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

ATIC-0032-2025
17 de julio de 2025

RESUMEN EJECUTIVO

El presente estudio se realizó de conformidad 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, implementación, socialización y cumplimiento del marco normativo en materia de Gobernanza y Gestión de Datos en la Caja Costarricense de Seguro Social.

Los resultados del estudio permitieron identificar debilidades que comprometen la implementación efectiva de la Política Institucional para la Gobernanza de Datos, aprobada por la Junta Directiva en abril de 2022. A pesar de su divulgación inicial, no se ha desarrollado la Agenda de Implementación, ni se han ejecutado acciones concretas por parte de las unidades responsables, lo que ha generado una desconexión entre el mandato estratégico y su aplicación práctica.

Se identificó la formulación de un proyecto de cooperación técnica con MIDEPLAN y el Banco Mundial, orientado a establecer una hoja de ruta para la gobernanza de datos, éste no incorporó desde su etapa inicial, el acuerdo de la Junta Directiva en torno a la hoja de ruta para la implementación de la Política Institucional de Gobernanza de Datos, ni contó con representación de la Gerencia General. Esta omisión podría debilitar la articulación institucional, generar duplicidad de esfuerzos y limitar la rendición de cuentas sobre el cumplimiento de los objetivos estratégicos en materia de datos.

Asimismo, se identificó la falta de implementación del Modelo de Gestión Integral para el cumplimiento de la Ley N.º 8968 sobre protección de datos personales. Aunque se desarrollaron productos claves como protocolos, convenios y plantillas, éstos no han sido formalmente adoptados, ni integrados en la gestión institucional, lo que incrementa los riesgos de incumplimientos normativos y vulneraciones a la privacidad de las personas usuarias.

El informe también evidencia debilidades en la alineación entre el Plan Estratégico Institucional (PEI) 2023–2033 y los Planes Tácticos Gerenciales. Varias gerencias no han definido objetivos, ni indicadores relacionados con las líneas de acción estratégicas sobre gobernanza de datos, ciberseguridad y analítica avanzada, lo que limita la capacidad institucional para monitorear avances, realizar ajustes y rendir cuentas de manera efectiva.

Adicionalmente, se señala la ausencia de un marco normativo integral que regule la gobernanza y gestión de datos, así como la falta de clasificación formal de los datos institucionales y de lineamientos sobre el uso de plataformas de inteligencia artificial. Estas carencias, sumadas a una gestión fragmentada de los equipos intergerenciales, debilitan el sistema de control interno y la capacidad de la CCSS para tomar decisiones informadas y proteger su información.

Finalmente, el informe destaca la falta de avances en la implementación de iniciativas de seguridad de la información y la conformación de múltiples equipos sin una estructura permanente han generado esfuerzos dispersos.

En virtud de lo expuesto, este Órgano de Fiscalización emitió conclusiones y recomendaciones, con la finalidad de que la Presidencia Ejecutiva en conjunto con el equipo definido, elabore un plan de implementación del Proyecto para la hoja de ruta de la Gobernanza de Datos, ya sea que se materialice el convenio con el Banco Mundial, o se gestione con recursos institucionales, asimismo para materializar la implementación de las iniciativas de Seguridad de la Información como componente importante de la Gobernanza de Datos, y la verificación de la implementación de las líneas de acción para el cumplimiento del objetivo 3 del Plan Estratégico Institucional que están relacionados con esta materia.

ATIC-0032-2025
17 de julio de 2025

ÁREA DE AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

AUDITORÍA DE CARÁCTER ESPECIAL REFERENTE A LA GOBERNANZA Y GESTIÓN DE DATOS EN LA CAJA COSTARRICENSE DE SEGURO SOCIAL

PRESIDENCIA EJECUTIVA 1102
GERENCIA GENERAL U.P. 1100

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo 2025 del el Área de Auditoría de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar las acciones efectuadas por la administración activa para el desarrollo, implementación, socialización y cumplimiento del marco normativo en materia de Gobernanza y Gestión de Datos en la Caja Costarricense de Seguro Social.

OBJETIVOS ESPECÍFICOS

1. Valorar los mecanismos de seguimiento, control y rendición de cuentas establecidos para la implementación y socialización de la “Política Institucional para la Gobernanza de Datos” y sus enunciados.
2. Verificar si el marco de gobernanza de los datos está alineado con los ejes estratégicos establecidos en Plan Estratégico Institucional 2023-2033.
3. Revisar las gestiones realizadas por la Gerencia General y otras unidades, para el desarrollo e implementación de un Modelo institucional de gobernanza de los datos.
4. Evaluar las gestiones realizadas por las unidades encargadas, en la emisión de lineamientos en torno a la gobernanza y gestión de datos.

ALCANCE

El estudio comprende la verificación de las acciones efectuadas por la Administración Activa en torno al desarrollo, implementación, socialización y cumplimiento del marco normativo en materia de Gobernanza y Gestión de Datos en la Institución, durante el periodo comprendido de enero de 2024 a mayo 2025, ampliándose en los casos que se estimaron necesarios.

La presente evaluación se realizó conforme a las disposiciones señaladas 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-DC-064-2014 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.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:

- Revisión y análisis de los documentos asociados a la Política Institucional de Gobernanza de Datos, Proyecto de Cooperación Técnica y Financiera no reembolsable con MIDEPLAN sobre la hoja de ruta para la Gobernanza de Datos de la CCSS, e iniciativas de Seguridad de la Información del Plan de Ciberseguridad.

- Verificación de la normativa vigente institucional en torno a la Gobernanza y Gestión de Datos, así como análisis de referencia de los marcos de trabajo COBIT 2019 en los procesos relacionados con la materia de estudio y la Guía del conocimiento para la Gestión de Datos DAMA (Data Management Body of Knowledge), DAMA-DMBOK, como un marco orientador no vinculante.

- Revisión y análisis del Plan Estratégico Institucional 2023-2033, así como los Planes Tácticos Gerenciales en torno a las actividades para el cumplimiento del objetivo 3 del PEI.

- Aplicación de instrumento de evaluación mediante herramienta Microsoft Forms a representantes de las Gerencias Médica, Financiera, Logística, Administrativa, Pensiones y de Infraestructura y Tecnología, con el fin de obtener información a nivel gerencial en torno a: estrategia y política de Gobernanza de Datos, estructura organizacional y roles en la gestión de datos, gestión de la calidad, seguridad y privacidad, ciclo de vida, interoperabilidad e integración de datos, uso de datos institucionales y otros aspectos.

- Aplicación de entrevistas a:

    - Máster Manuel Rodríguez Arce, director de CISADI y coordinador del Proyecto de Cooperación Técnica y Financiera no reembolsable con MIDEPLAN
    - Ing. Daniel Berrocal Zúñiga, jefe a.i. del área de Seguridad y Calidad Informática
    - Ing. Esteban Zamora Chaves, jefe de la Dirección de Tecnologías de Información y Comunicaciones
    - Ing. Ericka Sánchez Solís, funcionaria de la subárea de Seguridad Informática

- Solicitud de información a la Gerencia General respecto a la Agenda de Implementación de la Política Institucional de Gobernanza de Datos, y la atención del Modelo de Gestión Integral para el cumplimiento de la Ley de Protección de la Persona frente al tratamiento de sus datos personales 8968.

MARCO NORMATIVO

- Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, 8968, setiembre 2011.
- Ley General de Control Interno 8292, agosto 2002.
- Normas técnicas para la gestión y control de las tecnologías de información, MICITT, noviembre 2021.
- Guía de Formulación del Plan Táctico Gerencial, setiembre 2024.
- Política Institucional de Gobernanza de Datos, marzo 2022.
- Directriz para la gobernanza de TIC GG-DTIC-EDM01-IT002, setiembre 2020.

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 y 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 (…)"

LIMITACIONES

Mediante los oficios AI-0523-2025 del 24 de marzo de 2025 y AI-0631-2025 del 25 de abril de 2025, se solicitó información a la Dra. Jenny Madrigal Quirós, jefe de despacho de la Gerencia General, en torno a la "Política Institucional para la Gobernanza de Datos", asimismo del nivel de implementación de la Agenda establecida en atención del acuerdo segundo del artículo 5 de la sesión N°9253 de la Junta Directiva del 21 de abril de 2022, sin embargo, a la emisión del presente informe, no se obtuvo respuesta. De igual forma el 26 y 27 de marzo de 2025 se remitió instrumento de evaluación mediante herramienta Microsoft Forms a representantes de las Gerencias Médica, Financiera, Logística, Administrativa, Pensiones y de Infraestructura y Tecnología, con el fin de obtener información para el desarrollo del estudio, sin que se obtuviera información por parte de la Gerencia Financiera.

ANTECEDENTES

GOBERNANZA DE DATOS

Ante la llegada de la era digital, y con el avance acelerado de la automatización de los procesos, los diferentes entes del Estado enfrentan el reto de responder a las expectativas de una ciudadanía que exige servicios públicos más eficientes, transparentes y personalizados. En este contexto, la gobernanza de datos se convierte en la columna vertebral de un sector público moderno y basado en evidencia.

Actualmente, los datos son tan valiosos como cualquier otro recurso estratégico en una Institución. En el sector público, los datos no solo ayudan a tomar mejores decisiones, sino que también pueden mejorar la eficiencia, fomentar la transparencia y generar servicios más innovadores agregando valor Publico.

La gobernanza de datos se refiere al conjunto de reglas, estructuras, roles y procesos que permiten a las instituciones públicas gestionar, compartir, proteger y aprovechar los datos de manera estratégica. No se trata solo de tecnología, sino de liderazgo, cultura organizacional, marcos legales y capacidades humanas que aseguren que los datos se usen de forma ética, segura y útil. Involucra personas, procesos, políticas y herramientas para asegurar que los datos sean de calidad, estén protegidos, sean accesibles y se usen de manera ética y efectiva.

Una correcta gobernanza de datos es esencial para evitar que estos queden fragmentados en silos, se dupliquen esfuerzos, se tomen decisiones basadas en información incompleta o desactualizada, y se desaprovechen oportunidades de innovación. Además, en un entorno donde la ciudadanía demanda mayor transparencia y protección de sus datos personales, es imperativo que el Estado esté a la altura de estas expectativas.

Al respecto, la Organización para la Cooperación y el Desarrollo Económico (OECD por sus siglas en inglés), indica que una buena gobernanza de datos permite:

- **Anticiparse a las necesidades sociales**, planificando políticas públicas más efectivas.
- **Mejorar la entrega de servicios**, haciéndolos más rápidos, personalizados y accesibles.
- **Evaluar y monitorear el impacto de sus acciones**, promoviendo la mejora continua.
- **Fortalecer la confianza ciudadana**, al garantizar el uso ético, transparente y seguro de los datos.

La OCDE plantea que, para avanzar hacia un sector público verdaderamente basado en datos, los países deben construir un modelo integral de gobernanza que incluya:

- **Liderazgo y visión estratégica:** contar con autoridades que impulsen el uso de datos como prioridad nacional.
- **Implementación coherente:** asegurar que todas las instituciones públicas trabajen bajo un mismo marco.

- **Normas y marcos legales claros:** establecer reglas para la protección, apertura y uso compartido de datos.
- **Infraestructura de datos:** disponer de plataformas, catálogos y herramientas que faciliten el acceso y la reutilización.
- **Arquitectura de datos:** garantizar la interoperabilidad, calidad y estandarización de los datos.

Por otro lado, la Comisión Económica para América Latina y el Caribe (CEPAL), en su informe Análisis de los modelos de gobernanza de datos en el sector público "Una mirada desde Bogotá, Buenos Aires, Ciudad de México y São Paulo" emitido en el 2023, destaca tres pilares fundamentales para una buena gobernanza de datos:

1. **Un marco organizacional claro:** Esto implica tener estructuras y roles definidos, como oficinas responsables de datos, políticas públicas específicas y liderazgo institucional que impulse el uso estratégico de los datos.

2. **Integración e interoperabilidad:** Es decir, que los distintos sistemas y áreas del gobierno puedan compartir datos entre sí de forma segura y eficiente. Esto evita duplicidades, mejora la calidad de la información y permite una visión más completa para la toma de decisiones.

3. **Aspectos regulatorios:** Incluye normas sobre privacidad, seguridad, clasificación y calidad de los datos. La protección de los datos personales y la transparencia son claves para generar confianza en la ciudadanía.

ESTÁNDARES Y MARCOS DE REFERENCIA EN TORNO A LA GOBERNANZA DE DATOS

Existen varios estándares y marcos de referencia internacionales que abordan la gobernanza de datos y su gestión. Estos proporcionan directrices y mejores prácticas para la gestión efectiva y segura de los datos en una organización, entre los más relevantes se citan:

DAMA-DMBOK (Data Management Body of Knowledge)

Es un marco de referencia desarrollado por DAMA International (Data Management Association) que describe las mejores prácticas para la gestión de datos, teniendo como áreas clave: la Gobernanza de Datos, Calidad de los Datos, Gestión de Datos Maestros y de referencia, seguridad de Datos y Arquitectura de Datos.

Este Marco de Referencia profundiza en las Áreas de Conocimiento que conforman el alcance general de la gestión de Datos, por lo que ha establecido "La Rueda DAMA", colocando al Gobierno de Datos en el centro de las actividades de Gestión de Datos, ya que se requiere de un gobierno para lograr consistencia interna y equilibrio entre las funciones, tal y como se observa:

Imagen N° 1
Rueda de DAMA

Fuente: DAMA-DMBOOK Guía de Conocimiento para la Gestión de Datos

ISO/IEC 38505 - Gobernanza de datos dentro de la Gobernanza Corporativa de TI

Parte del estándar ISO 38500, enfocado en la gobernanza de TI, este conjunto de normas proporciona principios para la gobernanza de datos en un contexto organizacional, teniendo como principios clave: Responsabilidad, Estrategia, Adquisición de Datos y Gestión del Desempeño y Conformidad.

COBIT (Control Objectives for Information and Related Technologies)

Es un Marco de referencia desarrollado por ISACA para la gobernanza y gestión de TI, incluyendo aspectos relacionados con la gestión de datos, utilizado ampliamente por organizaciones para alinear los objetivos de TI con los objetivos de negocio, incluida la gestión de datos. Dicho marco incluye entre sus procesos los siguientes:

- APO014: Gestionar los Datos
- APO013: Gestionar la Seguridad
- APO011: Gestionar la Calidad

TOGAF (The Open Group Architecture Framework)

Es un marco de referencia para la arquitectura empresarial que incluye la gestión de datos como parte integral de la arquitectura de información, entre sus componentes se encuentra: la Arquitectura de Datos, Gestión de Metadatos, Integración con otros dominios de TI (aplicaciones, tecnología).

ISO/IEC 27001 e ISO/IEC 27701 - Seguridad y privacidad de los datos

Es un estándar para la gestión de la seguridad de la información, que incluye controles específicos para proteger datos sensibles y la gestión de la privacidad de la información (PII).

GOBERNANZA DE DATOS EN LA CCSS

En el artículo 14 de la sesión N° 9064 celebrada el 14 de noviembre de 2019, la Junta Directiva de la CCSS, instruyó a la Gerencia General para que conformara una comisión de alto nivel encargada de direccionar el manejo de la información de todos los sistemas institucionales, es así que a través del oficio GG-0244-2020 del 03 de febrero de 2020, la Gerencia General conformó la comisión encargada de analizar la temática y direccionar la creación de una Política Institucional para la Gobernanza de Datos.

Posteriormente, en la sesión ordinaria N° 600 del 14 de marzo de 2022 celebrada por el Consejo de Presidencia y Gerencias de la CCSS, se contó con la participación de la Coalición Costarricense de Iniciativas de Desarrollo (CINDE), en aras de que se expusiera sobre el tema de “Gobernanza de los datos”. En esta misma sesión, conforme se comunicó en el oficio PE-0768-2022 del 17 de marzo de 2022, el Consejo tomó los siguientes acuerdos:

> *“03-600-2022: Dar por recibida la presentación sobre el tema de gobernanza de datos y sus perspectivas a nivel nacional.*
>
> *04-600-2022: Reconocer lo valioso que deviene la promoción de una “Política Institucional para la Gobernanza de Datos”, al tener esta política impacto institucional.”*

El 08 de abril de 2022, mediante oficio GG-0958-2022, la Gerencia General remitió a la Presidencia Ejecutiva los documentos relacionados con la “Política institucional para la gobernanza de datos”, lo anterior, con el fin de que se pusieran en conocimiento del Consejo de Presidencia y Gerentes para su aprobación respectiva y poder continuar con el posterior trámite ante la Junta Directiva, por lo que en la sesión 603 del Consejo de Presidencia y Gerentes, celebrada el 18 de abril de 2022. Se acordó lo siguiente:

> *“a. 03-603-2022: Dar por conocida la “Política Institucional para la Gobernanza de Datos”.*

b. 04-603-2022: Solicitar a la Gerencia General gestionar la presentación de la "Política Institucional para la Gobernanza de Datos" ante Junta Directiva".

Mediante oficio GG-0981-2022 del 19 de abril de 2022, la Gerencia General remitió a la Junta Directiva los documentos relacionados con la "Política institucional para la gobernanza de datos", lo anterior, con el fin de someter a discusión la propuesta en cuestión, señalándose como propuesta de acuerdo, lo siguiente:

"PROPUESTAS DE ACUERDO:

Considerando la presentación realizada por la Gerencia General y lo expresado por el Dr. Roberto Cervantes Barrantes en el oficio GG-0981-2022, la Junta Directiva

ACUERDA:

ACUERDO PRIMERO: Dar por aprobada la "Política Institucional para la Gobernanza de Datos".

ACUERDO SEGUNDO: Instruir a la Gerencia General la elaboración de la Agenda de Implementación y desarrollar las acciones pertinentes para la implementación de la Política".

Es así como la Política Institucional para la Gobernanza de Datos fue aprobada por la Junta Directiva Institucional en el artículo 5, de la sesión N°9253 del 21 de abril de 2022, la misma pretende implementar mejores prácticas en materia de Gobierno y Gestión de Datos, optimizar el uso de los recursos disponibles y ampliar la perspectiva del potencial institucional mediante la investigación, desarrollo e innovación, lo anterior mediante la definición de 7 enunciados relacionados con los siguientes temas:

Imagen N° 2
Tópicos de los 7 enunciados de la Política Institucional de Datos
CCSS
2022

Fuente: Elaboración propia

PROYECTO DE COOPERACIÓN TÉCNICA Y FINANCIERA NO REEMBOLSABLE CON MIDEPLAN PARA LA HOJA DE RUTA PARA LA GOBERNANZA DE DATOS DE LA CCSS

El 5 de noviembre de 2024, mediante oficio sin número, la Señora Carine Clert, Gerente de país del Banco Mundial para El Salvador y Costa Rica, le informó al Señor Nogui Acosta Jaén, ministro de Hacienda, que en seguimiento a las conversaciones sostenidas durante las reuniones anuales pasadas en Washington sobre la Asistencia Técnica que el Banco Mundial puede ofrecer en el tema de "Uso Estratégico de datos e Información en la CCSS", en julio de 2024, el “Mecanismo de Asociación Corea - Banco Mundial”, aprobó fondos de donación para que dicha Organización pueda apoyar el "Uso Estratégico de datos e Información de la CCSS". Este Mecanismo tiene como objetivo apoyar a los países miembros del Banco Mundial en la consecución de un crecimiento económico inclusivo y sostenible, con la oportunidad de adaptar y aplicar la experiencia y los conocimientos técnicos de la República de Corea.

Los componentes incluidos en la iniciativa, de acuerdo con lo informado por el Banco Mundial son los siguientes:

1. **Compras estratégicas para la sostenibilidad financiera.** Este componente busca reforzar la capacidad de la CCSS de utilizar la información en forma estratégica para mejorar la asignación de recursos, garantizando así efectividad, equidad, rentabilidad y la sostenibilidad institucional a largo plazo. Incluye la elaboración de informes técnicos para orientar a Costa Rica en el financiamiento estratégico y sostenible de la atención de salud, como también talleres de intercambio de conocimiento con entidades coreanas que faciliten la implementación de las recomendaciones que puedan emerger de la asistencia.

2. **Uso de datos para mejorar la prestación de servicios de salud centrados en las personas.** Este componente busca fortalecer la producción y uso de datos en la CCSS para informar ajustes en los modelos de prestación de servicios, respondiendo a las necesidades cambiantes de la población costarricense, optimizando a su vez la gestión de costos. Como producto de la asistencia técnica se incluirá notas de política orientadas a la institucionalización de las redes integradas de salud, la adaptación del modelo de salud a los cambios demográficos y epidemiológicos, y recomendaciones para el uso de modelos predictivos que optimicen la atención de las enfermedades crónicas.

3. **Gobernanza de datos para mejorar el desempeño del sistema de salud.** Este componente proporcionará a la CCSS una evaluación de la madurez de los datos y una hoja de ruta para mejorar su gobernanza, basada en mejores prácticas internacionales y la experiencia de Corea. Mediante la implementación de mejores marcos de gobernanza de datos, la CCSS podrá avanzar en la utilización de los mismos para la toma de decisiones en el ámbito financiero y de prestación de servicios.

Posteriormente, el 20 de enero de 2025, mediante oficio MH-DM-OF-0051-2025, el Sr. Luis Antonio Molina Chacón, ministro de Hacienda a.i. y el Sr. Ariel Barrantes Soto, director General de Gestión de Deuda Pública, le responden a la Sra. Clarine Clert, Gerente de País el Salvador y Costa Rica del Banco Mundial, señalando que la asistencia técnica se alinea con los objetivos estratégicos institucionales y nacionales de sostenibilidad financiera de la CCSS, sin embargo se debe cumplir con la normativa sobre cooperaciones no reembolsables establecida en el Decreto Ejecutivo N°43951-PLAN-RE emitido por el MIDEPLAN a través de la Presidenta Ejecutiva de la CCSS, Sra. Mónica Taylor como punto focal, por lo que dicho Ministerio es el encargado de aprobar los proyectos de cooperación no reembolsables, para lo cual las instituciones públicas deben remitir una solicitud de aprobación al Área de Cooperación Internacional, por lo que una vez el proyecto tenga la aprobación del MIDEPLAN, el Ministerio de Hacienda realizará las gestiones necesarias de formalización de la cooperación técnica ante el Banco Mundial.

Por lo anterior, mediante oficio PE-0239-2025 del 28 de enero de 2025, la Presidencia Ejecutiva de la CCSS, solicitó al Dr. Juan Carlos Esquivel Sánchez, director del CENDEISSS y a la Ing. Susan Peraza Solano, directora de Planificación Institucional, colaboración para gestionar ante el MIDEPLAN los requerimientos para formalizar la asistencia técnica propuesta por el Banco Mundial en el tema de uso estratégico de datos e información en la CCSS, informando posteriormente mediante oficio PE-1061-2025 del 13 de marzo de 2025, que para apoyar dicha gestión se designó como enlace de la Presidencia a la Lcda. Carolina Gallo Chaves, asesora del Despacho

de la Presidencia Ejecutiva, y al Ing. Manuel Rodríguez Arce, coordinador del CISADI, como enlace técnico, debiendo remitir la información correspondiente del proyecto a más tardar el 17 de marzo de 2025.

PRODUCTOS DE AUDITORÍA RELACIONADOS CON LA GOBERNANZA DE DATOS

La Auditoría Interna en temas relacionados con la Gobernanza de Datos, así como en los componentes relacionado con la gestión de éstos, ha emitido en los últimos 7 años diversos productos donde se abordan además, aspectos de protección de la información personal y la seguridad institucional, identificando riesgos éticos y de gobernanza en el uso de tecnologías como la inteligencia artificial, así como debilidades en la trazabilidad, acceso y cultura organizacional respecto al manejo de datos personales. También se destacan aspectos de mejora en la infraestructura tecnológica, la ciberseguridad y el cumplimiento normativo, especialmente en relación con la Ley 8968. En general, los informes subrayan la necesidad de establecer modelos integrales de gestión, fortalecer la infraestructura TIC, actualizar la normativa institucional, implementar medidas de seguridad alineadas con la legislación vigente y promover una cultura organizacional basada en el riesgo y la capacitación continua, tal y como se observa:

Tabla N° 1
Resumen de Productos de Auditoría relacionados con Gobernanza y Gestión de Datos
Auditoría Interna CCSS
2018 - 2025

Nº DE PRODUCTO	FECHA DEL PRODUCTO	ASPECTOS EVIDENCIADOS	RECOMENDACIONES EMITIDAS
AS-ATIC-0010-2025 Oficio de asesoría respecto al uso responsable de la Inteligencia Artificial en el sector salud y pensiones	11 febrero 2025	Se identificaron riesgos éticos y de gobernanza. Se abordaron temas de gobernanza de datos, destacando la necesidad de lineamientos claros y éticos.	Establecer lineamientos éticos y técnicos para el uso de IA en salud.
AS-ATIC-0021-2024 Oficio de Asesoría referente a la sensibilización del manejo de datos personales en el Expediente Digital Único en Salud	12 marzo 2024	Riesgos en acceso y trazabilidad de datos clínicos. Se abordaron temas de gobernanza de datos, enfatizando la importancia de controles de acceso y trazabilidad.	Fortalecer controles de acceso, trazabilidad y capacitación en protección de datos.
AS-AATIC-168-2022 Oficio de Asesoría sobre la protección de datos adaptable al riesgo con un enfoque basado en el comportamiento	17 agosto 2022	Se evidenciaron debilidades en cultura organizacional. Se abordaron temas de gobernanza de datos, sugiriendo un modelo basado en riesgos.	Implementar modelo de protección de datos basado en riesgos y comportamiento.
AS-AATIC-107-2022 Oficio de Asesoría referente al tratamiento de los datos personales y medidas de seguridad	22 junio 2022	Falta de medidas de seguridad robustas. Se abordaron temas de gobernanza de datos, destacando la necesidad de mejorar la ciberseguridad.	Reforzar medidas de ciberseguridad y protocolos de respuesta ante incidentes.
ATIC-34-2020 Evaluación de carácter especial referente al análisis de datos a nivel institucional mediante soluciones	7 mayo 2020	Uso limitado en niveles estratégicos. Falta de integración y gobernanza. Se abordaron temas de gobernanza de datos,	Potenciar BI institucional, definir gobernanza de datos y mejorar interoperabilidad.

Nº DE PRODUCTO	FECHA DEL PRODUCTO	ASPECTOS EVIDENCIADOS	RECOMENDACIONES EMITIDAS
de Inteligencia de Negocios y Big Data		sugiriendo la necesidad de una mejor integración.	
2 9 2 Oficio sobre aspectos relacionados con seguridad de la información.	15 febrero 2019	Falta de modelo integral y cumplimiento parcial de Ley 8968. Se abordaron temas de gobernanza de datos, destacando la necesidad de un modelo integral.	Establecer modelo integral de seguridad y reforzar cumplimiento normativo.
1 1 0 6 9 Oficio de información sobre aspectos relacionados con la Seguridad de la Información Institucional.	20 diciembre 2018	Riesgos en infraestructura TIC y gobernanza débil. Se abordaron temas de gobernanza de datos, sugiriendo mejoras en la infraestructura.	Fortalecer infraestructura TIC y gobernanza de seguridad de la información.
ATIC-83-2018 Evaluación de Carácter Especial referente al cumplimiento de la Ley No. 8968 Protección de la Persona frente al tratamiento de sus datos personales en la CCSS	27 de julio de 2018	- Ausencia de un modelo de gestión integral para el tratamiento y protección de datos personales. - Falta de instancias institucionales con roles y responsabilidades claras. - No existe un inventario unificado de bases de datos con datos personales. - Bases de datos no clasificadas adecuadamente según su uso interno o externo. - Solo una base de datos inscrita ante la PRODHAB. - Medidas de seguridad no alineadas con la Ley 8968. - Normativa institucional desactualizada y no alineada con la ley. - Capacitación insuficiente al personal sobre protección de datos. - Prácticas institucionales que incumplen la normativa, como publicación de cédulas y uso de WhatsApp para compartir datos sensibles.	- Crear una comisión institucional para definir un modelo de gestión integral. - Elaborar un inventario institucional de bases de datos con datos personales. - Clasificar las bases de datos y designar formalmente responsables. - Inscribir las bases de datos ante la PRODHAB según corresponda. - Establecer medidas de seguridad conforme a la Ley 8968. - Actualizar la normativa institucional. - Implementar un plan de capacitación periódica. - Emitir directrices para eliminar prácticas que incumplen la ley

Fuente: Auditoría Interna, CCSS.

HALLAZGOS

1. SOBRE LA IMPLEMENTACIÓN DE LA POLÍTICA INSTITUCIONAL PARA LA GOBERNANZA DE DATOS EN LA CCSS

Se identificó que la Institución no ha implementado la Política Institucional para la Gobernanza de Datos aprobada por la Junta Directiva en el artículo 5, de la sesión N°9253 del 21 de abril de 2022, en la cual mediante acuerdo segundo se instruyó a la Gerencia General elaborar la Agenda de Implementación y desarrollar las acciones pertinentes para la ejecución de la Política.

Si bien la Política Institucional para la Gobernanza de Datos fue aprobada por la Junta Directiva y esta fue divulgada por correo electrónico mediante oficio GG-1128-2022 del 5 de mayo de 2022, suscrita por el Dr. Roberto Cervantes Barrantes, gerente General en ese entonces, esta Auditoría no tuvo acceso a evidencia sobre el desarrollo de la Agenda de Implementación instruida por el Órgano Colegiado de la Institución, asimismo de acuerdo con lo señalado por las Gerencias de la Institución, solo se procedió con la divulgación sin que se definiera un mecanismo formal para la implementación en estas unidades.

La Política Institucional para la Gobernanza de Datos GG-PO-001, en su apartado 9 “Enunciados”, indica:

> *“**Enunciado 1***
>
> *La Caja Costarricense de Seguro Social contará con una gobernanza de datos que promoverá su uso eficiente en cumplimiento del marco normativo aplicable; a partir de la cual se fortalezca la toma de decisiones en los diferentes niveles organizacionales y se potencie la investigación y desarrollo.*
>
> *(…)*
>
> ***Enunciado 7***
>
> *La Caja Costarricense de Seguro Social garantizará la implementación, seguimiento y control de la “Política Institucional para la Gobernanza de Datos” y su agenda de implementación, promoviendo la mejora continua, la socialización de los resultados y la rendición de cuentas a través de la Gerencia General o de la unidad que esta designe”.*

La Directriz para la Gobernanza de TIC GG-DTIC-EDM01-IT002, emitida por la Dirección de Tecnologías de Información y Comunicaciones y aprobada por Junta Directiva el 29 de abril de 2021, en su apartado 9 “Directrices sobre la Gestión de la Información” establece que:

> ***“9.2 Los datos transaccionales y la información de los procesos de negocio que se deriva de ellos, son activos valiosos para la CCSS.***
>
> *Las áreas de negocio son las encargadas de los datos, los cuales son indispensables para sustentar las operaciones y los procesos de toma de decisiones de la CCSS, adicionalmente, su disponibilidad y calidad impacta directamente en el servicio a los clientes y la atención de normativas y regulaciones externas. Por lo tanto, deben ser tratados como todo activo, deben ser inventariados, protegidos y administrados por un responsable de su aprovechamiento y correcto uso.*
>
> ***9.2.1 Mecanismos***
>
> *Se identificarán las entidades de información y los datos que las componen, así como un esquema de priorización de la información por parte del Negocio, en el cual se establezca la criticidad de los elementos de datos identificados”.*

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en su apartado V. Arquitectura Empresarial señala:

"La Institución debe disponer de prácticas formales que permitan gestionar la arquitectura empresarial orientada la gestión de los procesos institucionales para promover la implementación de la estrategia organizacional, en el que se establezca la ***identificación formal de la estructura de datos clasificada según su nivel de criticidad y uso****, la asociación de los procesos institucionales, de acuerdo con el uso de recursos tecnológicos (sistemas de información e infraestructura) para acceder, procesar y almacenar los datos e información.*

La entidad debe contar con un modelo de arquitectura que permita visualizar adecuadamente la estructura de procesos institucionales y la relación de uso de recursos instalados (sistemas de información, infraestructura tecnológica) ***para gestionar los datos e información requeridos en la operativa****". (La negrita no es del original)*

El 16 de setiembre de 2024, mediante oficio GG-1614-2024, la MBA. Vilma Campos Gómez, Gerente General a.i. en ese momento, le indicó al cuerpo Gerencial, así como a los directores del CISADI, CENDEISS, DTIC y Planificación Institucional, que, con el propósito de retomar la agenda y el desarrollo de acciones pertinentes para la implementación de la Política, agradecía remitir al 21 de setiembre 2024, el nombre de la persona designada por cada unidad para dicha implementación, señalando que estas debían conocer el negocio o procesos de la unidad.

Al respecto, las unidades respondieron el oficio GG-1614-2024, quedando asignados los siguientes funcionarios:

Tabla N° 2
Designación de funcionarios por unidades para retomar la implementación de la Política Institucional para la Gobernanza de Datos
CCSS
Setiembre – octubre 2024

N° DE OFICIO	UNIDAD	FECHA	PERSONA DESIGNADA
PE-DPI-1005-2024	Dir. Planificación Ins.	03 de octubre de 2024	Luis Diego Sandoval Salas
GA-1782-2024	Gerencia Administrativa	18 de setiembre de 2024	Roger Muñoz Díaz
GIT-1479-2024	Ger. Infraestructura y Tec.	27 de setiembre de 2024	Giovanni Campos Alvarado
GF-3506-2024	Gerencia Financiera	26 de setiembre de 2024	Cindy Madrigal Jiménez
GG-DTIC-5829-2024	Dir. Tecnologías y Comunic.	18 de setiembre de 2024	Esteban Zamora Chaves
GL-1884-2024	Gerencia de Logística	19 de septiembre de 2024	Paula Ballestero Murillo
GM-CENDEISSS-1020-2024	CENDEISSS	18 de setiembre del 2024	Sofia Carvajal Chaverri
GP-1518-2024	Gerencia de Pensiones	18 de setiembre de 2024	Marco González Jiménez

Fuente: Elaboración propia con los oficios indicados.

No obstante, a pesar de la conformación del equipo en mención, no consta en el Sistema Gestor de Seguimiento y Control (GESC), que se hayan desarrollado actividades para dar cumplimiento a lo instruido por la Junta Directiva, por lo que es criterio de esta Auditoría que la ausencia de una dirección adecuada, definición clara de las actividades a realizar y un seguimiento oportuno, ha generado entre otras causas, que la Institución no haya implementado la Política Institucional para la Gobernanza de Datos

Al consultarles a los representantes de las Gerencias asignados para la atención del presente estudio, respecto a la socialización de la Política Institucional para la Gobernanza de Datos, indicaron:

*"**Giovanni Francisco Campos Alvarado, GIT:** Se recibió oficio de comunicación mediante la Web Master. La Gerencia de Infraestructura y Tecnologías (GIT) la comunicó a lo interno de sus unidades en mayo del 2022 y actualmente, la Política se encuentra en el repositorio normativo de la gerencia para consulta de sus funcionarios.*

***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** La "Política Institucional para la Gobernanza de Datos" fue comunicada mediante publicación Webmaster de fecha 05 de mayo de 2022, por oficio GG-1128-2022, sin embargo, a la fecha no se tiene conocimiento de la agenda de implementación para la citada Política, de acuerdo con el artículo 5° de la sesión N° 9253, celebrada el*

21 de abril de 2022, Acuerdo Segundo, que cita: "Instruir a la Gerencia General la elaboración de la Agenda de Implementación y desarrollar las acciones pertinentes para la implementación de la Política".

***Leslie Vargas Vásquez, Gerencia Médica:** Únicamente se dio a conocer por medio de la WebMaster, pero no se conocen actividades específicas para socialización de la política.*

***Johanna Mora Ulate, Gerencia de Pensiones:** Según los registros de este Despacho, no se ha recibido de manera formal el acuerdo con la aprobación de la Política, sin embargo, mediante oficio GG-1614-2024 la Gerencia General solicitó designar a una persona para continuar con el proceso de la agenda de implementación y el desarrollo de acciones".*

La falta de implementación de la Política Institucional para la Gobernanza de Datos podría generar debilidades en la gestión y control de los datos institucionales. Al respecto, la ausencia de una Agenda de Implementación y de acciones concretas por parte de las dependencias a cargo, limita la capacidad de las unidades organizativas para establecer mecanismos formales que garanticen el cumplimiento de los principios de gobernanza de datos, traduciéndose en riesgos operativos, estratégicos y de cumplimiento normativo, al no contar con lineamientos claros para la administración, calidad, seguridad y uso ético de la información institucional.

2. SOBRE LA GESTIÓN DEL PROYECTO "HOJA DE RUTA PARA LA GOBERNANZA DE DATOS DE LA CCSS" GESTIONADO CON EL MINISTERIO DE PLANIFICACIÓN (MIDEPLAN)

Se identificó que la Presidencia Ejecutiva de la CCSS gestiona actualmente, una iniciativa denominada: *"Proyecto de Cooperación Técnica y Financiera no Reembolsable con MIDEPLAN para la Hoja de Ruta sobre la Gobernanza de Datos de la CCSS"*. No obstante, en su fase inicial, dicho proyecto no contempla la incorporación del acuerdo segundo del artículo 5 de la sesión N.° 9253 del 21 de abril de 2022, mediante el cual la Junta Directiva aprobó la Política Institucional para la Gobernanza de Datos e instruyó a la Gerencia General, la elaboración de su Agenda de Implementación. Asimismo, se evidenció que en el equipo conformado para la formulación de esta propuesta no se incluyó representación de la Gerencia General, lo que podría limitar la alineación del proyecto con los mandatos estratégicos institucionales.

El 13 de mayo de 2025, se firmó por parte del Dr. Juan Carlos Esquivel Sánchez, Licda. Carolina Gallo Chaves, Ing. Manuel Arce Rodríguez, e Ing. Susan Peraza Solano, como equipo conformado por la Presidencia Ejecutiva, el *"Instrumento de Formulación de Proyectos de Cooperación Internacional Técnica y Financiera no Reembolsable, con Fuentes Cooperantes Bilaterales y Multilaterales"*, con el nombre oficial del proyecto: *"Uso Estratégico de Datos e Información en la Caja Costarricense de Seguro Social (CCSS)"*, en el cual se identificaron las oportunidades de mejora señaladas.

El artículo 5, de la sesión N°9253 de la Junta Directiva de la CCSS, del 21 de abril de 2022 establece:

"Por tanto, considerando la presentación realizada por la Gerencia General y lo expresado por el Dr. Roberto Cervantes Barrantes en el oficio GG-0981-2022, la Junta Directiva -en forma unánime-

ACUERDA:

***ACUERDO PRIMERO:** Dar por aprobada la "Política Institucional para la Gobernanza de Datos".*

***ACUERDO SEGUNDO:** Instruir a la Gerencia General la elaboración de la Agenda de Implementación y desarrollar las acciones pertinentes para la implementación de la Política".*

La Política Institucional para la Gobernanza de Datos GG-PO-001, en su enunciado 7 señala:

"La Caja Costarricense de Seguro Social garantizará la implementación, seguimiento y control de la "Política Institucional para la Gobernanza de Datos" y su agenda de implementación, promoviendo la

mejora continua, la socialización de los resultados y la rendición de cuentas a ***través de la Gerencia General o de la unidad que esta designe****".* (La negrita no es del original)

Las Normas de Control Interno para el Sector Público en su apartado 1.8 "Contribución del SCI al gobierno corporativo" establece:

> *"El SCI debe contribuir al desempeño eficaz y eficiente de las actividades relacionadas con el gobierno corporativo, considerando las normas, prácticas y procedimientos de conformidad con las cuales la institución es dirigida y controlada, así como la regulación de las relaciones que se producen al interior de ella y de las que se mantengan con sujetos externos".*

Al respecto, el Ing. Manuel Arce Rodríguez, Coordinador del CISADI y del proyecto de Cooperación Técnica y Financiera no reembolsable con MIDEPLAN para la hoja de ruta para la Gobernanza de Datos de la CCSS, indicó:

> *"El apoyo que se busca a través del Banco y las diferentes instancias, es que se defina ese nivel de madurez y esa hoja de ruta, dentro de ese análisis lo que se ha planteado es que haya que pasar por esa etapa diagnóstica, con esto se debe de considerar todos los elementos, y la Política evidentemente es uno de los elementos claves, que si bien es cierto la Política aún no tiene fecha de implementación, si es uno de los elementos que se estarían incorporando para que se analicen, de cara a la implementación de la hoja de ruta.*
>
> *Hay una designación precisamente para la formulación del proyecto, pero si hay una claridad, ya para cuando inicie eventualmente el proceso, deben de incorporarse los diferentes actores que conforman los diferentes roles Institucionales, la designación es para la formulación, pero si eventualmente cuando entremos en la cooperación, hay que incorporar diferentes roles con base en el alcance del proyecto y establecer los diferentes equipos de trabajo".*

La falta de integración del acuerdo segundo del artículo 5 de la sesión N.° 9253 de la Junta Directiva de la CCSS, que instruía a la Gerencia General la elaboración de la Agenda de implementación de la Política Institucional de Gobernanza de Datos en la formulación inicial del proyecto "Uso Estratégico de Datos e Información en la Caja Costarricense de Seguro Social (CCSS)", gestionado por la Presidencia Ejecutiva con apoyo del Banco Mundial y MIDEPLAN, podría generar una desconexión entre las iniciativas estratégicas institucionales y los mandatos del máximo órgano colegiado. Esta omisión, sumada a la ausencia de representación de la Gerencia General en el equipo integrado para la formulación del proyecto, podría debilitar la gobernanza institucional sobre el uso estratégico de los datos. Además, compromete la articulación y seguimiento de la Agenda, lo cual puede generar duplicidad de esfuerzos, pérdida de sinergias y una limitada rendición de cuentas sobre el cumplimiento de los objetivos estratégicos en materia de datos.

3. OPORTUNIDADES DE MEJORA IDENTIFICADAS EN LA FORMULACIÓN DEL PROYECTO "HOJA DE RUTA PARA LA GOBERNANZA DE DATOS DE LA CCSS" GESTIONADO CON EL MIDEPLAN

Se evidenciaron oportunidades de mejora en la formulación del *"Proyecto de Cooperación Técnica y Financiera no reembolsable con MIDEPLAN para la hoja de ruta para la Gobernanza de Datos de la CCSS",* que deben ser considerados en la eventual planificación y ejecución del proyecto, ya que en esa fase inicial se omitieron aspectos como los siguientes:

a) No se aclara si el proyecto debe ser aprobado por la Junta Directiva de la CCSS y quién será la autoridad Institucional para suscribir el acuerdo, considerando que el Banco Mundial como ente externo, tiene entre sus responsabilidades: desarrollar evaluaciones técnicas en las tres áreas del proyecto, elaborar la hoja de ruta para la Gobernanza de Datos y documentos técnicos para la Institucionalización y acompañar metodológicamente las pruebas de concepto y apoyar el monitoreo y evaluación del proyecto, asimismo de que no se trata de una donación si no de una cooperación técnica y financiera.

b) El presupuesto total del proyecto es de $1,411,550 USD, con un aporte del Banco Mundial de $1,372,700 USD y un aporte institucional (CCSS) de $38,850 USD, sin identificarse ni consignarse en el documento la fuente y unidad de donde provendrían los recursos Institucionales.

c) Aunque el proyecto reconoce la necesidad de una Gobernanza de Datos Institucional, el enfoque operativo y técnico se centra en los sistemas clínicos (EDUS, SIAC, SIES, SIVA, SIOS, AppEdus, ARCA) y en la parte financiera mediante el SICERE, no se incluye en la formulación, procesos y sistemas concernientes a la Gerencia de Pensiones, Recursos Humanos, Plan de Innovación, entre otros que sean considerados importantes por la Administración.

d) No se define el nivel de acceso a los datos que tendrían los entes externos participantes del proyecto, considerando que entre las responsabilidades de las unidades de la CCSS involucradas se le asignan a la Gerencia Médica incorporar datos clínicos y modelos predictivos en los procesos asistenciales, la Gerencia de Logística apoyando con datos clave para la programación logística, compras y análisis de costos institucionales y al área de Estadísticas en Salud facilitar el acceso a datos provenientes del EDUS y otros sistemas clínicos.

e) Si bien se presenta un presupuesto total del proyecto, no se vinculan claramente los montos con productos o entregables específicos por componente.

f) No se definen indicadores cuantificables de impacto, ni línea base para medir avances en la ejecución del proyecto.

Respecto a la autoridad Institucional que debe firmar el acuerdo de Cooperación, la Dirección Jurídica en el análisis efectuado para un caso de similitud naturaleza, mediante oficio GA-DJ-07274-2021 del 22 de octubre de 2021, suscrito por la Licda. Mariana Ovares Aguilar, jefe a.i. del área de Asistencia Técnica y Asistencia Jurídica, y el Lic. Ricardo E. Luna Cubillo, abogado, indicó:

> *"Al no estar en presencia de una donación propiamente, sino, ante un convenio de cooperación internacional técnica, no resulta procedente acudir al procedimiento sobre el trámite de las intenciones de donación y donaciones en sí a favor de la Caja Costarricense de Seguro Social, regulado en el referido Reglamento para la tramitación de donaciones a favor de la Caja Costarricense de Seguro Social, siendo lo procedente acudir al "Procedimientos para la Aprobación de Programas, Proyectos y Otras Acciones de Cooperación Internacional Técnica y Financiera No Reembolsable", contenido en el "Reglamento del Artículo 11 de la Ley de Planificación Nacional No. 5525 del 2 de Mayo de 1974" (…).*
>
> *(…) lo procedente es que el convenio de cooperación sea sometido al conocimiento y aprobación de la Junta Directiva y a su vez, que el máximo órgano tome el respectivo acuerdo en relación con la autoridad que lo suscribirá, ya sea el Presidente Ejecutivo, o bien, los Gerentes respectivos, toda vez que ostentan facultades de Apoderado Generalísimo sin límite de suma de conformidad con el artículo 1253 del Código Civil de Costa Rica".*

La Política Institucional para la Gobernanza de Datos GG-PO-001, en su enunciado 2 señala:

> *"La Caja Costarricense de Seguro Social asegurará una gestión ética, segura y confiable de los datos albergados en sus bases institucionales, manteniendo un balance entre la privacidad y utilidad de estos.*

Las Normas de Control Interno para el Sector Público en su apartado 2.5.2 "Autorización y aprobación" establece:

> *"La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales".*

En el apartado 4.5.5 “Control sobre bienes y servicios provenientes de donantes externos”, de la misma norma señala:

> *“El jerarca y los titulares subordinados, según sus competencias, deben establecer, mantener, perfeccionar y evaluar las actividades de control necesarias en relación con los bienes y servicios provenientes de donantes externos, sean estos obtenidos bajo la modalidad de donación**, cooperación técnica o cooperación financiera no reembolsable**. Lo anterior, de manera que sobre esos bienes o servicios se ejerzan los controles de legalidad, contables, financieros y de eficiencia que determina el bloque de legalidad.*
>
> *Como parte del control ejercido, deben velar porque tales bienes y servicios cumplan con la condición de satisfacer fines públicos y estén conformes con los principios de transparencia, rendición de cuentas, utilidad, razonabilidad y buena gestión administrativa”.* **(La negrita no es del original)**

Asimismo, en el apartado 4.5.2 “Gestión de Proyectos”, señala:

> *“El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes.*
> *Las actividades de control que se adopten para tales efectos deben contemplar al menos los siguientes asuntos:*
>
> > *a. La identificación de cada proyecto, con indicación de su nombre, sus objetivos y metas, recursos y las fechas de inicio y de terminación.*
> > *b. La designación de un responsable del proyecto con competencias idóneas para que ejecute las labores de planear, organizar, dirigir, controlar y documentar el proyecto.*
> > *c. La planificación, la supervisión y el control de avance del proyecto, considerando los costos financieros y los recursos utilizados, de lo cual debe informarse en los reportes periódicos correspondientes. Asimismo, la definición de las consecuencias de eventuales desviaciones, y la ejecución de las acciones pertinentes.*
> > *d. El establecimiento de un sistema de información confiable, oportuno, relevante y competente para dar seguimiento al proyecto.*
> > *e. La evaluación posterior, para analizar la efectividad del proyecto y retroalimentar esfuerzos futuros”.*

Al respecto, el Ing. Manuel Arce Rodríguez, Coordinador del CISADI y del proyecto de Cooperación Técnica y Financiera no reembolsable con MIDEPLAN para la hoja de ruta para la Gobernanza de Datos de la CCSS, indicó:

> *“Hay una designación precisamente para la formulación del proyecto, pero si hay una claridad, ya para cuando inicie eventualmente el proceso, deben de incorporarse los diferentes actores que conforman los diferentes roles Institucionales, la designación es para la formulación, pero si eventualmente cuando entremos en la cooperación, hay que incorporar diferentes roles con base en el alcance del proyecto y establecer los diferentes equipos de trabajo. (…)*
>
> *Ahorita, es un proyecto de cooperación, sigue todo un flujo establecido para desarrollarlo, bajo ese flujo tenemos que esperar la aprobación formal, y eventualmente lo que se quiere es que cuando tengamos una aprobación del Banco y todas las instancias, sentarnos a aclarar ese alcance, en la identificación se tienen los elementos base, pero si ya cuando tengamos una aprobación, hay que sentarse a acotar alcance y definir elementos de planificación, ya no solo de formulación. (…)*
>
> *Una vez aprobado la formulación, había que entrar en un plan de proyecto con todo ese detalle. El banco establece su contraparte, seleccionan sus socios, y viene un tema de planificación detallada de la cooperación técnica”.*

Respecto a la inclusión de los datos referente a la Gerencia de Pensiones, indicó:

> *"Si, ese ha sido un tema que también se aclaró, la idea es que sea un Modelo de Datos Institucional, donde eventualmente las áreas de alcance lo abarquen, incluso se menciona un tema de logística, la idea es que sea un Modelo Institucional.*
>
> *Pueda que no quedara explícitamente en el documento, pero si la idea es que precisamente si se vea, se habla de datos de la Caja, no se está excluyendo ningún proceso".*

La omisión de aspectos clave como la definición de la autoridad institucional responsable de suscribir el acuerdo, la falta de claridad sobre la aprobación por parte de la Junta Directiva, la ausencia de una fuente identificada para el aporte institucional, y la exclusión de procesos relevantes como los de la Gerencia de Pensiones, Recursos Humanos, Plan de Innovación, comprometen la alineación del proyecto con el marco normativo y estratégico de la CCSS. Además, la no delimitación del acceso a los datos por parte de entes externos, la falta de vinculación entre presupuesto y productos, y la ausencia de indicadores cuantificables e información de línea base, limitan la capacidad de control, seguimiento y evaluación del proyecto, que podrían debilitar la gobernanza institucional sobre los datos y se incrementa el riesgo de una implementación fragmentada, sin una visión integral ni mecanismos efectivos de control y evaluación.

4. RESPECTO A LA EJECUCIÓN DEL MODELO DE GESTIÓN INTEGRAL PARA EL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES 8968 Y SU REGLAMENTO

4.1 IMPLEMENTACIÓN DEL MODELO DE GESTIÓN INTEGRAL PARA EL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

Se determinó que el Modelo de Gestión Integral para el cumplimiento de la Ley de Protección de la Persona frente al tratamiento de sus Datos Personales 8968 y su reglamento, formulado a partir de las recomendaciones emitidas en el informe de Auditoría ATIC-083-2018, no ha sido implementado. Dicho modelo contiene componentes que son fundamentales para una adecuada Gobernanza y Gestión de Datos.

Sobre lo anterior, el 27 de julio de 2018, la Auditoría Interna remitió el informe ATIC-083-2018 *"Evaluación de carácter especial referente al cumplimiento de la Ley N° 8968 Protección de la persona frente al tratamiento de sus datos personales en la Caja Costarricense de Seguro Social (CCSS)"*, recomendando a la Presidencia Ejecutiva, adoptar las acciones concretas para la atención de las recomendaciones de dicho informe, conformando para los efectos una Comisión Institucional integrada por representantes de ese nivel jerárquico, las gerencias institucionales, Dirección de Tecnologías de Información y Comunicaciones en su función de Asesoría técnica y demás instancias que se estimaran pertinentes. Esta Comisión fue conformada por los siguientes funcionarios:

- Ing. Roger Muñoz Díaz, Coordinador comisión, Gerencia Administrativa
- Ing. Ronald Guzmán Vásquez, representante Gerencia Médica
- Lic. Eithel Corea Baltodano, Gerencia de Pensiones (Representado por el Ing. Mario Villalobos Marín)
- Licda. Vanessa Carvajal Carmona, representante Gerencia de Infraestructura y Tecnologías
- Ing. Manuel Castro Villalobos, representante Gerencia Financiera
- Ing. Roy Armando Ovares Valerio, representante Gerencia de Logística
- Licda. Maleydis Figueroa Paiz, representante Dirección de Sistemas Administrativos
- Licda. Giselle Tenorio Chacón, representante Gerencia Administrativa

La Comisión desarrolló acciones al respecto, emitiendo las siguientes propuestas de productos:

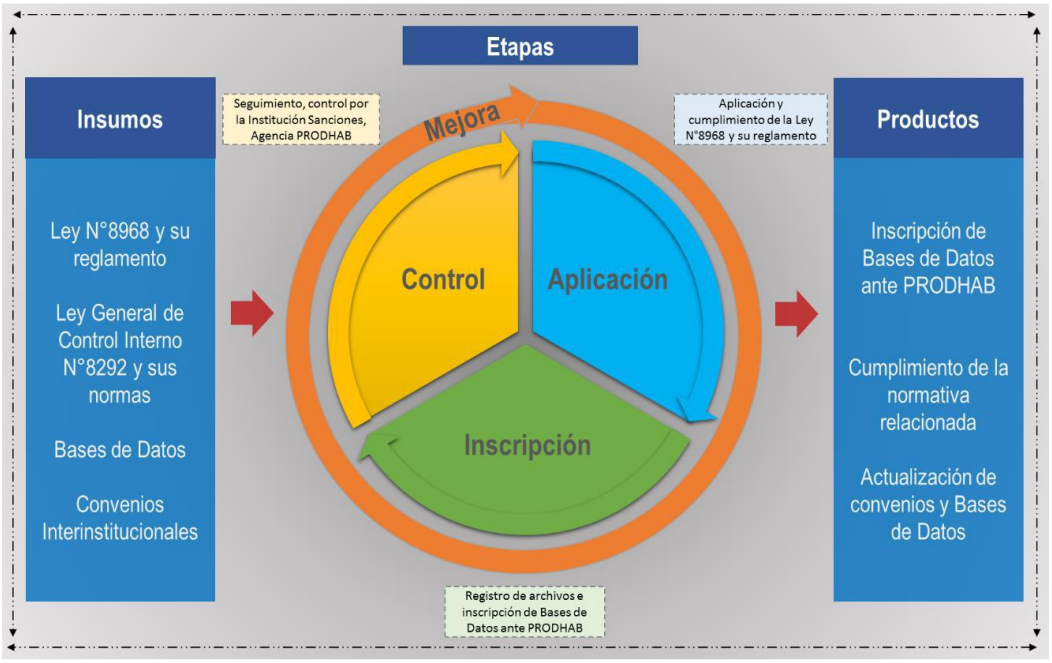
Tabla N° 3
Productos entregados por parte de la Comisión Interinstitucional para diseñar el Modelo de Gestión Integral para el cumplimiento de la Ley de Protección de la Persona frente al tratamiento de sus Datos Personales
octubre 2019

PRODUCTO	DETALLE DE PRODUCTO
Protocolo para la Protección de documentos de identificación en los Establecimientos de la CCSS	En el Protocolo para la Protección de documentos de identificación en los Establecimientos de la CCSS, se expone la normativa relacionada y se propone el proceso a seguir en caso de documentos de identificación que se extravían en los Establecimientos de la CCSS y el cumplimiento de las acciones para la protección de los datos personales.
Convenio marco de cooperación entre la Caja Costarricense de Seguro Social y la Agencia de Protección de Datos de los Habitantes	Se propone un convenio marco de cooperación interinstitucional entre la CCSS y la Agencia PRODHAB, con el objetivo de establecer mecanismos eficaces de colaboración entre instituciones para el desarrollo de programas, proyectos, capacitaciones, estudios técnicos y demás actividades contempladas dentro del marco de sus respectivas competencias legales
Plantilla de registro de convenios y bases de datos institucionales	Plantillas para recolectar información de los convenios y bases de datos institucionales con información sujeta a la ley de protección de datos personales y su reglamento, de manera que sirva de apoyo en la recopilación, actualización de las Bases de Datos.
Modelo de gestión integral para el cumplimiento de la Ley N° 8968 y su reglamento en la CCSS	Además de orientar a los funcionarios de la Institución, se constituye en un documento de referencia necesario para la inscripción de las bases de datos ante la Agencia PRODHAB; razón por la cual, este documento será de aplicación y acatamiento obligatorio a nivel Institucional (CCSS)

Fuente: Informe de acciones y productos realizados Comisión Institucional

Al respecto, el Modelo de gestión integral para el cumplimiento de la Ley N° 8968 y su reglamento en la CCSS, se propuso contemplando etapas y productos como se detalla a continuación:

Imagen 3 Modelo de Gestión Integral orientado a garantizar el cumplimiento de lo establecido en la Ley N°8968 y su Reglamento en la CCSS



Fuente: Modelo de Gestión Integral orientado a garantizar el cumplimiento de lo establecido en la Ley N°8968 y su Reglamento en la CCSS

Los productos mencionados anteriormente, se remitieron el 24 de octubre de 2019 por parte el Lic. Ronald Lacayo Monge, gerente Administrativo en ese momento, mediante oficio GA-1270-2019, al Dr. Román Macaya Hayes, presidente ejecutivo en esa fecha, quién posteriormente a través de la Dra. Liza Vásquez Umaña, jefe del

despacho de la Presidencia Ejecutiva, emitió el oficio PE-1580-2020 el 19 agosto de 2020 al Dr. Roberto Cervantes Barrantes, Gerente General, indicando:

> *"Adjunto remito para su consideración en relación con la materia de gobernanza de datos desde la perspectiva institucional, tema que es coordinado a la fecha por el Lic. David Hernández Rojas, Asesor de ese Despacho y según lo acordado en reunión sostenida en esta Presidencia el pasado 16 de enero del 2020.*
>
> *Al respecto valga señalar que la propuesta ofrece una serie de productos, formularios y directrices cuyo análisis y aprobación debe efectuarse acorde con otros proyectos en fase de desarrollo, tales como reestructuración, política institucional para gobernanza DTIC y de datos, entre otros, de tal forma que la implementación pueda darse de forma integrada y congruente".*

Posteriormente se hizo recordatorio al Dr. Roberto Cervantes Barrantes, Gerente General, mediante oficio PE-2903-2020, del 23 de octubre de 2020, sin que se identificaran respuestas a ambas misivas.

4.2 CONTROL SOBRE LOS CONVENIOS INTERINSTITUCIONALES DONDE SE SUMINISTRA INFORMACIÓN

Se identificó que la Institución carece de un procedimiento estandarizado que contemple criterios técnicos y jurídicos para autorizar, controlar y auditar el intercambio de datos e información entre instituciones del Estado, Entes internacionales o empresas privadas mediante los convenios suscritos, que aseguren que los datos compartidos cumplan con principios de minimización, finalidad, proporcionalidad y seguridad, y se establezcan las cláusulas contractuales que delimiten el uso, acceso y resguardo de la información por parte de las entidades receptoras.

Si bien como se mencionó en el punto anterior, como parte de productos entregados por parte de la Comisión Interinstitucional para diseñar el Modelo de Gestión Integral para el cumplimiento de la Ley de Protección de la Persona frente al tratamiento de sus Datos Personales, generó la "Plantilla de registro de convenios y bases de datos institucionales", dicho Modelo no se ha implementado, por lo que se podrían generar riesgos asociados a la protección de datos personales, la confidencialidad de la información institucional y el cumplimiento de la normativa vigente, considerando que actualmente, según la información aportada por las Gerencias[1], se disponen actualmente de los siguientes convenios:

- **Gerencia Administrativa:** Convenio con el Registro Nacional de la Propiedad en relación con la Ley N° 8220 Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos.
- **Gerencia Médica:** Convenios Caja-INS, Caja-CONAPDIS, Caja-IAFA, Caja-Ministerio de Justicia y Paz, Caja-MINSA.
- **Gerencia de Pensiones:** cuenta con varios convenios con instituciones gubernamentales para compartir datos de trámites debido a la aplicación de la Ley 8220.

Las Normas de Control Interno para el Sector Público en su apartado 4.5 "Garantía de eficiencia y eficacia de las operaciones" establece:

> *"El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas (…)".*

Asimismo, en el apartado 4.5.1 "Supervisión constantes" indica:

[1] Las Gerencias de Logística e Infraestructura y Tecnología, refirieron no tener convenios actualmente, y la Gerencia Financiera no respondió.

"El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos".

Además, en el apartado 4.6 "Cumplimiento del ordenamiento jurídico y técnico" señala:

"El jerarca y los titulares subordinados, según sus competencias, deben establecer las actividades de control que permitan obtener una seguridad razonable de que la actuación de la institución es conforme con las disposiciones jurídicas y técnicas vigentes. Las actividades de control respectivas deben actuar como motivadoras del cumplimiento, prevenir la ocurrencia de eventuales desviaciones, y en caso de que éstas ocurran, emprender las medidas correspondientes. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas"

La situación descrita podría deberse a falta de acciones u omisiones por parte de la Gerencia General en la implementación del Modelo de Gestión Integral orientado a garantizar el cumplimiento de lo establecido en la Ley N°8968, por cuanto al consultar a esta unidad información relacionada a la solicitud efectuada por parte de la Presidencia Ejecutiva, señalaron que, mediante el SAYC, no constaba las respuestas correspondientes.

Al consultarles a los representantes de las Gerencias asignados para la atención del presente estudio, respecto a si se han definido procedimientos a nivel de Gerencia para compartir datos entre unidades, sistemas y entes externos, indicaron:

*"**Paula Ballestero Murillo, Gerencia de Logística:** Sí.*

***Giovanni Francisco Campos Alvarado, Gerencia de Infraestructura:** No se han definido procedimientos a nivel de Gerencia para compartir datos entre unidades, sistemas y entes externos. Salvo si se cuenta con un procedimiento para brindar información a los diputados de la Asamblea Legislativa.*

***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** No se dispone de un procedimiento de nivel gerencial; sin embargo, se tiene lo siguiente: -En el caso de la información contenida en el sistema SIPE, se realiza la solicitud mediante oficio formal, informando la necesidad que se tiene, el sistema que alimenta y el manejo que se da a la información. El analista destacado confecciona el respectivo formulario F043 GESTIÓN DE CUENTAS DE USUARIOS Y PRIVILEGIOS, con el nombre del usuario o base de datos afectada; firmando así un "Compromiso de uso" el cual se detalle dentro del mismo formulario. Desde la Dirección de Administración y Gestión de Personal la información que se comparte entre unidades y sistemas se canaliza a nivel de la Dirección y por medio del Proyecto SIPE. -Con respecto al SCBM la Auditoría Interna dispone de un perfil restringido de consulta para los estudios que genera ese Órgano Fiscalizador. -Respecto al sistema JURIX, no se comparte información con otras unidades ni con entes externos; sin embargo, en algunas colecciones y para apartados específicos que requieren validación, se tiene acceso a vistas personalizadas de consulta (SICERE y Recursos Humanos) que permiten validar la información consultada, y almacenada en la misma en la base de datos de JURIX. Para tener acceso a dichas vistas tanto SICERE como Recursos Humanos establecen un procedimiento que debe completarse de manera previa a tener el acceso.*

***Leslie Vargas Vásquez, Gerencia Médica:** Si, los procedimientos están regulados en el Reglamento del Expediente Digital Único de Salud, además, se operacionalizado por medio de los protocolos de transferencias de datos, protocolo Medidas de seguridad mínimas a solicitar a la entidad receptora para el uso de datos EDUS.*

***Johanna Mora Ulate, Gerencia de Pensiones:** Para los entes externos, se debe desarrollar un convenio para compartir datos, a nivel interno, se gestiona mediante solicitudes formales a los dueños de los diferentes sistemas".*

La falta de implementación del Modelo de Gestión Integral podría limitar el cumplimiento efectivo de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.° 8968) en la CCSS, afectando negativamente la capacidad institucional para garantizar una gestión ética, segura y conforme con el marco legal vigente. Esta omisión también ha impedido el fortalecimiento de la gobernanza y gestión de datos, al no contar con lineamientos claros sobre el tratamiento, protección y uso de la información personal, incrementando los riesgos de incumplimientos normativos, vulneraciones a la privacidad, pérdida de confianza por parte de los usuarios.

Asimismo, la ausencia de un procedimiento estandarizado sobre los convenios interinstitucionales donde se comparten datos e información gestionados en la CCSS, podría derivar en un uso inadecuado o no autorizado de estos, afectando la privacidad de las personas usuarias, la integridad de los sistemas de información y la reputación institucional, incrementando el riesgo de incumplimientos normativos y de eventuales responsabilidades legales.

5. RESPECTO A LA GOBERNANZA DE DATOS Y SU ALINEAMIENTO CON EL PLAN ESTRATÉGICO INSTITUCIONAL Y PLANES TÁCTICOS GERENCIALES

Se identificó que el Plan Estratégico Institucional de la CCSS 2023–2033 incluye líneas de acción orientadas al cumplimiento de uno de sus objetivos relacionados con la Gobernanza y Gestión de Datos. Sin embargo, al revisar los Planes Tácticos Gerenciales vigentes se observó que no todas las gerencias definieron acciones en torno a dichas líneas para la atención de ese objetivo estratégico.

En el Plan Estratégico Institucional de la CCSS 2023–2033, en el Eje Estratégico *"Una CCSS a la vanguardia científica, tecnológica e innovadora al alcance de las personas"* se definió como Objetivo 3: *"Potenciar el bienestar de las personas usuarias, mediante el incremento en el uso de las tecnologías, la innovación e investigación para desarrollar soluciones más eficientes en la prestación de los servicios de salud y pensiones".*

Para el cumplimiento de este objetivo, se establecieron las siguientes líneas de acción:

- **3.a** Aseguramiento de la información institucional por medio de la ciberseguridad y la gestión adecuada de los datos, preservando la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y resiliencia de los activos digitales.

- **3.f** Incorporación de la analítica de datos (diagnóstica, predictiva, prescriptiva) y modelos de información mediante herramientas como big data, BI, IOT, entre otras, que fomente el pensamiento científico y la mejora de los procesos institucionales, la transparencia, la minimización de los riesgos, fraude y corrupción en la gestión institucional.

- **3.o** Implementación de un modelo de gobierno y gestión de la información institucional sustentado en los pilares fundamentales del desarrollo tecnológico, donde la investigación brinde resultados de fácil acceso, integridad, pertinencia, suficiencia, privacidad y seguridad de los datos.

No obstante, en revisión de los Planes Tácticos Gerenciales se identificó que las líneas de acción 3.a y 3.o, no fueron incluidas en las fichas de indicadores por parte de las Gerencias según se detalla:

- Gerencia Médica: incluye temas alineados solo a la línea de acción 3.f
- Gerencia de Logística: incluye temas alineados solo a la línea de acción 3.f
- Gerencia de Pensiones: no se incluyen temas alineados a ninguna de las 3 líneas de acción
- Gerencia Administrativa: no se incluyen temas alineados a ninguna de las 3 líneas de acción
- Gerencia de Infraestructuras y Tecnologías: incluye temas alineados solo a la línea de acción 3.f
- Gerencia Financiera: incluye temas alineados solo a la línea de acción 3.f

El Plan Estratégico Institucional 2023 – 2033, en su apartado "Seguimiento a la implementación de la estrategia institucional", señala:

"El seguimiento es fundamental para garantizar que el PEI 2023-2033 se implemente de manera efectiva y se logren los resultados deseados, por cuanto estas actividades permiten monitorear el progreso, identificar desviaciones y realizar ajustes necesarios para garantizar que el Plan se implemente de manera efectiva, así como determinar el alcance de los resultados esperados; de igual forma es preciso señalar, que permite una adecuada rendición de cuentas.

Se plantea para el plan estratégico un seguimiento y monitoreo anual basado en dos dimensiones, la primera asociada a los resultados, entendida como el monitoreo de los cambios esperables producto de la implementación directa del plan. Los resultados se derivan directamente del análisis de los objetivos estratégicos establecidos.

La segunda dimensión está basada en la implementación de las líneas de acción estratégicas, ***concentra su atención en el alineamiento de éstas en todo el sistema de planificación institucional (Planes Tácticos Gerenciales, Planes Presupuesto y otros instrumentos),*** *así como en su operacionalización efectiva".* (La negrita no es del original)

La Guía de Formulación del Plan Táctico Gerencial, en el apartado 7.1 "Planificación Táctica" señala:

"La Planificación Táctica al ser un proceso específico de la planificación dentro de la CCSS, se presenta un concepto institucional, el cual se conoce como un proceso de gestión que define las estrategias que seguirá la gerencia para su desarrollo y el cumplimiento de los objetivos estratégicos, este proceso es el responsable de crear las condiciones para la operacionalización de los lineamientos establecidos en la planificación estratégica

(…) De igual forma, el planeamiento táctico les permite a las gerencias, implementar acciones para su desarrollo, que resuelvan situaciones a corto plazo e innovar en la gestión para mejorar la prestación de los servicios; esta planeación permite visualizar el entorno futuro y anticiparse con acciones ante las posibles oportunidades y amenazas que podrían surgir".

Asimismo, en el 7.2 "Plan Táctico Gerencial" indica:

"Es un instrumento de gestión que detalla el conjunto de objetivos y su desglose en proyectos y/o actividades, que conducen al cumplimiento de la misión y visión institucional; es una declaración formal de la ruta que seguirá el gerente para el desarrollo de los propósitos sustantivos de su gerencia. Para elaborar este plan es recomendable que las gerencias contemplen otras herramientas de gestión como la prospectiva, la gestión para resultados, la gestión por proyectos, la gestión de riesgos y la innovación (Figura N°1), de forma que utilicen las mejores herramientas de gestión, según las buenas prácticas que aseguren la obtención de los mejores resultados posibles de acuerdo con las necesidades a solventar y las posibilidades de la organización"

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, 2021 emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, MICITT, señalan en el apartado Gobernanza TI, lo siguiente:

"(…) La institución debe disponer de un marco orientador que permita la definición de la acción institucional con un enfoque de valor público. Asimismo, debe considerar en la estrategia institucional la incorporación de iniciativas habilitadas por tecnologías de información.

La entidad pública debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones como un asesor en los modelos de habilitación de los objetivos, necesidades y oportunidades institucionales a través del uso de TI, así como elementos para la

rendición de cuentas sobre el uso adecuado de las TI para responder a las necesidades, objetivos y oportunidades institucionales."

Las Normas de Control Interno para el Sector Público en su apartado 3.3 "Vinculación con la planificación institucional" establece:

"La valoración del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión institucionales, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones, y en consecuencia, de los riesgos correspondientes.

Asimismo, los resultados de la valoración del riesgo deben ser insumos para retroalimentar ese proceso de planificación, aportando elementos para que el jerarca y los titulares subordinados estén en capacidad de revisar, evaluar y ajustar periódicamente los enunciados y supuestos que sustentan los procesos de planificación estratégica y operativa institucional, para determinar su validez ante la dinámica del entorno y de los riesgos internos y externos".

Al consultarles a los representantes de las Gerencias asignados para la atención del presente estudio, respecto a si se han definido indicadores o actividades en el Plan Táctico Gerencial que estén alineados con el objetivo 3 del Plan Estratégico Institucional 2023-2033, específicamente en las líneas de acción mencionadas, indicaron:

*"**Paula Ballestero Murillo, Gerencia de Logística:** Sí, en materia de desarrollo de proveedores, compra estratégica y con elementos funcionales de innovación y sustentables.*

***Giovanni Francisco Campos Alvarado, Gerencia de Infraestructura:** En relación con eje estratégico 3 que menciona y específicamente con las líneas de acción 3.a, 3.j, y 3.o, la GIT no definió objetivos o indicadores en el Plan Táctico Gerencial, dado que van enfocados más a gestión de la Dirección de Tecnologías de Información y Comunicación. La línea de acción 3.f si está asociada con algunos indicadores.*

***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** Expresamente vinculados con las líneas de acción 3a, 3f, 3j y 3o, no se tienen objetivos ligados como tal en el Plan Táctico Gerencia; sin embargo, en relación con el objetivo 3, sí se tiene un indicador ligado a la acción 3.c, y dos indicadores a la acción 3.k, éstos dos últimos relacionados con los sistemas de información SISO y SIPE, que representan una mejora en la gestión de datos, su disponibilidad, integridad, entre otros.*

***Leslie Vargas Vásquez, Gerencia Médica:** Sí, se incluyó en el plan táctico de la Gerencia Médica 2023-2027 el objetivo: Implementar la innovación en el ámbito de salud mediante la transformación digital que generen herramientas asistenciales, análisis de datos para la mejora de los procesos institucionales y la atención integral de las personas, relacionado con el desarrollo de modelos de inteligencia artificial para la predicción de ECNT.*

***Johanna Mora Ulate, Gerencia de Pensiones:** Según el Indicador 15 del PTG. "Diseñar e implementar una Estrategia Digital, de forma que se mejore la eficiencia y eficacia de cara al usuario de los servicios prestados." en las líneas 3b, 3c, 3d, 3j, 3k, adicionalmente con 2a,2d, 2i 4l, 5a, 5c, 5e, 5g y la Dirección de Planificación Institucional está revisando los alineamientos con el encargado de este tema en la Gerencia".*

La situación descrita, se debe – entre otros aspectos- a que no se ha llevado a cabo el debido seguimiento de las líneas de acción mediante la evaluación anual del PEI, lo que genera que no se identifique estas situaciones sobre el alineamiento de éste con los Planes Tácticos Gerenciales. Lo anterior con fundamento en lo señalado por la Ing. Susan Peraza Solano, directora de Planificación Institucional, que mediante oficio PE-DPI-0325-2025 del 31 de marzo de 2025, informó a esta Auditoría lo siguiente:

"En primer lugar, con respecto al seguimiento de las líneas de acción estratégicas correspondientes al objetivo 3 del Plan Estratégico Institucional (PEI) 2023-2033, esta Dirección se encuentra en el proceso de elaboración de la evaluación del PEI, abarcando todas las líneas de acción. Una vez concluido dicho proceso, los resultados obtenidos serán comunicados oportunamente".

La falta de objetivos o indicadores en algunos Planes Tácticos Gerenciales relacionados con las líneas de acción del objetivo 3 del Plan Estratégico Institucional representa una debilidad en la coordinación entre la planificación estratégica y táctica, comprometiendo la implementación efectiva de iniciativas clave como la gobernanza de datos, la ciberseguridad, la analítica avanzada y el modelo de gobierno de la información. Además, limita la capacidad institucional para monitorear progresos, realizar ajustes oportunos y rendir cuentas sobre el cumplimiento de los objetivos estratégicos, tal como lo establece el PEI.

6. SOBRE EL MARCO NORMATIVO INSTITUCIONAL ESTABLECIDO EN TORNO A LA GOBERNANZA DE DATOS

Se identificó la ausencia de un marco normativo institucional integral que regule la Gobernanza y Gestión de Datos en la CCSS, que contemple elementos esenciales como: la definición de roles y responsabilidades, inventarios de datos, criterios de precisión, integridad, consistencia y actualización, clasificación de la información, acuerdos de confidencialidad, seguridad de la información y lineamientos para el suministro de datos a entes externos o convenios interinstitucionales, entre otros aspectos fundamentales.

Aunque existen disposiciones emitidas a nivel gerencial, estas se limitan a aspectos específicos —como el procedimiento GA-DSI-API-PR004 sobre conservación y eliminación de documentos, enfocado en la gestión documental— o a lineamientos operativos definidos en los distintos sistemas de información bajo responsabilidad de las gerencias. Asimismo, si bien la Junta Directiva aprobó la Política Institucional para la Gobernanza de Datos, esta se limita a siete enunciados generales y, como se ha señalado previamente, no ha sido implementada mediante su correspondiente agenda de ejecución.

La Ley 8292: Ley General de Control Interno, en su artículo 15. Actividades de control, indica:

"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 (…)"

Las Normas de Control Interno para el Sector Público en su apartado 2.2 "Compromiso superior" establece:

"El jerarca y los titulares subordinados, según sus competencias, deben apoyar constantemente el SCI, al menos por los siguientes medios:

a. La definición y divulgación de los alcances del SCI, mediante la comunicación de las políticas respectivas y la difusión de una cultura que conlleve la comprensión entre los funcionarios, de la utilidad del control interno para el desarrollo de una gestión apegada a criterios de eficiencia, eficacia, economía y legalidad y para una efectiva rendición de cuentas. (…)".

La ausencia de un marco normativo institucional integral en materia de gobernanza y gestión de datos en la CCSS obedece -entre otros aspectos- a una falta de articulación entre los niveles estratégicos y tácticos de la Institución para desarrollar e implementar lineamientos transversales en esta materia. Aunque se han emitido disposiciones desde algunas gerencias y se cuenta con una Política Institucional aprobada, no se ha promovido una

coordinación efectiva para su ejecución, ni se ha definido una estructura normativa que establezca responsabilidades claras, mecanismos de control y criterios técnicos comunes.

Los representantes de las Gerencias asignados para la atención del presente estudio, respecto a si se han emitido directrices u otro tipo de normativa a nivel Gerencial, relacionadas con la gestión y uso de datos utilizando la "Política Institucional para la Gobernanza de Datos" aprobado por la Junta Directiva en abril del 2022, señalaron:

> *"**Paula Ballestero Murillo, Gerencia de Logística:** Elementos básicos de uso para monitoreo y evaluación de gestión, KPIs, BI basada en datos SIGES y confidencialidad de datos sensibles como parte del sistema de gestión antisoborno.*
>
> ***Giovanni Francisco Campos Alvarado, GIT:** No se han emitido otros lineamientos respecto a la gobernanza de los datos por parte de la GIT.*
>
> ***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** A nivel gerencial en general no se tiene conocimiento, y a nivel de la Gerencia Administrativa, no expresamente.*
>
> ***Leslie Vargas Vásquez, Gerencia Médica:** La política fue referenciada en el Protocolo mínimo de actuación para el tratamiento de los datos personales en la CCSS Expediente Digital Único de Salud EDUS-ARCA (GM-Protocolo-01-2023), el cual está vigente para su aplicación en apego a la Ley 8968 de protección de la persona frente al tratamiento de sus datos personales.*
>
> ***Johanna Mora Ulate, Gerencia de Pensiones:** Como no se trasladó de manera formal la política a esta Gerencia, no se han emitido directrices al respecto. Sin embargo, hay nombrada una persona que participará en atender la implementación y acciones posteriores.*

Asimismo, respecto a la existencia de procedimientos definidos a nivel de Gerencia en torno a la creación, almacenamiento, uso, archivado y eliminación de datos que se gestionan en los procesos y sistemas de información de la Gerencia y sus unidades adscritas, indicaron:

> *"**Giovanni Francisco Campos Alvarado, GIT:** Si existen los procedimientos definidos a nivel de la Gerencia para la creación, uso, archivado y eliminación de datos que se gestionan en los procesos y sistemas de información. Se hacen a través de los roles asignados en los diferentes sistemas de información y procesos. Se cuenta también con un procedimiento para la eliminación y conservación de documentos, emitido por el ente rector en gestión documental.*
>
> ***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** A nivel Institución se dispone de un marco regulatorio para la Gestión Documental, en el que, en relación con la eliminación de datos, se tiene el Procedimiento Conservación y Eliminación de Documentos GA-DSI-API-PR004. Asimismo, en relación con sistemas de información se tiene lo siguiente: -Para el sistema SIPE se maneja la información histórica con datos salariales la cual es custodiada en cumplimiento con las normas antes citadas. -Respecto a la operativa de transporte se actualizan los datos almacenados con respecto a los vehículos utilizados por cada unidad de acuerdo con la funcionalidad de este, desde su ingreso hasta su disposición final. -Para el Sistema SAYC, existen procedimientos con respecto a la creación, almacenamiento, uso, archivado y eliminación de datos con fundamento a la Ley del Sistema Nacional de Archivos 7202, que aplica para formatos físicos y digitales. -En referencia con el sistema SCBM, una de las funcionalidades del sistema es disponer del histórico de los datos vinculados a los bienes muebles, donde se contempla desde su ingreso hasta su disposición final. -En el caso de JURIX, los registros contenidos son de larga data, ya que el proceso depende de las instancias del Poder Judicial o de la instrucción de la investigación, lo cual hace que no se pueda establecer un plazo máximo para resguardar dicha información. Adicional a lo anterior, mucha de la información contenida, puede ser referencia y solicitada con posterioridad por la Junta Directiva, instancias judiciales, de supervisión o fiscalización, según sea el caso y debe mantenerse disponible.*

Leslie Vargas Vásquez, Gerencia Médica: *En el caso del EDUS-ARCA, los procedimientos de creación, almacenamiento, uso, archivado y eliminación de datos han sido definido en el reglamento a la Ley de Expediente Digital Único de Salud y sus manuales operativos específicos.*

Johanna Mora Ulate, Gerencia de Pensiones: *En los procesos de la GP existen la normativa sobre el archivado de documentos y nivel de los sistemas de información nos regimos por las normas y políticas de seguridad informática".*

La ausencia de un marco normativo institucional integral que regule la gobernanza y gestión de datos en la CCSS podría generar un efecto en la capacidad de la institución para garantizar una administración coherente, segura y eficiente de su información. Esta carencia limita la estandarización de prácticas entre unidades, genera ambigüedad en la asignación de responsabilidades y dificulta la implementación de controles efectivos sobre aspectos críticos como la calidad, seguridad, clasificación y uso de los datos, tanto internos, como aquellos compartidos con entes externos, incrementando el riesgo de inconsistencias, accesos no autorizados, pérdida de información y decisiones institucionales basadas en datos incompletos o no confiables, afectando la rendición de cuentas y la toma de decisiones estratégicas.

7. RESPECTO A LA CLASIFICACIÓN DE LOS DATOS INSTITUCIONALES

Se identificó que la Institución carece de un esquema formal y documentado de clasificación de los datos institucionales que contemple criterios como requisitos legales, valor institucional, criticidad y sensibilidad a la divulgación o modificación no autorizada, de tal forma que garantice cumplimientos normativos, correcta toma de decisiones estratégicas, continuidad operativa, protección de la privacidad y prevención de fraude.

Respecto a lo anterior, esta Auditoría, mediante el oficio de advertencia AD-ATIC-0085-2024 del 12 de agosto de 2024, referente a la gestión de Seguridad de la Información y Ciberseguridad en la CCSS de acuerdo con los estándares ISO 27001 y NIST, ya había señalado en el análisis de las capacidades operativas, específicamente en la protección de la información, que se requerían acciones inmediatas de mejora, el mismo fue visto el 14 de octubre de 2024 en sesión del Consejo Tecnológico, emitiéndose acuerdos donde se designan tareas al equipo intergerencial, mismas que se encuentran actualmente en ejecución.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el apartado IX. "Seguridad y Ciberseguridad", menciona 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****.*

(…)

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades ***que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución****. (…)"* (La negrita no es del original)

La Política Institucional para la Gobernanza de Datos GG-PO-001, en su enunciado 3 señala:

"La Caja Costarricense de Seguro Social promoverá una cultura organizacional en materia de gobernanza y gestión de datos, garantizando el uso seguro, confiable, innovador e integral, así como la socialización del conocimiento, fortaleciendo la gobernanza de estos".

Las Normas de Control Interno para el Sector Público en su apartado 4.4 "Exigencia de la confiabilidad y oportunidad de la información" establece:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional (…)".

Los representantes de las Gerencias asignados para la atención del presente estudio, respecto a si se han clasificado los datos que se gestionan en la Gerencia y sus unidades adscritas según su nivel de sensibilidad y riesgo, señalaron:

*"**Paula Ballestero Murillo, Gerencia de Logística:** Están identificados con su gestión.*

***Giovanni Francisco Campos Alvarado, GIT:** Si se han clasificado los datos que se gestionan en la gerencia y sus unidades adscritas según su nivel de sensibilidad y riesgo a nivel de sistemas de información.*

***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** No de la manera consultada; sin embargo, se dispone de lo siguiente: -A nivel de SIPE, se estableció la información salarial (Retenciones y/o deducciones) de cada trabajador como información sensible de acceso restringido. -La información que se administra a nivel del Área Diseño, Administración de Puestos y Salarios, por práctica administrativa se han catalogado como información sensible al responder a información salarial (índices salariales, pagos, deducciones, terminaciones de contrato, entre otros) -En el caso de la Gestión documental el sistema SAYC dispone de control a través de una funcionalidad y permisos especiales que contribuyen al acceso de la información, considerando la sensibilidad de los oficios que se gestionan. -Respecto a la gestión de la investigación y seguridad institucional dentro de las funciones sustantivas se encuentra la gestión de investigaciones preliminares, gestión de denuncias y gestiones referentes a modelo de prevención, las cuales son de acceso restringido. -En el sistema SCBM la información disponible y bases de datos es catalogada como sensible, por lo cual, los accesos que se otorgan dependen del perfil que se les asigne a los usuarios a fin de evitar la materialización de riesgos. -Para el caso de la atención de emergencias los datos que se manejan son para análisis en los CCO, y Junta Directiva, en virtud de la Información que se genera. -Referente al Sistema JURIX, es una herramienta de uso interno no público, y por la naturaleza y principios que conforman la materia relacionada a la gestión sancionatoria y litigiosa, entre estas el artículo 6 de la Ley General de Control Interno, 8 de la Ley Contra la Corrupción y Enriquecimiento Ilícito, la Normativa de Relaciones Laborales, Ley contra el Hostigamiento o Acoso Sexual en el Empleo y la Docencia, la información afín a esta, es confidencial y sensible, conocida únicamente por las partes intervinientes según corresponda. A nivel de la Gerencia, se atienden y son considerados todos los informes para la atención de riesgos informáticos que son remitidos por la DTIC o el MICIIT, a efecto de proteger la información en ella contenida; sin embargo, el factor humano es un riesgo que se mantiene presente en el uso de los sistemas de información.*

***Leslie Vargas Vásquez, Gerencia Médica:** No, la clasificación de los datos es una actividad que está pendiente de realizar.*

***Johanna Mora Ulate, Gerencia de Pensiones:** A nivel Institucional no existe un protocolo de etiquetado de datos, sin embargo, la Gerencia de Pensiones trabaja en apego a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales Ley N.º 8968.*

La situación descrita podría generar un efecto en la capacidad de la institución para proteger adecuadamente su información, cumplir con los marcos normativos y tomar decisiones estratégicas basadas en datos confiables. Esta carencia impide establecer niveles de protección diferenciados según la sensibilidad, criticidad o valor legal de los datos, lo que incrementa el riesgo de accesos no autorizados, pérdida de confidencialidad, errores en la integridad de la información y posibles afectaciones a la continuidad operativa.

8. RESPECTO A LAS INICIATIVAS INSTITUCIONALES EN TORNO A LA SEGURIDAD DE LOS DATOS

Como parte de los componentes de la Gobernanza y Gestión de Datos, se efectuó un seguimiento a las iniciativas institucionales relacionadas con la Seguridad de los Datos o Seguridad de la Información, determinándose avance limitado en la implementación de estas.

Al respecto, en diciembre del 2020, se emitió el "Plan de Ciberseguridad de la CCSS", producto de una contratación efectuada a la empresa Price Waterhouse Cooper, en la que se establecieron 23 iniciativas priorizadas para subsanar las brechas de ciberseguridad detectadas a nivel Institucional en esa época. Posterior al ataque cibernético sufrido en la Institución el 31 de mayo de 2022, la DTIC elaboró una actualización del Programa denominado: *"Fortalecimiento del Plan de Ciberseguridad"*, el cual contempló las necesidades originales, así como otras recomendaciones que fueron detectadas a raíz de dicho evento, definiéndose 35 iniciativas a desarrollar.
El 21 de junio de 2024 en la sesión N° 003, se aprobó en el Consejo Tecnológico, la propuesta de la hoja de ruta del Programa de Ciberseguridad, la cual diferenció 7 iniciativas correspondientes a la Seguridad de la Información para que fueran atendidas por las áreas de negocio, entre las cuales se encuentran las siguientes 3, relacionadas con la seguridad de los Datos:

- PCS-GI-22 Iniciativas para la implementación de la privacidad y protección de datos en los servicios TIC
- PCS-GI-32 Iniciativas para definir e implementar el programa de gestión de activos
- PCS-GI-33 Iniciativas para implementar el esquema de identificación y clasificación de información

En dicha sesión en el acuerdo 4 del tema 2 se instruyó lo siguiente:

> *"4. Conformar un equipo intergerencial coordinado por la Gerencia General que analice las iniciativas relacionadas con seguridad de la información, para revisar las fichas técnicas, planes de trabajo y cualquier otra documentación existente con esta materia, para su incorporación a la hoja de ruta del programa de ciberseguridad, en un plazo no mayor a cuatro meses, para su presentación al Consejo Tecnológico"*

El 17 de febrero de 2025, mediante oficio GG-0123-2025, se le solicitó a los Gerentes, por parte de la Dra. Jenny Madrigal Quirós, jefe de despacho de la Gerencia General, nombrar funcionarios para integrar el equipo Intergerencial para la atención del acuerdo N°4 de la sesión N°003 del Consejo Tecnológico celebrada el 21 de junio 2024, el cual quedó conformado por:

- Lic. Alexánder Solís Abarca, jefe del CGI de la Gerencia Financiera
- Ing. Roger Muñoz Díaz, asesor de la Gerencia Administrativa
- Ing. Diego Rodríguez Granados, funcionario de la Gerencia de Infraestructura y Tecnología
- Dr. Marvin Argüello Chinchilla, asesor de la Gerencia Médica
- Ing. Johanna Mora Ulate, asesora de la Gerencia de Pensiones
- Lic. Ericka Vindas Umañan, jefe de la subárea de Seguridad Informática de la DTIC

Dicho equipo Intergerencial se reunió el 5 de mayo de 2025 donde se realizaron los primeros acuerdos, por lo que no se ha tenido un avance significativo en la implementación de las iniciativas de marras, considerando su reciente creación.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en el punto "VI. Calidad de los Procesos Tecnológicos" indican:

"La institución debe implementar prácticas que permitan controlar los procesos organizacionales, posibilitando la mejora continua de productos y servicios, buscando asegurar la satisfacción de las necesidades institucionales, manteniendo estándares de documentación de los lineamientos requeridos, esquemas para la medición del desempeño y control sobre la vigencia de las prácticas aplicables a los procesos.

Igualmente, debe generar servicios de TI de conformidad con los requerimientos de los usuarios con base en un enfoque de eficiencia y mejoramiento continuo de los procesos que habilitan la gestión de las tecnologías de información".

Las Normas de Control Interno para el Sector Público, en el punto 4.5 "Garantía de eficiencia y eficacia de las operaciones establecen:

"El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas"

Asimismo, en el punto 4.5.2 Gestión de Proyectos se indica:

"El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes.

Las actividades de control que se adopten para tales efectos deben contemplar al menos los siguientes asuntos:

(…)

c. La planificación, la supervisión y el control de avance del proyecto, considerando los costos financieros y los recursos utilizados, de lo cual debe informarse en los reportes periódicos correspondientes. Asimismo, la definición de las consecuencias de eventuales desviaciones, y la ejecución de las acciones pertinentes.
d. El establecimiento de un sistema de información confiable, oportuno, relevante y competente para dar seguimiento al proyecto.
e. La evaluación posterior, para analizar la efectividad del proyecto y retroalimentar esfuerzos futuros"

La Ing. Ericka Sánchez Solís, funcionaria de la subárea de Seguridad Informática de la DTIC, indicó:

"(…) actualmente se dispone de un grupo de reciente creación que es coordinado por don Orlando Rivas, asesor de la Gerencia General, para atender un acuerdo de Junta Directiva sobre el tema de Seguridad de la Información y las 7 iniciativas del Plan de Ciberseguridad. Este equipo está conformado por todas las gerencias, sin embargo, a pesar de que se informó sobre la temática, siempre asignaron funcionarios de perfil TIC. Ahorita lo que este equipo está haciendo, es el análisis de las 7 iniciativas, se envió un oficio a todas las gerencias para que presenten todas las propuestas que se tienen sobre Seguridad de la Información, para hacer un inventario, y de acuerdo con la revisión de las iniciativas y estas propuestas, trasladar nuevamente a la Gerencia General para que se materialice la gestión de la Seguridad de la Información.

(…)

(…) a nivel de la comisión conformada, debido al acuerdo de Junta Directiva, la idea era hacer un análisis de esas iniciativas, por lo que esto fue lo primero que se conversó en una reunión, sin embargo, yo cuestioné ¿Qué criterio teníamos nosotros para hacer un análisis de iniciativas que fueron diseñadas por Deloitte, cuya empresa se dedica a Seguridad de la Información?, mi campo es Ciberseguridad, puedo conocer sobre Seguridad de la Información, pero no tengo criterio para cuestionar lo que plasmó Deloitte en esas iniciativas, hemos hablado sobre la estructura, y ver donde se plasma, analizar las iniciativas, y visualizar si hay que contratar un tercero, experto en Seguridad de la Información, que le diga a la Institución como plasmar esa infraestructura y empezar a poner a trabajar todas esas iniciativas.

Nosotros sí hemos venido trabajando con la parte de Ciberseguridad, pero esas iniciativas que desde que se plasmaron en el 2022 y 2023, no se ha gestionado nada, hay que hacerles la actualización correspondiente".

El Ing. Daniel Berrocal Zúñiga, jefe a.i. del área de Seguridad y Calidad de la DTIC, respecto al avance de las iniciativas de Seguridad de la Información, señaló:

"(…) en línea con lo comentado por la Ing. Sánchez, no se ha avanzado como un todo en el análisis, y de esa manera de forma individual tampoco, por lo menos desde el conocimiento que se tiene desde la DTIC, ya que es un tema que si se había asignado a la Gerencia General para que ellos fueran los coordinadores de todo este tema".

La falta de avances en la implementación de las iniciativas institucionales relacionadas con la seguridad de los datos y la información en la CCSS debilita la capacidad de la Caja para proteger sus activos digitales y manuales frente a amenazas internas y externas. Esta situación compromete el cumplimiento de estándares técnicos y normativos, así como la mejora continua de los procesos tecnológicos, incrementando los riesgos de exposición de datos sensibles, interrupciones operativas y pérdida de confianza institucional, afectando directamente la eficiencia, legalidad y resiliencia de la gestión pública.

9. SOBRE LA CONFORMACIÓN DE DIFERENTES EQUIPOS INTERGERENCIALES PARA GESTIONAR INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN O GOBERNANZA DE DATOS.

Se identificó que, en los últimos seis años, se han conformado al menos seis equipos intergerenciales distintos para abordar temas relacionados con la Gobernanza y Gestión de Datos y la Seguridad de la Información en la CCSS, lo que sugiere que la Caja carece de una estructura institucional permanente y articulada que lidere de forma integral dichos temas.

Al respecto, en el 2019, con el objetivo de atender el Modelo de Gestión Integral para el Cumplimiento de la Ley N° 8968 y su reglamento en la CCSS se conformó un equipo de trabajo integrado por los siguientes funcionarios:

- Ing. Roger Muñoz Díaz, Coordinador comisión, Gerencia Administrativa
- Ing. Ronald Guzmán Vásquez, representante Gerencia Médica
- Lic. Eithel Corea Baltodano, Gerencia de Pensiones (Representado por Ing. Mario Villalobos Marín)
- Licda. Vanessa Carvajal Carmona, representante Gerencia de Infraestructura y Tecnologías
- Ing. Manuel Castro Villalobos, representante Gerencia Financiera
- Ing. Roy Armando Ovares Valerio, representante Gerencia de Logística
- Licda. Maleydis Figueroa Paiz, representante Dirección de Sistemas Administrativos
- Licda. Giselle Tenorio Chacón, representante Gerencia Administrativa

Este equipo entregó los productos relacionados con el Modelo de Gestión Integral para el Cumplimiento de la Ley N° 8968 Protección de la persona frente al tratamiento de sus datos personales.

El 11 de febrero de 2021, mediante oficio GG-0406-2021, el Dr. Roberto Cervantes Barrantes, gerente general en ese momento, conformó el equipo para la creación de la "Política Institucional para la Gobernanza de Datos", integrándose de la siguiente manera:

- Lic. David Hernández Rojas, Gerencia General, coordinador
- Ing. Roger Muñoz Díaz, Gerencia Administrativa
- Licda. Mariela Pérez Jiménez, EDUS
- Licda. Natalie Fonseca Loaiciga, Dirección de Planificación Institucional
- Licda. Maleydis Figueroa Paiz, Gerencia Administrativa
- Licda. Johanna Valerio Arguedas, Dirección Jurídica

El equipo conformado entregó la "Política Institucional para la Gobernanza de Datos" que posteriormente fue aprobado por la Junta Directiva.

El 8 de mayo de 2023, mediante oficio GA-0652-2023/GG-DTIC-3145-2023, suscrito por la MBA. Vilma Campos Gómez, gerente Administrativa a.i. y el Lic. Eithel Corea Baltodano, subgerente de la DTIC a.i., le remitió a un nuevo equipo conformado por las diferentes gerencias, el oficio GG-3269-2022, "Remisión de los resultados del nivel de aplicación de prácticas de Seguridad de la Información en las Instituciones Públicas", para el análisis de la necesidad Institucional en materia de seguridad de la información, que permitiera identificar los esfuerzos requeridos para mejorar los niveles de madurez en la materia, este equipo lo integró:

- Lic. Minor Zúñiga Sedó, jefe del área facturación de cuotas obrero patronal, Gerencia Financiera
- Ing. Jacqueline Picado Sánchez, asesora de la Gerencia de Logística
- Dr. David Monge Durán, Gerencia Médica
- Ing. Manuel Rodríguez Arce, jefe EDUS (en ese momento), Gerencia Médica
- Máster Leslie Vargas Vásquez, jefe área Estadísticas en Salud, Gerencia Médica
- Máster Esteban Zúñiga Chacón, jefe del CGI de la Gerencia Médica
- David Arguedas Zamora, funcionario de la Gerencia de Pensiones
- Ing. Jorge A. Porras Pacheco, asesor de la Gerencia de Infraestructura y Tecnologías
- Ing. Ericka Sánchez Solís, funcionaria de la subárea de Seguridad Informática de la DTIC

El equipo conformado emitió el 29 de setiembre de 2023, el oficio CISI-001-2023, dirigido a la MBA. Vilma Campos Gómez, gerente Administrativa y al Ing. Danilo Hernández Monge, subgerente a.i de la DTIC, las conclusiones del análisis realizado, recomendando presentar ante la Gerencia General la hoja de ruta elaborada por la DTIC, para el abordaje de las iniciativas, así como por parte del equipo para reforzar de manera integral el enfoque de seguridad de la información.

El 16 de setiembre de 2024, mediante oficio GG-1614-2024, la MBA. Vilma Campos Gómez, Gerente General a.i. en ese momento, solicitó al cuerpo Gerencial, así como a los directores del CISADI, CENDEISS, DTIC y Planificación Institucional, designar un funcionario por unidad para de retomar la agenda de implementación y el desarrollo de acciones pertinentes para la implementación de la Política Institucional para la Gobernanza de Datos, por lo que posteriormente el equipo quedó conformado por los siguientes funcionarios:

- Luis Diego Sandoval Salas, Dirección de Planificación Institucional
- Roger Muñoz Díaz, Gerencia Administrativa
- Giovanni Campos Alvarado, Gerencia de Infraestructura y Tecnología
- Cindy Madrigal Jiménez, Gerencia Financiera
- Paula Ballestero Murillo, Gerencia Financiera
- Marco González Jiménez, Gerencia de Pensiones
- Esteban Zamora Chaves, Dirección de Tecnologías y Comunicaciones}
- Sofia Carvajal Chaverri, CENDEISSS

De este equipo no se identificó entregables en torno a la implementación de la Política Institucional para la Gobernanza de Datos.

El 17 de febrero de 2025, mediante oficio GG-0123-2025, se le solicitó a los Gerentes, por parte de la Dra. Jenny Madrigal Quirós, jefe de despacho de la Gerencia General, nombrar funcionarios para integrar el equipo Intergerencial para la atención del acuerdo N°4 de la sesión N°003 del Consejo Tecnológico celebrada el 21 de junio 2024 referente a la Gestión de la Seguridad de la Información y Ciberseguridad en la CCSS, el cual quedó conformado por:

- Lic. Alexánder Solís Abarca, jefe del CGI de la Gerencia Financiera
- Ing. Roger Muñoz Díaz, asesor de la Gerencia Administrativa
- Ing. Diego Rodríguez Granados, funcionario de la Gerencia de Infraestructura y Tecnología
- Dr. Marvin Argüello Chinchilla, asesor de la Gerencia Médica
- Ing. Johanna Mora Ulate, asesora de la Gerencia de Pensiones
- Lic. Ericka Vindas Umaña, jefe de la subárea de Seguridad Informática de la DTIC

Este equipo se encuentra actualmente en ejecución de actividades.

Asimismo, mediante oficio PE-0239-2025 del 28 de enero de 2025, la Presidencia Ejecutiva solicitó al Dr. Juan Carlos Esquivel Sánchez, director del CENDEISSS y a la Ing. Susan Peraza Solano, directora de Planificación Institucional, colaboración para gestionar ante el MIDEPLAN los requerimientos para formalizar la asistencia técnica propuesta por el Banco Mundial en el tema de uso estratégico de datos e información en la CCSS, informando posteriormente mediante oficio PE-1061-2025 del 13 de marzo de 2025, que para apoyar dicha gestión se designó como enlace de la Presidencia a la Lcda. Carolina Gallo Chaves, asesora del Despacho de la Presidencia Ejecutiva, y al Ing. Manuel Rodríguez Arce, coordinador del CISADI, como enlace técnico.

Las Normas de Control Interno para el Sector Público en su apartado 4.5 “Garantía de eficiencia y eficacia de las operaciones” establece:

> *“El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas (…)”.*

Asimismo, en el apartado 4.5.1 “Supervisión constantes” indica:

> *“El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos”.*

La Ing. Ericka Sánchez Solís, funcionaria de la subárea de Seguridad Informática de la DTIC, indicó:

> *“Se han conformado 5 grupos en diferentes momentos, para abordar temas de seguridad de la información, y actualmente se dispone de un grupo de reciente creación que es coordinado por don Orlando Rivas, asesor de la Gerencia General, para atender un acuerdo de Junta Directiva sobre el tema de Seguridad de la Información y las 7 iniciativas del Plan de Ciberseguridad. Este equipo está conformado por todas las gerencias, sin embargo, a pesar de que se informó sobre la temática, siempre asignaron funcionarios de perfil TIC. Ahorita lo que este equipo está haciendo, es el análisis de las 7 iniciativas, se envió un oficio a todas las gerencias para que presenten todas las propuestas que se tienen sobre Seguridad de la Información, para hacer un inventario, y de acuerdo con la revisión de las iniciativas y estas propuestas, trasladar nuevamente a la Gerencia General para que se materialice la gestión de la Seguridad de la Información”.*

El Ing. Manuel Arce Rodríguez, Coordinador del CISADI y del proyecto de Cooperación Técnica y Financiera no reembolsable con MIDEPLAN para la hoja de ruta para la Gobernanza de Datos de la CCSS, respecto a la conformación del equipo de trabajo indicó:

> *"Hay una designación precisamente para la formulación del proyecto, pero si hay una claridad, ya para cuando inicie eventualmente el proceso, deben de incorporarse los diferentes actores que conforman los diferentes roles Institucionales, la designación es para la formulación, pero si eventualmente cuando entremos en la cooperación, hay que incorporar diferentes roles con base en el alcance del proyecto y establecer los diferentes equipos de trabajo".*

Esta Auditoría considera que la conformación de múltiples equipos intergerenciales obedece a la ausencia de una estructura institucional permanente y claramente definida para liderar y coordinar temas estratégicos en torno a la Gobernanza de Datos y Seguridad de la Información, aunado a debilidades de coordinación y seguimiento entre los diferentes actores estratégicos de la Institución.

La creación de diferentes equipos intergerenciales sin una articulación efectiva entre ellos podría generar duplicación de esfuerzos o redundantes que no se traducen en resultados concretos en algunos casos. Lo que podría debilitar la capacidad de la Institución para cumplir con sus obligaciones legales, mitigar riesgos tecnológicos y garantizar la protección de la información institucional.

10. SOBRE LA REGULACIÓN DEL USO DE DATOS INSTITUCIONALES EN PLATAFORMAS DE INTELIGENCIA ARTIFICIAL

Se determinó que la Institución carece de una regulación normativa en cuanto al uso de datos Institucionales en plataformas de Inteligencia Artificial (IA), asimismo a nivel Gerencial tampoco se han emitido lineamientos sobre el uso de los datos en estas herramientas en los diferentes procesos Institucionales.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información del MICITT en el punto "XI. Seguridad y Ciberseguridad" indican:

> *"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados. (…)*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución".*

Las Normas de Control Interno para el Sector Público, en el punto 5.8 "Control de sistemas de información" establecen:

> *"El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter."*

Los representantes de las Gerencias asignados para la atención del presente estudio, respecto a si han emitido desde la Gerencia, directrices o normas relacionados con el uso de los datos institucionales en plataformas tecnológicas de Inteligencia Artificial, señalaron:

> *"**Paula Ballestero Murillo, Gerencia de Logística:** No aún. Se están explorando las tecnologías, recomendaciones de AI y normativa país.*
>
> ***Giovanni Francisco Campos Alvarado, GIT:** No se han emitido directrices desde la Gerencia, directrices o normas relacionados con el uso de los datos institucionales en plataformas tecnológicas de inteligencia artificial, y/u otras tecnologías emergentes, debido a que no se han implementado este tipo de tecnologías de la Gerencia.*
>
> ***Aracelly del Mar Palma Moreno, Gerencia Administrativa:** No se han emitido directrices según la consulta planteada; sin embargo, se tiene conocimiento de lo señalado por parte de la Auditoría Interna en el Informe ATIC-0080-2023, así como del acuerdo 4 de la sesión del Consejo Tecnológico N° 005, celebrada el 17 de diciembre del año 2023", en el que se estableció textualmente: "(…) El Consejo Tecnológico instruye a la secretaría de este, la conformación de un equipo de trabajo intergerencial para presentar en sesión del Consejo Tecnológico la hoja de ruta para la gestión de las tecnologías emergentes en la CCSS (…)". En ese sentido, con oficio GA-0124-2025, del 29 de enero del 2025, esta gerencia designó -en atención del oficio GG-DTIC-0194-2025 de enero de 2025- un representante para conformar el equipo de trabajo que estará brindando atención a la recomendación 1 y 2 del informe ATIC-0080-2023.*
>
> ***Leslie Vargas Vásquez, Gerencia Médica:** No se tiene información en torno a normas o directrices para el uso de estas plataformas.*
> ***Johanna Mora Ulate, Gerencia de Pensiones:** A nivel institucional no hay normativa que regule el uso de información institucional en plataformas de inteligencia artificial.*

La ausencia de una regulación normativa institucional que defina el uso de datos en plataformas de Inteligencia Artificial podría generar un efecto en la seguridad, legalidad y eficiencia del manejo de la información en la CCSS, esta carencia impide establecer criterios claros sobre la protección, confidencialidad y uso ético de los datos institucionales cuando se integran en herramientas de IA, lo que incrementa el riesgo de exposición no autorizada, decisiones automatizadas sin supervisión adecuada y posibles incumplimientos normativos. Además, la falta de lineamientos desde las gerencias limita la capacidad de las unidades organizativas para evaluar, adoptar o controlar el uso de estas tecnologías emergentes de forma segura y alineada con los objetivos institucionales.

11. SOBRE LA GOBERNANZA DE DATOS EN EL CATÁLOGO DE RIESGOS INSTITUCIONAL

Esta Auditoría identificó que, en el Catálogo Institucional de Riesgos se incluyen riesgos relacionados con la Gobernanza y Gestión de Datos, así como de Seguridad de la Información, mencionados en el presente informe, de tal forma que existe razonablemente una identificación de éstos para que sean considerados en los niveles estratégicos y operativos.

Al respecto, el 7 de marzo de 2024, mediante oficio DSA-AGCI-0024-2024, suscrito por el Ing. Berny Montoya Fonseca, jefe del área de Control Interno, de la dirección de Sistemas Administrativos, se comunicó la actualización del Catálogo Institucional de Riesgos Versión 3, señalando:

> *"(…) como parte de las acciones para el fortalecimiento y mejora continua del control interno en la gestión, comunica que se ha actualizado el Catálogo Institucional de Riesgos en su versión 3. La actualización de este Catálogo contiene una sección de riesgos operativos y otra de riesgos estratégicos, además de ajustar algunas categorías a la necesidad institucional".*

Sobre lo anterior, al analizar el "Catálogo Institucional de Riesgos Estratégicos", se identificaron 3 riesgos definidos, que pueden estar relacionados con los aspectos señalados en los diferentes hallazgos del informe:

- ES-21 Inadecuada gestión de la planificación
- ES-22 No contar con la información requerida
- ES-23 Debilidades en el monitoreo, supervisión y control de las actividades

En esa misma línea, al verificar el "Catálogo Institucional de Riesgos Operativos", se identificaron los siguientes riesgos:

- TI-02 Acceso a sistemas e información digital por parte de personas no autorizadas
- TI-04 Pérdida de información digital
- OP-01 Pérdida de información física
- OP-02 No contar con información requerida
- CO-05 Uso indebido de información
- EX-03 Acceso a la información física por parte de personas no autorizadas
- EX-05 Accesos no autorizados a las instalaciones

Debido a lo anterior no se emitirá recomendación adicional en el presente estudio, considerando que además la Guía Institucional de Valoración de Riesgos en su punto 9.6 "Catálogo Institucional de Riesgos" señala que ambos catálogos se actualizan periódicamente como parte de la mejora continua que desarrolla el Área Gestión de Control Interno.

CONCLUSIONES

En el contexto actual de transformación digital y creciente dependencia de la información para la toma de decisiones, la implementación de una adecuada gobernanza y gestión de datos se vuelve esencial para garantizar la eficiencia, transparencia y seguridad institucional. En el caso de la Caja Costarricense de Seguro Social, disponer de una estructura sólida que regule el ciclo de vida de los datos —desde su generación hasta su eliminación— no solo fortalece la rendición de cuentas y el cumplimiento normativo, sino que también permite optimizar los servicios de salud y pensiones, proteger la privacidad de las personas usuarias y fomentar la innovación basada en evidencia.

La gobernanza de datos no debe entenderse como un fin en sí mismo, sino como un habilitador estratégico que potencia la capacidad institucional para responder a los desafíos actuales y futuros con agilidad, integridad y responsabilidad.

Al respecto, la Auditoría evidenció la falta de implementación efectiva de la Política Institucional para la Gobernanza de Datos, aprobada por la Junta Directiva en abril de 2022. A pesar de su divulgación inicial, no se desarrolló la Agenda de Implementación, ni se establecieron mecanismos formales para su ejecución en las distintas unidades gerenciales, esta omisión genera una desconexión entre el mandato estratégico y su aplicación operativa, debilitando la capacidad institucional para gestionar los datos de forma coherente y segura.

Asimismo, se identificó que el proyecto "Hoja de Ruta para la Gobernanza de Datos de la CCSS", gestionado con el MIDEPLAN y el Banco Mundial, no integró desde su formulación el acuerdo de la Junta Directiva, ni contó con representación de la Gerencia General. Esta falta de alineación institucional compromete la articulación entre iniciativas estratégicas y puede derivar en esfuerzos duplicados, pérdida de sinergias y una limitada rendición de cuentas.

Otro hallazgo relevante fue la no implementación del Modelo de Gestión Integral para el cumplimiento de la Ley N.º 8968 sobre protección de datos personales. Aunque se desarrollaron productos claves como protocolos, convenios y plantillas, estos no fueron formalmente adoptados ni integrados en la gestión institucional, lo que incrementa el riesgo de incumplimientos normativos y vulneraciones a la privacidad.

También se evidenció una débil vinculación entre el Plan Estratégico Institucional (PEI) 2023–2033 y los Planes Tácticos Gerenciales. Varias gerencias no han definido objetivos ni indicadores alineados con las líneas de

acción estratégicas relacionadas con la gobernanza de datos, lo que limita la capacidad de seguimiento, evaluación y ajuste de las acciones institucionales en esta materia.

Finalmente, se constató la ausencia de un marco normativo integral sobre gobernanza de datos, la falta de clasificación formal de los datos institucionales, y la inexistencia de lineamientos sobre el uso de datos en plataformas de inteligencia artificial. Estas carencias, sumadas a una gestión fragmentada de los equipos intergerenciales, debilitan el control interno y la capacidad de la CCSS para tomar decisiones informadas, proteger su información y cumplir con sus objetivos estratégicos.

RECOMENDACIONES

A LA MÁSTER MÓNICA TAYLOR HERNÁNDEZ, EN SU CALIDAD DE PRESIDENTA EJECUTIVA O QUIÉN EN SU LUGAR OCUPE EL CARGO

1. Considerando que el *"Proyecto de Cooperación Técnica y Financiera no Reembolsable con MIDEPLAN para la Hoja de Ruta para la Gobernanza de Datos de la CCSS"* es una iniciativa impulsada desde la Presidencia Ejecutiva, se recomienda valorar la incorporación de representantes de todas las gerencias, así como de otros actores institucionales clave, en el equipo responsable de acompañar dicha asistencia técnica. Esta integración debe garantizar una visión integral y multisectorial para la implementación efectiva de la hoja de ruta.

   En conjunto con este equipo, se deberá definir un Plan de Implementación del proyecto que contemple los requerimientos de los entes externos involucrados, siempre en apego al marco legal vigente. Este plan deberá considerar, entre otros aspectos que se estimen pertinentes:

   - La inclusión de la Agenda de Implementación de la Política Institucional para la Gobernanza de Datos, conforme al acuerdo segundo del artículo 5 de la sesión N.° 9253 de la Junta Directiva del 21 de abril de 2022.
   - La definición de la autoridad institucional competente para suscribir el respectivo acuerdo con el Banco Mundial.
   - La planificación y gestión del proyecto con enfoque en presupuesto, alcance, cronograma e indicadores de desempeño.
   - La incorporación de un enfoque institucional en la gestión de datos, incluyendo a la Gerencia de Pensiones y otras áreas más allá de los sistemas de salud y financieros.
   - El análisis del nivel de acceso a los datos por parte de los entes externos, asegurando el cumplimiento de la Ley N.° 8968 sobre Protección de Datos Personales y demás normativa aplicable.
   - La consideración de los productos desarrollados por la Comisión Interinstitucional para el Modelo de Gestión Integral de cumplimiento de la Ley N.° 8968.
   - Elaboración de un procedimiento estandarizado que contemple criterios técnicos y jurídicos para autorizar, controlar y auditar el intercambio de datos e información entre instituciones del Estado, Entes internacionales o empresas privadas mediante convenios,
   - La definición de un marco normativo institucional integral en materia de gobernanza y gestión de datos, alineado con estándares internacionales.
   - La implementación de un esquema formal de clasificación de los datos institucionales.
   - Hacer de conocimiento al equipo intergerencial conformado, sobre las diferentes iniciativas realizadas por los diversos grupos de trabajo, para evitar duplicidad de esfuerzos y mejorar la coordinación.
   - La elaboración de una regulación normativa sobre el uso de datos institucionales en plataformas de Inteligencia Artificial.

   El Plan de implementación del proyecto debe definir actividades, responsables y plazos de ejecución, así como los mecanismos de seguimiento de tal forma que se garantice el éxito de este, en atención además de los señalado en los **hallazgos 1, 2, 3, 4, 6, 7, 9, 10 y 11** del presente informe.

Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de **doce meses**, a partir de la recepción del presente informe, la documentación que respalde el Plan de Implementación y el cumplimiento de aquellas actividades que fueron definidas dentro de este plazo de atención.

A LA MÁSTER MÓNICA TAYLOR HERNÁNDEZ, EN SU CALIDAD DE PRESIDENTA EJECUTIVA O QUIÉN EN SU LUGAR OCUPE EL CARGO, EN EL TANTO NO EXISTA GERENTE GENERAL EN EJERCICIO

2. Llevar a cabo un plan de atención y seguimiento de la implementación de las iniciativas correspondientes a la Seguridad de la Información de la hoja de ruta del Programa de Ciberseguridad, de acuerdo con lo instruido en el acuerdo 4 del tema 2 de la sesión N° 003 del Consejo Tecnológico del 21 de junio de 2024, y según lo descrito en el **hallazgo 8** del presente informe.

   Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de **doce meses**, a partir de la recepción del presente informe, la documentación que respalde la definición de dicho plan y la ejecución de las actividades que fueron definidas dentro de dicho plazo de atención de la recomendación.

A LA MÁSTER SUSAN PERAZA SOLANO, DIRECTORA DE PLANIFICACIÓN INSTITUCIONAL, O A QUIEN EN SU LUGAR OCUPE EL CARGO

3. Efectuar un análisis en la evaluación del Plan Estratégico Institucional 2023 – 2033, respecto al establecimiento de las líneas de acción para el cumplimiento del objetivo 3 por parte de las Gerencias de la Institución, de identificarse debilidades para la atención de dichas líneas de acción, efectuar las medidas correctivas de tal forma que se garantice el cumplimiento de los objetivos institucionales trazados en el PEI y en línea con lo descrito en el hallazgo 5 del presente informe.

   Para acreditar el cumplimiento de la presente recomendación, deberá remitirse a este Órgano de Fiscalización en un plazo de **ocho meses**, a partir de la recepción del presente informe, la documentación que respalde el análisis realizado y las acciones efectuadas.

En relación con las recomendaciones expuestas en el presente informe, en el plazo de 10 días hábiles[2] se deberá remitir a esta auditoría el "cronograma de acciones[3]" 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-0032-2025. De esta misma forma, se remitirá posteriormente, la evidencia que constate los avances.

[2] 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.
[3] Art. 68 del Reglamento de Organización y Funcionamiento de la Auditoría Interna.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 62 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 11 de julio del 2025 de conformidad con la convocatoria realizada por la Auditoría Interna, mediante oficio AI-1040-2025 del 4 de julio de 2025, estando presentes los siguientes funcionarios de la Administración Activa: Licda. Angeline Badilla Berrocal y Licda. Deily Carolina Gallo Chaves, asesoras de la Presidencia Ejecutiva, Lic. Mayid Morales Madrigal y Lic. Orlando José Rivas Acosta, asesores de la Gerencia General, Ing. Adriana Chavarría Loría, directora a.i.de la Dirección de Planificación Institucional.

A continuación, se indican las observaciones realizadas en torno a los hallazgos y recomendaciones:

- **Sobre los hallazgos:**

Hallazgo 1

El Lic. Mayid Morales Madrigal señala que recientemente se han tenido varias reuniones respecto a la Política de Datos y la implementación, y hay un oficio que salió recientemente, emitido por doña Mónica, a cargo de la Gerencia General, conformando ya un equipo para trabajar en la agenda de implementación y eso fue producto de 2 sesiones de trabajo que se tuvo de previo, estamos hablando de una sesión específicamente para conocer la política, ver todos los enunciados y otro en el cual se conoció el contexto de lo que tenían los equipos de la Gerencia Médica sobre un modelo de Gobernanza interno que están desarrollando que se va a incluir, entonces son dos antecedentes que es bueno considerarlo.

Hallazgo 2

La Licda. Carolina Gallo Chaves, señala que comprende que la información recabada por la Auditoría fue hasta mayo de 2025, pero quería comentar que ya el proyecto fue aprobado por MIDEPLAN, el 1 de julio ya hubo una reunión donde se expuso a los Gerentes, cual es el alcance general de ese proyecto, se expuso por parte del Banco Mundial, cuáles son los productos esperados que se entregarían con esta cooperación, y precisamente en el tema de la incorporación de la Gerencia General, ya hemos estado conversando precisamente con Mayid, y lo que se acordó hacer un solo equipo, uno coordinador y otro técnico, que puedan paralelamente apoyar la agenda de implementación con la cooperación del Banco Mundial, empezaría incluso ya la otra semana, donde se agendó varias entrevistas con el Banco Mundial, para revisar y hacer una consultoría contratada por el Banco, que efectúe un análisis de la madurez de datos, para posteriormente generar la hoja de ruta, si bien la Gerencia General no estuvo al inicio del desarrollo de la propuesta, si están con conocimiento de esto y estamos trabajando de la mano.

Al respecto el Ing. Leonardo Díaz, aclara que la información expuesta en los hallazgos del informe contempla la propuesta inicial, la formulación, ya que el alcance fue a mayo de 2025 y a esa fecha lo que se disponía era de la documentación de dicha formulación.

La Licda. Angeline Badilla Berrocal indicó que recientemente se presentó en Consejo Tecnológico, el avance y actividad del cronograma que atiende el informe ATIC-113-2023, que está relacionado con el tema de Seguridad de la Información, con algunas actividades que ya presentó la DTIC, y ya se vio en Consejo Tecnológico y fue aprobado, entonces también se está avanzando por ese lado.

Hallazgo 3

La Licda. Carolina Gallo Chaves, menciona que inicialmente si se tenía ese vacío en cuanto a la aprobación, y que incluso se conversó con la Dirección Jurídica, para consultarles, y dijeron que ya había un formato para la cooperación y que se debía hablar con el CENDEISSS, pero en aras de la honestidad no se había visto lo de la aprobación por parte de Junta Directiva y tampoco lo señalaron, por lo que agradece si se puede compartir dicho criterio para corregir lo correspondiente. Al respecto se le comparte el oficio correspondiente por parte de la Auditoría.

Respecto a la fuente de financiamiento señaló la Licda. Gallo Chaves que es un poco difícil de definirlo, porque en lo que se va a fundamentar es en cuantas horas podría el equipo conformado estar trabajando en apoyar lo que solicite el Banco Mundial y se estima con base a salarios.

Sobre el alcance la Licda. Gallo Chaves, señala que la Caja al ser muy grande, el Banco Mundial no sabía si iba haber espacio para poder analizar todo, pero si se insistió en que la Gobernanza no podía ser parcial en ver solo Gerencia Médica o Financiera, y lo que se quería es que la cooperación se convirtiera en un insumo que vaya a generar a la Institución un producto ya real y no seguir con un diagnóstico o iniciativas, o con aspectos que si bien es cierto apoya, no permite construir lo que verdaderamente la Institución necesita, de ahí que si nació y quedó muy claro que la hoja de ruta no es para la Gerencia Médica, si no es a nivel Institucional, que la cooperación nos alcance para mapear solo una gerencia, no quiere decir que no estemos visualizando que esto es integral y ya sea mediante la cooperación o no, la hoja de ruta debe de quedar adecuadamente planteada para que la Institución pueda finalizar esto.

La Licda. Carolina Gallo, señala que, en cuanto a la definición del nivel de acceso a los datos, hay responsables de las bases de datos, y se tiene pleno conocimiento de que las bases de datos deben de ir con datos anonimizados, eso también lo tiene claro el Banco, tal vez no quedó muy claro en los documentos, pero si es un tema que si se ha valorado y definido con ellos.

Hallazgos 4, 5, 6, 7 y 8: no hubo comentarios

Hallazgo 9

La Licda. Carolina Gallo señala que precisamente cuando se tiene el acercamiento, se avanza y se consulta con diferentes personas, mencionan que ciertos aspectos ya se hicieron, y lo que se necesita es la unidad, porque ya se ha avanzado en algunos diagnósticos, desde la Gerencia Médica ya se han hecho esfuerzos, creo que es donde más se han hecho esfuerzos, porque les tocó por el EDUS, la ley les obligó, pero si, se han hecho muchos esfuerzos aislados incluso con personas que ya no trabajan en las unidades, y es un tema que habrá que analizar conforme se vayan obteniendo los productos.

Hallazgos 10 y 11 no hubo comentarios

- **Sobre las recomendaciones:**

Recomendación 1

La Licda. Carolina Gallo señala que en la recomendación se indica “de formalizar dicha asistencia” sin embargo ya está formalizada por lo que se debe considerar el cambio. Asimismo, señala que, respecto a la actualización del Catálogo Institucional de Riesgos, ya que existe una instancia en la Institución que maneja este tema actualmente, por lo que debería asumir la actualización, y no la Presidencia.

Al respecto, el Lic. Mayid Morales señala que concuerda que la actualización del Catálogo es una tarea más propia del área de Gestión de Control Interno. Además, señala que en cuanto a la consolidación del equipo intergerencial, debería considerarse más bien que se verifique que el equipo intergerencial conozca las diferentes iniciativas para evitar duplicidad de esfuerzos, y que no se entienda que hay que consolidar un equipo.

Se solicita ampliar el plazo a 12 meses por la complejidad del tema y el involucramiento de diferentes actores.

Recomendación 2

La Licda. Angeline Badilla señala que como ya se tiene una hoja de ruta para el tema de Ciberseguridad y Seguridad de la Información, e inclusive ya hay actividades que se han ido desarrollando, y considerando que ya se vio en Consejo Tecnológico, lo ideal sería darle seguimiento al acuerdo de la sesión del Consejo Tecnológico, en cuanto al plazo, se podría ajustar de conformidad con los plazos establecidos en el cronograma, dar por

atendida la recomendación, presentando las actividades con los plazos establecidos, por lo que se acordó que la Licda. Badilla remitiera a la Auditoría los acuerdos del Consejo Tecnológico que hace referencia para valorar los ajustes.

(Al respecto, se gestionó con la Licda. Carolina Gallo la remisión de la información del Consejo Tecnológico, y una vez trasladada se identificó que el tema visto en la sesión del Consejo mencionado por la Licda. Badilla correspondía al tema de Continuidad del Negocio, por lo que se llegó al acuerdo de que se mantuviera la redacción de la recomendación inicial, modificando el plazo de atención a 12 meses por cuanto es un tema complejo que requiere coordinación intergerencial y llevarlo nuevamente a Consejo Tecnológico)

Recomendación 3

No hubo observaciones, respecto al plazo la Ing. Adriana Chavarría Loría solicita ampliar a 8 meses ya que el proceso de modificaciones del PEI finaliza en marzo de 2026.

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Firmado Digitalmente

Ing. Leonardo Díaz Porras
Asistente de Auditoría

Firmado Digitalmente

Ing. Rafael Ángel Herrera Mora, jefe
Área

OSC/RJS/RAHM/LFDP/ayms