INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LA DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA

15 de diciembre, 2023
Informe N° DFOE-GOB-IAD-00014-2023

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

CUADROS

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría de carácter especial tuvo como objetivo determinar si las acciones implementadas por la Administración para resguardar la información brindan una protección razonable a los activos tecnológicos y de información de la Dirección General de Migración y Extranjería de acuerdo con el marco regulatorio y buenas prácticas aplicables. Para ello se valoró las acciones implementadas por la Administración para garantizar el resguardo de la información y activos tecnológicos en el período comprendido entre el 1 enero de 2022 y el 30 de junio de 2023, y se amplió cuando se consideró necesario.

¿POR QUÉ ES IMPORTANTE?

La Dirección General de Migración y Extranjería es el ejecutor de la política migratoria con la responsabilidad de garantizar la seguridad ciudadana a través de la efectiva administración de los flujos migratorios, regulación de permanencia e integración de las personas extranjeras a la sociedad costarricense, a través de un proceso ágil y transparente en la gestión de los servicios institucionales en favor de los derechos humanos. Cuenta con sistemas informáticos para gestionar muchas de las funciones que le corresponde realizar, tales como el control del ingreso y egreso de personas (nacionales y extranjeros) al territorio nacional, la promoción de la integración de las personas extranjeras a la sociedad costarricense, la regulación de la permanencia y actividades de las personas extranjeras en el país, el combate contra los delitos de trata de personas y tráfico ilícito de migrantes. La custodia y procesamiento de este tipo de información convierten a la DGME en un blanco de interés para los ciberdelincuentes y, siendo que durante el año 2022 diversas instituciones públicas fueron atacadas por grupos organizados conocidos como ciberdelincuentes internacionales, es necesaria la presente auditoría para determinar si dicha institución cuenta con los controles necesarios para garantizar la seguridad de la información.

¿QUÉ ENCONTRAMOS?

Se determinó que las acciones implementadas por la Administración para resguardar la información cumplen parcialmente con el marco regulatorio y buenas prácticas aplicables, por lo que requiere acciones de mejora inmediatas para brindar una protección a los activos tecnológicos y de información de la Dirección General de Migración y Extranjería. Al respecto, poseen políticas de asignación de usuarios, atención de incidentes y monitoreo de seguridad. Han implementado parcialmente controles sobre clasificación y etiquetado de la información, revisión de derechos de acceso, gestión de activos y continuidad. Por último, no se ha documentado la totalidad de requisitos obligatorios y la normativa establecida debe actualizarse a la realidad institucional y el marco adoptado.

También, se identificaron debilidades de ciberseguridad las cuales podrían comprometer la seguridad de la información institucional. Al respecto, la Dirección General de Migración y

Extranjería atendió durante la ejecución de la auditoría el 49% de las vulnerabilidades comunicadas.

Por su parte, la Dirección General de Migración y Extranjería posee una guía para la identificación y comunicación de vulnerabilidades sin embargo no establece responsables, periodicidad ni actividades para subsanar los hallazgos de ciberseguridad.

Asimismo, parte de la documentación institucional de seguridad de la información debe actualizarse según los requisitos vigentes de negocio y el marco de gestión adoptado. Además, se carece de normativa para gestionar la ciberseguridad que contemple el análisis periódico de los riesgos de ciberseguridad y los planes de remediación de vulnerabilidades.

Las situaciones encontradas exponen a la institución a riesgos de pérdida de confidencialidad, integridad y disponibilidad, así como riesgos de accesos no autorizados a los activos tecnológicos y de información de la DGME.

¿QUÉ SIGUE?

Se emiten disposiciones a la Dirección General de Migración y Extranjería, con el propósito de integrar y ejecutar labores correspondientes al cuerpo colegiado de alto nivel para la toma de decisiones sobre temas estratégicos asociados con las TIC según lo establece Marco normativo de Tecnologías de Información adoptado por la Institución; así como actualizar e implementar la normativa para gestionar la seguridad de la información institucional que considere al menos la clasificación, resguardo de la información institucional, revisión de accesos y verificación periódica del cumplimiento de la normativa vigente. También se dispone actualizar e implementar la normativa de ciberseguridad para que incluya el análisis periódico de los riesgos sobre ciberseguridad, la remediación de las vulnerabilidades y planes de mitigación cuando corresponda, considerando al menos actividades, responsables y periodicidad de ejecución.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LA DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA (DGME)

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. Durante el año 2022 diversas instituciones públicas fueron blanco de grupos organizados conocidos como ciberdelincuentes internacionales, los cuales lograron vulnerar sistemas informáticos y afectar la continuidad de servicios, en consecuencia los ciudadanos se han visto afectados en los trámites que involucren el uso de esos sistemas informáticos.

1.2. Lo anterior, impactó la integridad, confiabilidad y disponibilidad de la información sensible que interviene en la gestión de los recursos públicos, por lo tanto, toma relevancia contar con sistemas y mecanismos de defensa, para identificar amenazas previsibles y reaccionar de manera apropiada.

1.3. Por su parte, la Dirección General de Migración y Extranjería (DGME), cuenta con sistemas informáticos para gestionar muchas de las funciones que le corresponde realizar, tales como el control del ingreso y egreso de personas (nacionales y extranjeros) al territorio nacional, la promoción de la integración de las personas extranjeras a la sociedad costarricense, la regulación de la permanencia y actividades de las personas extranjeras en el país, el combate contra los delitos de trata de personas y tráfico ilícito de migrantes; la custodia y procesamiento de este tipo de información convierten a la DGME en un blanco de interés para los ciberdelincuentes.

1.4. En virtud de lo anterior, es necesario e importante que la CGR, como órgano de fiscalización superior, realice una auditoría para determinar si dicha institución cuenta con los controles necesarios para garantizar la seguridad de la información que se genera y que también impacta de forma directa el proceso Migratorio, con el propósito de brindar recomendaciones y emitir disposiciones que contribuyan con su labor.

OBJETIVO GENERAL

1.5. La auditoría tuvo como propósito determinar si las acciones implementadas por la Administración para resguardar la información brindan una protección razonable a los activos tecnológicos y de información de la Dirección General de Migración y Extranjería de acuerdo con el marco regulatorio y buenas prácticas aplicables.

ALCANCE

1.6. La auditoría comprendió el análisis de las acciones implementadas por la Administración para garantizar el resguardo de la información y activos tecnológicos conforme al marco regulatorio aplicable. El período de estudio corresponde del 01 de enero de 2022 al 30 de junio de 2023.

CRITERIOS DE AUDITORÍA

1.7. Los criterios de evaluación aplicados en la presente auditoría, y los parámetros de cumplimiento utilizados para llegar a las conclusiones de este informe, se comunicaron en sesión del 12 de octubre de 2023 a los funcionarios de la Dirección General de Migración y Extranjería, Jean Paul San Lee Lizano, Subdirector; Jenny Gamboa Rodríguez, Jefa Gestión de Tecnologías de Información y Karol Rivera Gonzalez, Asistente Despacho. Posteriormente, dichos criterios se comunicaron mediante oficio n.° 14820 (DFOE-GOB-0437) del 20 de octubre de 2023.

1.8. Con el fin de presentar un informe sobre el grado en que la entidad auditada cumple con los criterios establecidos,[1] se presentan seguidamente los parámetros de cumplimiento definidos y validados con la Administración, para poder redactar la conclusión del presente informe.

Cuadro 1

Parámetros de cumplimiento del área de examen de la auditoría

Cumplimiento	Puntaje	Criterio
No	0%	Falta cualquier elemento básico. Estrategia incompleta para abordar el propósito. El proceso puede haberse definido o no.
Parcial	50%	Logra más o menos su propósito. Actividades completas básicas. No están estandarizadas.
Si	100%	Se logra el propósito. Las actividades están definidas. Se definieron estándares.

Fuente: Elaboración CGR.

METODOLOGÍA APLICADA

1.9. 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

[1] ISSAI 400:13.

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).

1.10. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas a funcionarios de la Dirección General de Migración y Extranjería, así como las respuestas a las consultas planteadas por escrito ante diferentes funcionarios de esa institución.

1.11. Asimismo, se realizaron pruebas sustantivas para validar la efectividad operativa de controles específicos tanto a nivel de aplicaciones como a nivel de gestión de TI; por otra parte, se aplicó una herramienta de evaluación de la seguridad de la información a los funcionarios de la Unidad de Tecnologías de Información, con el fin de indagar sobre aspectos vinculados con controles organizativos, personas, físicos y tecnológicos, y se solicitó adjuntar a una carpeta compartida la información de respaldo que se considerara pertinente.

1.12. Finalmente, se realizó un ejercicio con funcionarios de seguridad de la información, desarrollo y servidores y monitoreo, de la Unidad Tecnologías de Información, con el fin de conocer causas y opciones de solución sobre las temáticas encontradas en la auditoría, las cuales fueron consideradas para la elaboración del informe.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.13. La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de los activos de información en los diferentes procesos de la entidad, por medio de la gestión de los riesgos, implementación de programas, controles y políticas de seguridad de la información.

1.14. La DGME es el ente público ejecutor de la política migratoria que controla el ingreso y el egreso de personas al territorio nacional y busca a través de su modelo de gestión, brindar transparencia en sus labores. Para alcanzar esa transparencia, es vital que la DGME asegure la confidencialidad, disponibilidad y la integridad de la información contenida en sus sistemas de información, de manera que se garantice un adecuado cumplimiento de sus funciones.

1.15. Para ello, la DGME cuenta con un Departamento de Gestión de Tecnología de la Información, conformado por Seguridad Física y Lógica, Administración de Servidores y Monitoreo, Desarrollo de Sistemas, Redes y Comunicaciones, Bases de Datos y Soporte técnico.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.16. El 06 de diciembre de 2023, mediante oficio N.° 17433 (DFOE-GOB-0528) se remitió el borrador del informe de auditoría sobre la seguridad de la información en la Dirección

General de Migración y Extranjería, con el fin de que formulara las observaciones que estimara pertinentes sobre el contenido del informe.

1.17. En reunión efectuada el jueves 7 de diciembre de 2023, en las instalaciones de la Dirección General de Migración y Extranjería, se presentaron los resultados de esta auditoría a Jenny Gamboa Rodríguez Jefa de Gestión de Tecnologías de Información; Jean Paul San Lee Lizano, Subdirector General Administrativo; María Eugenia Víctor Sánchez, Jefa de Planificación Institucional; Karol Rivera González, Asistente Subdirección General; Pablo Bustamante Aguilar, Coordinador Unidad de Servidores; Oscar Jiménez Salazar, Coordinador Unidad de Seguridad Informática; Emiyer Jimenez Zuniga, Auditora interna; Sheila Madrigal Chaves, Encargada de Auditoría de parte de la DGME; Giocongda Chaves, Planificación Institucional; Marta Carvajal, Subdirección General.

1.18. Finalmente, la Dirección General de Migración y Extranjería no remitió observaciones al borrador del informe de auditoría.

SIGLAS Y ABREVIATURAS

1.19. A continuación, se indica el detalle de las siglas utilizadas en este informe:

Siglas / Abreviaturas	Significado
CGR	Contraloría General de la República
CVSS	Sistema Común de Calificación de Vulnerabilidad
CGI	Comité Gerencial de Informática
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DGME	Dirección General Migración y Extranjería
ISO	Organización Internacional para la Estandarización
LGCI	Ley General de Control Interno
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
NIST	Instituto Nacional de Estándares y Tecnología
OWASP	Proyecto Abierto de Seguridad de Aplicaciones Web

Fuente: Elaboración CGR.

2. RESULTADOS

2.1. Los resultados obtenidos en la auditoría de carácter especial sobre la seguridad de la información en la Dirección General de Migración y Extranjería, se detallan a continuación.

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

2.2. La seguridad de la información considera las acciones efectuadas por la Administración para proteger la información contra el acceso, uso, divulgación, alteración, modificación o destrucción no autorizada, con el fin de asegurar la preservación razonable de los activos tecnológicos y de información así como garantizar razonablemente la confidencialidad, integridad y disponibilidad. A continuación se detallan los resultados determinados.

Se necesita fortalecer la gestión de la seguridad de la información

2.3. De acuerdo con lo establecido en los artículos 7 y 10 de la Ley n.° 8292[2], el jerarca y los titulares subordinados de las instituciones tienen la obligatoriedad de disponer de un sistema de control interno, el cual deberá ser aplicable, completo, razonable, integrado y congruente con las competencias y atribuciones institucionales. Además, deberá proporcionar seguridad en el cumplimiento de esas atribuciones y competencias. Asimismo, el jerarca y del titular subordinado tienen la responsabilidad de establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, la administración activa tiene la responsabilidad de realizar las acciones necesarias para garantizar su efectivo funcionamiento.

2.4. Asimismo, las Normas técnicas para el gobierno y gestión de las tecnologías de la información en el apartado de Responsabilidades le establece al máximo jerarca institucional, la responsabilidad del establecimiento del Gobierno Corporativo que apoye y supervise la adecuada implementación de Marco Normativo y su gestión, por parte de la instancia competente en la materia.

2.5. A su vez, el apartado I Gobernanza de TI[3], determina que la institución debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones.

2.6. Dicho apartado también establece que la conceptualización de este órgano rector debe ser una instancia de alto nivel que busca habilitar la gobernanza en torno a las Tecnologías de la Información y Comunicaciones, estableciendo un espacio de diálogo y coordinación entre las gerencias de la institución y la unidad responsable de las Tecnologías de Información y Comunicaciones, con el fin de asegurar el apoyo de las TIC a la gestión y el cumplimiento de la estrategia institucional. Al establecer dicha integración

[2] Ley General de Control Interno
[3] Normas técnicas para el gobierno y gestión de las tecnologías de la información

de alto nivel, asume como cuerpo colegiado, la toma de decisiones sobre temas estratégicos asociados con las TIC.

2.7. Además, en el apartado XI Seguridad y Ciberseguridad[4], la Institución debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

2.8. Asimismo, el apartado anterior señala que se debe propiciar un ambiente seguro, considerando la seguridad física, lógica y ambiental así como establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones.

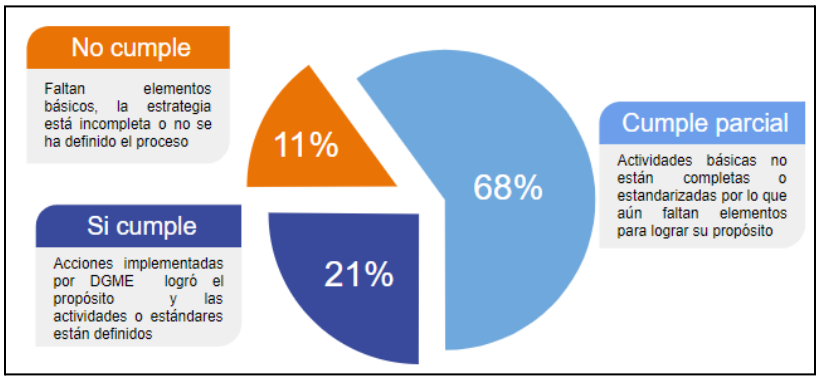
2.9. Adicionalmente, en el apartado XI señalado, establece que la Institución debe realizar una valoración de controles a implementar a través de una declaración de aplicabilidad, que permita contrarrestar los riesgos de seguridad de la información, incluyendo una valoración de madurez; además debe establecer e implementar los mecanismos que permitan contrastar los controles definidos contra los controles que se están aplicando.

2.10. También, el Anexo A de la ISO 27001[5] define los controles de seguridad de la información, como buenas prácticas para establecer los controles organizativos, de personas, físicos y tecnológicos en la materia.

2.11. Al respecto, se determinó un cumplimiento parcial de las acciones implementadas en la gestión de la seguridad de la información por lo cual la DGME requiere establecer acciones inmediatas para la protección y el resguardo de la información y los activos tecnológicos. A continuación se muestran los resultados generales obtenidos:

Cuadro 2

Resultados de cumplimiento en seguridad de la información



Fuente: Elaboración CGR.

[4] Normas técnicas para el gobierno y gestión de las tecnologías de la información

[5] Estándar Seguridad de la información, ciberseguridad y protección de la privacidad, versión 2023.

2.12. Asimismo, en el 21% de las acciones implementadas por la Administración para resguardar la información la DGME logró el propósito y las actividades o estándares están definidos, es decir, poseen políticas de asignación de usuarios, atención de incidentes y monitoreo de seguridad.

2.13. A su vez, en el 68% de las acciones evaluadas de seguridad de la información, las actividades básicas no están completas o no están estandarizadas por lo que aún faltan elementos para lograr su propósito; se han implementado parcialmente controles sobre clasificación y etiquetado de la información, revisión de derechos de acceso, gestión de activos y continuidad.

2.14. Por último, en el 11% de las acciones evaluadas no se acreditó cumplimiento, dado que faltan elementos básicos, la estrategia está incompleta o no se ha definido el proceso; dado que aún no se ha documentado la totalidad de requisitos obligatorios y la normativa establecida debe actualizarse a la realidad institucional y el marco adoptado.

2.15. Al respecto, la evaluación consideró la clasificación de la capacidad operativa, resultando que las capacidades en las cuales se requiere una intervención inmediata son: "Aseguramiento de la seguridad de la información" y así como la de "legal y cumplimiento", a continuación se muestra el porcentaje de cumplimento por capacidad operativa evaluado:

Cuadro 3

Resultados de las acciones implementadas por capacidad operativa en materia de seguridad de la información

Capacidad operativa	Porcentaje de cumplimiento
Gestión de la identidad y del acceso	75%
Seguridad de las relaciones con los proveedores	64%
Seguridad física	63%
Seguridad de los sistemas y de las redes	61%
Seguridad de las aplicaciones	60%
Gestión de activos	59%
Gestión de eventos de seguridad de la información	57%
Gobernanza	55%
Configuración segura	55%
Gestión de amenazas y vulnerabilidades	50%
Seguridad de los recursos humanos	50%
Protección de la información	50%
Continuidad	43%
Aseguramiento de la seguridad de la información	40%
Legal y cumplimiento	25%

Fuente: Elaboración CGR.

2.16. Las situaciones señaladas obedecen al débil funcionamiento del Comité Gerencial de Informática (CGI) en la toma de decisiones estratégicas acorde con el marco de tecnologías de información adoptado. Es importante señalar que el CGI fue constituido como una "instancia **técnica** entre la administración superior y la Gestión de Tecnologías de Información", con funciones en la línea de **asesorar** en temas y decisiones en materia de tecnologías de información cuyas competencias se establecieron para **conocer y recomendar** a la Dirección General en los citados temas.

2.17. Asimismo, la normativa institucional de seguridad de la información requiere actualizarse.

2.18. Los resultados expuestos aumentan el riesgo de pérdida de confidencialidad, integridad y disponibilidad, en caso de que se mantengan los controles actuales o se tarde en implementar las acciones de mejora.

2.19. Al respecto, la Administración indicó[6] que según el criterio expuesto por la Asesoría Jurídica se mantendrá la conformación del Comité Gerencial de Informática asimismo que se analizarán y convalidarán los acuerdos tomados por los miembros nombrados mediante circular DG-16-02-2023. Asimismo, que el Reglamento del CGI debe ser revisado y actualizado a la luz del Marco Normativo de TI emitido por el MICITT.

Oportunidades de mejora en la gestión de ciberseguridad

2.20. De acuerdo con lo establecido en los artículo 14 y 18 de la Ley n.° 8292[7], el jerarca y los titulares subordinados de las instituciones tienen la obligatoriedad de identificar y analizar los riesgos y establecer mecanismos operativos que los minimicen, así como el deber de contar con un sistema específico de valoración de riesgo que permita identificar y administrar el nivel de riesgo institucional.

2.21. Además, en el apartado XI Seguridad y Ciberseguridad[8], la Institución debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

2.22. Asimismo, el apartado anterior señala que se debe propiciar un ambiente seguro, considerando la seguridad física, lógica y ambiental así como establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones.

2.23. A su vez, el TopTen 2021[9] determina las principales causas que hacen que el software sea inseguro, dentro de las cuales se tienen las siguientes: A01 Pérdida de Control de Acceso. A02 Fallas Criptográficas. A03 Inyección. A04 Diseño Inseguro. A05

[6] Acta n.° 265 del Comité Gerencial de Informática del 11 de octubre de 2023
[7] Ley General de Control Interno
[8] Normas técnicas para el gobierno y gestión de las tecnologías de la información
[9] Open Web Application Security Project (OWASP)

Configuración de Seguridad Incorrecta. A06 Componentes Vulnerables y Desactualizados. A07 Fallas de Identificación y Autenticación. A08 Fallas en el Software y en la Integridad de los Datos. A09:2021-Fallas en el Registro y Monitoreo de la Seguridad. A10:2021-Falsificación de Solicitudes del Lado del Servidor (SSRF).

2.24. Adicionalmente, en el Marco abierto CVSS[10] se establecen las características y gravedad de las vulnerabilidades de software, con la siguiente calificación de gravedad: Informativas 0, Bajo 0.1-3.9, Medio 4.0-6.9, Alto 7.0-8.9 y Crítico 9.0-10.0

2.25. Dentro de este contexto, una vez realizado el análisis por parte del Órgano Contralor, se determinó que la DGME atendió el 49% en promedio de las vulnerabilidades comunicadas durante la ejecución de la auditoría. Al respecto, la DGME subsanó el 54% de las vulnerabilidades externas, atendiendo la totalidad de las críticas, el 47% de las altas y un 29% de las medias. En línea con lo anterior, para las vulnerabilidades internas lograron atender el 43% de las comunicadas, es decir un 49% de las críticas, el 41% de las altas y un 28% de las informativas.

2.26. Asimismo, la DGME posee una guía para la identificación y comunicación de vulnerabilidades sin embargo no establece responsables, periodicidad ni actividades para subsanar los hallazgos de ciberseguridad.

2.27. Las situaciones expuestas obedecen a la ausencia de normativa para gestionar la ciberseguridad que contemple el análisis periódico de los riesgos de ciberseguridad y los planes de remediación de vulnerabilidades.

2.28. Los resultados señalados podrían aumentar los riesgos de accesos no autorizados a los activos tecnológicos y de información de la DGME.

[10] Sistema común de calificación de vulnerabilidad (Common Vulnerability Scoring System) del NIST (National Institute of Standards and Technology /U.S Department of Commerce) versión 3.1 de CVSS.

3. CONCLUSIÓN

3.1. Las acciones implementadas por la Administración para resguardar la información cumplen parcialmente con el marco regulatorio y buenas prácticas aplicables, por lo que requiere acciones de mejora inmediatas para brindar una protección a los activos tecnológicos y de información de la DGME.

3.2. La DGME posee documentación relacionada con seguridad de la información sin embargo requiere analizarla a luz del marco normativo adoptado, el cual requiere una participación integral de todos los involucrados o partes interesadas.

3.3. El Departamento de Gestión de Tecnologías de información gestionó razonablemente las vulnerabilidades comunicadas durante la auditoría en un corto período de tiempo, dando prioridad a las más críticas y las que se lograron subsanar con los recursos o herramientas disponibles.

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 Nro. 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.

A MARTA VINDAS GONZÁLEZ DIRECTORA GENERAL DE LA DGME O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Integrar y ejecutar las labores correspondientes del cuerpo colegiado de alto nivel para la toma de decisiones sobre temas estratégicos asociados con las TIC conforme el Marco normativo de Tecnologías de Información adoptado por la Institución. Una vez integrado y en funcionamiento deberá actualizar la reglamentación donde se especifiquen sus funciones. Remitir a la Contraloría General una certificación que acredite la integración de dicho órgano rector, a más tardar el 15 de marzo de 2024. Así como una certificación al 15 de abril de 2024 que acredite la emisión de la reglamentación actualizada para su

funcionamiento. Finalmente, una certificación al 14 de junio de 2024 que acredite la celebración de sesiones y ejecución de labores. (ver párrafos del 2.3 al 2.19).

4.5. Actualizar, divulgar, implementar y mantener a disposición de todo el personal la normativa para gestionar la seguridad de la información institucional que considere al menos la clasificación, resguardo de la información institucional, revisión de accesos y verificación periódica del cumplimiento de la normativa. Remitir a más tardar el 31 de mayo de 2024, a la Contraloría General una certificación que acredite la actualización y divulgación de la normativa indicada. Además, remitir a la Contraloría General a más tardar el 30 de agosto de 2024, una certificación que acredite la existencia de medio en el que se encuentre a disposición del personal la normativa actualizada así como un primer reporte de avance en la implementación de la normativa. Finalmente, a más tardar al 13 de diciembre de 2024 remitir a la Contraloría General una certificación que acredite un segundo reporte de avance de la implementación de dicha normativa. (ver párrafos del 2.20 al 2.28).

4.6. Actualizar e implementar la normativa de ciberseguridad para que incluya el análisis periódico de los riesgos sobre ciberseguridad, la remediación de las vulnerabilidades y planes de mitigación cuando corresponda, considerando al menos actividades, responsables y periodicidad de ejecución. Al respecto, deberá remitirse a la Contraloría General una certificación en la cual se haga constar que se actualizó la normativa a más tardar el 23 de abril de 2024. Así como una certificación señalando el grado de avance respecto a la implementación de la normativa a más tardar el 19 de julio de 2024 y el 30 de setiembre de 2024. (ver párrafos del 2.20 al 2.28).

Falon Stephany Arias Calero
Gerente de Área

Mario Alberto Pérez Fonseca
Asistente Técnico

Viria Melissa Rodríguez Salas
Coordinadora

Jennifer Priscilla Villarreal Sequeira
Colaboradora

Kevin Rodríguez Muñoz
Colaborador

CGR | Firmado digitalmente
Valide las firmas digitales