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

AD-ATIC-014-2022
3 de marzo de 2022

Ingeniero.
Roberto Blanco Topping., Subgerente a.i
DIRECCION TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

Estimado señor:

ASUNTO:	**Oficio de Advertencia referente a la aplicación institucional de nueva versión del Código Nacional de Tecnologías Digitales (CNTD).**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, esta Auditoría informa sobre aspectos relacionados con la aplicación institucional de nueva versión del Código Nacional de Tecnologías Digitales (CNTD).

Mediante oficio GG-DTIC-1019-2022 del 22 de febrero del 2022, esa Direccion remitió a la Gerencia General y a los seis gerentes de la Institución, la nueva versión del Código Nacional de Tecnologías de Digitales (CNTD), actualizado por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT*), indicándoles que era para su conocimiento y aplicación para los fines pertinentes.*

Al respecto, es importante indicar que este Código es un compendio de políticas públicas estableciendo los mínimos deseables para la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense, aportando las mejores prácticas aplicadas a la gestión de iniciativas y proyectos que incorporen componentes de tecnologías de información y comunicaciones a nivel nacional en el sector público que generan una inclusión en los servicios digitales del Estado.

El CNTD brinda criterios técnicos básicos que todo proyecto digital debe contemplar para su desarrollo dentro de las instituciones de la administración pública.

En última instancia, esto posibilitaría la estandarización de un marco de referencia que les permitirá a las Instituciones Públicas brindar servicios digitales de calidad, lo cual se espera se traduzca en eficiencia y eficacia, generando facilidades a los usuarios y así un mayor bienestar para la población costarricense.

Si bien es cierto, esta Auditoría estima importante la tarea de divulgación que realizó la Direccion de Tecnologías de Información y Comunicaciones (DTIC) de la versión 3.0 de este código, la cual fue generada en enero del 2022, es relevante señalar algunos aspectos que la Administración debe considerar, entre ellos, los siguientes:

1. La Institución debe avocarse a la revisión de los seis temas contenidos en el CNTD, ya que cada uno de ellos incluye una serie de políticas generales y específicas en torno a:

    - Accesibilidad, Usabilidad y Experiencia de Usuario.
    - Identificación y Autenticación Ciudadana.
    - Seguridad Tecnológica.
    - Infraestructura y Tecnología en la Nube.
    - Interoperabilidad.
    - Neutralidad Tecnológica.

Lo anterior, con el objetivo de valorar la viabilidad de su aplicación, tanto en proyectos con componente tecnológico ya implementados, en desarrollo o nuevos, debido al posible impacto en costos, tiempo y otros recursos que eventualmente se requieran.

2. El CNTD es también la guía base para que la Secretaría Técnica puedan valorar objetivamente los proyectos tecnológicos de importancia nacional y de cumplir con los criterios expuestos, puedan contar con el Sello de Gobierno Digital[1].

En ese orden de ideas conviene someter a conocimiento del Consejo tecnológico y otras Autoridades institucionales, las condiciones y requisitos que se requieren para recibir el Sello de Gobierno Digital y si la Institución dispone de los recursos para optar por este reconocimiento.

3. Conviene efectuar revisión y eventual actualización de la normativa interna relacionada con los temas abordados en el CNTD, a fin de ser concordante con la adopción de políticas incluidas.

4. Una vez efectuada las valoraciones mencionadas deben generarse actividades de concientización, divulgación o capacitación sobre los temas que generaron modificaciones, que incluyan los diferentes actores, entre ellos: Centros de Gestión Informática, profesionales en TIC no ligados a unidades de tecnología, directores de sede y jefaturas; así como desarrollar mecanismos de control para generar uniformidad en los desarrollos y maximizar los recursos institucionales

5. También, señaló el oficio remitido por esa Dirección, lo siguiente:

"(…) Adicionalmente, y dado el proceso de implementación del Programa de Modelo Meta y Gestión de las Tecnologías de Información y comunicaciones, agradezco se pueda realizar las coordinaciones respectivas con el Ing. Daniel Berrocal Zúñiga, en su rol de Director de dicho Programa, considerando que es necesario la aplicación de distintos estándares o marcos de referencia (mejores prácticas), que deben ser en total sintonía con el Programa:

- *ITIL (Information Technology Infrastructure Library)*
- *COBIT 2019 (Control Objectives for Information and related Technology)*
- *ISO 27001*
- *ISO 27002*
- *ISO 27032*
- *ISO 22301*
- *ISO 31000*
- *OWASP*
- *NIST*

En ese sentido, la indicación de coordinación que señala el oficio debe orientarse más y ser precisa sobre lo que realmente se requiere de las Gerencias, en qué situaciones, proyectos se deben aplicar los marcos o estándares de referencia indicados.

6. El 11 de noviembre de 2021, con oficio MICITT–DGD-OF-215-2021, el Lic. Jorge Mora Flores, director de Gobernanza Digital del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones informa a los directores(as) y jefes(as) de Tecnologías de Información y a los Auditores(as) Internos(as) de las Instituciones de la Administración Pública, sobre el desarrollado el nuevo Marco Normativo de Gobierno y Gestión de las Tecnologías de Información, indicando:

[1] Aprobación otorgada por la Comisión de Alto Nivel en colaboración con una secretaría técnica, a instituciones que sometan a análisis un determinado proyecto y este cumpla con las buenas prácticas definidas en el Código Nacional de Tecnologías Digitales (CNTD), además de que evidencie el impacto que tendrá su implementación a nivel nacional.

"(…) Este Ministerio como ente rector en materia de Tecnología y Gobernanza Digital en conjunto con un equipo de expertos nacionales, ha desarrollado el nuevo Marco Normativo de Gobierno y Gestión de las Tecnologías de Información, que sustituyen las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CODFOE) derogadas por la Contraloría General de la República mediante la resolución N° R-DC-17-2020 del diecisiete de marzo del dos mil veinte. Las nuevas normas técnicas de Tecnologías de Información entrarán en vigor a partir del 1 de enero del 2022.

Los documentos adjuntos corresponden a la declaración del marco de gestión de las tecnologías de información y comunicación indicado en el transitorio I de la resolución N° R-DC-17-2020. Las instituciones pueden indicar dentro de su proceso de aprobación con las autoridades correspondientes que usarán el marco definido por el ente rector y adjuntar estos documentos para cumplir con el segundo punto de la resolución de derogatoria, y finalmente una vez que se cuente con su aprobación proceder con la divulgación de estas a nivel institucional…"

Al respecto, esta Auditoría había señalado la relevancia de que la Institución valorara la emisión de normativa específica, dado que el perfil tecnológico de la Caja Costarricense del Seguro Social, era diferente al de otras instituciones del sector público, desde su naturaleza, complejidad, tamaño, presupuesto e incluso la prestación de los servicios que brinda, así como el volumen de operaciones y transacciones, su criticidad de los procesos, así como los riesgos que se presentan en el desarrollo de sus funciones, para la atención de sus pacientes, pensionados y demás usuarios.

Por lo que es necesario que la Caja considere variables como: marco de procesos para la gestión de TI, mapeo de procesos y subprocesos de negocio, modelo de gobierno de las TIC, conformación Comités de TI, proveedores de TI, servicios de TI, inventario y criticidad de tipos documentales, centros de procesamiento y almacenamiento de datos, inventario de equipos y sistemas de información que soportan los servicios, software, proyectos de TI, planes de adquisición sobre TI, modelo de gestión de servicios, plataformas y canales electrónicos, así como los riesgos de TI.

La Ley General de Control Interno, señala en el artículo 15 Actividades de Control, 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 Manual de Organización de la Dirección de Tecnologías de Información señla en las funciones de la Subárea de Aseguramiento de la Calidad en Tecnologías de Información, entre otras, las siguientes

> *"Participar en la formulación, actualización y evaluación de la regulación, la normativa técnica, proponer los protocolos y los estándares en su ámbito de competencia, con base en la tecnología en uso y los procesos de investigación, con el propósito de lograr uniformidad en los sistemas y la maximización de los recursos institucionales…*
>
> *(…) Controlar el cumplimiento de las regulaciones en materia de calidad informática, de conformidad con las disposiciones establecidas por las entidades fiscalizadoras y la normativa a nivel interno y externo (Auditoría Interna, Contraloría General de la República y la legislación costarricense), con el propósito de contar con productos de calidad que satisfagan las necesidades de los usuarios.*

El citado Manual señala también en las funciones de la Subárea de Servicios Digitales Estratégicos, lo siguiente:

> *"Crear el ambiente tecnológico necesario, en aplicación de la normativa técnica vigente y las políticas gubernamentales para apoyar el concepto de democratización de la información y el proyecto de Gobierno Digital."*

En virtud de lo expuesto, se previene y advierte a esa Administración con el propósito de que se adopten las medidas pertinentes, a fin de contribuir con la valoración sobre el uso y aplicación del Código Nacional de Tecnologías Digitales, así como el apoyo a los procesos de adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en la institución, el cual debe ser sometido a valoración y revisión según corresponda.

Adicionalmente, es necesario considerar los aspectos indicados en este oficio en la valoración y planificación de las actividades por desarrollar para la adopción y ajustes a la normativa interna dentro del nuevo Marco Normativo de Gobierno y Gestión de las Tecnologías de Información emitidos por el MICIIT

De lo actuado se solicita informar a este Órgano de Fiscalización a efecto del seguimiento posterior que se realizará al presente oficio de advertencia.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.03.08 10:41:38 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/IMS/ghc

C. Lic. Roberto Cervantes Barrantes, gerente general - 1100
Auditoría

Referencia: ID-71702