud de autorización a la citada área y tenemos un equipo que realiza la valoración, revisión técnica y análisis de vulnerabilidades y riesgos, para finalmente emitir un criterio donde se indica si se acepta o no la utilización de ese software, en este proceso se incluye el tema de lenguajes de desarrollo.

Lo que se vaya a desarrollar, debería de tener un criterio o autorización de la DTIC, ese procedimiento lo tienen que cumplir indistintamente que sea software libre o no.

La respuesta es no y yo no creo que algún día se vaya a tener una normativa o una especificación de desarrollo de software cuando llevan un componente de software libre. Lo que sí se tiene que velar es por el cumplimiento de lo que ya está normado y que incluye de manera general el desarrollo de sistemas, indistintamente de las tecnologías y las modalidades con las que se pretende desarrollar o adquirir una solución de software que atienda una necesidad particular".

En relación con lo anterior, en consulta efectuada al Ing. Daniel Berrocal Zuñiga, jefe del Área de Seguridad y Calidad de la Dirección de Tecnologías de Información y Comunicaciones, respecto a la existencia de un marco normativo o regulaciones para el desarrollo de aplicaciones y/o sistemas de información con software libre -a nivel institucional-, indicó:

"(…) me permito indicarte que actualmente por lo indicado en la sesión, la Dirección de Tecnologías de información y Comunicaciones no ha emitido y comunicado a las unidades institucionales, algún lineamiento o directriz -especifica- en torno al desarrollo de sistemas o aplicaciones con software libre y/o lenguaje de código abierto".

Es criterio de esta auditoría que, la situación anteriormente señalada podría obedecer a los atrasos surgidos en la implementación del Modelo de Gobierno TI y consecuentemente a las oportunidades de mejora en la gestión de direccionamiento, control y regulación tecnológica ejercida por parte de la Dirección de Tecnologías de Información y Comunicaciones, en su rol rector, así como, de los Centros de Gestión Informática Gerenciales en su ámbito de acción; lo cual, ha generado la ausencia de lineamientos para orientar y estandarizar la utilización de software libre y/o lenguaje de código abierto para el desarrollo de aplicaciones y/o sistemas.

Lo anterior, genera incertidumbre y confusión en cuanto a los procedimientos que se deben seguir, a nivel institucional, para poder hacer un uso adecuado de estas herramientas libres de desarrollo, permitiendo, a su vez, una utilización sin regulaciones que podría generar vulnerabilidades en la plataforma tecnológica de la Caja Costarricense de Seguro Social.

4. REFERENTE AL SITIO PARA DESCARGA DE SOFTWARE LIBRE, HABILITADO POR LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

En revisión efectuada por esta auditoría el 20 de febrero de 2025, se constató la existencia de un sitio (https://intranet.ccss.sa.cr/sitios/TIC/SA/SitePages/Descargas.aspx) para la descarga de software libre habilitado en la intranet por la Dirección de Tecnologías de Información y Comunicaciones, el cual podía ser accesado por cualquier funcionario o unidad que requiera hacer uso de esas herramientas, según se muestra en la siguiente imagen:

Imagen 1
Sitio para la descarga de software libre de la
Dirección de Tecnologías de Información y Comunicaciones
20 de febrero de 2025

Fuente: sitio (https://intranet.ccss.sa.cr/sitios/TIC/SA/SitePages/Descargas.aspx) para la descarga de software libre.

En dicho se sitio, al momento de la revisión, se podía tener acceso a las siguientes carpetas con software libre para descargar:

- Gestión de Bases de Datos.
- Gestión de infraestructura.
- Desarrollo de Software.
- Gestión de Usuario Final.
- Ofimática para usuarios.
- Sistemas Operativos Servidores.
- Sistemas Operativos para Usuario Final.
- Software para Servicios Médicos.

Específicamente en la carpeta de *"Desarrollo de Software"*, cualquier funcionario que dispusiera de un usuario institucional tenía la posibilidad de acceso libre para descargar 33 herramientas de software libre, mismas que se detallan a continuación:

Tabla 3
Software libre para descargar en la carpeta
de "Desarrollo de Software"
al 20 de febrero 2025

1.Jaspersoft Studio	11.Pencil Project	21.Spoon	31.Xampp
2. MELD	12.Cobol IDE Open Cobol	22.Java	32.NetBeans
3.Pentaho	13.PHP	23.SqlDeveloper	33.Xcode
4.QGIS	14.CVS	24.Jdeveloper 12	---------
5.R	15.PnpMyAdmin	25.Studio3T	---------
6.Android Studio	16.Git	26.Joomia	---------
7.Nodejs	17.Post-Man	27.SubVersion	---------
8.Apache	18.Inkscape	28.LimeSurvey	---------
9.Notepad++	19.Process Explorer	29.WampServer	---------
10.ATOM	20.Ireport/Jasper Report	30.Moodle	---------

Fuente: Elaboración propia de auditoría, con datos extraídos del sitio de descarga de Software Libre de la DTIC.

Además, no se observa un control de la cantidad de descargas realizadas, los funcionarios que las efectuaron y la justificación para su uso, posterior a la aprobación e inclusión en este sitio.

Las Normas de Control Interno para el Sector Público, en el inciso 1.4.5 sobre el control de Accesos, refieren:

> *"La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*
> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación (…)*
> *e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio.*
> *Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones".*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el apartado XI. Seguridad y ciberseguridad, lo siguiente:

> *"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 (…)".*

Ese mismo marco normativo, en el apartado *"Gestión del Riesgos Tecnológicos"*, refiere:

> *"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.*
>
> *La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución".*

De conformidad con lo anterior, en entrevistas realizadas al Ing. Danilo Hernández Monge, jefe, Área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones, respecto a los criterios utilizados para tomar la decisión de recomendar o autorizar la utilización de estas herramientas de lenguaje de código abierto para el desarrollo de aplicaciones a nivel institucional, indicó:

> *"Para una mejor respuesta a esta consulta, te voy a direccionar al área de soporte técnico a cargo de Vanessa Berrocal (sic), ya que ellos tienen un equipo (lo coordina Luis Angel Gómez Alfaro) que se encargan de analizar, avalar o denegar las solicitudes de utilización de software libre que hacen las unidades a nivel institucional, ellos tienen un procedimiento para revisar estos casos.*

De hecho, esta área se encuentra actualmente revisando el proceso que se ha realizado hasta la fecha, porque hemos detectado que se ha malinterpretado el tema del software libre, nosotros sí hemos realizado algunas observaciones para hacer un manejo distinto del tema, ya que, lo correcto sería que, si alguien presenta una solicitud para el uso de una herramienta de software libre con un objetivo específico, la respuesta y autorización debería de darse solo para esa unidad solicitante y sobre la versión especifica revisada, no como se está haciendo, donde se incorpora en un sitio donde cualquier persona o unidad institucional puede descargar y hacer uso de esa herramienta indiscriminadamente, porque ahí se está perdiendo el control y se estaba propiciando un mensaje que no era el correcto.

En este tema alguien tiene que hacerse responsable de la utilización, actualización (de las nuevas versiones que se generen de esa herramienta) y la coordinación respectiva para la revisión de nuevas versiones, por eso, con este replanteamiento lo que se busca es crear u compromiso por parte del solicitante y hacerle ver la responsabilidad que conlleva la utilización de esas herramientas".

En relación con lo anterior, en entrevista efectuada al Ing. Marlon Delgado Álvarez, jefe a.i y el Ing. Luis Angel Gómez Alfaro, coordinador de la Comisión de Validación de Software Libre, ambos funcionarios del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, respecto a parámetros o criterios utilizados para tomar la decisión de recomendar o autorizar la utilización de estas herramientas de lenguaje de código abierto para el desarrollo de aplicaciones a nivel institucional y si se efectuaron estudios de vulnerabilidades de estas herramientas, indicaron:

*"**Ing. Luis Angel Gómez Alfaro:** Cuando una persona requiere hacer una solicitud de autorización, porque necesita utilizar un software libre, hay un procedimiento que deben seguir, a través de la Mesa de Servicios, ponen en un caso en mesa y ahí se les informa que tienen que llenar un formulario con varias preguntas (información básica del software, versión, en qué sistema operativo se va a correr, quienes lo van a usar, porqué necesitan esa herramienta, etc.) y cuando ya se tienen esos documentos llenos y firmados, mesa los traslada a la Comisión de Validación de Software Libre, para hacer un análisis (bajo ciertos criterios que se han determinado) y con base a ese análisis se hace un informe donde se indican los principales elementos a considerar.*

Parte de ese análisis involucra que la persona que está solicitando la autorización debe de pasarnos el software y hacernos una presentación del mismo (cuando no es conocido), posteriormente, eso se traslada a la Subárea de Seguridad para que ellos hagan un análisis de vulnerabilidades, el cual, es subcontratado a una empresa que da ese servicio, ahorita esa empresa es Deloitte, ellos procesan la solicitud y entregan a la Comisión un informe, este informe es muy importante porque lo realiza una empresa experta en este tema; si en el análisis de vulnerabilidades se detecta algún elemento sospecho o malicioso la solicitud se rechaza, o por el contrario, si no se hay nada extraño (todo está bien) se aprueba, con todos los fundamentos correspondientes.

Una vez hecho el informe, la Comisión lo traslada al Comité de Control de Cambios, ese es el ente de aprobación, por medio de un RFC se presenta como una solicitud de cambio, donde se presentan los resultados con toda la documentación y ellos son los que deciden si se aprueba o no el software y en qué condiciones.

***Ing. Marlon Delgado Álvarez:** Nosotros utilizamos una plantilla donde se evalúan elementos como: infraestructura, seguridad, compatibilidad del software con la plataforma institucional, lenguaje operativo, entre otros elementos; todo esto y el estudio de vulnerabilidades es lo que se utiliza para el análisis y elaboración del informe final, donde se establece si puede o no utilizarse en el ambiente institucional".*

Además, al consultarles si, una vez que se da la aprobación del software libre solicitado por una unidad específica, estos se incluyen en el sitio de descargas y pueden ser utilizados por cualquier otra unidad institucional, los funcionarios señalaron:

> ***"Ing. Luis Angel Gómez Alfaro:*** *Eso antes era así, pero precisamente esta semana se realizaron unos cambios. Ahora, cuando el Comité de Control de Cambios aprueba un software ellos indican las condiciones para su uso, ahí se va a indicar si la autorización es para una persona, una subárea o un equipo de trabajo en específico. Como primera medida nos solicitaron deshabilitar el sitio de descarga para que no estuviera disponible para cualquier persona.*
>
> ***Ing. Marlon Delgado Álvarez:*** *En seno del Comité de Control de Cambios se dio de baja las descargas porque como parte de las observaciones que nos hicieron, es que las personas deben de suscribir un acuerdo de uso para limitar el uso del software, porque antes se daba de manera generalizada y ahora solo se va a autorizar a la persona que hace la solicitud, el cual, ellos tienen que cumplir ciertos requisitos para su uso".*

Si bien, el 28 de febrero de 2025, funcionarios del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones indicaron que, ya se estaba realizando un replanteamiento del proceso de autorización y uso de software libre, y además se había bloqueado la posibilidad de descarga de estas herramientas en el sitio de intranet; preocupa a esta auditoría, aquellas descargas realizadas, anteriormente, para el desarrollo de aplicaciones -muchas de ellas sin conocimiento o autorización de la DTIC- que carecen de alguna documentación que sirva de fundamento o respalde, ante cualquier eventualidad, el nivel de responsabilidad de estos usuarios o unidades, lo cual, ante la materialización de un ciberataque podría generar vulnerabilidades en el acceso y exposición de datos, así como, posibles sanciones administrativas o legales.

5. RESPECTO AL ANALISIS DE VULNERABILIDADES Y SOPORTE TÉCNICO DEL SOFTWARE LIBRE

Se determinó que, el análisis de vulnerabilidades del software libre para el desarrollo de aplicaciones -a la ejecución del presente estudio- se realiza como uno de los procedimientos establecidos por la Comisión de Validación de Software Libre y el Comité de Control de Cambios de la DTIC, para brindar el aval para su utilización a nivel institucional, estas pruebas se efectúan únicamente a la versión especifica indicada en la solicitud de aval; posterior a su autorización, tanto el análisis de vulnerabilidades (de versiones que se descarguen o apliquen posteriormente) como la actualización a nuevas versiones de estas herramientas, queda a valoración y solicitud de los funcionarios o unidades que descargaron y utilizaron el software libre.

En relación con lo anterior, según lo indicado por funcionarios del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, al 28 de febrero de 2025, se encontraba en proceso un replanteamiento del procedimiento de aval para las nuevas solicitudes de utilización de software libre a nivel institucional, donde por medio de la firma de un acuerdo de uso, la persona responsable se compromete a mantener el software actualizado, no realizarle modificaciones (sin previa autorización de la DTIC) ni compartirlo; sin embargo, anteriormente estas responsabilidades no se tenían delimitadas o establecidas formalmente, quedando a criterio de los funcionarios, su adecuada utilización; situación que causa incertidumbre o preocupación respecto a los componentes que previamente habían sido descargados y utilizados sin haberse efectuado ningún acuerdo.

Aunado a lo anterior, preocupa a esta auditoría que la planificación o establecimiento de la hoja de ruta de los análisis de vulnerabilidades, a nivel institucional, se realice según demanda y que no es un tema exclusivo de sistemas (de conformidad con lo indicado por la Subárea de Seguridad en Tecnologías de Información), ya que esta situación disminuye, aún más, las posibilidades de detectar cualquier vulnerabilidad existente en las versiones de servicio de las herramientas de software libre y/o lenguaje de código abierto utilizadas en el desarrollo de sistemas.

En relación con la existencia de vulnerabilidades detectadas –a nivel institucional- en herramientas de software libre utilizadas para el desarrollo de sistemas, mediante oficio DTIC-2150-2018 del 10 de abril de 2018, la Msi. Ana María Castro Molina, jefe a.i. del Área de Seguridad y Calidad Informática Subarea de Seguridad en TI de la Dirección de Tecnologías de Información y Comunicaciones trasladó al Master Ronald Lacayo Monge, gerente,

Gerencia Administrativa en esa oportunidad, las recomendaciones pendientes de aplicar para efectos de la contratación 2014CD000003-1150 "Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en TIC" referencia a oficio ASCI-0079-2016 con fecha 05 de enero 2016; indicándose, a continuación, algunas de las relacionadas con software libre:

Lugar	Sistema	Oportunidades de Mejora	Segundo Seguimiento
Gerencia Administrativa	Portal Web de Recursos Humanos	Sitio Web vulnerable ataques cross site scripting debido a la versión de JQuery	(…) También se recomienda analizar la posibilidad de actualizar a la versión de JQuery 1.11.2 ya que el problema en esta versión se encuentra solucionado (…)
Gerencia Administrativa	Portal Web de Recursos Humanos	Versión de PHP está obsoleta y presenta múltiples vulnerabilidades	Actualizar a la última versión liberada de PHP, que corresponde a la versión 5.6.1. (...) implementar un plan de cambio y de contingencia (…)
Gerencia Administrativa	Portal Web de Recursos Humanos	Múltiples vulnerabilidades en la versión APACHE	Se recomienda analizar la factibilidad de actualizar a la versión 2.4 de Apache HTTP que no cuenta con estas vulnerabilidades identificadas (...)
Gerencia Administrativa	Portal Web de la Caja Costarricense de Seguro Social	Múltiples vulnerabilidades en la versión APACHE	Se recomienda analizar la factibilidad de actualizar a la versión 2.4 de Apache HTTP que no cuenta con estas vulnerabilidades identificadas (...)
Gerencia Administrativa	Portal Web de la Caja Costarricense de Seguro Social	Múltiples vulnerabilidades en versiones de OpenSSH	Se recomienda revisar las configuraciones de los servicios y de ser posible actualizar el OpenSSH a la versión 6.8 (…) implementar un plan de cambio y de contingencia (…)

Asimismo, en revisión realizada por esta auditoría, se constató la emisión del oficio CGI-GADMIN-143-2018 del 23 de abril del 2018 en respuesta al oficio DTIC-2150-2018 del 10 de abril de 2018, no obstante, dicho documento carece de acciones efectuadas en relación con la atención de las oportunidades de mejora citadas en el cuadro anterior. Además, en la información suministrada tanto por el Centro de Gestión Informática de la Gerencia Administrativa como por la Subárea de Seguridad en Tecnologías de Información no se constató algún otro seguimiento realizado posterior.

Por otra parte, en los informes de análisis de vulnerabilidades internas del Sistema de Información de Sostenibilidad Ambiental (SISA) de noviembre 2023 y el Sistema Integrado Gestión Personas Trabajadoras CCSS (SIPE) de diciembre 2023, se establecieron oportunidades mejora respecto a la actualización de la versión de servicio de las herramientas OpenSSH, Payara y jQuery debido a la existencia de vulnerabilidades que podrían ocasionar o facilitar ciberataques a la red tecnológica institucional.

Además, es de conocimiento de esta auditoría que, en diversos sitios web como www.tarlogic.com, www.incibe.es, www.csirt.telconet.net, www.cybersecuritydive.com, www.greynoise.io, entre otras, se indica que el desarrollo de sistemas con herramientas de software libre -particularmente PHP- han presentado vulnerabilidades de ciberseguridad que, aunado a la falta de un esquema formal de soporte (respecto a la atención de incidencias por parte de una marca o casa matriz particular con acuerdos de servicio) podrían afectar la seguridad de la información generada y administrada por sistemas desarrollados en dicha plataforma.

Las Normas de Control Interno para el Sector Público, en el inciso 1.4.5 sobre el control de Accesos, refieren:

> *"La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*
> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación (…)*
> *e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio.*

Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones".

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el apartado XI. Seguridad y ciberseguridad, lo siguiente:

"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 (…)".

Ese mismo marco normativo, en el apartado *"Gestión del Riesgos Tecnológicos"*, refiere:

"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.

La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución".

En relación con lo anterior, es importante mencionar que, mediante oficio de advertencia AD-ATIC-8137-2018 "Oficio de Advertencia sobre la gestión efectuada en el cumplimiento de los planes remediales para la gestión de vulnerabilidades y riesgos en TIC de la CCSS" del 24 de setiembre de 2018, esta auditoría informó a los gerentes de infraestructura y tecnología, logística, administrativo, financiero, médico y de pensiones, respecto a la atención de las oportunidades de mejora emitidas en la contratación 2014CD-000003-1150 *"Adquisición de servicios profesionales para el análisis de vulnerabilidades y riesgos de la Seguridad en TIC"* , lo siguiente:

"(…) Las evaluaciones efectuadas generaron 1287 hallazgos a los cuales la empresa consultora asignó planes remediales para mitigar los riesgos asociados.

Con respecto a los dos seguimientos incluidos en la consultoría, el primero fue realizado entre enero y marzo del 2017 y el segundo entre octubre y noviembre del 2017, sin embargo, los informes respectivos fueron recibidos y aceptados por los responsables institucionales en agosto 2017 y enero 2018 (…)

Con base en lo indicado en el cuadro anterior, así como la evidencia aportada por el Área de Seguridad y Calidad Informática se identificaron los siguientes temas a valorar:

- *Se identificó 560 planes remediales pendientes de atender, es decir un 50.85% en los que no se han generado acciones para mitigar los riesgos identificados.*
- *De las acciones realizadas por las unidades a cargo de los planes remediales, únicamente se corrigió 68 de ellos, luego de haberse efectuado el primer seguimiento. Lo anterior a pesar de que transcurrió 7 meses entre la finalización del primer seguimiento y el segundo.*

- *La cantidad de acciones en proceso disminuyó a 88, a pesar de la cantidad de planes remediales pendientes.*

Esta situación adquiere relevancia si se considera la comunicación de hallazgos a las diferentes unidades desde hace más de dos años y aproximadamente tres años luego de haberse identificado por parte de la firma consultora (…)"

El Ing. Danilo Hernández Monge, jefe, Área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones, respecto a quién es el encargado de actualizar y comunicar las nuevas versiones de estas herramientas de lenguaje de código abierto para el desarrollo de aplicaciones a nivel institucional, el Ing. Danilo Hernández Monge, señaló:

> *"Igualmente, para una respuesta más amplia sería importante hacer esta consulta al Área de Soporte Técnico, pero creo que en la respuesta anterior, se menciona que con el nuevo replanteamiento que se le está dando al proceso del aval de utilización de herramientas de software libre, lo que se busca es establecer es crear un compromiso para que esas unidades solicitantes se hagan responsable de la utilización, actualización (de las nuevas versiones que se generen de esa herramienta) y la coordinación respectiva para la revisión de nuevas versiones".*

La Ing. Laura Paz Morales, jefe, Subárea Sistema Automatizado en Recursos Humanos, Dirección de Administración y Gestión de Personal, al consultarle si se han solicitado estudios de vulnerabilidades para las aplicaciones desarrolladas con lenguaje de código abierto, indicó:

> *"Sí, correcto, por parte de Deloitte nos han hecho escaneos de los sitios, donde se ha encontrado algunas áreas de mejora, que hemos aplicado y que ellos posteriormente han revisado. Esto se ha acentuado desde que se dio el hackeo en la Caja, después de eso han hecho como 3 revisiones y se han aplicado las recomendaciones que ellos indican.*
>
> *De hecho, una de las cosas que la DTIC toma como base para decir que sigan con sistemas PHP en producción, es precisamente porque cumplimos con los requerimientos de seguridad establecidos por esos monitoreos".*

Asimismo, al consultarle cómo se gestiona el soporte técnico de estas aplicaciones y quién es el encargado de actualizar y comunicar las nuevas versiones de estas herramientas, señaló:

> *"Soporte técnico va en dos vías, la parte del mantenimiento y administración de los servidores lo da el Área de soporte técnico institucional, el desarrollo y soporte en sistemas lo damos la Subárea de Sistemas Automatizados en Recursos Humanos (SSARH) de la DAGP.*
>
> *Es que es compartido porque, cuando usted va a realizar una actualización del lenguaje lo aplica soporte, pero tienen que coordinar con nosotros, porque nosotros tenemos que revisar que esa nueva versión no que tenga cambios drásticos que interfiera en el sistema, ya que si trae cambios de peso se debe aplicar primero en un ambiente de desarrollo o de pruebas para hacer los cambios de programación que se requieran, para posteriormente ponernos de acuerdo para aplicarlo en producción, por tanto, es algo coordinado. Después del hackeo SSAHR ha determinado que cada seis meses actualizamos la versión de PHP, ya sea que yo lo pida al área de soporte o que se solicite por algún informe de Deloitte o que soporte nos diga que se debe actualizar Apache y que se debe actualizar también PHP, hay una coordinación entre ambos, una responsabilidad compartida".*

El Ing. George Aguilar Prieto, encargado de la unidad de desarrollo de software del Centro de Gestión Informática del Hospital San Vicente de Paúl, sobre la solicitud de estudios de vulnerabilidades para las aplicaciones desarrolladas con lenguaje de código abierto, indicó:

"No se han solicitado estudios, sin embargo, en una oportunidad eso se realizó mediante una asesoría de un proveedore externo bajo instrucción de la DTIC, con la empresa Deloitte".

Asimismo, al consultarle cómo se gestiona el soporte técnico de estas aplicaciones y/o sistemas de información y quién es el encargado de actualizar y comunicar las nuevas versiones de estas herramientas de software libre, señaló:

"El soporte técnico se asume desde el equipo del CGI del Hospital, sin embargo, se está en proceso de entregar el conjunto de soluciones que se usan a nivel nacional a la DTIC para que ellos como ente llamado a, asuman lo que corresponde".

"Los equipos siguen las buenas prácticas a nivel de arquitectura y desarrollo de aplicaciones que se dictan desde el Área de Desarrollo de Software del CGI".

El Ing. Marlon Delgado Álvarez, jefe a.i y el Ing. Luis Angel Gómez Alfaro, coordinador de la Comisión de Validación de Software Libre, ambos funcionarios del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones, respecto a parámetros o criterios utilizados para autorizar la utilización herramientas de lenguaje de código abierto para el desarrollo de aplicaciones a nivel, indicaron:

*"**Ing. Luis Angel Gómez Alfaro**: Cuando una persona requiere hacer una solicitud de autorización, porque necesita utilizar un software libre, hay un procedimiento que deben seguir, a través de la Mesa de Servicios, ponen en un caso en mesa y ahí se les informa que tienen que llenar un formulario con varias preguntas (información básica del software, versión, en qué sistema operativo se va a correr, quienes lo van a usar, porqué necesitan esa herramienta, etc.) y cuando ya se tienen esos documentos llenos y firmados, mesa los traslada a la Comisión de Validación de Software Libre, para hacer un análisis (bajo ciertos criterios que se han determinado) y con base a ese análisis se hace un informe donde se indican los principales elementos a considerar.*

Parte de ese análisis involucra que la persona que está solicitando la autorización debe de pasarnos el software y hacernos una presentación del mismo (cuando no es conocido), posteriormente, eso se traslada a la Subárea de Seguridad para que ellos hagan un análisis de vulnerabilidades, el cual, es subcontratado a una empresa que da ese servicio, ahorita esa empresa es Deloitte, ellos procesan la solicitud y entregan a la Comisión un informe, este informe es muy importante porque lo realiza una empresa experta en este tema; si en el análisis de vulnerabilidades se detecta algún elemento sospechoso o malicioso la solicitud se rechaza, o por el contrario, si no se hay nada extraño (todo está bien) se le da el visto bueno, para completar la documentación, con todos los fundamentos correspondientes.

Una vez hecho el informe, la Comisión lo traslada al Comité de Control de Cambios, ese es el ente de aprobación, por medio de un RFC se presenta como una solicitud de cambio, donde se presentan los resultados con toda la documentación y ellos son los que deciden si se aprueba o no el software y en qué condiciones.

***Ing. Marlon Delgado Álvarez:** Nosotros utilizamos una plantilla donde se evalúan elementos como: infraestructura, seguridad, compatibilidad del software con la plataforma institucional, lenguaje operativo, entre otros elementos; todo esto y el estudio de vulnerabilidades es lo que se utiliza para el análisis y elaboración del informe final, donde se establece si puede o no utilizarse en el ambiente institucional.*

Como ejemplo y respaldo de lo señalado anteriormente, el Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones suministró a esta auditoria los "Formularios de solicitud de uso de software libre", "Plantilla de instrumento de evaluación", "Informe de revisión de software" y el "Análisis de software desarrollado por la empresa Deloitte" de las herramientas de software libre JMeter y RStudio.

Además, al consultarles si, una vez que se da la aprobación del software libre solicitado por una unidad específica, estos se incluyen en el sitio de descargas y pueden ser utilizados por cualquier otra unidad institucional, los funcionarios señalaron:

> ***"Ing. Luis Angel Gómez Alfaro:*** *Eso antes era así, pero precisamente esta semana se realizaron unos cambios. Ahora, cuando el Comité de Control de Cambios aprueba un software ellos indican las condiciones para su uso, ahí se va a indicar si la autorización es para una persona, una subárea o un equipo de trabajo en específico. Como primera medida nos solicitaron deshabilitar el sitio de descarga para que no estuviera disponible para cualquier persona.*
>
> ***Ing. Marlon Delgado Álvarez:*** *En seno del Comité de Control de Cambios se dio de baja las descargas porque como parte de las observaciones que nos hicieron, es que las personas deben de suscribir un acuerdo de uso para limitar el uso del software, porque antes se daba de manera generalizada y ahora solo se va a autorizar a la persona que hace la solicitud, el cual, ellos tienen que cumplir ciertos requisitos para su uso".*

Asimismo, se consultó si, en este acuerdo de uso se tiene contemplado quién va a ser el responsable de la actualización de nuevas versiones que surjan del software libre, respondiendo el Ing. Luis Angel Gómez Alfaro, lo siguiente:

> ***"****Al firmar el acuerdo de uso, la persona responsable se compromete a mantener el software actualizado, no realizar modificaciones al software (sin previa autorización de la DTIC y no puede compartirlo, las mismas restricciones que tiene la utilización de cualquier otro software licenciado. Lo que se pretende con este acuerdo es que la persona que firma sienta la responsabilidad y el compromiso de hacer un uso correcto de estas herramientas, además, se les indica que la DTIC no se compromete a darle un soporte a un software sobre el cual no tenemos un contrato de mantenimiento****".***

Por otra parte, respecto al tipo de soporte técnico que se les brinda a los sistemas que ya fueron desarrollados con lenguaje de código abierto a nivel institucional, como PHP, estos funcionarios indicaron:

> ***"Ing. Marlon Delgado Álvarez:*** *Nosotros como Área de Soporte Técnico, no les damos soporte a los desarrollos que realizan las unidades, no se encuentra dentro del ámbito de acción de nuestra área, porque es algo que desarrolla cada unidad a nivel interno.*
>
> *Es que ellos son los desarrolladores del aplicativo, ellos tienen un equipo de informáticos destacados en sus unidades para darle mantenimiento y atención a esos sistemas.*
>
> *Nosotros somos los que administramos la infraestructura, les colaboramos a ellos en ese proceso.*
>
> ***Ing. Luis Angel Gómez Alfaro:*** *Soporte lo que provee es la infraestructura (servidores y almacenamiento) y les colaboramos en ese sentido, con todo lo que conlleva la administración de esa infraestructura. Realizamos un soporte compartido, en donde los desarrolladores le dan mantenimiento a la aplicación y Área de Soporte Técnico colabora con el mantenimiento de la infraestructura y cuando corresponde aplicar actualizaciones de las versiones se hace en conjunto entre ambos equipos de trabajo".*

En consulta realizada al Ing. Erick David Vindas Umaña, jefe a.i. Subárea de Seguridad en Tecnologías de Información, respecto a la existencia de un cronograma o programación de los estudios de vulnerabilidades que debe de realizar la empresa Deloitte durante el año, indicó:

> *"No formalizado. Y por no formalizado, se debe a raíz de que el servicio es el más saturado, por ser un servicio a demanda, no podemos comprometer al cumplimiento de una agenda o cronograma por las necesidades que van surgiendo de camino.*
>
> *Cuatrimestralmente acordamos la hoja de ruta para el establecimiento de análisis de vulnerabilidades, ya que no es un tema exclusivo de revisión de sistemas.*
>
> *Por ejemplo, a través del servicio se hacen validaciones de hardening de plataformas, para el establecimiento de lineas base de seguridad. O en el próximo cuatrimestre se tiene proyectada la ejecución a gran escala de revisión de análisis de vulnerabilidades físicas, pruebas de phishing, vishing.*
>
> *Y tenemos de por medio y emergente, y urgente análisis de vulnerabilidades de servicios que están en proceso de migración a nube (...)"*

Asimismo, respecto a la ejecución de seguimientos para verificar el cumplimiento de las recomendaciones emitidas en los informes de vulnerabilidades, señaló:

> *"Actualmente por inopia de personal no se hace un seguimiento activo de las recomendaciones emitidas, no obstante, se planifica al cierre del primer semestre 2025 dar inicio con los seguimientos semestrales de cumplimiento. Esta tarea fue delegada mediante oficio a las Licdas. Yeudy Mesén Bonilla y Grace Monge Picado".*

Lo anteriormente expuesto, es producto de la carencia de lineamientos formalmente establecidos y comunicados -basados en buenas prácticas nacionales e internacionales-, donde se instruyera, institucionalmente, la adecuada metodología de utilización, administración y soporte de estas herramientas de software libre para el desarrollo de aplicaciones y que, a su vez, se delimitara, de manera clara, la asignación de responsabilidades para aquellos funcionarios o unidades a los cuales se les otorgaba el aval para el uso de estos componentes. Asimismo, es importante mencionar, que la mayoría de los programas de código abierto carecen de un nivel de soporte diferente al del software propietario, lo que dificulta a ejecución de solicitudes y atención de requerimientos, ante la existencia o surgimiento de problemas de funcionamiento o seguridad.

Esta situación podría representar un riesgo de ciberseguridad, ya que no existe certeza de que esas herramientas de software libre -descargadas y utilizadas- hayan recibido, a través del tiempo, el soporte técnico y actualizaciones requeridas para su adecuado funcionamiento, lo cual, aunado a la carencia de un proceso de seguimiento continuo a la atención de las oportunidades de mejora detectadas en los análisis de vulnerabilidades -formalmente establecido-, aumenta las posibilidades de que existan debilidades de seguridad que podrían facilitar el acceso a la plataforma tecnológica e información resguardada en medios digitales por la Caja Costarricense de Seguro Social.

CONCLUSIONES

A nivel internacional, se mencionan diversas ventajas presentes en el uso de software libre para el desarrollo de aplicaciones y/o sistemas de información, tales como: el ahorro económico derivado de la eliminación de costos de licencias; la capacidad de personalizar el software para satisfacer las necesidades específicas del usuario; la interoperabilidad, que facilita la integración con otros sistemas y plataformas, así como, la innovación y colaboración, que permite la implementación ágil de mejoras y nuevas funcionalidades. No obstante, se debe tener presente la existencia de ciertos riesgos asociados a su uso, entre los más relevantes, la falta de soporte comercial, que puede representar un desafío en la resolución de incidencias y en la actualización del software, debiendo el usuario asumir la responsabilidad de cualquier fallo o vulnerabilidad.

En el ámbito de la seguridad de la información, es fundamental proteger los datos sensibles producto de las atenciones en los servicios de salud, garantizando la confidencialidad, integridad y disponibilidad de la información. Un ciberataque que explote vulnerabilidades existentes en el software libre podría tener

consecuencias graves, incluyendo la interrupción de servicios críticos, la exposición de datos personales de los pacientes y la pérdida de confianza por parte de los usuarios; además, los funcionarios involucrados podrían enfrentar sanciones administrativas y legales, en caso de incumplir con las normativas de protección de datos y seguridad de la información.

Esta Auditoría a través del presente estudio referente a la gestión de desarrollo de aplicaciones y/o sistemas de información mediante software libre y/o lenguaje de código abierto en la CCSS, evidenció oportunidades de mejora en cuanto a la gestión de monitoreo y control respecto a los desarrollos de sistemas que se realizan en las diversas unidades y que se encuentran en funcionamiento dentro de la red institucional, existiendo, en la actualidad, varios de ellos que aún no han sido identificados por la Dirección de Tecnologías de Información y Comunicaciones.

En lo referente al Catálogo Institucional de Aplicaciones Informáticas (CIAI), se concluye sobre la necesidad de fortalecer la gestión de control y seguimiento por parte del Área de Ingeniería de Sistemas en su rectoría del tema por parte de la DTIC a nivel institucional, así como, velar por el cumplimiento de las regulaciones normativas existentes respecto a la obligatoriedad –de los CGI Gerenciales, regionales y locales- de notificar y solicitar autorización a la Dirección de Tecnologías de Información y Comunicaciones, para realizar estas aplicaciones o sistemas de información.

En adición, los resultados del estudio permitieron identificar que, la mayoría de los Centros de Gestión de Informática consultados señalaron no tener conocimiento sobre un marco normativo (institucional, nacional o extranjero) en torno al desarrollo de aplicaciones y/o sistemas de información con software libre o lenguaje de código abierto, así mismo, indicaron no haber recibido comunicado oficial alguno o rectoría por parte de la Dirección de Tecnologías de Información y Comunicaciones en dicha materia; lo cual, refleja la necesidad de fortalecer la gestión de direccionamiento, control y regulación tecnológica ejercida por parte de la Dirección de Tecnologías de Información y Comunicaciones, el Área de Ingeniería de Sistemas y los Centros de Gestión Informática Gerenciales, así como, la implementación del Modelo de Gobierno TI.

Es crucial que las autoridades institucionales en materia de tecnologías de información y comunicaciones fortalezcan los mecanismos de control interno y establezcan directrices o lineamientos que definan con claridad cada uno de los procedimientos que se deben seguir para el aval, utilización y administración del software libre, así como, las responsabilidades de cada uno de los participantes en los citados procesos.

Preocupa a esta Auditoría que, según lo evidenciado en el presente estudio, así como, lo señalado mediante oficio AD-ATIC-0120-2023 del 2 de noviembre de 2023, en la Caja Costarricense de Seguro Social no se ha definido -de manera formal- un planteamiento en torno a las mejores prácticas para la implementación de estas tecnologías de formato abierto, lo cual, genera incertidumbre y confusión en cuanto a los procedimientos que se deben seguir, a nivel institucional, para poder hacer un uso adecuado de estas herramientas libres de desarrollo, permitiendo, a su vez, una utilización sin regulaciones que podría generar vulnerabilidades en la plataforma tecnológica de la Caja Costarricense de Seguro Social.

Asimismo, la investigación e implementación de buenas prácticas -con resultados positivos- a nivel nacional e internacional, podría no solo ayudar a mitigar los riesgos asociados al uso de software libre, sino que también asegurar el cumplimiento de las normas vigentes y fortalecer la confianza de los usuarios internos y externos.

RECOMENDACIONES

AL MÁSTER ROBERT PICADO MORA, EN SU CALIDAD DE SUBGERENTE DE LA DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES O A QUIEN EN SU LUGAR OCUPE EL CARGO

1. Considerando que la Dirección de Tecnologías de Información y Comunicaciones es la unidad rectora de TI, y de acuerdo con lo evidenciado en los hallazgos 1, 2, 3, 4 y 5 del presente estudio, con la integración de un equipo de trabajo conformado por representantes de las distintas Gerencias y las instancias que

se estimen pertinentes -según sus competencias-, establecer un plan de acción orientado a atender las oportunidades de mejora determinadas en la gestión de aval, utilización y administración de software libre para el desarrollo de aplicaciones y/o sistemas de información en la institución, contemplando al menos los siguientes elementos:

1.1 De conformidad con lo señalado en los hallazgos 1 y 2 del presente estudio, efectuar un diagnóstico institucional, con el fin de establecer la totalidad de desarrollos realizados fuera de la Dirección de Tecnologías de Información y Comunicaciones, el cual contenga, al menos, los datos que actualmente se solicitan para el registro de aplicaciones en el Catálogo Institucional, otorgándole una mayor relevancia al entorno de programación y la versión utilizada en cada uno de los sistemas.

- Una vez realizado el diagnóstico anteriormente solicitado, con la totalidad de los datos recopilados, realizar la actualización del Catálogo Institucional de Aplicaciones Informáticas (CIAI) de aquellas aplicaciones que cumplen con los requerimientos establecidos en la normativa institucional en dicha materia, lo anterior, con el fin de disponer de información confiable para el análisis y toma de decisiones por parte de las autoridades institucionales u órganos de fiscalización, de ser requerido.

- De conformidad con los resultados generados en el diagnóstico solicitado en el punto anterior (si se determinara -en la plataforma institucional- el desarrollo de sistemas de información **no autorizados por la DTIC**), efectuar una sesión con el Consejo Tecnológico para exponer la situación establecida, lo anterior, con el fin de que en dicho órgano colegiado se tomen las decisiones y acuerdos correspondientes para garantizar el cumplimiento normativo en dicha materia, así como, la protección de información sensible para la institución -ante la existencia de posibles vulnerabilidades-.

1.2 De acuerdo con lo evidenciado en los hallazgos 3, 4 y 5 del presente estudio, realizar la emisión de lineamientos o directrices que definan con claridad cada uno de los procedimientos que se deben seguir para el aval, utilización, comunicación a los usuarios de vulnerabilidades y administración (soporte técnico, análisis y atención de vulnerabilidades, seguimiento y actualización de nuevas versiones y resolución de incidencias, etc.) del software libre para el desarrollo de aplicaciones y cualquier otro utilizado en la plataforma institucional, así como, la delimitación de responsabilidades para cada uno de los participantes en los citados procesos.

- Al respecto, dentro de las acciones efectuadas por la administración activa para la atención de la presente recomendación, considerar los alcances del replanteamiento del proceso de autorización y uso de software “Acuerdo de Uso” que según lo mencionado por los funcionarios del Área de Soporte Técnico -en el hallazgo 4 y 5 del presente informe-, actualmente se encuentra en proceso de elaboración y oficialización. Lo anterior, con el fin de lograr un mayor aprovechamiento de los recursos y evitar futuros reprocesos que pudieran generarse ante un posible incumplimiento del marco normativo.

1.3 Realizar las gestiones necesarias con el fin de reiterar a las Gerencias y CGI (gerenciales, regionales y locales) las responsabilidades establecidas en la normativa institucional respecto al acatamiento obligatorio de efectuar la solicitud de autorización previa de la DTIC para el desarrollo de los sistemas y aplicaciones en su ámbito de competencia, así como, las posibles implicaciones administrativas o legales en las que se puede incurrir ante la materialización de un ciberataque debido a la existencia de vulnerabilidades por la carencia de supervisión u omisión de la reglamentación existente en dicha materia.

Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de **9 meses**, a partir de la recepción del presente informe, el plan de acción definido (que deberá

incluir actividades de monitoreo, responsables y plazos), así como la documentación que evidencie el abordaje de la ejecución del diagnóstico institucional de sistemas, la actualización del Catálogo Institucional de Aplicaciones Informáticas (CIAI) según corresponda, acciones que correspondan (según los resultados del diagnóstico), la emisión de lineamientos o directrices (que se consideren necesarias) y las gestiones necesarias con el fin de reiterar a las Gerencias y CGI (gerenciales, regionales y locales) las responsabilidades y posibles implicaciones administrativas o legales establecidas en la normativa institucional.

En relación con las recomendaciones expuestas en el presente informe, en el plazo de 10 días hábiles[6] se deberá remitir a esta auditoría el "cronograma de acciones"[7] con las actividades o tareas, encargados designados y tiempo de ejecución previstos en función del plazo total acordado para el cumplimiento de cada una. Asimismo, se deberá informar periódicamente sobre los avances del cronograma y aportar las evidencias respectivas, a fin de que se pueda verificar el cumplimiento oportuno.

Se recuerda que, **si por motivos debidamente justificados**, durante la ejecución del cronograma la administración requiere ampliar el plazo de alguna recomendación, el jerarca o titular subordinado responsable de su cumplimiento, deberá solicitar formalmente la respectiva prórroga, **en tiempo y forma**, conforme lo establecido en el artículo 93 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, aportando además, el cronograma actualizado, conforme con el nuevo plazo que se esté solicitando y las actividades que presenten el respectivo retraso justificado.

El formato estandarizado del "Cronograma de acciones para el cumplimiento de recomendaciones" puede ser descargado del SIGA desde la ventana de inicio, en siguiente ícono  . Se solicita que; en el plazo señalado se remita el oficio de respuesta al informe, incluyendo como adjunto el "Cronograma de acciones para el cumplimiento de recomendaciones" adecuadamente completado, a través del SIGA, en el módulo de "Oficios" apartado "Respuesta informe", vinculándolo al número de informe ATIC-0025-2025. De esta misma forma, se remitirá posteriormente, la evidencia que constate los avances.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 62 del Reglamento de Organización y Funcionamiento de la Auditoría Interna de la Caja Costarricense de Seguro Social, los resultados del presente informe fueron comentados el 6 de junio de 2025 con Máster Robert Picado Mora, director con rango de Subgerente; el Ing. Daniel Berrocal Zúñiga, jefe Área de Seguridad y Calidad Informática; la Ing. Vanessa Carvajal Carmona, jefe, Área Soporte Técnico; el Ing. Alexander Angelini Mora, jefe a.i, Área de Ingeniería de Sistemas; el Ing. Erick David Vindas Masís, jefe a.i. Subárea Seguridad de Tecnologías de Información; el Ing. Sergio Paz Morales, jefe a.i. Área Ingeniería de Sistemas; la Ing. Ericka Sánchez Solís, jefe a.i. Subárea de Seguridad Informática; la Licda. Criselda Sánchez Rojas, Asistente Despacho y el Lic. Julián Gerardo Chaves Chaves, Asistente Despacho, todos ellos funcionarios de la Dirección de Tecnologías de Información y Comunicaciones.

Respecto a la recomendación del informe, la Administración Activa efectuó, las siguientes observaciones:

"Recomendación 1:

Referente al punto 1.1 de la recomendación 1, se efectuaron los siguientes comentarios:

[6] Plazo máximo establecido en la Ley General de Control Interno (Art. 17 inciso d / Art. 36 inciso a), para iniciar la implantación de las recomendaciones de los informes de auditoría.
[7] Art. 68 del Reglamento de Organización y Funcionamiento de la Auditoría Interna.

El Máster Robert Picado Mora, subgerente de la Dirección de Tecnologías de Información y Comunicaciones, *indicó: No, estoy entendiendo muy bien, yo estoy entendiendo que en el punto 1.1 de la recomendación, la Auditoría solicita que legalicemos lo ilegal, es que así lo estoy interpretando.*

Al respecto el ***Ing. Anthony Esteban Bonilla Bonilla****, respondió: No, lo que se busca con la recomendación es que si en el diagnostico ustedes detectan sistemas de información que fueron desarrollados con herramientas de software libre y no fueron notificados a ustedes o no se le solicitó autorización a la DTIC, se efectúen las acciones administrativas que correspondan para garantizar el principio de legalidad, así como, la protección de información sensible.*

El ***Máster Robert Picado Mora,*** *señaló: No podemos, no son subalternos de nosotros, yo no tengo ninguna injerencia sobre los CGI, creo que esa recomendación debería de ir dirigida a las gerencias, yo estoy de acuerdo en que se debería de sancionar estos incumplimientos, pero la DTIC no puede hacerlo.*

En relación con lo anterior, el ***Ing. Anthony Esteban Bonilla Bonilla,*** *consultó: ¿Don Robert, la Dirección de Tecnologías de Información y Comunicaciones no puede hacer una notificación a la unidad correspondiente para que ellos efectúen las sanciones que correspondan? Porque la auditoría comprende que la DTIC no tiene injerencia para poder sancionar, pero si no se notifica o se realiza las gestiones administrativas necesarias, se estaría siendo permisivo con estas unidades de hacer lo que ellos gusten con respecto al desarrollo del software.*

El ***Máster Robert Picado Mora,*** *indicó: En eso si estoy de acuerdo, pero yo creo y lo digo francamente, es probable que esto no termine en nada, porque la recomendación va dirigida a la DTIC, es muy posible que los responsables de las unidades no realicen las acciones que correspondan, porque la auditoría no se los dirigió específicamente a ellos; bajo las condiciones actuales para las gerencias y direcciones de hospitales es muy sencillo que todos los problemas tecnológicos recaigan sobre la DTIC, pero que no se interfiera con sus informáticos. Si desde el informe se está determinando que, para el desarrollo de sistemas los CGI no solicitaron los avales e incumplieron la normativa, ellos tienen jefes, lo lógico es que a ellos se les remita la recomendación también.*

Al respecto el ***Ing. Anthony Esteban Bonilla Bonilla****, respondió: Don Robert, para eso es que, específicamente le estamos haciendo a la DTIC la solicitud del diagnóstico, porque actualmente no tenemos un panorama total que nos pueda decir: ¿Cuáles son los sistemas que se han desarrollado incumpliendo la norma y si ustedes han autorizado o no ese desarrollo? Una vez que se tenga ese diagnóstico, a nivel institucional, ya se contaría con el insumo para poder notificar a las jefaturas correspondientes, ya sean gerentes, directores regionales o médicos las irregularidades o incumplimientos normativos detectados en su unidad, donde se traslada la responsabilidad de efectuar las gestiones administrativas correspondientes; la auditoría, actualmente, no puede orientar la recomendación a alguna gerencia porque todavía no tenemos ese insumo del diagnóstico. La Auditoría Interna comprende que la Dirección de Tecnologías de Información y Comunicaciones no tiene injerencia para poder sancionar incumplimientos normativos de los CGI, pero si tiene la responsabilidad de saber cuál es la situación real a nivel de tecnologías en la institución.*

En relación con lo anterior, el ***Ing. Leonardo Díaz Porras,*** *indicó: Lo que podríamos valorar es que se haga la modificación, tal vez, no en los términos que están redactados actualmente, sino que, una vez efectuado el diagnóstico -de identificarse incumplimientos normativos- se notifique a las unidades o actores competentes, porque si se debiera efectuar alguna sanción, efectivamente, le correspondería a quién tiene la potestad sancionatoria realizar las acciones correspondientes; sin embargo, el diagnóstico o la identificación sí le corresponde a la DTIC.*

En relación con lo anterior, el ***Máster Robert Picado Mora,*** *indicó: Sí, que se indique que se traslade a las unidades, porque yo no tengo injerencia sancionatoria.*

Además, consultó: ¿En el primer punto, sería incluir en el catalogó institucional aquellas aplicaciones que su desarrollo sí fue avalado por la Dirección de Tecnologías de Información y Comunicaciones?

*El **Ing. Anthony Esteban Bonilla Bonilla**, respondió: Sí Don Robert, es hacer una actualización del catálogo con las aplicaciones autorizadas o los datos que no se completaron en su momento, otorgándole una mayor relevancia al entorno de programación y la versión utilizada en cada uno de los sistemas.*

*Asimismo, respecto al punto 1.1 de la recomendación, la **Ing. Vanessa Carvajal Carmona, jefe, Área Soporte Técnico**, señaló: No estoy de acuerdo que esta recomendación vaya dirigida solamente a la DTIC o al Master Robert Picado, creo que debería dirigirse también a las gerencias, porque la ejecución de las acciones correctivas para garantizar la legalidad y protección de la información sensible es un tema de la seguridad de la información, es institucional. Nosotros como DTIC no podemos responsabilizarnos de toda esa información y tiene que haber participación de las gerencias, ya que ellos son los responsables de los Centros de Gestión Informática, si la recomendación viene dirigida solo a la DTIC ellos posiblemente van a decir que, tienen mucho trabajo, no tenemos el recurso humano necesario para hacerlo o esas tareas no me corresponden a mí, porque no le estamos dando la responsabilidad a la parte que le corresponde también.*

*Al respecto, el **Máster Robert Picado Mora**, indicó: Complementando el comentario de Vanessa, por ser un tema donde podría haber presuntos implicados de los Centros de Gestión de Informática, yo creo que debería de haber un representante por gerencia, que no sea necesariamente el CGI.*

Para efectos prácticos con las herramientas que tiene Deloitte o inclusive con las mismas herramientas que tenemos con Microsoft pareciera que podemos llegar a efectuar ese diagnóstico, yo creo que el espíritu de la recomendación de auditoria está superbién y es una gran oportunidad para ir ordenando todos estos elementos; sin embargo, nosotros hemos sido insistentes en el tema de la gobernanza y de la gestión de las TIC (que no ha calado por diferentes situaciones), entonces yo creo que bajo el modelo de gobernanza actual, las gerencias tienen que asumir la responsabilidad que les corresponde.

Nuestra propuesta es que la recomendación vaya dirigida a los gerentes también.

*Asimismo, el **Ing. Daniel Berrocal Zúñiga, jefe Área de Seguridad y Calidad Informática**, mencionó: Tal vez esta recomendación debería ir dirigida a la Gerencia General o Presidencia Ejecutiva, por ejemplo: Presidencia ejecutiva (pues cubre a todos) o Gerencia General (ya que cubre tanto a la Dirección de Tecnologías de Información como a las diferentes gerencias).*

*Al respecto, el **Máster Robert Picado Mora**, respondió: Presidencia no, porque es un tema de gestión y actualmente no hay Gerente General, entonces quedamos en la misma condición, yo diría que se dirija a los gerentes.*

*Además, el **Ing. Leonardo Díaz Porras,** señaló**:** Respondiéndole a lo que decía Vanessa, nosotros entendemos y la auditoria siempre ha sido insistente en señalar a los mismos gerentes y a la presidencia que, el tema de seguridad de la información y seguridad de los datos es competencia del negocio.*

Vamos a discutir todas estas anotaciones con nuestras jefaturas, para ver la posibilidad o tomar la decisión de, eventualmente, dividir la recomendación o redirigirla a los gerentes u otra autoridad competente.

Además, el ingeniero Díaz Porras, consultó: Don Robert, entonces ¿mantendríamos el primer punto del diagnóstico y analizaríamos a quién se dirigiría la recomendación en el tema de la injerencia (ante la

posible ejecución de acciones que a derecho correspondan) si en ese diagnóstico se establecieran posibles irregularidades o incumplimientos normativos en materia de desarrollo de sistemas información?

*El **Máster Robert Picado Mora**, respondió: Sí, yo el lunes me comprometo a conversar con Daniel, Alex y Vanessa para ver posibles estrategias para el levantamiento de la información que se requiere para el diagnóstico y, además, conversar con los proveedores que nosotros tenemos contratados para ver la factibilidad de abordaje que tenemos actualmente y a futuro.*

Respecto al punto 1.2 de la recomendación 1:

La administración está de acuerdo con el punto 1.2 de la recomendación.

Referente al punto 1.3 de la recomendación 1, se efectuaron los siguientes comentarios:

*El **Máster Robert Picado Mora**, indicó: Sí, en este punto a mí me gustaría que los jefes de los CGI (gerencias) pudiesen recibir algo al respecto, tal vez, como sugerencia, si se pudiera meter algo de esto en esa recomendación que ustedes van a analizar, sería muy bueno, porque yo creo que debe existir una conciencia por parte del cuerpo gerencial de lo que está pasando en los Centros de Gestión de Informática. De mi parte, no tengo ningún problema en mandar el recordatorio, yo lo voy a hacer, pero no se lo voy a enviar a los CGI, se lo voy a remitir a los gerentes, ellos también deben de asumir su responsabilidad.*

La Administración activa, solicitó ampliar el plazo para la atención de la recomendación 1 de 6 a 9 meses, lo anterior, para establecer la estrategia y los recursos con el fin de realizar todo el trabajo que la atención de la recomendación implica".

Este órgano de fiscalización, después del análisis realizado a los comentarios realizados por la Administración Activa, efectuó los ajustes en la redacción de los términos establecidos en la recomendación 1, además, de la ampliación del plazo solicitado para su atención de 6 a 9 meses.

Las modificaciones realizadas a la recomendación 1 fueron comunicadas a la Administración Activa el 23 de junio de 2025, los cuales, indicaron estar de acuerdo con los cambios efectuados.

ÁREA AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Firmado Digitalmente

Lic. Anthony Esteban Bonilla Bonilla
Asistente de Auditoría

Firmado Digitalmente

Lic. Rafael Ángel Herrera Mora, jefe
Área

OSC/RJS/RAHM/AEBB/ayms