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

Al contestar refiérase a: **ID-108928**

AD-ATIC-0011-2024
15 de febrero de 2024

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA – 1103

Máster
Robert Picado Mora, subgerente
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimado(a) señor(a):

ASUNTO:	**Oficio de Advertencia relacionado con la implementación de la Norma Técnica sobre requisitos de Ciberseguridad para participar en el SINPE emitida por el Banco Central de Costa Rica.**

En cumplimiento de las actividades de asesoría y fiscalización consignadas en el Plan Anual Operativo del Área de Tecnologías de Información y Comunicaciones de esta Auditoria para el período 2024, asimismo con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se emite el presente documento con aspectos importantes a ser considerados por esa Gerencia Financiera y la Dirección de Tecnologías de Información y Comunicación, en cuanto a la implementación de la Norma Técnica sobre requisitos de Ciberseguridad para participar en el SINPE, emitida por el Banco Central de Costa Rica (BCCR).

ANTECEDENTES

El 17 de abril de 1997, fue puesto en marcha el Sistema Nacional de Pagos Electrónicos (SINPE) cuya plataforma tecnológica es desarrollada y administrada por el Banco Central de Costa Rica, la misma que conecta a entidades financieras e instituciones públicas del país a través de una red privada de telecomunicaciones, la cual les permite realizar la movilización electrónica de fondos entre cuentas IBAN y participar en los mercados de negociación que organiza dicho banco, asimismo, se han desarrollado otros servicios como Transferencias de Fondos a Terceros, Créditos Directos, Débitos Directos y otros que permiten mayores opciones para movilizar los fondos de una entidad financiera hacia otra.

A nivel de la CCSS, la plataforma SINPE es utilizada en diversos procesos institucionales como lo son los de recaudación, pago a proveedores, pago de incapacidades, entre otros.

El Banco Central de Costa Rica, desarrolló el Reglamento del Sistema de Pagos, mismo que se encuentra vigente con la modificación realizada el 21 de diciembre de 2022 y publicada en el diario oficial La Gaceta el 17 de enero de 2023, en el cual se regula la organización y el funcionamiento del SINPE y los sistemas de pago de importancia sistémica (liquidación del mercado bursátil, liquidación del mercado de pagos con tarjeta, pago en el transporte público, entre otros), con el objetivo de promover la eficiencia y el normal funcionamiento del sistema de pagos costarricense. En dicha norma en el artículo 10 se define el cumplimiento del marco regulatorio por parte de las entidades afiliadas, en el que señala:

> *"Los afiliados deben someterse a las disposiciones establecidas en el presente reglamento y cumplir con los lineamientos y acuerdos definidos en los libros de la Serie de Normas y Procedimientos del SINPE; en particular, cumplir con la certificación de las reglas definidas para cada servicio en la relación con el cliente final".*

Al respecto, el BCCR emitió el comunicado SINPE 015-2023, enviado mediante correo electrónico el 23 de mayo de 2023, a los afiliados del Sistema Financiero Nacional indicando:

> *"El creciente desarrollo del Sistema Nacional de Pagos Electrónicos (SINPE) ha llevado a la aceleración de los procesos de digitalización de los movimientos de fondos a nivel interbancario, derivando en un incremento en el acceso de los clientes a los canales digitales de sus entidades participantes y una mayor cantidad de transacciones en línea, lo cual incrementa los riesgos de ciberataques.*
>
> *Dado este panorama, resulta conveniente ampliar el alcance de los controles en materia de seguridad de la información, más allá del ámbito de acción del BCCR, llegando a ciertas áreas tecnológicas propias de las entidades que operan en el SINPE, con la finalidad de fortalecer aún más dicha seguridad y con ello prevenir los riesgos de ciberataques a esta plataforma.*
>
> *La División de Sistemas de Pago, en cumplimiento de las funciones que le han sido encomendadas por la Junta Directiva del BCCR, y conforme con lo establecido en el artículo 19 del Reglamento de Sistemas de Pago, se permite enviar en consulta la Norma Técnica "Requisitos de Ciberseguridad para participar en el SINPE". El cumplimiento de los requisitos definidos en esta norma, por parte de los afiliados, nos permitirá como sistema, disponer de un ambiente más seguro y robusto para mitigar de una forma más adecuada posibles ataques informáticos".*

Es así como el 21 de julio de 2023, entró en vigencia la Norma Técnica "Requisitos de Ciberseguridad para participar en el SINPE", la cual establece los requisitos y disposiciones de carácter complementario al Reglamento del Sistema de Pagos y el marco normativo emitido por el Banco Central de Costa Rica para regular los aspectos relacionados con los controles de ciberseguridad que deben cumplir los afiliados al SINPE, con el fin de ampliar el alcance de los controles de seguridad de la información, para extender el radio de acción hasta ciertas áreas tecnológicas propias de las entidades participantes en el SINPE, fortalecer la red de seguridad del sistema y prevenir riesgos de ciberataques.

La Norma Técnica en mención, es de acatamiento obligatorio por parte de los afiliados al SINPE, y como tal constituye un requisito para mantener la condición de afiliado, por lo que se debe cumplir una serie de regulaciones dirigidas a adoptar marcos de ciberseguridad adecuados para la protección del sistema, considerando los servicios particulares que cada afiliado tiene autorizados, de manera que el nivel de rigurosidad de los controles esté determinado por el nivel de exposición que tiene los servicios por medios digitales, la misma debe ser cumplida a mas tardar el 30 de junio de 2024, en cuyo caso de incumplimiento y dependiendo del impacto que esto provoque en el ambiente de seguridad, el BCCR podrá ordenar la apertura de un procedimiento administrativo.

Esta Norma contempla 48 controles que los afiliados deben cumplir, de las cuales 40 son obligatorias y 8 opcionales, las mismas están relacionadas con la infraestructura requerida para operar el SINPE, equipos de conexión, usuario de SINPE, capa de intercambio de datos y servidores interconectados. Dichos controles están clasificados en:

1. Inventario y control de activos de hardware
2. Inventario y control de activos de software
3. Protección de los datos
4. Configuración segura de la infraestructura
5. Administración de cuentas y control de accesos
6. Gestión de vulnerabilidades
7. Gestión de bitácoras de auditoría
8. Protección del correo electrónico y navegación por internet
9. Defensa contra código malicioso
10. Recuperación de datos

11. Gestión de infraestructura de red
12. Monitoreo y defensa de la red
13. Concientización en Ciberseguridad y formación de habilidades
14. Gestión de proveedores de servicios
15. Seguridad en las aplicaciones
16. Gestión de respuesta ante incidentes

Para dar por atendido el cumplimiento de la Norma Técnica, la misma en artículo 5.4 “Cumplimiento” señala:

> *“Los afiliados actuales y los interesados en afiliarse al Sinpe deberán presentar un informe de cumplimiento de parte de un auditor, con no más de un mes de emitida, en la que se especifique que la entidad cumple a cabalidad con los controles establecidos, según sea el nivel de riesgos en el que se ubique.*
>
> *Con la finalidad de garantizar que las labores sean ejecutadas por expertos certificados, el profesional a cargo de la certificación deberá contar con al menos una de las siguientes certificaciones:*
>
> - *ISACA: Certified Information Systems Auditor (Solicitado por las ODM’s)*
> - *ISO: ISO 27001 Lead Auditor*
> - *GIAC: GIAC Systems and Network Auditor (GSNA)*
>
> *La entidad que presenta la certificación es responsable de verificar y dar garantía ante el BCCR de que el auditor elegido cumple con los atestados exigidos por esta norma, debiendo manifestar que se efectuó dicha validación, en el oficio de la certificación que envíe al Banco Central. En caso de que el auditor incumpla con los atestados exigidos, el BCCR dará como inválida la certificación presentada”*

Al respecto, la certificación de Auditoría debe ser enviada con una nota formal firmada digitalmente por el Gerente General o el Representante Legal de la entidad al Departamento Sistema Nacional de Pagos Electrónico del BCCR, por medio de un caso enviado por el responsable de Servicios de la entidad, y en caso de que el informe de auditoría señale controles incumplidos, se debe aportar un plan remedial para solventar las brechas detectadas y su atención deberá finalizarse a más tardar el 31 de octubre del año en curso, así definido en el artículo 5.4.1 de la norma de marras.

I. GESTIONES EFECTUADAS POR LA CCSS PARA EL CUMPLIMIENTO DE LA NORMA TÉCNICA SOBRE REQUISITOS DE CIBERSEGURIDAD PARA PARTICIPAR EN EL SINPE

Esta Auditoría, mediante oficio AI-2477-2023 del 13 de diciembre de 2023, le consultó a la Licda. Paula Chaves Sánchez, jefe a.i. del Área de Tesorería General, sobre el avance en la implementación de los controles establecidos en la Norma Técnica sobre requisitos de Ciberseguridad para participar en el SINPE, por lo que mediante oficio DFC-ATG-1618-2023 del 20 de diciembre de 2023 indicó:

“

- *Mediante el oficio **GF-DFC-1621-2023 de fecha 01 de agosto del 2023 suscrito por la Dirección Financiero Contable,** se le notifica al Centro de Gestión de Informática de la Gerencia Financiera la recepción del documento denominado “Requisitos de Ciberseguridad para participar en el SINPE” sobre el cual se solicitó realizar las observaciones que se consideren necesarias. De igual manera, en este documento se solicita la colaboración a efectos de coordinar, en conjunto con el Área Tesorería General, lo correspondiente desde el punto de vista técnico, a efectos de cumplir con las regulaciones establecidas por el Banco Central de Costa Rica (BCCR) con ocasión al uso de la plataforma SINPE.*

- *Con el oficio **ATG-SARE-0361-2023 de fecha 30 de agosto del 2023 suscrito por el Subárea de Recaudación Externa,** dirigido al Ing. Danilo Hernández Monge, del Área de Ingeniería en Sistemas de la Dirección de Tecnologías, en el cual se solicita la intervención para analizar la Norma Técnica; así como la disponibilidad para organizar una sesión de trabajo en forma conjunta organizar las sesiones de trabajo para abordar el tema.*

- *En línea con lo anterior, se han estado realizando sesiones de trabajo con los representantes de la Dirección de Tecnologías, Centro de Gestión de Informática de la Gerencia Financiera y de la Gerencia de Pensiones, compañeros del Área de Tesorería y Sub-Área de Recaudación Externa, a efectos de analizar cada uno de los requerimientos explicitados en la Norma Técnica, así como el cumplimiento y ajustes que se requieran en los procesos para dar cumplimiento a cada uno de estos.*

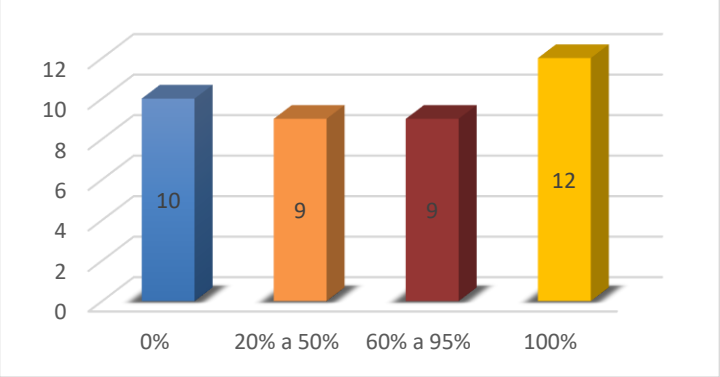
- *Con el oficio **DFC-ATG-1158-2223 de fecha 06 de setiembre 2023 suscrito por el Área de Tesorería,** se hace la designación de la jefatura del Subárea de Recaudación Externa para que trabaje en la atención de la parte técnica y administrativa, relacionado con el abordaje de la implementación de la Norma Técnica "Requisitos de Ciberseguridad para la participación en el SINPE". Al respecto, actualmente se están elaborando las justificaciones técnicas, así como la ficha técnica de la contratación, con el objetivo de realizar el estudio de mercado e iniciar con la compra de la Contratación de la Auditoría, a efectos de certificar el cumplimiento con la Norma Técnica de Requisitos de Ciberseguridad para participar en el SINPE".*

II. AVANCE EN LA IMPLEMENTACIÓN DE CONTROLES DE LA NORMA TÉCNICA

Mediante oficio DFC-ATG-1618-2023 del 20 de diciembre de 2023, suscrito por la Licda. Paula Chaves Sánchez, jefe a.i. del Área de Tesorería General, se adjuntó la "Matriz de Requerimientos de la Norma Técnica de Ciberseguridad SINPE", en la cual se lleva el registro de porcentajes de avances, estado del control, responsables, entre otros.

Al respecto, esta Auditoría analizó la Matriz de Requerimientos[1], identificándose que, de los 40 controles obligatorios, 10 registran un avance del 0%, 9 un avance del 20% al 50%, misma cantidad (9) para el rango de 60% a 95% de avance y 12 presentan un cumplimiento del 100% tal y como se observa:

Gráfico 1
Cantidad de Controles según porcentaje de avance en la implementación de la Norma Técnica sobre Requisitos de Ciberseguridad para participar en el SINPE
20 de diciembre de 2023



Fuente: Oficio DFC-ATG-1618-2023

[1] En el Anexo 1 se adjunta la Matriz completa sobre el avance de los requerimientos de la Norma Técnica

Sobre lo anterior, los 10 controles que registran 0% de avance en la implementación son los siguientes:

Tabla 1
Controles con 0% de avance en la implementación de la Norma Técnica sobre Requisitos de Ciberseguridad para participar en el SINPE
20 de diciembre de 2023

CONTROL	ESTADO	%AVANCE
6.3.2 Cifrar los datos confidenciales en tránsito.	Pendiente	0
6.4.1 Establecer y mantener un proceso de configuración seguro.	Pendiente	0
6.4.2 Implementar y administrar un firewall.	En Proceso	0
6.7.1 Recopilar registros de auditoría.	Pendiente	0
6.7.2 Almacenar de forma adecuada los registros de auditoría.	Pendiente	0
6.7.3 Estandarizar la hora de los registros de auditoría.	Pendiente	0
6.7.4 Realizar revisiones de los registros de auditoría.	Pendiente	0
6.11.1 Establecer y mantener una arquitectura de red segura.	En Proceso	0
6.15.2 Establecer y mantener un proceso de desarrollo de aplicaciones seguro.	En Proceso	0
6.15.3 Establecer y mantener un proceso para gestionar las vulnerabilidades de las aplicaciones.	En Proceso	0

Fuente: Oficio DFC-ATG-1618-2023

Al respecto, los requerimientos o controles a implementar de acuerdo con lo definido en la Normativa Técnica deben de estar implementados y certificados por una Auditoría a mas tardar el 30 de junio del presente año, por lo que la Licda. Paula Chaves Sánchez, referente a la finalización de la implementación indicó:

> *"Se espera que esté listo el cumplimiento de los requerimientos con los funcionarios de la Dirección de Tecnologías finalizando el mes de enero. Lo cual es un requisito para finiquitar lo relacionado con la compra de la Contratación de la Auditoría que certifique el cumplimiento institucional de cada uno de los requerimientos, al respecto esta compra se requiere concluir en el mes de febrero".*

III. CONSIDERACIONES

La situación expuesta, en cuanto al cumplimiento de la Normativa Técnica sobre los requisitos de Ciberseguridad para participar en el SINPE, deben ser de atención de la administración activa, dado su importancia en el uso de este medio de pago y transacciones financieras, en diversos procesos que se llevan a cabo en la CCSS como lo son el pago a proveedores, incapacidades, recaudación, entre otros, no solo por el cumplimiento normativo que está requiriendo el Banco Central de Costa Rica, sino además por el fortalecimiento de la Ciberseguridad a nivel institucional que tiene como efecto la implementación de los controles establecidos en dicha norma.

Considera esta Auditoría, que es importante que se gestionen adecuadamente los controles requeridos por el BCCR, garantizando el cumplimiento técnico en el tiempo correspondiente, y teniendo presente el plazo otorgado el cual vence el 30 de junio de 2024, estimando además la duración del proceso de contratación de la Auditoría que debe certificar la atención de la Normativa Técnica expuesta, por lo que se debe prestar especial atención en aquellos controles que tienen un porcentaje de avance bajo, a 5 meses de que se cumpla el plazo estipulado.

Es importante que se lleven a cabo los ajustes correspondientes en materia de Ciberseguridad, de tal forma que los servicios brindados por la Institución no se vean impactados, y tampoco se exponga a la Institución a un procedimiento administrativo o de otra índole ante una eventual materialización de riesgos en esta materia por ausencia de acciones en el fortalecimiento de la seguridad informática en la CCSS.

El Reglamento del Sistema de Pagos en el artículo 10 “Cumplimiento del marco regulatorio” establece:

> *“Los afiliados deben someterse a las disposiciones establecidas en el presente reglamento y cumplir con los lineamientos y acuerdos definidos en los libros de la Serie de Normas y Procedimientos del SINPE; en particular, cumplir con la certificación de las reglas definidas para cada servicio en la relación con el cliente final. El director de la División Sistemas de Pago podrá suspender a un afiliado de su participación en cualquiera de los servicios del SINPE, en caso de que incumpla con alguna de las disposiciones regulatorias establecidas y ponga en riesgo el funcionamiento del sistema”.*

Las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de la Información emitidas por el Ministerio de Ciencia, Tecnologías y Telecomunicaciones, en el apartado XI “Seguridad y Ciberseguridad”, establece lo siguiente:

> *“La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.*
>
> *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.”.*

Así mismo en el apartado XIV “Aseguramiento” refiere:

> *“La institución debe disponer de prácticas formales que permitan la valoración de la disponibilidad y adecuada aplicación de un sistema de control interno para el uso eficiente de los recursos tecnológicos de la institución para lograr mantener la continuidad de las operaciones, salvaguarda y protección de la información y los activos asociados a su captura, procesamiento, consulta, almacenamiento y transferencia y la gestión apropiada de los riesgos asociados. (…)*
>
> *La institución debe estar comprometida en la aplicación de buenas prácticas y seguimiento en la gestión de las TI estableciendo criterios efectivos para el cumplimiento de regulaciones internas y externas, así como disposiciones contractuales”.*

Las Normas de Control Interno para el sector público, en el punto 4.5 ”Garantía de eficiencia y eficacia de las operaciones”, establece lo siguiente:

> *“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, así como los requisitos indicados en la norma 4.2.”.*

En virtud de lo expuesto, esta Auditoría previene y advierte de la situación planteada en el presente oficio, con el propósito de ser sometida a valoración y revisión por esa Gerencia Financiera y la Dirección de Tecnologías de Información y Comunicaciones, se adopten las medidas pertinentes y coadyuvar así al cumpliendo de los objetivos institucionales siempre en mejora de los servicios brindado a la población.

Finalmente, se realiza un recordatorio sobre lo establecido en el artículo No. 17 de la Ley General de Control Interno No. 8292, en el cual se hace énfasis en la atención con prontitud de los hallazgos u observaciones de la Auditoría por parte la administración activa, por lo cual se solicita respetuosamente informar a este Ente Fiscalizador respecto a las labores efectuadas en torno a las observaciones planteadas en el presente documento.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones a ejecutar para la administración del riesgo y atención de la situación comunicada, razón por la cual deben remitir a esta Auditoría en el **plazo de 10 días (contados a partir de recibido este oficio)** el plan de acción anexado al presente, donde se consideren los plazos estipulados por la Normativa Técnica emitida por el Banco Central de Costa Rica.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2024.02.16 14:45:31 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

Anexo (2)

1. Matriz de Requerimientos Norma Técnica de Ciberseguridad SINPE
2. Plan de Acción para la atención de riesgos.

C. Máster Marta Eugenia Esquivel Rodríguez, presidente, - coordinadora, Consejo Tecnológico, Presidencia Ejecutiva -1102.
Máster Vilma Campos Gómez, gerente a.i., Gerencia General -1100.
Licenciado Luis Rivera Cordero, director a.c. Dirección Financiero Contable- 1121
Licenciada Paula Chaves Sánchez, jefe a.i., Área de Tesorería General, Dirección Financiero Contable- 1121
Auditoría-1111

Referencia: ID-108928