INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DE LA JUNTA ADMINISTRATIVA DEL REGISTRO NACIONAL (JARN)

20 de diciembre, 2024

Informe N.° DFOE-GOB-IAD-00012-2024

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

CONTENIDO

Resumen Ejecutivo 3
1. INTRODUCCIÓN 5
ORIGEN DE LA AUDITORÍA 5
OBJETIVO GENERAL 6
ALCANCE 6
CRITERIOS DE AUDITORÍA 6
METODOLOGÍA APLICADA 6
GENERALIDADES ACERCA DE LA MATERIA AUDITADA 7
MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA 8
COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA 8
SIGLAS Y ABREVIATURAS 9
2. RESULTADOS 9
GOBIERNO DE SEGURIDAD 10
Ausencia de una estrategia para orientar el Gobierno de Seguridad 10
CONTROLES DE CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO 11
Debilidades en los controles de ciberseguridad y continuidad del negocio 12
OPERACIÓN, GESTIÓN Y MANTENIMIENTO DE LOS SISTEMAS 14
Debilidades en la aplicación de controles de Operación, Gestión y Mantenimiento de los Sistemas que inciden la seguridad de la información 14
3. CONCLUSIÓN 19
4. DISPOSICIONES 19

CUADROS

Cuadro N.° 1 Siglas utilizadas en el informe 9
Cuadro N.° 2 Detalle de sistemas de la JARN con inclumplimientos de la política de gestión de contraseñas del Registro Nacional 17
Cuadro N.° 3 Debilidades de seguridad de la información en los sistemas de la JARN 18

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como objetivo determinar si la seguridad de la información de los sistemas críticos de la Junta Administrativa del Registro Nacional responde al marco normativo y buenas prácticas aplicables, en atención a los principios de confidencialidad, integridad y disponibilidad de información, a efectos de prevenir afectaciones en los servicios. Para ello, se analizó la gobernanza en seguridad de la información, la aplicación de controles en operación, gestión y mantenimiento, así como la ciberseguridad y continuidad del negocio, durante el período comprendido entre enero de 2022 y diciembre 2023.

¿POR QUÉ ES IMPORTANTE?

De conformidad con la Ley N.° 5695, el Registro Nacional tiene por objeto la administración del sistema nacional de registros e inscripciones de bienes y personas jurídicas. Dicha institución tiene altísima relevancia para la seguridad jurídica del país mediante la protección de la fe pública registral, y debe velar por todos los medios que no se generen daños al particular con sustento en información derivada de bases de datos inexactas o erróneas en los distintos registros que lo conforman y en los cuales se ampara a los terceros adquirentes de derechos, en base a la información contenida en los registros. Para ello cuenta con sistemas de información para la gestión de registros de bienes muebles, bienes Inmuebles, propiedad intelectual, personas jurídicas, el Instituto Geográfico Nacional; y procesos de soporte como Administración, Finanzas, Recursos Humanos y Tecnología de Información. Así, resulta relevante verificar la aplicación rigurosa de las normativa y buenas prácticas de seguridad de la información por parte de esa institución.

¿QUÉ ENCONTRAMOS?

Se determinó que la seguridad de la información en los sistemas críticos del Registro Nacional no cumple razonablemente con el marco regulatorio y buenas prácticas aplicables. Aunque existen políticas, procedimientos y manuales, carece de una estrategia que oriente las acciones a nivel institucional, de capacidades de la auditoría interna, de una aplicación de controles en la gestión, operación y mantenimiento de sistemas, y robustez en ciberseguridad y continuidad de negocio, lo cual compromete la seguridad de la información.

A nivel de gobernanza, el Registro Nacional no cuenta con una estrategia de seguridad de la información que oriente el manejo y resguardo de la información y articule las políticas, procedimientos, directrices y controles de seguridad existentes, así como la definición de un programa de seguridad y la cartera proyectos para un abordaje progresivo de las necesidades de esa entidad en la materia; aspecto que tampoco se contempla en su Plan Estratégico 2022-2026. Además, mantiene en desarrollo el Sistema de Gestión de Seguridad de la Información, sin definir sus componentes a nivel estratégico, los roles y responsabilidades directivas, así como acciones claramente definidas y estructuradas para la sensibilización institucional sobre la importancia de la seguridad.

Por otra parte, los controles definidos para la operación, gestión y mantenimiento de los sistemas del Registro Nacional tienen debilidades de implementación que restan efectividad a las prácticas de seguridad de la información. Así, el Comité de Cambios no tiene representantes de usuarios para supervisar y autorizar modificaciones a la infraestructura de TI; la suspensión de usuarios por ausencia prolongada no es automática; no hay cifrado de datos; no hay controles para prevenir ataques de denegación de servicios, ni sitio de procesamiento alterno. Tampoco se ha instalado una política en dispositivos móviles. No todos los sistemas críticos cuentan con doble factor de autenticación, sitios en web no tienen mecanismos de validación humana, permiten varias sesiones en simultáneo y no con política de contraseñas.

Finalmente, se determinó que los controles de ciberseguridad y continuidad del negocio son insuficientes para asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información. Así, no hay controles para gestionar de forma activa y periódica vulnerabilidades de infraestructura de tecnologías de información. Además, no se ha concluido la implementación del sistema de gestión de continuidad del negocio; el Análisis de impacto de Negocios no ha priorizado los sistemas críticos institucionales, el Plan de Continuidad del Negocio no indica cómo operar en contingencia y existe el Plan de recuperación de desastres que no obedece a un análisis de escenarios ni se somete a pruebas. Lo anterior, aumentando el riesgo de funcionamiento de los servicios críticos en caso de que se exploten vulnerabilidades por atacantes maliciosos.

¿QUÉ SIGUE?

Se dispone a las autoridades del Registro Nacional definir e implementar un procedimiento para integrar en la planificación estratégica el análisis de riesgos y debilidades en seguridad de la información, controles de ciberseguridad y continuidad de negocio. Además, definir e implementar mecanismos que permitan aplicar y automatizar en lo correspondiente, los controles establecidos seguridad de la información institucionales. Asimismo, diseñar, formalizar, divulgar e implementar el Sistema de Gestión de la Continuidad del Negocio y elaborar, aprobar e implementar un plan de remediación de las vulnerabilidades identificadas por la Contraloría General.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE INFORMACIÓN EN LA JUNTA ADMINISTRATIVA DEL REGISTRO NACIONAL (JARN)

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La auditoría se efectuó con fundamento en las competencias que le confieren a la Contraloría General los artículos 183 y 184 de la Constitución Política, así como los numerales 17, 21 y 37 de su Ley Orgánica N° 7428 del 7 de setiembre de 1994, en cumplimiento de los objetivos de mediano plazo de la División de Fiscalización Operativa y Evaluativa (DFOE), así como del plan anual operativo del Área de Fiscalización para el Desarrollo de la Gobernanza.

1.2. El Registro Nacional tiene bajo su responsabilidad la administración del sistema nacional de registros e inscripciones de bienes y personas jurídicas, de ahí la altísima relevancia para la seguridad jurídica del país mediante la protección de la fe pública registral, y velando por todos los medios que no se generen daños al particular con sustento en información inexacta o errónea en los distintos registros que lo conforman y en los cuales se ampara a los terceros adquirentes de derechos, con base en la información contenida en los registros.

1.3. Así, la seguridad de la información, gestionada a través de los sistemas registrales y de apoyo a la gestión y toma de decisiones, son clave para garantizar razonablemente su confidencialidad, integridad y disponibilidad. Siendo en este caso una prioridad para el Registro Nacional quien tiene una responsabilidad de orden superior para proteger y asegurar derechos y deberes fundamentales de sus distintos usuarios.

OBJETIVO GENERAL

1.4. Determinar si la seguridad de la información de los sistemas críticos de la Junta Administrativa del Registro Nacional (JARN) responde al marco normativo y buenas prácticas aplicables, de forma que respalden la gestión sustantiva institucional en atención a los principios de confidencialidad, integridad y disponibilidad de información, a efectos de prevenir afectaciones en la prestación de los servicios.

ALCANCE

1.5. La auditoría comprendió el análisis prácticas de gobierno y gestión de Tecnologías de Información, así como la seguridad física y lógica mediante los controles implementados por la administración, para asegurar la disponibilidad de los datos en los sistemas de información, así como su integridad y confidencialidad, en los procesos de recopilación, procesamiento y comunicación. El período de análisis comprendió del 01 de enero de 2022 al 31 de diciembre de 2023, extendiéndose cuando resultó aplicable.

CRITERIOS DE AUDITORÍA

1.6. Los términos de auditoría fueron comunicados verbalmente el 17 octubre de 2024 a las siguientes personas funcionarias del Registro Nacional: Jorge Moreira Gómez, Subdirector General; Adelita Abarca Ortega, Jefa de Planificación; Roger Araya Fonseca, Director de Informática; y Oscar Morales Segura, Jefe de Aseguramiento de la Información. Estos se comunicaron formalmente mediante oficio DFOE-GOB-0515 del 22 de octubre de 2024.

1.7. Como parte de las fuentes de criterios de auditoría utilizados destacan la Ley General de Control Interno, 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 27002 y Cobit 5.

METODOLOGÍA APLICADA

1.8. 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 Contraloría General de la República (CGR), el Procedimiento de Auditoría vigente, establecido por la DFOE, que está basado en la ISSAI 100: Principios Fundamentales de Auditoría del Sector Público, y los principios de la ISSAI 400: Principios de la Auditoría de Cumplimiento de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI por sus siglas en inglés).

1.9. Además, se utilizó la información suministrada por el personal del Registro Nacional, mediante consultas por escrito, entrevistas, sesiones de trabajo y visitas que fueron documentadas, entre ellas, una al centro de datos de la institución para verificar el cumplimiento de mejores prácticas en seguridad física[1].

1.10. También, se ejecutaron pruebas con una muestra de usuarios finales de los sistemas que se encuentran operando en el Registro Nacional, para la verificación de controles de entrada, mecanismos de autenticación, entre otros. Además, se realizaron análisis de vulnerabilidades no intrusivas a los sitios web, sin generar afectación en los servicios

[1] Visita realizada el 22 de agosto de 2024.

brindados por la institución, cuyos resultados se reportaron a la administración mediante oficio con carácter de acceso restringido[2].

GENERALIDADES ACERCA DE LA MATERIA AUDITADA

1.11. Mediante la Ley N° 5695[3] fue creado el Registro Nacional, el cual depende del Ministerio de Justicia y Paz. Como parte de las competencias de esa cartera ministerial le corresponde administrar el sistema nacional de registros e inscripciones de bienes y personas jurídicas.

1.12. El Registro Nacional tiene relevancia a nivel país, en la protección de un interés valioso como lo es la fe pública registral. Por lo cual el Registro Nacional es el primero de los obligados de velar, por todos los medios, que no se generen daños al particular con sustento en información derivada de bases de datos inexactas o erróneas que pudieran contenerse en los diferentes registros que lo conforman. De esa forma, la inscripción registral, se convierte en el instrumento garante de la publicidad, el ordenamiento jurídico determina, para cada caso, las actuaciones que deben presentarse al registro para su debida inscripción.

1.13. El principio de publicidad registral busca proteger los actos jurídicos que se hayan producido confiando en el contenido del registro; es decir, ampara a los terceros adquirentes de derechos, en base a la información contenida en los Registros. Se trata de una exteriorización continua e ininterrumpida de un acontecimiento jurídico que organiza e instrumenta el Estado mediante un órgano operativo, con el fin de generar la cognoscibilidad general a los terceros, creando con ello, la tutela de los derechos y la seguridad en el tráfico de los mismos. Dicha actividad va encaminada a hacer notorio un hecho, una situación o una relación jurídica, siendo además, una actividad dirigida a hacer cognoscible una situación jurídica real con el fin de proteger el crédito y la seguridad del tráfico jurídico.

1.14. El propósito fundamental de la institución es: registrar, en forma eficaz y eficiente, los documentos que se presenten ante el Registro Nacional, para su inscripción, así como garantizar y asegurar a los ciudadanos los derechos con respecto a terceros. Además, custodiar y suministrar a la colectividad la información correspondiente a bienes y derechos inscritos o en proceso de inscripción, mediante el uso eficiente y efectivo de tecnología y de personal idóneo, con el fin de facilitar el tráfico jurídico de bienes, con el propósito de contribuir a fomentar el desarrollo social y económico del país[4].

1.15. La JARN se compone de varias direcciones para su labor sustantiva tales como la Dirección de Inmobiliario, Dirección de Servicios, Dirección Instituto Geográfico Nacional, Dirección de Propiedad Intelectual, Dirección de Personas Jurídicas y la Dirección de Bienes Muebles. Estas direcciones llevan a cabo su labor sustantiva con el soporte de la plataforma tecnológica del Registro Nacional, que soporta diferentes sistemas sustantivos tales como: El Portal de Servicios Digitales, Diario Único, Ventanilla Digital, Sistema del Registro Inmobiliario (SIRE), Bienes Muebles, Personas Jurídicas, Sistema de placas,

[2] Oficio N.° DFOE-GOB-0567(20520) del 05 de diciembre de 2024.
[3] Ley de Creación del Registro Nacional.

Sistema de Información de planos (SIP), ePower, Sistema de información del Registro Inmobiliario (SIRI), Sistema de Presentación en línea de Patentes, Modelos de Utilidad y Diseños Industriales (WIPO Files Patentes), Sistema de Presentación en línea de Marcas Comerciales y otros Signos (WIPO Files Marcas) , Sistema de Derechos de Autor (GDA – Derechos de autor), Sistema de Certificaciones (SEC) y Spider Web. Además de sistemas administrativos como el Sistema Financiero Administrativo (SIFA) y el Sistema de Recursos Humanos (RH Gestor).

1.16. Además dentro de la estructura de la JARN se cuenta con una Dirección de Informática (DI) la cual depende de la Dirección General, y brinda servicios a todas las demás direcciónes de la JARN. La DI tiene como objetivo[4] coadyuvar a los procesos sustantivos y de apoyo, basándose en la visión institucional, procurando el uso de tecnologías de información idóneas para mejorar los servicios que brinda el Registro Nacional. Tiene a su cargo 4 Departamentos: Desarrollo de Soluciones, Infraestructura Tecnológica y Servicio al Usuario de Tecnologías de Información y Aseguramiento de la Información.

1.17. La seguridad de la información está a cargo del Departamento de Aseguramiento de la Información, la cual tiene como objetivo el gestionar los programas y directrices de seguridad de tecnologías de información del Registro Nacional, para mantener la confidencialidad, integridad y disponibilidad de los activos de información de la Institución. Además tiene a cargo funciones, que entre otras, está el orientar a funcionarios de la Institución en cuanto a la gestión del aseguramiento de la información y el cumplimiento del Manual de normas de aseguramiento de la información, así como atender los aspectos relacionados con la ciberseguridad del Registro Nacional[4].

MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA

1.18. Durante la ejecución de la auditoría, la JARN remedió algunas de las vulnerabilidades identificadas por la Contraloría General durante la ejecución de las pruebas de ciberseguridad no intrusivas a la infraestructura.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.19. El 17 de diciembre de 2024, en sesión virtual, se presentaron los resultados de la auditoría a las siguientes personas funcionarias del Registro Nacional: Agustín Meléndez García, Director General; Tracy Castro Mora, Directora a.i. de Informática; Oscar Morales Segura, Jefe Departamento de Aseguramiento de la Información; Brenda Chan Castillo, Directora de Recursos Humanos; Emerson Machado Cruz, Auditor Interno; Charlotte Morales Abarca, Subauditora Interna; Kattia Vargas Mena, supervisora en la Auditoría Interna. Durante dicha sesión se efectuaron observaciones al borrador, las cuales se consignaron en el Acta de comunicación y se consideraron en lo correspondiente.

1.20. El borrador de informe fue remitido a la Administración del Registro Nacional mediante oficio 20678 (DFOE-GOB-0574) del 11 de diciembre de 2024. Al respecto se recibió, el

[4] Manual de organización del Registro Nacional versión 11 Diciembre 2023

oficio N.° DGL-1176-2024 del 18 de diciembre de 2024, en el cual los funcionarios del Registro Nacional, informaron al Órgano Contralor, las observaciones relacionadas con el borrador del informe. Lo resuelto sobre las observaciones efectuadas se comunicó mediante oficio DFOE-GOB-0600 (21373) del 20 de diciembre de 2024.

SIGLAS Y ABREVIATURAS

1.21. En el cuadro N.°1 se indican las principales siglas utilizadas en este informe y su significado.

Cuadro N.° 1 Siglas utilizadas en el informe

Siglas / Abreviaturas	Significado
BCP	Plan de Continuidad de Negocio (Siglas en inglés:Business Continuity Plan)
BIA	Análisis de Impacto en el Negocio (Siglas en inglés:Business Impact Analysis)
CGR	Contraloría General de la República
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas (Siglas en inglés:Control Objectives for Information Systems and related Technology)
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DI	Dirección de Informática
DRP	Plan de recuperación en caso de desastre (Siglas en inglés: Disaster Recovery Plan)
ISO	Organización Internacional para la Estandarización (Siglas en inglés:International Organization for Standardization)
JARN	Junta Administrativa del Registro Nacional
LGCI	Ley General de Control Interno
MGTI	Marco Normativo de Gobierno y Gestión de las Tecnologías de Información
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones
SGCN	Sistema de Gestión de Continuidad del Negocio
SI	Seguridad de la Información

2. RESULTADOS

2.1. Se determinó que Junta Administrativa del Registro Nacional, en adelante JARN, cuenta con una política de seguridad de la información debidamente oficializada y vigente, implementación de respaldos de la información y medidas de seguridad física y ambiental para su resguardo; además está en curso la implementación de un Sistema de Gestión de Continuidad de Negocio (SGCN). No obstante, presenta varias debilidades relacionadas

con la gobernanza de la seguridad, la implementación de controles de ciberseguridad y continuidad, así como en controles de aplicación para sistemas de misión crítica.

2.2. Los resultados de la auditoría se dividen en tres áreas a saber: Gobierno de seguridad, Ciberseguridad y Continuidad de Negocio, y Controles de Operación, Gestión y Mantenimiento.

GOBIERNO DE SEGURIDAD

2.3. La gobernanza de seguridad o gobierno de seguridad, se refiere a la implementación y supervisión del programa de seguridad de la información de la organización, orientada al logro de objetivos y gestión de riesgos mediante el establecimiento de un marco de gestión de seguridad de la información que incluye: liderazgo y patrocinio gerencial, asignación formal de roles y responsabilidades, programa de sensibilización, capacitación técnica, y como un complemento la implementación y control de contratos para la prestación de servicios tercerizados, entre otras medidas administrativas.

Ausencia de una estrategia para orientar el Gobierno de Seguridad

2.4. Se determinó que la administración del Registro Nacional no cuenta con una Estrategia de Seguridad, que permita orientar el manejo y resguardo de la información y articule los controles que en conjunto determinan el estado de la seguridad de información y la protección de activos[5]; así como la definición de programa de seguridad y una cartera de proyectos para un abordaje progresivo de las necesidades de esa entidad.

2.5. Al respecto, esa institución tiene en desarrollo el Sistema de Gestión de Seguridad de la Información (SGSI), sin definir sus componentes a nivel estratégico, los roles y responsabilidades directivas, así como acciones claramente definidas y estructuradas para la sensibilización institucional sobre la importancia de la seguridad. Así, en el caso de los roles y responsabilidades, relacionados con seguridad, se encontró que las funciones se han delegado en la Jefatura de Aseguramiento de Información, que a su vez depende de la Dirección de Informática (DI), sin contar con el rol estratégico institucional en Seguridad de la Información.

2.6. Además, en materia de sensibilización de seguridad de información las acciones se circunscriben al envió de comunicaciones masivas vía correo electrónico para alertar sobre riesgos de seguridad; sin que ello constituya un programa de sensibilización, con objetivos claros, audiencias definidas y material de formación desarrollado para crear conciencia. Lo anterior, aunado a que la cobertura no alcanza a toda la organización y a los terceros relacionados con TI, sino a un conjunto específico de usuarios.

2.7. Las mejores prácticas en materia de seguridad establecen la necesidad de “proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado”, para Cobit 5 en su proceso APO02

[5] Como proceso se parte del diagnóstico de la postura actual de seguridad, y de la definición de una postura deseada, se traza un programa de seguridad que contiene una cartera de proyectos. Los proyectos que hacen parte de la cartera permiten implementar controles específicos que satisfacen necesidades del negocio en términos de seguridad

Gestionar la estrategia plantea que se debe “Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella” y “Demostrar trazabilidad de la estrategia del negocio y sus necesidades”, como parte del proceso se plantea “Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos”.

2.8. En lo que respecta a roles y responsabilidades, la norma ISO 27001 señala en su aparte 5.1 como parte de las responsabilidades de la gerencia el “establecer roles y responsabilidades para la seguridad de información” y operativamente en la norma ISO 27002 se detalla “La dirección debería apoyar activamente la seguridad dentro de la organización a través de una orientación clara, compromiso demostrado, y la asignación explícita de las responsabilidades de seguridad de la información y su reconocimiento”.

2.9. La estrategia de seguridad se implementa a través del Sistema de Gestión de Seguridad de Información (SGSI), el cual se puede considerar desde la perspectiva de la norma ISO 27001 o inclusive desde el proceso APO 13 de Cobit 5 Gestionar la Seguridad el cual indica que se debe entre otras cosas “Establecer y mantener un SGSI”, “Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información” así como “Supervisar y revisar el SGSI”.

2.10. En esa misma línea, la norma ISO 27001 remite a la necesidad de desarrollar el programa de sensibilización en seguridad de información como parte de los requisitos de implementación del SGSI. Por su parte la norma ISO 27002 en su aparte 8.2.2 trata la “Toma de conciencia, educación y formación en seguridad de la información” y describe el control de la siguiente manera “Todos los empleados de la organización y, donde sea pertinente, contratistas y usuarios de terceras partes deberían recibir formación adecuada en toma de conciencia y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral”.

2.11. Las situaciones anteriores, se deben a que la JARN no ha priorizado la seguridad de la información como parte de sus estrategias institucionales, pese a que el resguardo de la información registral resulta un factor medular de su actividad sustantiva.

2.12. La capacidad de implementar las políticas, procedimientos y directrices para proteger los activos de información esenciales, es dispersa y puede dejar vacíos que la dejen en condiciones vulnerables. Además, las acciones prioritarias para el fortalecimiento de la seguridad de la información puede limitarse al estar excluida de las estrategias institucionales.

CONTROLES DE CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO

2.13. Este apartado se refiere al conjunto de medidas técnicas que permiten brindar aseguramiento y protección a los activos digitales, entendidos como todos los recursos disponibles para el procesamiento de información, infraestructura, redes, bases de datos, etc. A esto se suman los controles para garantizar la disponibilidad de recursos informáticos, esto es la Continuidad del Negocio y la contingencia tecnológica.

Debilidades en los controles de ciberseguridad y continuidad del negocio

2.14. Se determinó que los controles de ciberseguridad y continuidad del negocio son insuficientes para asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información. Así, en lo correspondiente a los controles de ciberseguridad, no existen acciones para gestionar de manera activa y periódica posibles vulnerabilidades a la infraestructura; sobre el particular, la Contraloría General remitió el oficio DFOE-GOB-0567(20520) del 05 de diciembre de 2024, con carácter de de acceso restringido, en el cual se detallaron los aspectos técnicos y riesgos identificados, considerando su clasificación CVSS[6], CWE[7] y CVE[8], los cuales deben gestionarse mediante controles de forma activa y periódica.

2.15. En cuanto a las vulnerabilidades de ciberseguridad detectadas, se debe considerar que en las Normas de control interno para el Sector Público[9], 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 Sistema de Control Interna (SCI), de conformidad con los objetivos y recursos institucionales. Asimismo, el numeral 12.6[10] de la norma ISO 27001, refiere a la necesidad de obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información usados, evaluar la exposición de la organización a estas y tomar las medidas apropiadas.

2.16. Por su parte, en lo referente a la continuidad de negocio se determinó que la JARN no ha concluido la implementación del Sistema de Gestión de Continuidad de Negocios (SGCN). Al respecto, en el Análisis de Impacto de Negocios (BIA) no se han priorizado los sistemas críticos institucionales, no se han alineado los controles operativos como el respaldo y recuperación de información con el (BIA), el modelo de continuidad de negocio ni los los respaldos de información han sido sometidos a prueba como parte del plan de continuidad, y no se ha capacitado al personal.

2.17. Aunado a lo anterior, se encontró que el plan de recuperación de desastre (DRP) no está basado en el diseño de escenarios de riesgo y no contempla todos los elementos técnicos que deben acompañar este proceso tales como protocolos de declaración de eventos y comunicación, roles y responsabilidades, actividades de contención, erradicación, forense, relaciones con autoridades y cuerpos de socorro, manejo de terceros y protocolos de respuesta, lo cual se debe alinear con el Análisis de Impacto de Negocio

[6] Common Vulnerability Scoring System (CVSS), es un sistema de puntuación numérica que se asigna a una vulnerabilidad del marco abierto del NIST (National Institute of Standards and Technology /U.S Department of Commerce) para comunicar las características y la gravedad de las vulnerabilidades del software.

[7] Common Weakness Enumeration (CWE) es una lista desarrollada por la comunidad de tipos de debilidades de software y hardware. Sirve como un lenguaje común para medir las herramientas de seguridad y como una línea de base para los esfuerzos de identificación, mitigación y prevención de debilidades.

[8] Common Vulnerabilities and Exposures (CVE), lista de información registrada sobre vulnerabilidades de seguridad conocidas.

[9] Norma 6.4 Acciones para el fortalecimiento del SCI de la Norma N-2-2009-CO-DFOE (NCISP).

[10] Sección A.12.6 Gestión de vulnerabilidades técnicas

(BIA) y el Plan de Continuidad de Negocio (BCP). Además en el tema de respaldos de información, éstos no se relacionan con el BIA institucional establecido, y no están alineados a las necesidades de los procesos sustantivos.

2.18. Sobre el particular, de acuerdo con el apartado APO11.01 del COBIT 2019, relacionado con el establecimiento del un sistema de gestión de calidad (SGC), la continuidad de negocio parte de la definición de procesos de negocio, sistemas, infraestructura crítica y los indicadores relacionados con umbrales de recuperación de sistemas y de pérdida de datos aceptable, entre otros. Esta definición se documenta en el Análisis de Impacto de Negocio (BIA por sus siglas en inglés). Luego se debe establecer un proceso llamado Continuidad de Negocio en el cual se definen los pasos a seguir para operar el negocio en contingencia, es decir ante la ausencia de un recurso como sistemas o energía. Ese proceso se documenta en un Plan de Continuidad de Negocio (BCP por sus siglas en inglés).

2.19. El tercer componente, clave en Continuidad de negocio (se desarrolla posterior al BIA y al BCP) es el plan de recuperación en caso de desastre (DRP por sus siglas en inglés) un documento que desarrolla escenarios de recuperación para que la Dirección de Informática pueda resolver si se presenta un evento disruptivo.

2.20. Como complemento al BCP y al DRP se deberían programar pruebas para garantizar que estos planes son funcionales, esto en atención a buenas prácticas como Cobit e ISO 22301[11]. Existen diversas formas de probar la continuidad del negocio, y en el caso de la JARN dado que el proceso está en desarrollo de implementación, aún no se ha probado.

2.21. Al respecto, el artículo 4 de la Ley General de la Administración Pública establece que la actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, eficiencia, adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios. En ese sentido, el apartado XIII de las Normas técnicas para la gestión y control de las tecnologías de información emitidas por el MICITT, señalan que la institución debe establecer prácticas formales para contar con una estrategia viable para mantener la continuidad de las operaciones y recuperación ante desastres o incidentes, estableciendo roles y responsabilidades para ello.

2.22. Por su parte, en la norma DSS04 Gestionar la Continuidad, se detalla que las instituciones tienen la necesidad de establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios de TI requeridos con el fin de mantener la disponibilidad de la información a un nivel aceptable.

2.23. Además, en la citada norma, se establecen prácticas para poder dar continuidad de las operaciones críticas para el negocio y mantener la disponibilidad de la información, tales como: definir la política de continuidad del negocio, objetivos y alcance; mantener una estrategia de continuidad; desarrollar e implementar una respuesta a la continuidad del

[11] ISO 22301 para la Gestión de la Continuidad de Negocio (SGCN). Secciones 4.3 Determinar el alcance del SGCN, 5 Liderazgo, 6 Planeación, 8.2 Análisis de impacto al negocio, 8.3 Estrategia para la continuidad del negocio y soluciones, 8.4 Planes y procedimientos para la continuidad del negocio, 8.5 Programa de ejercicios.

negocio; ejercitar, probar, revisar, mantener y mejorar el plan de continuidad; proporcionar formación en el plan de continuidad; gestionar acuerdos de respaldo y ejecutar revisiones post-reanudación.

2.24. En cuanto al tema de respaldos las buenas prácticas[12] indican que se deberían establecer procedimientos de rutina para implementar una política y estrategia acordada de respaldo (…) haciendo copias de respaldo de datos y ensayando su oportuna restauración. Además, señala que se debería elaborar procedimientos documentados de restauración y registros exactos y completos de las copias de respaldo; además, en el inciso f) de la guía de implementación se establece que los medios de respaldo se deberían probar regularmente para asegurarse que pueden ser confiables para el uso cuando sean necesarios.

2.25. Las situaciones señaladas obedecen a que la priorización estratégica de la seguridad de la información, considerando los riesgos en los controles de ciberseguridad y continuidad del negocio; no ha sido contemplada por la Junta Administrativa del Registro Nacional, lo cual no permite la consistencia en el desarrollo, aplicación, seguimiento y evaluación de controles asociados.

2.26. Las debilidades en los controles de ciberseguridad y continuidad del negocio, aumenta el riesgo de dejar fuera de funcionamiento los servicios críticos en caso de que se exploten vulnerabilidades por un atacante. Además las deficiencias en materia de seguridad lógica pueden tener un impacto sobre la confidencialidad y la integridad de la información y los sistemas.

OPERACIÓN, GESTIÓN Y MANTENIMIENTO DE LOS SISTEMAS

2.27. La gestión de los sistemas críticos de la JARN debe asegurar la existencia de controles de entrada y autenticación, se encuentren actualizados y con posibilidad de actualizarse periódicamente, cuentan con políticas y comité para gestionar los cambios necesarios, así como los problemas e incidentes en cuanto a la seguridad de la información, y se realiza un mantenimiento preventivo y correctivo en la materia. Además las operaciones de TI como conjunto de prácticas deben asegurar la sostenibilidad y estabilidad de los sistemas de información.

Debilidades en la aplicación de controles de Operación, Gestión y Mantenimiento de los Sistemas que inciden la seguridad de la información

2.28. Los controles de seguridad de la información definidos en políticas, manuales y procedimientos, para la operación, gestión y mantenimiento de los sistemas del Registro Nacional tienen debilidades de implementación que restan efectividad a las prácticas de seguridad de la información.

2.29. De esta forma, se identificó que el Comité de Tecnologías de Información, encargado de unir esfuerzos de negocio con el consejo de los equipos técnicos para tomar decisiones

[12] ISO 27002 Apartado 10.5 Respaldos.

con respecto a iniciativas y proyectos que involucran operaciones de TI y seguridad, no ha operado sobre una base regular en los últimos dos años. Además, en lo referente a la gestión de cambios, el Comité de Cambios, encargado de gestionar los cambios en el estado de la infraestructura y los sistemas, no tiene representantes de usuarios para supervisar/autorizar modificaciones.

2.30. En relación con lo anterior, las buenas prácticas[13] establecen la necesidad de gestionar todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Además de asegurarse de que los cambios se registran, priorizan, clasifican, evalúan, autorizan, planifican y programan. Finalmente, se debe considerar que cada cambio debe ser aprobado por parte de los dueños de los procesos de negocio, gestores de servicios y partes interesadas técnicas de TI, según corresponda.

2.31. Además, se identificó que no se encuentra implementado software que permita fortalecer la seguridad de la información, para aquellos funcionarios del Registro Nacional que optan por utilizar dispositivos personales para realizar funciones laborales. Al respecto la norma ISO 27001 en su capítulo Dispositivos móviles y teletrabajo[14], indica que se debe adoptar una política y medidas de soporte de seguridad para gestionar los riesgos que se presentan por el uso de dispositivos móviles.

2.32. Por otra parte, se determinó que el procedimiento para la destrucción segura de información en medios de almacenamiento físicos (por ejemplo discos extraíbles), es insuficiente para asegurar la destrucción de la información almacenada, pues no considera el tratamiento que debe darse al dispositivo físico. También en el caso de la papelería, se identificó que el archivo central, delega el reciclaje y destrucción de papel con información a un tercero, sin la seguridad de que cualquier tipo de información que pueda ser sensible o confidencial para desecho, sea debidamente resguardada y destruida durante el proceso.

2.33. La JARN ha implementado una Política de Seguridad de Información, bajo la denominación de “Manual de Normas de Aseguramiento de la Información”, este documento establece las bases para la implementación de controles y se hace acompañar de otras políticas que le complementan.

2.34. La norma ISO 27002 señala con respecto a la eliminación de medios de almacenamiento que “Se debería eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales” en ese sentido “Los procedimientos formales de eliminación segura de los medios minimicen el riesgo que personas no autorizadas accedan a información sensible.Los procedimientos para la eliminación segura de los medios que contengan información sensible, deberían estar en consonancia con la sensibilidad de esa información”.

2.35. También, se identificó que el Registro Nacional ha implementado el cifrado de tablas de contraseñas, así como el cifrado de datos biométricos como mecanismo de protección de datos sensibles. Sin embargo esta medida no se extiende a otras estructuras como bases

[13] COBIT 5 proceso BAI06 Gestionar los cambios de TI.
[14] A.6.2 Dispositivos móviles y teletrabajo.

de datos de sistemas de aplicación y a información en tránsito, sea a lo interno de la red o hacia direcciones en el exterior.

2.36. Lo señalado pese a que la información se debe proteger en todo momento y sin importar su estado, se trate de información en uso, en tránsito o en reposo, se espera una garantía de confidencialidad e integridad. Por esa razón se ha desarrollado el cifrado de datos como medio de control técnico para salvaguardar información[15].

2.37. El marco de gestión del COBIT 5, en su proceso DSS05 sobre gestión de servicios de seguridad, establece como parte de las prácticas el cifrar la información en tránsito de acuerdo con su clasificación, así como cifrar la información almacenada de acuerdo a su clasificación. A su vez, el código de prácticas ISO 27002 indica en el apartado 10.5.1 sobre respaldos, en su inciso h), que ante situaciones donde la confidencialidad es de importancia, los respaldos deberían ser protegidos por medio del cifrado, mientras que en el apartado 10.9.2 sobre transacciones en línea, el inciso c) plantea que el canal de comunicación entre todas las partes implicadas debe ser cifrado.

2.38. Ahora bien, en lo correspondiente a los controles para prevenir ataques de denegación de servicio, se determinó en el análisis de sistemas que si bien se implementan controles como el uso de un WAF[16], no se ha considerado el uso de un captcha o un mecanismo de validación humana.Dicha medida no es mandatoria, pero es altamente recomendada como buena práctica y control compensatorio; lo cual amerita una valoración desde el punto de vista de estrategia de seguridad.

2.39. En cuanto a continuidad de las operaciones, si bien la JARN cuenta con un sitio de procesamiento principal que cumple de manera adecuada con las buenas prácticas de la industria en cuanto seguridad física, respaldos, controles de TI, etc; no existe un sitio alterno con condiciones y características similares al principal que permita asegurar la continuidad de la infraestructura tecnológica en todo momento ante eventos fortuitos; dada la importancia o relevancia de la criticidad tanto de la información como de los sistemas que resguardan ésta en la JARN. En ese sentido, tampoco se localizó un estudio que analice los riesgos y la factibilidad tanto técnica como financiera de no contar con éste sitio.

2.40. La norma ISO 27002 en su aparte 10.5.1 sobre respaldos de información establece que “Se deberían hacer regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo” para luego puntualizar que “la información de respaldo debería tener un nivel apropiado de protección ambiental y físico consistente con las normas aplicadas en el sitio principal; los controles aplicados a los medios en el sitio principal se deberían ampliar para cubrir el sitio de respaldo”

2.41. Como parte de las valoraciones sobre seguridad lógica, se realizaron pruebas de fortaleza de las contraseñas utilizadas en los algunos de los sistemas críticos del Registro

[15] El cifrado es una técnica mediante la cual se aplican recursos computacionales de procesamiento para convertir un conjunto de datos a una forma no legible, para luego restablecerlo a su forma original si el lector cuenta con los medios necesarios y la respectiva autorización.
[16] Web Application Firewall por sus siglas en inglés, es una barrera lógica entre un entorno de red seguro y uno desconocido.

Nacional, para un total de 12 sistemas (incluyendo el Sistema de Administración de Usuarios -Directorio Activo) para éstos efectos) que se comparan con la política establecida, como se observa en el cuadro siguiente:

Cuadro N.° 2

Detalle de sistemas de la JARN con incumplimientos de la política de gestión de contraseñas del Registro Nacional

Característica	Número de sistemas	Ejemplo de sistema
Se autentica contra el Active Directory	8	SIS Patentes RH Gestor SIS Persojas Jurídicas SIS Diario Servicios
Cuenta con un gestor de identidades propio	4	SIFA SIP E Power Spider Web
Incumple política de contraseñas por longitud	7	SIP SIFA Spider Web SIS Marcas
Incumple política de contraseñas por complejidad	8	SIFA SIP E Power Spider Web SIS Muebles
Permite reciclar contraseñas	7	SIP E Power Spider Web SIS Derechos Autor

Fuente: Elaboración CGR a partir del análisis en las pruebas realizadas en 12 sistemas de la JARN.

2.42. Otros aspectos a considerar en la valoración sobre confidencialidad y mecanismos de autenticación tiene que ver con el uso de mecanismos que permiten garantizar que el usuario que ingresa es quien dice ser, a esto se llama factor de autenticación y es altamente recomendable utilizar dos factores[17] para alcanzar una autenticación fuerte. También se recomienda utilizar un bloqueo automático de sesión[18], en caso de que el

[17] El doble factor de autenticación permite combinar el uso de dos de tres alternativas: contraseña o PIN (algo que el usuario conoce) con algo que el usuario posee (un token, gafete, clave dinámica o similar) o algo que el usuario es (reconocimiento facial, huella dactilar).

[18] Este control remite a la necesidad de inhabilitar la sesión de trabajo del usuario o su acceso al sistema operativo en el momento que se ha dejado el computador sin utilizar por un periodo de tiempo considerable, por lo general de 15 a 20 minutos para evitar que usuarios no autorizados puedan acceder a recursos que no les corresponde.

equipo quede desatendido y configurar el sistema para evitar la concurrencia de sesiones [19] y la reutilización de contraseñas[20].

2.43. En relación con lo anterior, se determinó que no todos los sistemas críticos cuentan con el mecanismo de doble factor de autenticación para el inicio de sesión de los usuarios en los sistemas y plataformas para reducir los riesgos derivados de errores humanos en la gestión de las contraseñas y dispositivos. En este particular se determinó lo siguiente lo que se observa en el siguiente cuadro:

Cuadro N.° 3

Debilidades de seguridad de la información en los sistemas de la JARN

Característica	Número de sistemas	Ejemplo de sistema
No cuenta con doble factor de autenticación	7	RH Gestor SIFA Spider Web SIS Marcas
Permite Concurrencia de sesiones	7	RH Gestor SIFA E Power SIS Marcas
No bloquea al usuario por intentos fallidos de inicio de sesión	5	E Power SIS Marcas SIS Personas Jurídicas

Fuente: Elaboración CGR a partir del análisis en las pruebas realizadas en 12 sistemas de la JARN.

2.44. Finalmente se constata que, en términos generales no se ha implementado la suspensión de usuarios por ausencia prolongada. Esto es automatizar la suspensión de todos los usuarios que se ausenten de sus funciones por un periodo de tiempo superior a un número de días seleccionado, sea por vacaciones, incapacidad, licencia, o cualquier otro motivo, este particular no se aplica en todos los casos y no se ha automatizado, por lo que la implementación es discrecional, solamente un área reportó realizar esta tarea manualmente.

2.45. En relación con la gestión de identidades y el acceso lógico a los usuarios, las buenas prácticas[21] indican que se debe asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las respectivas unidades que gestionan sus propios derechos de acceso con los procesos de negocio. Para eso, se indica que se debería mantener los derechos de acceso de los

[19] La concurrencia de sesiones ocurre cuando el mismo usuario abre una sesión de trabajo en dos equipos diferentes o más al mismo tiempo, esto atenta contra la integridad de la información que se conserva en base de datos. Salvo una justificación de negocio, esta situación no es recomendable.
[20] La reutilización de contraseñas ocurre cuando el sistema advierte al usuario que debe cambiar su contraseña y este utiliza la contraseña anterior o una de las anteriores. La configuración de sistema debería prevenir esta situación y dar una respuesta acorde.
[21] COBIT 5 Proceso DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio, alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y de conocer, además de realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.

2.46. Las situaciones anteriores se deben a la falta de acciones para operativizar lo dispuesto en el marco normativo de seguridad de la información y buenas prácticas, como la integración de usuarios en el comité para la definición de modificaciones y para la suspensión por ausencia prolongada. También ante sistemas que no permiten fortalecer la seguridad y los que no se han ajustado pese a ser técnicamente viable.

2.47. La JARN Se expone a riesgo de pérdida de disponibilidad e integridad de la información. Se incrementa el riesgo de pérdida de disponibilidad de recursos como sistemas e información.

3. 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. Aunque existen políticas, procedimientos y manuales, 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.

3.2. La ausencia de una estrategia para orientar el Gobierno de Seguridad de la Información incide en la capacidad de implementar las políticas, procedimientos y directrices para proteger los activos de información esenciales, y puede dejar vacíos que la dejen en condiciones vulnerables.

3.3. Los controles de ciberseguridad y continuidad del negocio son insuficientes para asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información, lo cual aumenta el riesgo de dejar fuera de funcionamiento los servicios críticos en caso de que se exploten vulnerabilidades por un atacante.

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 e incrementan el de disponibilidad de recursos como sistemas e información.

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 n.° 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 N.° R-DC-144-2015, publicados en La Gaceta n.° 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.

AL LICENCIADO GERALD CAMPOS VALVERDE, EN SU CALIDAD DE PRESIDENTE DE LA JUNTA ADMINISTRATIVA DEL REGISTRO NACIONAL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Definir y oficializar un procedimiento para integrar dentro de la elaboración de la planificación estratégica institucional el análisis de los riesgos y debilidades en seguridad de la información, los controles de ciberseguridad y la continuidad del negocio. Remitir a la Contraloría General de la República, una certificación que acredite la definición y oficialización del procedimiento a más tardar seis meses después de que el asunto sea conocido por la Junta Administrativa del Registro Nacional. (Ver párrafos del 2.3 al 2.26).

4.5. Implementar el procedimiento para integrar en la elaboración de la planificación estratégica el análisis de los riesgos y debilidades en seguridad de la información, los controles de ciberseguridad y la continuidad del negocio, que haya definido y oficializado en el cumplimiento de la disposición contenida en el párrafo 4.4. Remitir a la Contraloría General de la República una certificación en la cual se acredite el inicio de la implementación del plan, a más tardar dos meses después de su oficialización. Además un informe de avance semestral acerca de la implementación del Plan. (Ver párrafos del 2.3 al 2.26).

4.6. Elaborar, formalizar, divulgar e implementar el Sistema de Gestión de la Continuidad del Negocio, que contemple e integre al menos: a) la política de continuidad de negocio en la cual se defina el alcance y los objetivos de continuidad del negocio en la institución, b) el plan de continuidad de negocio (BCP) con sus respectivos escenarios, c) el plan de recuperación de desastres (DRP) en atención a los escenarios que surgen del análisis de riesgos de seguridad, d) el análisis de impacto de negocio (BIA), con la estrategia de respaldo y recuperación, y calendario de pruebas e) objetivos, f) alcance, g) roles y responsabilidades de las partes interesadas, h) pruebas al modelo de continuidad de negocio. i) estrategia de respaldo y recuperación en concordancia con BIA que incluya el calendario de pruebas. Remitir a la Contraloría General un informe de avance de la elaboración del Sistema de Gestión de Continuidad de Negocio a más tardar el 01 de setiembre de 2025. Una certificación en la que se haga constar que se elaboró y formalizó

el SGCN, a más tardar el 25 de febrero de 2026. Una certificación en la que se haga constar la divulgación del SGCN, con los contenidos mínimos solicitados, a más tardar el 24 de abril de 2026. Dos Informes de avances en la implementación del SGCN, a más tardar el 25 de agosto de 2026, y un segundo informe a más tardar el 25 de febrero de 2027. (Ver párrafos del 2.13 al 2.26).

AL LICENCIADO AGUSTÍN MELÉNDEZ GARCÍA, EN SU CALIDAD DE DIRECTOR GENERAL DEL REGISTRO NACIONAL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.7. Definir e implementar las acciones para que se incorpore al Comité de Cambios del Registro Nacional a los usuarios de negocio en la supervisión, incorporación y autorización de las modificaciones a la infraestructura de Tecnologías de Información. Remitir a la Contraloría General una certificación en cual se haga constar que se definieron y formalizaron las acciones, a más tardar el 25 de febrero de 2025. Además, una certificación en la cual se acredite la implementación de las acciones, a más tardar el 23 de mayo de 2025. (Ver párrafos del 2.27 al 2.47).

4.8. Elaborar, aprobar e implementar un plan de remediación de las vulnerabilidades sobre seguridad de la información comunicadas mediante el oficio n.° 20520 (DFOE-0567) del 5 de diciembre de 2024, 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. Remitir a la Contraloría General una certificación en la cual se acredite la elaboración y aprobación del plan de remediación, a más tardar el 25 de febrero de 2025. Además, remitir una certificación en la cual se acredite la implementación del plan a más tardar el 23 de mayo de 2025. (Ver párrafos del 2.13 al 2.26).

AL LICENCIADO RÓGER ARAYA FONSECA, EN SU CALIDAD DE DIRECTOR DE INFORMÁTICA DEL REGISTRO NACIONAL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.9. Definir e implementar los mecanismos que permitan aplicar los controles establecidos en el marco normativo de seguridad de la información del Registro Nacional, que considere al menos; a) Estandarización del cumplimiento de la política de contraseñas para la totalidad de los sistemas y servicios del Registro Nacional; b) la concurrencia de sesiones para la totalidad de los sistemas y servicios; c) controles adicionales como el cifrado de paquetes en las bases de datos e información en tránsito; d) Implementación de políticas (agentes) en los dispositivos móviles personales que acceden a recursos de información para efectos laborales; e) la destrucción segura de información. Remitir a la Contraloría General una certificación en la cual se acrediten los mecanismos definidos para aplicar los controles establecidos en las políticas y procedimientos de seguridad, a más tardar el 25 de marzo de 2025. Además dos informes de avance acerca de la implementación de los mecanismos, el primero a más tardar el 25 de setiembre 2025 y el segundo al 18 de diciembre de 2025. (Ver párrafos del 2.27 al 2.47).

4.10. Efectuar un análisis de riesgos, definir e implementar las acciones en relación con las debilidades encontradas en los controles de seguridad de la información, según las buenas prácticas, en lo referente a la prevención ante ataques de denegación de servicio en sistemas publicados en la web y la factibilidad técnico- financiera de implementar un sitio de procesamiento alterno. Remitir a la Contraloría General una certificación en la cual se acredite que se realizó el análisis de riesgos y se definieron las acciones, a más tardar el 25 de abril de 2025. Además dos informes de avance acerca de la implementación de las acciones, el primero al 24 de octubre de 2025 y el segundo al 24 de abril de 2026. (Ver párrafos del 2.27 al 2.47).

A LA LICENCIADA BRENDA CHAN CASTILLO, EN SU CALIDAD DE DIRECTORA DE RECURSOS HUMANOS DEL REGISTRO NACIONAL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.11. Definir, formalizar e implementar los mecanismos que permitan ejecutar de manera automatizada la suspensión de cuentas de usuarios por ausencias prolongadas. Remitir a la Contraloría General de la República una certificación en cual se haga constar que se definieron y formalizaron los mecanismos, a más tardar el 25 de marzo de 2025. Además, una certificación en la cual se acredite la implementación de los mecanismos definidos, a más tardar el 25 de junio de 2025. (Ver párrafos del 2.27 al 2.47).

Falon StephanyArias Calero
Gerente de Área

Marvin Mejía Vargas
Asistente Técnico

Alejandro Zúñiga Gómez
Coordinador

Grettel Camacho Aguilar
Colaboradora

CGR | Firmado digitalmente
Valide las firmas digitales

msb
G: 2024000427-1