**Al contestar refiérase**

**al oficio N.° 02217**

**DFOE-GOB-0080**

**Resolución N.° R-DFOE-GOB-0005-2025. CONTRALORÍA GENERAL DE LA REPÚBLICA. ÁREA DE FISCALIZACIÓN PARA EL DESARROLLO DE LA GOBERNANZA.** San José, a las trece horas del once de febrero de dos mil veinticinco----------

Se resuelve Recurso de Revocatoria presentado por el señor Agustín Meléndez García, en su condición de Director General del Registro Nacional, contra el Informe N.° DFOE-GOB-IAD-00012-2024 de fecha 20 de diciembre de 2024, en relación con las conclusiones 3.1, 3.2, 3.3 y 3.4 y las disposiciones 4.7 y 4.8 del del Informe----------.

## CONSIDERANDO

**I.**Que el Área de Fiscalización para el Desarrollo de la Gobernanza emitió el informe N.° DFOE-GOB-IAD-00012-2024, de 20 de diciembre del 2024; correspondiente a la Auditoría de Carácter Especial sobre la Seguridad de la información de la Junta Administrativa del Registro Nacional (JARN), el cual se remitió el viernes 20 de diciembre de 2024 a las siguientes personas: al Licenciado Gerald Campos Valverde Presidente, Junta Administrativa del Registro Nacional por medio del oficio N.° DFOE-GOB-0601 (21379); al Licenciado Agustín Meléndez García, Director General, mediante el oficio N.° DFOE-GOB-0602 (2138); al Licenciado Róger Araya Fonseca, Director de Informática, mediante el oficio N.° DFOE-GOB-0603 (21383); a la Licenciada Brenda Chan Castillo Directora Administrativa, mediante el oficio N.° DFOE-GOB-0604 (21386); y al Licenciado Emerson Machado Cruz, Auditor Interno, mediante el oficio N.° DFOE-GOB-0605 (21390).

**II.** Que mediante oficio DGL-017-2025 de 9 de enero de 2025; recibido en la Contraloría General vía correo electrónico el 10 de enero del año en curso; suscrito por el señor Agustín Meléndez García, en su condición de Director General del Registro Nacional, se

interpuso recurso de revocatoria contra el Informe N.° DFOE-GOB-IAD-00012-2024 del 20 de diciembre de 2024, en cuanto a las conclusiones 3.1, 3.2, 3.3 y 3.4 y las disposiciones 4.7 y 4.8, emitido por el Área de Fiscalización para el Desarrollo de la Gobernanza de la Contraloría General de la República.

**III.** Que la presente resolución se emite dentro del plazo fijado en el ordenamiento jurídico y en su trámite se han observado las prescripciones reglamentarias correspondientes.-----.

## RESULTANDO

**I. Sobre la legitimación y admisibilidad:** De conformidad con lo establecido en los artículos 33 y 34 de la Ley Orgánica de la Contraloría General de la República (LOCGR), N.° 7428, los actos finales que dicte el Órgano Contralor que no atiendan a la materia presupuestaria, aprobación de contratos administrativos o que se dicten en procedimientos de contratación administrativa, estarán sujetos al régimen común de impugnación de los actos administrativos, contenidos en la Ley General de la Administración Pública, N.° 6227, cuando se considere que lesionan derechos subjetivos o intereses legítimos o que impidan su origen. Los artículos 342, 343 y 346 de la Ley General de Administración Pública regulan que el recurso de revocatoria es un recurso ordinario que se interpone contra actos administrativos finales.

Que el oficio N.° DGL-017-2025 recibido en la Contraloría General vía correo electrónico el 10 de enero del año en curso; fue presentado dentro del término de tres días hábiles posteriores a partir de la última comunicación del acto al señor Agustín Meléndez García, en su condición de Director General del Registro Nacional); por lo que el mismo se encuentra presentado a derecho, de conformidad con el artículo 346 de la Ley General de la Administración Pública (LGAP).

Que del oficio N.° DGL-017-2025 de 9 de enero de 2025, no se desprende con claridad el uso de la potestad del administrado de presentar recursos ordinarios de revocatoria y apelación en subsidio. Pese a no haberse presentado como recurso el Órgano Contralor decide gestionarlo como tal para asegurar que las acciones que puedan impactar actos administrativos puedan ser revisadas adecuadamente; así, infiriendo que se trata de un recurso de revocatoria exclusivamente, se le dará dicho tratamiento, en aplicación de los artículos 347 y 348 de la LGAP.

**II. Señalamientos del recurrente: 1)** Considera el recurrente que la frase de la conclusión 3.1: "La seguridad de la información en los sistemas críticos del Registro Nacional no cumple con el marco regulatorio y buenas prácticas aplicables" se encuentra fuera de lugar, toda vez que desconoce todos los esfuerzos e inversión que ha realizado la Institución para mantener niveles razonables de seguridad en los aplicativos de software y la infraestructura tecnológica. Al respecto manifiesta que "En el Registro Nacional se tiene claro que ninguna institución u organización puede lograr un nivel de seguridad del 100%; para las organizaciones sería sumamente complejo y costoso cumplir con la totalidad de buenas prácticas, y es normal que se encuentren aspectos por fortalecer, eso es parte de la mejora continua. Esa frase excluye la consideración de las decisiones que ha tomado la Junta, las acciones que ha impulsado la Dirección General y el trabajo que realiza la Dirección de Informática para mantener razonablemente segura la información que gestiona el Registro Nacional; todos esos elementos constan en el legajo de documentos que se suministraron al equipo de trabajo de la Contraloría, las visitas y entrevistas realizadas, las revisiones de herramientas que realizaron en sitio y todas las evidencias que aportó la Administración."

**2).** Que la frase de la conclusión 3.1 que indica: "…la falta de una estrategia que oriente las acciones de una aplicación de controles en la gestión, operación y mantenimiento de sistemas, y robustez en ciberseguridad y continuidad de negocio, compromete la seguridad de la información", no se ajusta a la realidad institucional, ya que deja de

considerar todos los elementos probatorios que se suministraron al equipo de trabajo de la Contraloría, elementos tales como:

-La organización del Registro Nacional, que considera un departamento para la seguridad de la información, con personal especializado en el tema. Se suministró el organigrama, las funciones, y competencias entre otros elementos.
-El Marco de gestión de las tecnologías de información y comunicaciones.
-La constitución del Órgano Rector de tecnologías de Información y Comunicación del Registro Nacional (ORTIC).
-La política de seguridad, incluidas en las Políticas Institucionales aprobadas por la Junta.
-El Manual de normas de aseguramiento de la información, debidamente aprobado por la Junta.
-Las metodologías para el mantenimiento de los sistemas, con sus procedimientos y estándares correspondientes.
-Las directrices emitidas por las diferentes instancias de la Dirección de Informática.
-Los procedimientos, guías, protocolos e instructivos que se aplican en la operación de la infraestructura tecnológica.
-El plan de trabajo anual del Departamento Aseguramiento de la Información.
-Las herramientas de seguridad de la información que se mantienen en operación.

Indica que: “A la Contraloría se informó sobre el trabajo realizando para implementar los procesos de continuidad de negocio, el cual se encuentra en la fase final de aprobación por parte de la Junta, encontrándose en agenda desde el mes de diciembre de 2024 y a la espera de la conformación del nuevo órgano colegiado que tiene una vigencia de 2 años.”.

**3).** Sobre la frase de la conclusión 3.2 que señala: “La ausencia de una estrategia para orientar el Gobierno de Seguridad de la Información incidente en la capacidad de implementar las políticas, procedimientos y directrices…”*;* manifiesta el recurrente que “Como ya se mencionó en el punto anterior, el Registro Nacional ha trabajado por muchos

años en definir, planificar, documentar, implementar y dar seguimiento a múltiples estrategias para ir fortaleciendo la seguridad de la información, de acuerdo con la disponibilidad de recursos presupuestarios y humanos, en respuesta constante a los cambios en el entorno en cuanto a la ciberseguridad, y en los últimos años también se están atendiendo oportunamente las directrices recibidas del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. Todas esas acciones respondan a una estrategia institucional que está delineada en las líneas de acción descritas en el Plan Estratégico Institucional 2022-2026, documento que fue entregado al equipo de trabajo de la Contraloría.”.

**4).** Sobre la frase de la conclusión 3.3 **:**“Los controles de ciberseguridad y continuidad de negocio son insuficientes para asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información”, indica que: “La manera de presentar esta conclusión es lo que se consignó en el punto 6 del documento DGL-1176-2024 como un señalamiento donde la Administración encuentra ambigüedad ya que no se profundiza en cuáles controles faltan o cuáles son insuficientes, según el criterio de la Contraloría. Un ejemplo de los controles de ciberseguridad que ha implementado el Registro Nacional es el firewall de aplicaciones web (WAF) que se encuentra en operación; herramienta que los técnicos de la Contraloría solicitaron deshabilitar para poder analizar el portal de servicios digitales del Registro Nacional debido a que el firewall no les permitió profundizar en los aspectos de configuración de nuestra infraestructura tecnológica, siendo ese precisamente el propósito de ese muro de fuego y por ello la herramienta se mantuvo en operación. Para las instituciones es sumamente complejo cumplir con la totalidad de buenas prácticas, y es posible que existan controles que se pueden mejorar. **En ese sentido hubiera sido muy valioso para la Administración que esta conclusión indicara cuáles son los controles insuficientes en una mesa de trabajo, que no se realizó como en casos de informes precedentes.** En el desarrollo del informe DFOE-GOB-IAD-00012-2024 también se encuentran señalamientos de carácter general, donde hubiera sido muy

importante para la Administración que se profundizara. Ejemplos: 2.4, 2.11, 2.12, 2.25, 2.26, 2.28, 2.47.”. (Resaltado es de su original)

**5).** Sobre la frase de la conclusión 3.4: “Las debilidades en la aplicación de controles de Operación, Gestión y Mantenimiento de los sistemas exponen al riesgo en la pérdida de disponibilidad e integridad de la información…”; señala que: “Este es otro ejemplo donde la manera de presentar la conclusión le dificulta a la Administración comprender el señalamiento de la Contraloría ya que no queda claro a qué se deben las debilidades; por ejemplo, de documentación, de implementación, que los controles utilizados son incorrectos, u otras situaciones donde el criterio de la Contraloría debería aportarle valor a la Administración para mejorar continuamente.”.

**6).** En relación con la disposición 4.7 del Informe el recurrente indica que: “La participación de los usuarios de negocio en la supervisión, incorporación y autorización de las modificaciones a la infraestructura de Tecnologías de Información es una actividad normal dentro de todos los desarrollos y proyectos tecnológicos que realiza la institución, es por ello que estamos a la vanguardia a nivel nacional en la digitalización y prestación de servicios y posicionados a nivel mundial como uno de lo mejores registros del mundo; esta Dirección General tiene plena certeza de la participación activa de los usuarios del negocio y en la guía que brinda la Dirección de Informática para atender las necesidades que como Dirección de apoyo le remiten las diferentes unidades administrativas de una institución tan compleja como lo es el Registro Nacional. Se han girado instrucciones a la Dirección de Informática para revisar y ajustar en lo que corresponda el Protocolo del Comité de Cambios a efectos de reflejar en debida forma lo que ocurre hoy en la práctica y poder cumplir en tiempo con los plazos previstos en esta disposición.”

**7).** En relación con la disposición 4.8 del Informe, indica que: **“**Las vulnerabilidades sobre seguridad de la información comunicadas mediante el oficio N.° 20520 (DFOE-0567) del 5 de diciembre de 2024; fueron debidamente analizadas por la Dirección de Informática y

comunicadas a esta Dirección General, iniciándose de forma inmediata con la valoración del esfuerzo y costo para atenderlas, ya que son valiosas oportunidades de mejora de nuestra infraestructura que deben ser oportunamente atendidas e implementadas. A efectos de elaborar, aprobar e implementar el plan de remediación de vulnerabilidades se nos otorga un plazo al 25 de febrero de 2025, que si bien es corto lo consideran viable y en ese sentido se han girado las debidas instrucciones a la Dirección de informática. Sin embargo, en relación al plazo otorgado para certificar y acreditar la implementación del plan al 23 de mayo de 2025, es materialmente imposible de cumplir ya que el recurso humano y financiero para la implementación del plan en el tiempo requerido es insuficiente y atender dicho plazo implicaría necesariamente desatender otras de las prioridades del plan de trabajo de la Dirección de Informática y la operativa diaria de todos los sistemas de la institución, que como reitero es una muy compleja, con más de 30 sistemas informáticos a los cuales debe darse mantenimiento y mejoras constantes, motivo por el cual respetuosamente se solicita ampliar el plazo para la emisión de la certificación hasta el 25 de setiembre de 2025; es decir, que dicho plazo se amplíe en cuatro meses adicionales.”.

**II. Criterio del Área de Fiscalización para el desarrollo de la Gobernanza:** Siendo que las observaciones vertidas en el oficio N.° DGL-017-2025 por el recurrente se efectuaron una vez precluida la etapa de comunicación de resultados de la auditoría y la recepción de observaciones por parte de la administración estas resultan improcedentes. Aunado a ello, el recurrente no aporta nueva evidencia que pueda justificar una variación en el análisis y evidencia que ya se tuvo a la vista por parte de la Contraloría General, ni se presentan nuevos argumentos que justifiquen un nuevo análisis o una variación sobre el realizado en el curso de la auditoría. Sin embargo, en atención al reproche presentado respecto de la conclusión que que “la seguridad de la información en los sistemas críticos del Registro Nacional no cumple con el marco regulatorio y buenas prácticas aplicables” y por tanto califica a la conclusión como “fuera de lugar”, el mismo se rechaza por cuanto las conclusiones alcanzadas como resultado de la elaboración de la auditoría en cuestión se

basan en los hallazgos que emanan de los procedimientos abordados, tanto en la etapa de planificación como en la etapa de examen, y en todo momento se tiene apego al criterio técnico comunicado a la administración.

En atención al procedimiento de auditoría vigente, las conclusiones se desarrollan a partir de los resultados descritos en los párrafos que hacen parte del informe en su conjunto. Así, las conclusiones responden al objetivo de la auditoría de manera integral dando a conocer si en la materia auditada se cumple o no en todos sus aspectos significativos, esto en función de los resultados obtenidos del proceso de auditoría, los cuales fueron desarrollados a lo largo del apartado de resultados del informe de cita. En el caso de la seguridad de la información, la suma de las partes en la implementación de controles, es fundamental a efectos de resguardar este activo, dado que una sola debilidad, un solo control deficitario, expone a riesgo a la totalidad de la infraestructura. Por ejemplo, si se cuenta con controles fuertes para autenticar a los usuarios ante los sistemas, y se establecen bitácoras, y controles de entrada robustos, se protegen aspectos importantes de la seguridad, pero si en ese mismo entorno, los usuarios utilizan contraseñas inseguras, esto perjudica toda la estructura de control y la debilita, dado que la autorización, la rendición de cuentas y el ingreso de datos son todos dependientes de la autenticación en la que se encuentra una contraseña débil o en su efecto un solo factor de autenticación. Toda debilidad en el control introduce vulnerabilidades, por ende cada control que no es efectivo genera una posible brecha de seguridad y expone a algún riesgo, estos riesgos se definen en términos de los criterios técnicos que guían la seguridad, a saber la confidencialidad, disponibilidad e integridad de la información.
En el caso particular del informe emitido, se hace mención expresa de los aspectos en los que se observó cumplimiento del marco normativo por parte del Registro Nacional, en la materia auditada. Así también se hace referencia a los aspectos que presentaron brechas, no conformidades, con el marco de términos de auditoría que fueron comunicados en su momento mediante oficio N.° DFOE-GOB-0515 del 22 de octubre 2024 y aceptados por el Registro Nacional.

En cuanto al reproche sobre la conclusión de que no existe una estrategia para orientar el Gobierno de Seguridad de la Información “no se ajusta a la realidad”, también debe rechazarse. En primer término, por cuanto todos los demás aspectos que menciona el recurrente como evidencia de las acciones emprendidas por el Registro Nacional para atender la seguridad de la información, tales como contar con un departamento especializado, un marco de gestión, un órgano rector, entre otros, no son sustituto de la existencia de la estrategia. En el informe se reconoce y menciona el cumplimiento del marco normativo en esos aspectos, sin embargo, su existencia no exime de la necesidad de contar con la estrategia.

El recurrente sostiene que todas las actividades ejecutadas para la seguridad de la información en el registro se encuentran representadas y alineadas con lo indicado en el Plan Estratégico Institucional 2022-2026, sin embargo, ello no es de recibo por cuanto no explica, menciona ni aporta evidencia acerca de la forma en cómo se da ese alineamiento, situación que tampoco pudo ser demostrado durante el proceso de auditoría ejecutado por el Área de Fiscalización de la Contraloría General. Los planes estratégicos institucionales no sustituyen ni excluyen la existencia de estrategias de seguridad de la información debido a que la gestión de la seguridad es una actividad de negocio con independencia, concordante con la planificación estratégica pero con características propias, el plan estratégico trata los asuntos de negocio; la estrategia de seguridad atiende las variables técnicas y administrativas que van a colaborar en la protección de los activos de información, como una cadena de proyectos y controles que al final se ajustan a las necesidades estratégicas del negocio. En una institución como el Registro Nacional cuyo activo principal es la gestión de la información para asegurar el principio de fe registral, es reflejo claro de la alta sensibilidad que tiene la protección y seguridad de la información.

Aunado a lo anterior, se le aclara al recurrente que la estrategia de seguridad de información, hace parte de un proceso, que denota justamente la madurez institucional en la materia, que debe seguir su ruta hacia el mejoramiento contínuo, de ahí que

considerando los avances del Registro Nacional y la relevancia que tiene el manejo de la información para la seguridad jurídica del país, es relevante un avance más allá de la sola implementación de controles, en la articulación del esfuerzo con la participación de las áreas de negocio, TI, los proveedores, socios comerciales y otras partes interesadas. Así, la estrategia de seguridad es una actividad gerencial de alto nivel que se documenta para lograr tres cosas: a) Conocer a fondo el estado actual o postura actual de seguridad de información, es decir, tomar una fotografía en el presente, que muestre el estado de los controles implementados y cómo esto incide en la seguridad y en la percepción de riesgo que tiene la administración. b) Señalar o plantear la expectativa de la administración y de TI con respecto a la seguridad en el mediano y largo plazo, es decir, definir una postura deseada o futura, aquella situación de robustez que se pretende alcanzar en un horizonte de tiempo. c) Elaborar e implementar un plan para pasar del estado actual al estado deseado, esto es desarrollar un programa de seguridad que se detalla en la forma de proyectos que permiten por medio de la implementación de controles específicos ir cambiando la postura de seguridad para pasar del punto A al punto B.

Por otra parte, en relación a lo señalado por el recurrente como ambigüedades o falta de claridad en las conclusiones 3.3 y 3.4 del informe por cuanto no permiten conocer controles que falten o sean insuficientes. Se le aclara que en el contenido del informe se consignan las no conformidades detectadas en elementos de significativa relevancia para la Seguridad de la Información, a saber continuidad de negocio, gestión de contraseñas, políticas y procedimientos para la destrucción segura de medios y de información impresa, uso de dispositivos móviles personales, autenticación en sistemas críticos, articulación de la estrategia de seguridad, definición de roles en materia de seguridad, sensibilización de usuarios finales, entre otros elementos. Por consiguiente se rechaza lo señalado por el recurrente en cuanto a ambigüedades del informe, además se le aclara que conforme a lo señalado previamente, las conclusiones del informe constituyen el apartado en el cual se responde el objetivo de la auditoría de manera integral en cuanto al cumplimiento o no de

los aspectos auditados, y no a una reiteración de todo lo desarrollado en la sección de resultados del informe.

En cuanto al reproche presentado en contra de la disposición 4.7, que refiere a la conformación y operación del Comité de Cambios, señala el recurrente que tiene “plena certeza de la participación activa de los usuarios de negocio”; el mismo se rechaza por los motivos que se exponen de seguido. El recurrente no aporta evidencia adicional que permita respaldar lo señalado y sustentar cambios al contenido del informe y la disposición en particular. Además, en relación al proceso de gestión de cambios, en la auditoría se identificó el proceso seguido en el desarrollo e implementación de software, en el cual participa el personal que hace parte de las actividades de negocio, a lo largo del ciclo de vida del desarrollo. Sin embargo, como se indica en el informe, la gestión de cambios aborda el análisis técnico y operacional del impacto de los cambios que se llevan a producción, esto requiere una valoración conjunta entre TI y el personal de negocio, que en atención a los documentos suministrados, tanto en la etapa de planificación como de examen, la conformación del comité a la fecha, está integrado exclusivamente por personal de TI. Es importante mencionar que la gestión de cambios es independiente del desarrollo de sistemas y es una tarea específica que desarrolla el equipo técnico en coordinación con las gerencias.

Por último, en relación con la solicitud de ampliación de plazo para la atención de la disposición 4.8, se debe dejar claro que no procede dar trámite a la solicitud de ampliación planteada por el recurrente, por cuanto las disposiciones aún se encuentran en plazo, en los cuales el Registro Nacional debe ejecutar las acciones necesarias para procurar el cumplimiento de las disposiciones y comunicar lo que corresponda a la Contraloría General. Al respecto, los Lineamientos Generales para el Cumplimiento de las Disposiciones y Recomendaciones emitidas por la Contraloría General de la República en sus Informes de Auditoría (Resolución N.° R-DC-144-2015. Publicada en La Gaceta N.°

242 del 14 de diciembre del 2015) en su acápite 3.3 describe el proceso de ampliación de plazo de las señala:

> "**3.3. Ampliación de plazo.** En casos excepcionales, cuando medien circunstancias que fundamentan en términos de razonabilidad, lógica y conveniencia, los motivos que imposibilitan al sujeto fiscalizado a dar término a las acciones correctivas en el plazo establecido, ésta podrá solicitar una prórroga. Para ello, el destinatario de la disposición o recomendación deberá gestionar por escrito ante el Órgano Contralor, en el transcurso de los quince días hábiles anteriores a su vencimiento, la referida solicitud de prórroga, la cual deberá cumplir los siguientes requisitos: a. La gestión deberá presentarse por medio de documento debidamente firmado por el destinatario de la disposición o recomendación, o por quien fuere delegado formalmente para este acto. b. La relación fundamentada de hechos que impidieron el cumplimiento de la disposición o recomendación en la fecha prevista. c. La fecha propuesta para el cumplimiento definitivo de la disposición o recomendación. d. Una certificación que detalle las acciones realizadas en atención a la disposición o recomendación, con referencia a los folios del expediente de cumplimiento de las disposiciones y recomendaciones, en los que están debidamente respaldadas dichas actuaciones. Esta certificación deberá elaborarse de acuerdo con el formato contenido en el Anexo N.°2. e. Un cronograma con el detalle de las acciones pendientes de realizar, el responsable de llevarlas a cabo y el plazo que se requiere para la ejecución de cada una de esas actividades. Aquellas solicitudes de ampliación de plazo que cumplan con los requisitos citados, se admitirán para su atención y resolución correspondiente por parte del Órgano Contralor. Se rechazará de plano y sin más trámite aquellas solicitudes de ampliación que no cumplan con los requisitos establecidos

> o su plazo de vencimiento supere los quince días hábiles. La Contraloría General de la República se reserva la facultad de prevenir por única vez el cumplimiento de los otros requisitos establecidos. De igual manera, valorará circunstancias de excepción relevantes, cuya procedencia quedará a criterio del Órgano Contralor. En aquellos casos en los que se prevenga el cumplimiento de uno o varios requisitos, se concederá un plazo de hasta diez días hábiles al solicitante, bajo el apercibimiento de archivar la gestión en caso de incumplimiento".

Como se desprende de la normativa indicada, la ampliación del plazo para el cumplimiento de disposiciones es un proceso formal regulado ex-post a la emisión del Informe de auditoría definitivo, durante el curso o la fase de cumplimiento de las disposiciones; por lo que en definitiva el momento procesal oportuno para discutir los plazos de las disposiciones o exponer observaciones al Informe es al momento de la comunicación del oficio que da traslado al borrador del Informe a la administración, donde esta puede verter sus observaciones justificadas para que se valoren por parte del Órgano Contralor antes de la emisión del Informe definitivo. Lo indicado significa, que el recurso de revocatoria no es el medio procesal para solicitar una ampliación del plazo de una disposición o exponer observaciones al Informe, ya que implica revertir etapas procesales ya precluidas del proceso de auditoría, como ha quedado indicado previamente.

## POR TANTO

Con sustento en las consideraciones de hecho y de derecho que sirven de fundamento a esta resolución, y lo señalado en los artículos 183 y 184 de la Constitución Política, **SE RESUELVE: 1) DECLARAR SIN LUGAR** el recurso presentado contra las conclusiones 3.1, 3.2, 3.3 y 3.4; así como contra las disposiciones 4.7 y 4.8 del Informe DFOE-GOB-IAD-00012-2024, el cual se mantiene incólume en todos los aspectos. **2) SE RECHAZA DE PLANO** la solicitud de ampliación a los plazos de las disposiciones; al ser

improcedente por la vía recursiva su modificación de acuerdo a los Lineamientos Generales para el Cumplimiento de las Disposiciones y Recomendaciones emitidas por la Contraloría General de la República en sus Informes de Auditoría **NOTIFÍQUESE----------.**

Falon Stephany Arias Calero
**Gerente de Área**

Pablo Pacheco Soto
**Fiscalizador**

CGR Firmado digitalmente
Valide las firmas digitales

PPS/msb

NI 240-2025
Gestión:2024000427-4
Expediente:CGR-INAU-2024000485