INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL CONSEJO NACIONAL DE PRODUCCIÓN (CNP)

16 de noviembre de 2023

Informe N° DFOE-SOS-IAD-00007-2023

Contraloría General de la República
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización para el Desarrollo Sostenible
Auditoría de Carácter Especial - Compromiso de informe directo

F-GE-50 V7

CONTENIDO

IMÁGENES

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos del Consejo Nacional de Producción (CNP) responde al marco normativo y buenas prácticas aplicables, de manera que se promueva el logro de sus objetivos. El periodo evaluado comprende desde 01 de enero de 2023 al 31 de julio de 2023.

¿POR QUÉ ES IMPORTANTE?

El Consejo Nacional de Producción cumple un papel relevante en la comercialización y en el fomento de la producción agropecuaria, mediante actividades relacionadas con la compra de productos hortofrutícolas, cárnicos, abarrotes, embutidos y lácteos a los productores nacionales y el abastecimiento institucional de alimentos a través del Programa de Abastecimiento Institucional (PAI), así como en la elaboración y comercialización de alcoholes y bebidas alcohólicas mediante la Fábrica Nacional de Licores (FANAL).

El soporte de esos procesos y el cumplimiento de sus objetivos institucionales, conlleva el uso cada vez más intensivo de las tecnologías de información y sistemas informáticos, por lo que es una necesidad relevante garantizar de forma razonable la seguridad de la información de los sistemas sustantivos, pues contienen información de carácter crítico para la prestación de los servicios y cumplimiento de las competencias institucionales y por lo tanto, requieren ser protegidos ante cualquier uso fraudulento, accesos no autorizados, pérdida, alteración, difusión o en general ante cualquier evento que los coloque en riesgo.

¿QUÉ ENCONTRAMOS?

Se determinó que el Consejo Nacional de Producción presenta un cumplimiento bajo del marco normativo y buenas prácticas aplicables en materia de seguridad de la información, ya que si bien ha implementado una nueva infraestructura y controles de seguridad física y ha gestionado servicios para el control del malware, aún no ha implementado una estructura formal de tecnologías de información (TI) para el logro de los objetivos, no cuenta con un sistema de gestión de la continuidad de negocio ni tampoco con un sistema de gestión de la seguridad de la información.

En consecuencia, se determinó que la institución no cuenta con un área de tecnologías de información dentro de su estructura organizativa, que se encuentre acorde con las necesidades y la dinámica de las circunstancias institucionales, por lo tanto, no se han establecido funciones formales para los funcionarios encargados de la gestión de las tecnologías de información. A su vez, no existe una gestión de riesgos de tecnologías de información ni de seguridad de información, pues no se ha implementado el Marco de Gestión de Tecnologías de Información requerido para brindar de forma oportuna los servicios a través del uso y administración de los recursos tecnológicos; ni se han identificado, analizado y priorizado los riesgos a nivel institucional en esta materia.

Además, se evidenciaron debilidades en el sistema de gestión de la seguridad de la información, relacionadas con las contraseñas del sistema de administración de usuarios y la aplicación de parches críticos, definición e implementación de la política de seguridad de la información institucional y los procedimientos de control y monitoreo de respaldos, desempeño de las redes y prevención de eventos por amenazas o malware. Así como, debilidades en la detección y atención de vulnerabilidades críticas y altas comunicadas por la Contraloría General mediante oficio DFOE-SOS-0392, las cuales no han sido atendidas en su totalidad.

Por su parte, se identificó que la institución no ha definido e implementado un sistema de gestión de la continuidad de negocio, mediante el cual se tengan claramente identificados y clasificados los activos críticos para el negocio, que sirvan de insumo para diseñar su política de continuidad de negocio, considerando el análisis de impacto y riesgos, el plan de continuidad de negocio institucional y el plan de recuperación ante desastres.

Todo lo anterior, obedece a la ausencia de direccionamiento y monitoreo de la máxima autoridad para implementar la seguridad de la información como parte esencial del giro de negocio, lo que afecta negativamente el logro de los objetivos institucionales, conforme a sus competencias y al ordenamiento jurídico. A su vez, obedece a un débil ambiente de control en el establecimiento de acciones integrales y continuas para diseñar, adoptar, implementar y evaluar un sistema de gestión de la seguridad de la información e implementar, mantener y mejorar de manera integral el sistema de gestión de la continuidad de negocio en el Consejo Nacional de Producción.

En consecuencia, las situaciones señaladas pueden comprometer la integridad, disponibilidad y confidencialidad de la información, así como a una posible interrupción de servicios y tiempo excesivo de recuperación ante un evento. Además, pérdida de disponibilidad de sistemas comerciales que pueden impactar a terceras personas e interrumpir actividades comerciales en el sector agropecuario, máxime en mercados donde esta institución tiene exclusividad de distribución de productos.

¿QUÉ SIGUE?

Se emiten disposiciones al Presidente Ejecutivo y al Gerente General, con el propósito de que se implemente el Sistema de Gestión de la Continuidad del Negocio y el Sistema de Seguridad de la Información a nivel institucional en concordancia con la definición del Marco de Gestión de Tecnologías de Información y se formalicen las funciones, roles y responsabilidades del personal asignado a la gestión de las tecnologías de información, acorde con las necesidades de la institución de manera que maximice los beneficios y la disponibilidad de los recursos institucionales. Finalmente, que se implemente un plan de remediación de las vulnerabilidades sobre seguridad de la información que permita subsanar las situaciones identificadas.

INFORME DE
AUDITORÍA DE CARÁCTER ESPECIAL ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL CONSEJO NACIONAL DE PRODUCCIÓN (CNP)

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La presente auditoría se realizó en cumplimiento del Plan Anual Operativo de la DFOE, con fundamento en las competencias que le son conferidas a la Contraloría General de la República en los artículos 183 y 184 de la Constitución Política y los artículos 12, 17 y 21 de su Ley Orgánica, n°. 7 428.

1.2. El Consejo Nacional de Producción se encarga de la comercialización y el fomento de la producción agropecuaria, mediante actividades relacionadas con la compra de productos, el soporte de esos procesos y el cumplimiento de sus objetivos institucionales conlleva el uso cada vez más intensivo de las tecnologías de información y sistemas informáticos, por lo que resulta relevante garantizar de forma razonable la seguridad de la información de los sistemas para la prestación de los servicios y cumplimiento de las competencias institucionales.

OBJETIVO GENERAL

1.3. Determinar si la seguridad de la información de los sistemas críticos del Consejo Nacional de Producción responden al marco normativo y buenas prácticas aplicables de manera que se promueva el logro de sus objetivos.

ALCANCE

1.4. La auditoría comprendió el análisis de la gestión de tecnologías de información relacionada con la preparación que tiene el Consejo Nacional de Producción en materia de seguridad de la información y en su capacidad para detener, atenuar y responder a posibles ataques cibernéticos a sus sistemas. El período de análisis comprendió del 1 de enero de 2023 al 31 de julio de 2023.

CRITERIOS DE AUDITORÍA

1.5. El 7 de setiembre de 2023, se presentaron los términos de auditoría a los funcionarios del Consejo Nacional de Producción: Adolfo Ramirez Carballo Presidente Ejecutivo, David Adolfo Araya Amador Gerente General, María Teresa Muñoz Hernández Asistente

Técnica Administrativa y Sindy Mayorga Matarrita Coordinadora de Tecnologías de Información. Además, dichos criterios fueron comunicados mediante oficio DFOE-SOS-0450(12435) del 13 de setiembre de 2023.

1.6. Como parte de las fuentes de criterios de auditoría utilizados destacan las Normas técnicas para la gestión y el control de las tecnologías de la información del MICITT y las Normas de control interno para el sector público (N-2-2009-CO-DFOE), así como buenas prácticas de la industria y la seguridad tales como ISO/IEC 27001, ISO 22301, ISO 20072 y Cobit 2019.

METODOLOGÍA APLICADA

1.7. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR, el Procedimiento de Auditoría vigente, establecido por la DFOE, que está basado en la ISSAI 400: Principios de la Auditoría de Cumplimiento de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI por sus siglas en inglés).

1.8. Para el desarrollo de esta auditoría se utilizó la información suministrada por el personal del Consejo Nacional de Producción, mediante consultas por escrito, entrevistas y visitas que fueron documentadas.

1.9. Asimismo, se realizó una visita[1] al centro de datos de la institución para verificar el cumplimiento de mejores prácticas en la seguridad física, se ejecutaron pruebas no intrusivas de ciberseguridad a nivel de direcciones IP públicas[2] y dominios registrados del CNP y de la Fábrica Nacional de Licores, con el fin de determinar la suficiencia de los controles en dicha infraestructura para la protección de los componentes digitales institucionales y la seguridad de los datos. Además, se realizó un análisis, en el cual se relacionó la información del personal de la institución con los usuarios registrados en el servicio de directorio.

1.10. Finalmente, se realizó un taller[3] con personal de la ATSI y la Gerencia General, para identificar las causas y soluciones de las situaciones que se comunican en este informe, lo que contribuyó a lograr una visión integral de las causas, los desafíos, retos y oportunidades de mejora de la institución.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.11. Se destaca la colaboración prestada por parte de la Administración en la atención de consultas y sesiones de pruebas ejecutadas, así como las acciones oportunas emprendidas para abordar parcialmente las vulnerabilidades comunicadas mediante oficio DFOE-SOS-0392 (10984) del 21 de agosto de 2023, así como el ajuste a las debilidades

[1] Visita realizada el 06 de setiembre de 2023.
[2] Información suministrada mediante oficios GG-ATSI-OFIC-098-2023 y GG-OFIC-936-2023 del 30 de junio y 17 de julio de 2023 respectivamente.
[3] Taller realizado el 30 de octubre de 2023 con personal del CNP.

en las contraseñas del sistema de administración de usuarios y aplicación de parches críticos.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.12. El Consejo Nacional de Producción (CNP) es una Institución autónoma, con personalidad jurídica propia, autonomía funcional y administrativa[4], la cual tiene como finalidad específica el fomento de la producción agrícola, pecuaria y marina[5], así como la estabilización de los precios de los artículos requeridos para la alimentación de los habitantes del país y de las materias primas que requiera la industria nacional, en procura de un equilibrio justo en las relaciones entre productores y consumidores, para ello podrá intervenir en el mercado interno, industrializar los productos agrícolas, pecuarios y marinos, directamente o a través de empresas a las que el Consejo respalde o avale.

1.13. En el plan estratégico 2021-2031, el CNP se ha propuesto fortalecer la gestión institucional mediante la optimización y coordinación de los procesos administrativos, financieros, capacidades técnicas y tecnológicas para la prestación de servicios institucionales para el sector agropecuario.

1.14. En la memoria institucional del año 2022, se detalla que el principal reto de la institución es la modernización integral de los procesos, estructura y recursos tecnológicos para una operación robusta que responda a las necesidades y el valor público de la Institución.

1.15. Por otra parte, según este documento el CNP ha reconocido que tiene necesidades de transformación digital, cumplimiento normativo en la implementación del Marco de Gobierno y Gestión de las Tecnologías de Información, implementación de sistemas administrativos-financieros y operativos, mejora de los equipos de cómputo, seguridad de la información, análisis de riesgos y su tratamiento, metodología de proyectos y procedimientos que apoyen la administración, planes de continuidad del negocio, planes de contingencia, entre otros; y su impacto en cada uno de los procesos institucionales.

MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA

1.16. El Consejo Nacional de Producción implementó este año una nueva infraestructura mediante la cual actualizó completamente los equipos y licencias, concretó la migración y configuración de sus bases de datos en alta disponibilidad. Además, cuenta con un alto cumplimiento en la gestión de controles de seguridad física y malware.

1.17. Asimismo, implementó el Sistema de Planificación de Recursos Empresariales, que contempla los procesos de administración financiera, planificación y recursos humanos. Además, atendió de manera oportuna las debilidades encontradas en el sistema de administración de usuarios relacionadas con contraseñas inseguras o genéricas utilizadas por los usuarios tanto del CNP como la FANAL.

[4] Artículo 1, Ley Orgánica del Consejo Nacional de Producción
[5] Artículo 3 Ley Orgánica 6050

1.18. Por otra parte, la institución cuenta con un plan de capacitación y concientización al personal considerando temas relacionados con la seguridad de la información y su avance es de un 80% aproximadamente.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.1. El borrador del presente informe fue remitido al Consejo Nacional de Producción mediante oficio DFOE-SOS-0546 del 07 de noviembre de 2023, dirigido al señor Gerardo Duarte Sibaja, Presidente Ejecutivo; con el propósito de formular y remitir a la Contraloría General, las observaciones pertinentes sobre su contenido, con la respectiva documentación de respaldo.

1.2. El 08 de noviembre de 2023 se presentaron los resultados de la auditoría en reunión virtual con las personas funcionarias del CNP que se detallan a continuación: Gerardo Duarte Sibaja, Presidente Ejecutivo; David Adolfo Araya Amador, Gerente General; Sindy Mayorga Matarrita, Coordinadora del Área Tecnología y Sistemas de Información (ATSI); así como el señor Gustavo Chaves Vargas, Auditor interno de la institución.

1.3. Las observaciones al borrador de informe fueron remitidas por la institución mediante el oficio PE-OFIC-806-2023 el 10 de noviembre de 2023, relacionadas con la ampliación del plazo para atender las disposiciones. Lo resuelto sobre las observaciones efectuadas se comunicó mediante el oficio DFOE-SOS-0552 (16387) del 16 de noviembre de 2023.

SIGLAS Y ABREVIATURAS

1.19. En el siguiente cuadro se indican las principales siglas utilizadas en este informe y su significado.

Siglas / Abreviaturas	Significado
ATSI	Área de Tecnología y Sistemas de Información
BIA	Análisis de Impacto en el Negocio (Siglas en inglés:Business Impact Analysis)
CGR	Contraloría General de la República
CNP	Consejo Nacional de Producción
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
FANAL	Fábrica Nacional de Licores
LGCI	Ley General de Control Interno
MGTIC	Marco Gobierno y Gestión de las Tecnologías de la Información
PAI	Programa de Abastecimiento Institucional
SEVRI	Sistema Específico de Valoración de Riesgo
SGCN	Sistema de Gestión de la Continuidad de Negocio
SGSI	Sistema de Gestión de la Seguridad de la Información

2. RESULTADOS

SEGURIDAD DE LA INFORMACIÓN DE LOS SISTEMAS CRÍTICOS

2.1. La seguridad de la información comprende impulsores de valor específicos como la confidencialidad, integridad y disponibilidad de la información, la continuidad de los servicios y la protección de los activos de la información. Las debilidades en la gestión de la seguridad de la información, reducen la capacidad de una organización para mitigar el riesgo y aprovechar las oportunidades de las tecnologías de información en el mejoramiento de sus procesos de negocio. Por lo tanto, la seguridad y sus impulsores son un aspecto significativo sujeto de evaluación ante las amenazas y vulnerabilidades a las que están expuestas las instituciones del país.

2.2. El Consejo Nacional de Producción implementó[6] en agosto de este año una nueva infraestructura tecnológica, así como herramientas de seguridad de red para protegerse de amenazas externas como malware y ransomware, además, cuenta con una contratación para gestionar la seguridad y rendimiento de sus aplicaciones de Internet, también, ha implementado controles de seguridad física y gestión de la capacitación y concientización a usuarios.

2.3. Sin embargo, se identificaron debilidades relacionadas con la ausencia de una estructura formal de tecnologías de información que apoye el logro de los objetivos de seguridad de la información, tampoco cuenta con los sistemas de gestión de la continuidad de negocio y seguridad de la información que considere controles de monitoreo de respaldos, desempeño de las redes y prevención de eventos, los cuales se señalan seguidamente.

No se ha implementado una estructura de tecnologías de información que apoye el logro de los objetivos de seguridad de la información

2.4. Se determinó que el Consejo Nacional de Producción no ha establecido formalmente una estructura que defina la organización formal de las tecnologías de información, sus relaciones jerárquicas, líneas de dependencia y coordinación, así como la relación con otros elementos que conforman la institución, y que apoye el logro de los objetivos. Cabe señalar, que el CNP cuenta con el Área de Tecnologías y Sistemas de Información (ATSI), la cual pertenece según organigrama a la Dirección de Planificación desde el año 2020[7]; sin embargo, a nivel operativo la ATSI ha estado bajo la dirección directa de la Gerencia General durante los últimos años.

2.5. De conformidad con lo indicado sobre la ausencia de una estructura formal de TI, tampoco se han definido las funciones formales para los funcionarios de tecnologías de

[6] Contratación 2022LA-000001-0034100001 sobre suscripciones, renovación de contratos: equipo donde se adquirió las herramientas de seguridad.
[7] Aprobado por MIDEPLAN en oficio DM-050-2000 del 30 de mayo de 2000.

información conforme a la dinámica institucional, por lo tanto, no existe una definición de las responsabilidades correspondientes, para la toma de decisiones y ejecución de la labores pertinentes.

2.6. Con respecto, a las situaciones identificadas en el CNP, las Normas de control interno para el sector público establecen la obligación del jerarca y los titulares subordinados de procurar una estructura[8] que defina la organización formal acorde a la dinámica institucional, del entorno y de los riesgos relevantes; aunado a que se deben delegar[9] funciones de conformidad con el bloque de legalidad.

2.7. Por otra parte, acorde a la derogatoria[10] de las normas de la CGR, el CNP adoptó[11] el Marco Normativo de Gobierno y Gestión de las Tecnologías de la Información (MGTIC), elaborado por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), sin embargo, no ha iniciado su implementación y se encuentra realizando un análisis de brechas en la institución que les permita definir un diseño personalizado del marco conforme a COBIT, el cual será llevado a cabo mediante una contratación que ya fue adjudicada[12].

2.8. Al respecto, en las Normas de control interno para el sector público se establece que de conformidad con el perfil tecnológico de la institución, el jerarca deberá establecer un proceso de implementación gradual de cada uno de sus componentes del MGTIC.

2.9. Por otra parte, se determinó que el CNP no ha ejecutado acciones para identificar, clasificar, analizar y priorizar, los riesgos a nivel institucional desde el año 2019[13], es decir, no se ha ejecutado el (SEVRI) en los últimos tres años, asimismo, tampoco se han realizado esfuerzos para gestionar los riesgos correspondientes a las tecnologías de información y la seguridad de la información.

2.10. La ausencia de una gestión de los riesgos en el CNP incumple con la norma[14] de valoración del riesgo en la cual se establece que el jerarca y los titulares subordinados deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure.

2.11. Las situaciones evidenciadas obedecen a la ausencia de direccionamiento, priorización y monitoreo de la máxima autoridad de la institución para implementar la seguridad de la información como parte esencial del giro de negocio, lo que afecta negativamente el logro de los objetivos institucionales, conforme a sus competencias y al ordenamiento jurídico, aunado a una serie de reorganizaciones infructuosas que han invisibilizado a TI en la estructura formal.

[8] Norma 2.5 Estructura organizativa, N-2-2009-CO-DFOE.
[9] Norma 2.5.1 Delegación de funciones, N-2-2009-CO-DFOE.
[10] Norma 5.9. Tecnologías de información, N-2-2009-CO-DFOE.
[11] Acuerdo N° 39933 de la sesión ordinaria N° 3092, Artículo 4°, del 15 de diciembre de 2021.
[12] Contratación 2023LE-000003-0034100001 sobre equipos portátiles, garantías, servicio de mantenimiento de impresoras y MGTIC
[13] Memoria institucional CNP del 2022.
[14] Norma 3.1 Valoración del Riesgo, N-2-2009-CO-DFOE.

2.12. La ausencia de los elementos indicados impacta en la capacidad del CNP para controlar la implementación y operación de la seguridad de la información,además, la ausencia de un área de tecnologías formal y una lenta implementación del MGTIC puede afectar la gestión de riesgos de TI, el cumplimiento de los objetivos institucionales y la prestación de los servicios de forma continua.

Ausencia de un Sistema de Gestión de la Continuidad de Negocio

2.13. Se determinó que el Consejo Nacional de Producción no ha gestionado la continuidad de negocio institucional por cuanto no ha elaborado e implementado una política de continuidad de negocio en la cual se defina el alcance del esfuerzo institucional en este tema, que derive en la confección de los planes de continuidad de negocio (BCP) y de recuperación de desastre (DRP). Además, no ha formulado el análisis de impacto de negocio (BIA) considerando los procesos, las operaciones y sus activos, para direccionar integralmente las herramientas que le permitirán administrar los recursos en en caso de eventos que puedan provocar una interrupción.

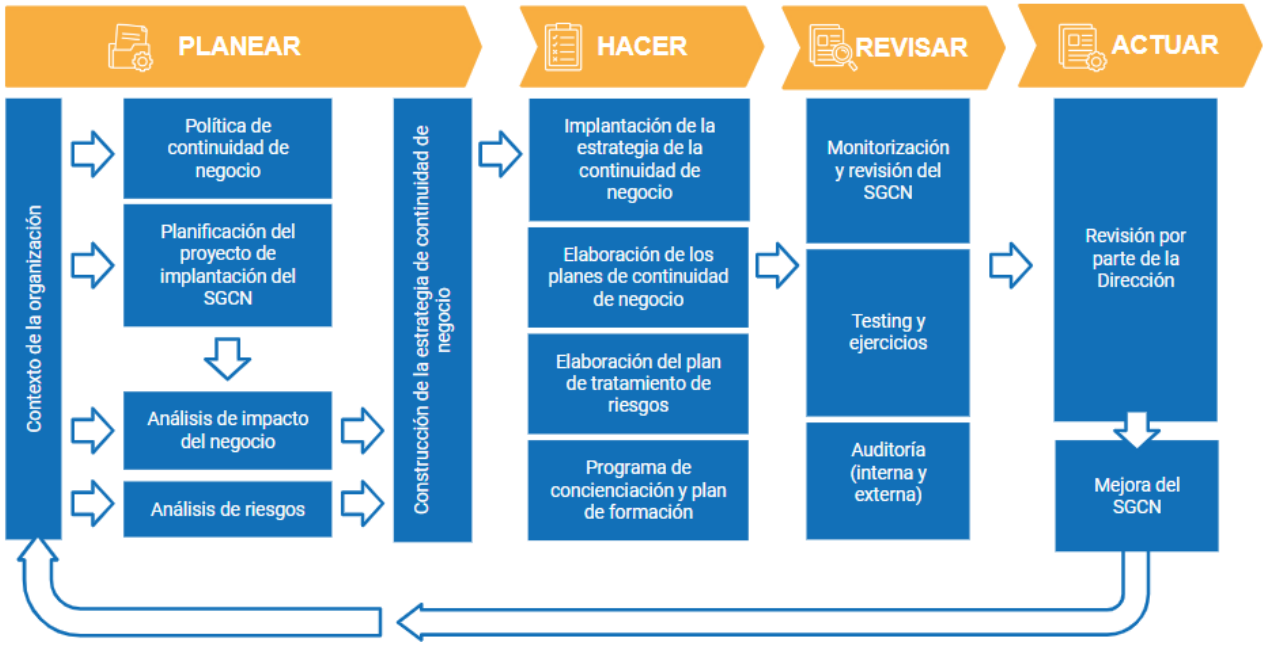
2.14. En relación con lo anterior, se identificó que el CNP cuenta con un protocolo para la atención de incidentes; sin embargo, ante la ausencia de la gestión de continuidad de negocio, este documento no se encuentra integrado o alineado a un plan de continuidad, además, no es específico por tipo de ataque, ni ha sido probado mediante la simulación de escenarios por tipo de ataque; por último, no cuenta con la clasificación de los incidentes de seguridad por su criticidad.

2.15. Como parte de las acciones operativas para mejorar la continuidad de los servicios que brinda la ATSI, el CNP renovó su infraestructura tecnológica, configurando los nuevos servidores y equipos de telecomunicaciones, asimismo se han trasladado aplicaciones, actualizado los sistemas operativos y se adquirió un sistema para virtualizar y respaldar la información. Sin embargo, la institución tiene claro[15] que requiere de un esfuerzo integral que le permita direccionar estos esfuerzos aislados para fortalecer su capacidad de gestión de la continuidad de negocio institucional.

2.16. La continuidad del negocio permite que una organización continúe ofreciendo los servicios críticos en caso de que se presenten eventos que provoquen una interrupción. Para tales efectos, las mejores prácticas sobre continuidad de negocio indican[16] que la organización debe establecer, implementar, mantener y mejorar continuamente estos procesos, a través de un Sistema de Gestión de Continuidad de Negocio (SGCN), incluyendo los procesos necesarios y sus interacciones. También, se indica que la organización debe implementar y mantener procesos sistemáticos para analizar el impacto comercial y evaluar los riesgos de interrupción para realizar los ajustes correspondientes, en caso de que se identifiquen cambios significativos dentro o fuera del contexto de la organización.

[15] Apartado VIII. Limitaciones de la Memoria institucional CNP para el 2022.
[16] Artículo 4 de la ISO 22301:2019.

Imagen 1. Sistema de Gestión de la Continuidad del Negocio



Fuente: Elaboración CGR con base en la ISO 22301

2.17. Por su parte, en las Normas de control interno para el Sector Público[17], se indica que se debe garantizar razonablemente la disponibilidad y acceso a la información por parte de los distintos usuarios, en la oportunidad y con la prontitud que se requiera. En ese sentido, el establecimiento de la continuidad de negocio del CNP debe promover la cohesión y continuidad de las acciones para obtener los resultados propuestos y el cumplimiento de los objetivos definidos a nivel institucional en este proceso.

2.18. Las situaciones evidenciadas tienen origen en que la Administración no ha elaborado, divulgado e implementado el Sistema de Gestión de la Continuidad del Negocio que cubra a toda la entidad; por cuanto, no se ha dimensionado su impacto en la prestación de sus servicios, en el logro de sus objetivos y en el cumplimiento de sus funciones, en caso de que se presenten eventos que provoquen una interrupción.

2.19. Las debilidades asociadas a la planificación de la continuidad del negocio, atentan contra la disponibilidad, integridad y confidencialidad de los sistemas críticos y los procesos de negocio vinculados a éstos; con el consecuente riesgo de afectación a la oportuna prestación de los servicios del CNP, entre los cuales está el abastecimiento institucional de alimentos a través del Programa de Abastecimiento Institucional.

[17] Norma 5.7.4 Seguridad, N-2-2009-CO-DFOE (NCISP).

Debilidades en el Sistema de Gestión de la Seguridad de la Información

2.20. La auditoría realizada permitió determinar que el Consejo Nacional de Producción tiene oportunidades de mejora en la gestión de la seguridad de la información. Ello, considerando que no se ha definido ni implementado una política de seguridad de la información institucional, tampoco se han documentado formalmente y puesto en operación los procedimientos de control relacionados con diferentes temáticas de TI tales como la gestión de sistemas de información, los servicios administrados por terceros, la seguridad física, los respaldos, el desempeño de las redes y la prevención de eventos por amenazas o malware, por lo tanto, tampoco se cuenta con mecanismos estandarizados para el monitoreo y mejora continua de los mismos.

2.21. Asimismo, el CNP no cuenta con la clasificación de todos sus activos institucionales para los cuales debe conocer y analizar su ubicación, clasificar por tipo de información, definir dueños y responsables, elementos que le permiten calificar cada activo según su criticidad con base en los valores de confidencialidad, integridad y disponibilidad.

2.22. Las situaciones descritas anteriormente, se agravan al considerar que el CNP no ha establecido formalmente los roles y responsabilidades para el Área de Tecnología y Sistemas de Información (ATSI) ni para la seguridad de la información de la institución; aunado a que no se han gestionado los riesgos en toda la institución desde el año 2019, como se abordó en el apartado denominado “No se ha implementado una estructura de TI que apoye el logro de los objetivos de seguridad de la información”, de este informe.

2.23. Por otra parte, se identificaron debilidades en las contraseñas del sistema de administración de usuarios, como la práctica de utilizar una misma contraseña para diferentes usuarios y diferentes sistemas, además, el uso de contraseñas débiles que son fáciles de descifrar.

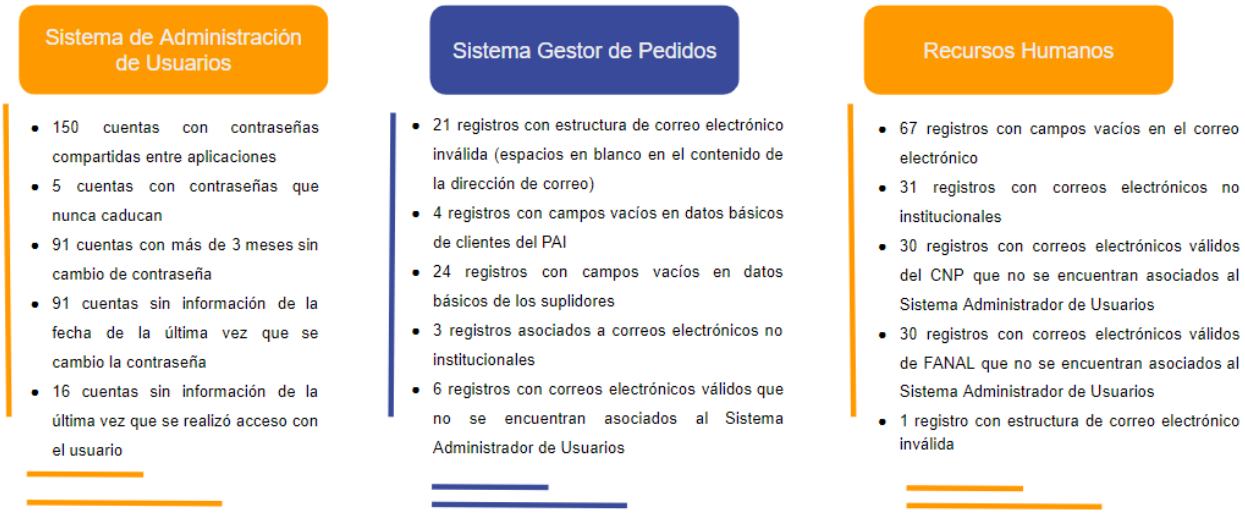
2.24. Si bien el CNP cuenta con un sistema para la aplicación y control de las actualizaciones en equipos y sistemas, durante la revisión se identificó que no se habían aplicado 732 actualizaciones críticas, debido a un error presentado por uno de los equipos durante la actualización. Al respecto, la ATSI indicó que para finales de octubre se tienen pendientes de aplicar 136 actualizaciones críticas, lo que permitió determinar que no se cuenta con puntos de restauración que posibiliten regresar al estado anterior.

2.25. También, se determinó que el CNP cuenta con un plan de concientización de seguridad de la información para el personal, dicho plan aborda temas como el compromiso de la administración, normas y obligaciones de seguridad, responsabilidades y sanciones; además, temas especializados como atención de incidentes, seguridad de contraseñas, malware, soporte técnico, puntos de contacto. Dicho plan se encuentra en un 80% de avance; sin embargo, se debe señalar que no se realiza inducción al personal de nuevo ingreso sobre temas de seguridad de la información, ni tampoco se han definido y publicado recomendaciones de seguridad sobre el uso de los servicios a los usuarios externos.

2.26. En cuanto al diseño de la seguridad de la red del CNP, se debe señalar que se implementó la nueva infraestructura[18], por lo tanto, se cuenta con un diseño de seguridad de red en donde se diagraman los principales elementos de la plataforma tecnológica. Sin embargo, no se cuenta con una descripción detallada y actualizada conforme a la citada implementación.

2.27. Por otra parte, se revisó información relacionada con algunos de los servicios críticos del CNP, donde se determinaron las siguientes inconsistencias:

Imagen 2. Inconsistencias en datos de los servicios críticos



Fuente: Elaboración CGR con base en información suministrada por el CNP

a) En el sistema de administración de usuarios,[19] se identificaron cuentas con contraseñas que nunca caducan, cuentas con más de 3 meses sin cambio de contraseña, cuentas sin información de la fecha de la última vez que se cambió la contraseña y cuentas sin información de la última vez que se realizó acceso con el usuario.

b) En el Sistema Gestor de Pedidos[20] que permite llevar la información del PAI, se identificó campos de cuentas de correo con estructuras no válidas, campos con correos electrónicos no institucionales (cuentas comerciales), campos vacíos sin registros relevantes como la fecha de asignación del rol en el sistema, nombre del funcionario que otorga el acceso al sistema y fecha del último cambio de contraseña.

[18] Contratación 2022LA-000001-0034100001 sobre suscripciones, renovación de contratos: equipo donde se adquirió las herramientas de seguridad y de red.

[19] Es una base de datos y un conjunto de servicios que conecta a usuarios con los recursos de red, y que proporciona los métodos para almacenar datos de directorio y poner dichos datos a disposición de los usuarios y administradores de la red.

[20] De conformidad con la Ley Orgánica del CNP este sistema permite atender necesidades de suministros alimenticios que requieren las instituciones del Estado, que por ley están obligadas a adquirir por contratación directa a través de la institución y así proceder en, garantizar que dichos suministros procedan prioritariamente, de productos de micro, pequeños y medianos productores agropecuarios y agroindustriales nacionales.

c) En información de Recursos Humanos, se identificó registros sin cuenta de correo electrónico, cuentas de correo con estructuras no válidas (cuentas comerciales: gmail, hotmail, yahoo), cuentas de correo electrónico asignadas a más de un funcionario y cuentas de correo que no se encuentran registradas en el sistema de administración de usuarios institucional.

2.28. Adicionalmente, se identificó que el CNP no cuenta con la capacidad de personal para ejecutar labores de monitoreo en temas como respaldos, desempeño de la red y prevención de eventos; por cuanto no se almacenan registros históricos de los equipos y aplicaciones, el análisis que se ejecuta es en tiempo real en horas hábiles con base en las alertas del MICITT o de la solución de seguridad contratada.

2.29. Por su parte, con respecto a la seguridad de la información y ciberseguridad, se determinaron vulnerabilidades que pueden comprometer la integridad, disponibilidad y confidencialidad de la información de la institución. En ese sentido, la Contraloría General remitió el oficio DFOE-SOS-0392 el 21 de agosto de 2023, en el cual se detallaron los aspectos técnicos y riesgos identificados, considerando su clasificación CVSS[21], CWE[22], CVE[23]. Al respecto, el CNP ha gestionado[24] ajustes con sus proveedores para subsanar varias de las vulnerabilidades, sin embargo, a la fecha el avance en las remediaciones es de un 20%.

2.30. En relación con lo indicado, en las Normas técnicas para la gestión y el control de las TI del MICITT, se establece que el CNP 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 normativos asociados. Para lograrlo, en las mejores prácticas de seguridad de la información se plantea que la institución deberá[25] establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información alineado[26] a la política de seguridad de la información, incluyendo la documentación de los procesos necesarios y sus interacciones.

2.31. En cuanto a la clasificación de activos, se debe[27] mantener un registro actualizado y preciso de todos los activos de información y tecnología requeridos para ofrecer servicios y que son propiedad o están controlados por la organización, a la espera de un futuro beneficio. Además, su identificación y clasificación, garantiza la capacidad para la

[21] Marco abierto de la NIST (National Institute of Standards and Technology /U.S Department of Commerce).
[22]Common Weakness Enumeration (CWE) es una lista desarrollada por la comunidad de tipos de debilidades de software y hardware.
[23] Common Vulnerabilities and Exposures (CVE), lista de información registrada sobre vulnerabilidades de seguridad conocidas.
[24] Oficio GG-ATSI-OFIC-191-2023 del 11 de octubre de 2023.
[25] Norma 4.4 Sistema de gestión de la seguridad de la información, ISO27001.
[26] Norma 5.2 Política de Seguridad de la Información, ISO/IEC 27001:2022(E).
[27] Cobit 2019: BAI09.01 Identificar y registrar los activos actuales.

prestación del servicio, maximizan su confiabilidad y disponibilidad para atender las necesidades de negocio[28].

2.32. En lo correspondiente al uso de contraseñas débiles, las mejores prácticas exigen[29] a los usuarios mantener confidencialidad sobre la contraseña, cambiar las contraseñas toda vez que haya una indicación de riesgo en el sistema o en la contraseña; seleccionar contraseñas de calidad con suficiente largo mínimo y que estas no se basen en en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona.

2.33. En lo que corresponde a los parches se debe asegurar la integridad de los sistemas operativos, mediante la implementación de procedimientos para controlar la instalación de software en los sistemas en operación[30], a su vez se debe garantizar que sean instalados de manera correcta; ejecutando pruebas antes y después de su instalación, mediante un ambiente de pruebas controlado; considerando la creación de puntos de restauración que posibiliten regresar al estado anterior en caso de error. Además, los procedimientos de operación se deben[31] documentar y tener disponibles para todos los usuarios que los necesiten. Se deben implementar y actualizar medidas preventivas, detectivas y correctivas, especialmente parches de seguridad y controles antivirus[32].

2.34. En cuanto al diseño de redes, la ISO 27001 detalla[33] que las configuraciones, incluidas las de seguridad, hardware, software, servicios y redes deberían establecerse, documentarse, implementarse, monitorearse y revisarse. Además, en las mejores prácticas del Código Nacional de Tecnologías Digitales del MICITT se promueve que las comunicaciones y transferencia de datos sean seguras, considerando que para la protección de la información en redes e infraestructura de soporte, se deben garantizar controles para el aseguramiento de la red, servicios de red seguros, así como la segregación de redes, entre otros.

2.35. En cuanto a las vulnerabilidades de ciberseguridad detectadas, se debe considerar que en las Normas de control interno para el Sector Público,[34] se detalla que cuando se detecte alguna deficiencia o desviación en la gestión o en el control interno, se deben emprender oportunamente las acciones preventivas o correctivas pertinentes para fortalecer el SCI, de conformidad con los objetivos y recursos institucionales.

2.36. Las debilidades expuestas obedecen a un débil ambiente de control por parte del CNP en el establecimiento de acciones integrales y continuas para diseñar, adoptar, implementar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI) que considere al menos una estrategia de seguridad de información acorde con los objetivos estratégicos institucionales y que permita conocer el estado actual y el estado deseado en materia de seguridad de información y ciberseguridad, así como los recursos necesarios para implementar, operar y mejorar ese sistema.

[28] Cobit 2019: BAI09.02 BAI09.02 Gestionar activos críticos.
[29] Norma ISO 20072: Código de prácticas para la gestión de la seguridad de la información. Uso de contraseña.
[30] ISO/IEC 27001:2022 Anexo A.12.5.1 Instalación de software en los sistemas en operación.
[31] ISO/IEC 27001:2022 Anexo A.12.1.1 Procedimientos de operación documentados.
[32] Cobit 2019:DSS05.01 Proteger contra software malicioso.
[33] ISO/IEC 27001: Control 8.9 Gestión de la configuración.
[34] Norma 6.4 Acciones para el fortalecimiento del SCI de la Norma N-2-2009-CO-DFOE (NCISP).

2.37. La ausencia de un SGSI impacta al CNP en su capacidad de establecer e implementar las políticas, procedimientos y directrices para proteger sus activos de información esenciales, por lo tanto, se potencia el riesgo de accesos no autorizados, pérdida o modificación de información y degradación parcial o total de los servicios. Cabe mencionar que las vulnerabilidades no corregidas permiten que la institución se encuentre susceptible a fallos de seguridad, o vulnerabilidades que pueden ser aprovechadas para intentar acceder a los sistemas y obtener información sensible o confidencial de la institución.

3. CONCLUSIONES

3.1. Una vez obtenidos los resultados con base en la recopilación de la evidencia suficiente y apropiada, se concluye que la seguridad de la información del Consejo Nacional de Producción tiene un cumplimiento bajo conforme a los criterios de auditoría.

3.2. El CNP ha implementado una nueva infraestructura y controles de seguridad física, además, cuenta con la gestión de la capacitación y concientización a usuarios, y ha gestionado servicios para el control del malware. Sin embargo, no ha implementado una estructura formal de TI que apoye el logro de los objetivos de seguridad de la información, tampoco cuenta con un sistema de gestión de la continuidad de negocio que contenga por ejemplo un análisis de impacto de negocio, ni cuenta con un sistema de gestión de la seguridad de la información que considere, por ejemplo, controles de monitoreo de respaldos, desempeño de las redes y prevención de eventos.

4. DISPOSICIONES

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, Nro. 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los “Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría”, emitidos mediante resolución Nro. R-DC-144-2015, publicados en La Gaceta Nro. 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016.

4.3. Este Órgano Contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

A DAVID ARAYA AMADOR EN SU CALIDAD DE GERENTE GENERAL DEL CNP O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Establecer, divulgar e implementar las funciones, roles y responsabilidades del personal asignado a la gestión de las tecnologías de información acorde con las necesidades de la institución, de manera que maximice los beneficios y la disponibilidad de los recursos institucionales. (Ver párrafos 2.04 a 2.12). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Certificación del establecimiento y divulgación de las funciones, roles y responsabilidades del personal a más tardar el 28 de junio de 2024.

ii) Informe sobre la implementación de las funciones, roles y responsabilidades, que contenga al menos la documentación del seguimiento sobre las funciones de las personas funcionarias de ATSI, a más tardar el 20 de diciembre de 2024.

A GERARDO DUARTE SIBAJA EN SU CALIDAD DE PRESIDENTE EJECUTIVO O A QUIEN EN SU LUGAR OCUPE EL CARGO.

4.5. Implementar el Marco de Gestión de Tecnologías de información definido por la institución, considerando el análisis de los riesgos de tecnología (Ver párrafos 2.04 a 2.12). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Una certificación en la que se haga constar que implementó el Marco de Gestión de Tecnologías de Información, a más tardar el 20 de diciembre de 2024.

ii) Informes sobre la implementación del Marco de Gestión de Tecnologías de Información que contenga al menos los resultados del monitoreo y control efectuados, a más tardar el 31 de mayo del 2025, y un segundo informe a más tardar el 30 de setiembre del 2025.

4.6. Elaborar, formalizar, divulgar e implementar el Sistema de Gestión de la Continuidad del Negocio, que contemple al menos: a) la política de continuidad de negocio en la cual se defina el alcance del esfuerzo de continuidad del negocio en la institución, b) el plan de continuidad de negocio (BCP), c) el plan de recuperación de desastre (DRP), d) el análisis de impacto de negocio (BIA) de forma tal que se subsanen las debilidades comentadas en este informe (Ver párrafos 2.13 a 2.19). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Una certificación en la que se haga constar que se elaboró, formalizó y divulgó el Sistema de Gestión de la Continuidad del Negocio, con los contenidos mínimos solicitados, a más tardar el 20 de diciembre del 2024.

ii) Informes sobre la implementación del Sistema de Gestión de la Continuidad del Negocio, a más tardar el 30 de abril del 2025, y un segundo informe a más tardar el 31 de octubre del 2025.

4.7. Elaborar, aprobar e implementar un plan de remediación de las vulnerabilidades sobre seguridad de la información comunicadas mediante el oficio DFOE-SOS-0392(10984), mediante el cual se subsanen las debilidades identificadas y los planes de mitigación cuando corresponda, que contenga los plazos de ejecución, los responsables y los mecanismos para supervisar el avance en dicha remediación (Ver párrafos 2.20 a 2.37). Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación en la cual se haga constar que se elaboró y aprobó el plan solicitado, a más tardar el 29 de marzo del 2024.

ii) Remitir informes donde se haga constar el avance respecto a la implementación del plan de remediación de las vulnerabilidades sobre seguridad de la información a más tardar el 28 de junio del 2024 y un segundo informe a más tardar el 30 de agosto del 2024.

4.8. Elaborar, divulgar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), que considere al menos: a) Política de seguridad de la información institucional aprobada y divulgada b) Clasificación de los activos institucionales (considerando ubicación, tipo de información, responsable, calificación del nivel de criticidad con base en los valores de confidencialidad, integridad, disponibilidad) c) Plan de capacitación y actualización para el personal encargado en seguridad de la información y ciberseguridad e) Establecimiento formal de los roles y responsabilidades para la seguridad de la información considerando la evaluación y mejora continua del SGSI f) Documentar e implementar procedimientos de control para la operación, mantenimiento y monitoreo de los acuerdos de confidencialidad, servicios brindados por terceros, sistemas de información, base de datos, respaldos, redes y comunicación, seguridad física, así como prevención de eventos por amenazas o malware. (Ver párrafos 2.20 a 2.37). Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación en la que se haga constar que se elaboró y se divulgó el Sistema de Gestión de la Seguridad de la Información (SGSI), con los contenidos mínimos solicitados, a más tardar el 20 de diciembre del 2024.

ii) Informes sobre la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), a más tardar el 27 de junio del 2025, y un segundo informe a más tardar el 19 de diciembre del 2025.

A SINDY MAYORGA MATARRITA EN SU CALIDAD DE COORDINADORA ÁREA TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN O A QUIEN EN SU LUGAR OCUPE EL CARGO.

4.9. Elaborar, divulgar e implementar procedimientos de control para prevenir, detectar y corregir las debilidades de la seguridad de la información detalladas en este informe considerando las actividades y los responsables. Adicionalmente, realizar las acciones necesarias para corregir las inconsistencias en la información de los usuarios: a) Sistema

de administración de usuarios, con base en su pertinencia y utilidad. b) Recursos Humanos, con base en su pertinencia y utilidad. c) Ajustes al proceso de creación de usuarios en el sistema gestor para que en adelante se registren los campos correspondientes a correo electrónico, número de cédula, fecha de asignación del rol, el nombre del funcionario que otorga el acceso y la fecha del último cambio de contraseña. d) Garantía que el nuevo sistema de pedidos contemple de forma automatizada la recopilación de los campos antes indicados en el inciso anterior (Ver párrafos 2.20 a 2.37). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General:

i) Una certificación donde se haga constar que se elaboraron y divulgaron los procedimientos de control solicitados a más tardar el 28 de junio del 2024.

ii) Una certificación donde se haga constar que se ajustó el proceso de creación de usuarios del sistema gestor de pedidos conforme a lo solicitado, a más tardar el 30 de agosto del 2024.

iii) Una certificación donde se haga constar que se corrigieron las inconsistencias en la información de los usuarios del sistema de administración de usuarios, información de recursos humanos, a más tardar el 30 de agosto del 2024.

iv) Informes sobre la implementación de los procedimientos de control, a más tardar el 29 de noviembre de 2024, y un segundo informe a más tardar el 31 de enero del 2025.

Licda. Carolina Retana Valverde
Gerente de Área

Lic. Erick Alvarado Muñoz
Asistente Técnico

MATI. Marcela Ramírez Rojas
Coordinadora

Licda. Grettel Camacho Aguilar
Colaboradora

Lic. Juan Luis Camacho Segura
Colaborador

CGR Firmado digitalmente
Valide las firmas digitales

pmt

G: 2023000222-1