INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVICIOS CRÍTICOS Y SU CONTINUIDAD ANTE POSIBLES AMENAZAS EN EL CONSEJO TÉCNICO DE AVIACIÓN CIVIL

28 de junio de 2023

Informe N.° DFOE-CIU-IAD-00001-2023

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

CONTENIDO

CUADROS

IMÁGENES

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos del Consejo Técnico de Aviación Civil (CETAC) responden al marco regulatorio y buenas prácticas aplicables de manera que promueva el logro de sus objetivos. El periodo evaluado comprende desde el 01 de enero de 2021 al 30 de abril de 2023, y se extendió cuando se consideró pertinente.

¿POR QUÉ ES IMPORTANTE?

La actividad aeroportuaria es fundamental para el país, debido a que el transporte aéreo permite generar beneficios socioeconómicos ligados al desarrollo nacional e implica crecimiento económico, generación de empleos, facilita el comercio internacional y el turismo, para ello la Dirección General de Aviación Civil (DGAC) debe planificar, regular y proveer los servicios de la aviación civil de Costa Rica.

En ese sentido, el soporte de los servicios aeroportuarios y el cumplimiento de las competencias institucionales de la DGAC, conlleva la coordinación de diferentes actores, así como el uso de sistemas de información, en los cuales se recopila, procesa, almacena y comunican los datos críticos, los cuales resulta fundamental que sean protegidos ante cualquier uso fraudulento, accesos no autorizados, pérdida, alteración o difusión.

¿QUÉ ENCONTRAMOS?

Se determinaron debilidades en la DGAC sobre el Sistema de Gestión de la Seguridad de la Información, ya que se carece de lineamientos sobre los roles y responsabilidades para los encargados de la Unidad de Tecnologías de Información (UTI) y de la seguridad de la información, así como de procedimientos y políticas para proteger la confidencialidad, autenticidad, privacidad e integridad de la información de los sistemas. Además, la Dirección no ha clasificado la información y los activos tecnológicos según los criterios de confidencialidad, integridad, disponibilidad, valor, criticidad y sensibilidad. Tampoco se cuenta con un plan de capacitación y actualización para el personal encargado en seguridad de la información y ciberseguridad, planes integrados para la sensibilización o concientización del personal y tampoco se disponen de acuerdos de confidencialidad o no divulgación de la información.

Por otra parte, se presentan debilidades en los mecanismos de control y coordinación con la Corporación Centroamericana de Servicios de Navegación Aérea, ente encargado de brindar los servicios de navegación aérea en el país, ya que la DGAC no lleva un seguimiento ni control sobre las funciones asignadas a la Corporación, en cuanto al resguardo de información o sistemas de información de los procesos críticos de Aviación Civil.

Asimismo, se determinó que la DGAC no ha desarrollado la política de continuidad de negocio, el análisis de impacto de negocio (BIA), el plan para la recuperación ante desastres (DRP), ni el plan de continuidad de negocio institucional, que le permita direccionar los esfuerzos aislados que han ejecutado los diferentes actores involucrados en esta materia; ello aunado a las debilidades identificadas en los planes de continuidad existentes en los principales aeropuertos del país.

En cuanto a controles específicos de la Seguridad de la información y ciberseguridad, se encontraron vulnerabilidades relacionadas con la disponibilidad, integridad y confidencialidad de la seguridad de la información en los servicios web de la DGAC, Aeropuerto Daniel Oduber y Aeropuerto Juan Santamaría, las cuales en el caso de la DGAC permanecen pendientes de ser atendidas.

Finalmente se determinó que la Dirección carece de controles para la depuración de la solución de administración de identidades y acceso utilizada en entornos de redes del sistema operativo, en sus sistemas y plataformas no se aplica la autenticación multifactor y existen debilidades a nivel de actualización de los equipos institucionales; en lo correspondiente a actualizaciones de sistema operativo, parches y antivirus. Además, se identificaron debilidades en la seguridad física de los equipos para el acceso a áreas restringidas de tecnologías de la DGAC.

¿QUÉ SIGUE?

Se dispone a las Autoridades de la DGAC, para que elabore e implemente un Sistema de Gestión de Seguridad de la información y un Sistema de Gestión de la Continuidad del Negocio a nivel institucional. Además, que se realice un análisis de riesgos integral sobre las debilidades en la estructura de las tecnologías de información y se implementen mecanismos de coordinación con COCESNA. También que se implemente un plan de remediación para atender las vulnerabilidades sobre seguridad de la información, así como implementar mecanismos de control para monitorear e identificar posibles riesgos y vulnerabilidades futuras en la infraestructura tecnológica. Finalmente que se definan e implementen controles para prevenir, detectar y corregir las debilidades de la seguridad de la información relacionadas con la gestión de los respaldos, seguridad física, las actualizaciones del software, gestión del antivirus; depuración y gestión en en el sistema de administración de usuarios.

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN PARA EL DESARROLLO DE LAS CIUDADES

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVICIOS CRÍTICOS Y SU CONTINUIDAD ANTE POSIBLES AMENAZAS EN EL CONSEJO TÉCNICO DE AVIACIÓN CIVIL (CETAC)

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. Durante el 2022 diversas instituciones públicas fueron blanco de grupos organizados conocidos como ciberdelincuentes internacionales, los cuales lograron vulnerar sus sistemas informáticos y afectar la continuidad de sus servicios.

1.2. Por lo anterior, durante ese año se declaró un estado de emergencia ante los ciberataques recibidos por varias instituciones públicas[1], por lo cual considerando que la actividad aeroportuaria es fundamental para el país, resulta relevante analizar los controles implementados por el CETAC, para prevenir, detectar y atender eventos que puedan afectar la seguridad de la información y la continuidad en la prestación de sus servicios.

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

OBJETIVO GENERAL

1.4. La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos del Consejo Técnico de Aviación Civil (CETAC) responden al marco regulatorio y buenas prácticas aplicables de manera que promueva el logro de sus objetivos.

ALCANCE

1.5. La auditoría comprendió el análisis de la gestión de tecnologías de información relacionada con la preparación que tiene el Consejo Técnico de Aviación Civil, ante posibles ciberataques y sobre los mecanismos de control que tiene para el resguardo de

[1] Decreto Ejecutivo N.° 43542-MP-MICIT, Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información, publicado en La Gaceta N.° 86 del 11 de mayo de 2022.

la información contenida en las bases de datos de los sistemas informáticos. El periodo evaluado comprende desde el 01 de enero de 2021 al 30 de abril de 2023, y se extendió cuando se consideró pertinente.

CRITERIOS DE AUDITORÍA

1.6. El 14 de marzo de 2023, se presentaron los criterios de auditoría a los funcionarios de la Dirección General de Aviación Civil (DGAC) Fernando Naranjo Elizondo, Director General; Allan Monge Hernández, jefe de la Unidad de Tecnologías de Información (UTI); Maribel Muñoz Arrieta, Subauditora Interna y Jonathan Escalante Jiménez, Auditor de Tecnologías de Información. Además, dichos criterios fueron comunicados mediante oficio n.° DFOE-CIU-0096 del 20 de marzo de 2023.

METODOLOGÍA APLICADA

1.7. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la Contraloría General y el Procedimiento de Auditoría vigente, establecido por la DFOE.

1.8. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas al personal de la Dirección General de Aviación Civil así como funcionarios encargados de los sistemas de información de COCESNA, además se realizaron visitas a los aeropuertos Juan Santamaría y Daniel Oduber, y se obtuvieron respuestas a las consultas planteadas por escrito ante diferentes instancias de esa institución.

1.9. Asimismo, se realizó una visita al centro de datos de la DGAC para verificar el cumplimiento de mejores prácticas en la seguridad física[2]. Además se realizaron pruebas tipo análisis de vulnerabilidades, no intrusivas a los dominios públicos de la DGAC[3] Aeropuerto Internacional Juan Santamaría[4] y Aeropuerto Internacional Daniel Oduber[5]; lo anterior sin generar afectación en los servicios brindados por la institución, cuyos resultados se reportaron a la administración mediante oficios con carácter de acceso restringido.

1.10. Finalmente, se realizó un taller[6] con personal de la UTI y otras instancias de la DGAC, para identificar las causas y soluciones de las situaciones que se comunican en este informe, lo que contribuyó a lograr una visión integral de las causas, los desafíos, retos y oportunidades de mejora.

---

2 Visita realizada el 21 de abril de 2023.

3 Información suministrada mediante correo electrónico el 15 de diciembre de 2022 por el señor Alexander Chaves Lopez, funcionario de la UTI.

4 Información suministrada mediante correo electrónico por la señora Violeta Blanco Echandi Encargada Órgano Fiscalizador de la Gestión Interesada (OFGI), el 2 de enero de 2023.

5 Información suministrada mediante correo electrónico por la señora Karla Cascante Ureña Gerente de proyecto -Contrato de Concesión Aeropuerto Internacional Daniel Oduber Quirós, el 31 de marzo de 2023.

6 Taller realizado el 17 de mayo de 2023 con personal de la DGAC.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.11. El Consejo Técnico de Aviación Civil (CETAC) y la Dirección General de Aviación Civil (DGAC), se crean mediante la Ley General de Aviación Civil, Ley N.° 5150, como entes encargados por el Poder Ejecutivo para la regulación de la aviación civil en el país.

1.12. Al CETAC, como organismo técnico, le corresponde, la supervisión de toda la actividad aeronáutica del país, gestionar lo referente a certificados de explotación para servicios de transporte aéreo, permisos o concesiones de instalaciones aeronáuticas y servicios auxiliares (aeródromos, aeropuertos, despacho aéreo, comunicaciones, radioayudas, entre otros), establecer, modificar y cancelar rutas aéreas, conocer y resolver sobre tarifas relativas al transporte de pasajeros y de carga, emitir normativa para el cumplimiento de obligaciones contraídas de tratados internacionales de aviación, entre otros.

1.13. Por su parte, a la DGAC le corresponde ejecutar las resoluciones emitidas por el CETAC, supervisar e inspeccionar las operaciones aeronáuticas, velar por la seguridad de la navegación aérea y del transporte aéreo y por el cumplimiento de obligaciones de ley, reglamentos, tratados y convenios internacionales sobre aviación civil, entre otros.

1.14. El control y la fiscalización de los aeropuertos nacionales e internacionales y consecuentemente de las entidades que operan y tienen actividades en tales instalaciones, están a cargo de la DGAC.

1.15. La gestión de los aeropuertos internacionales Daniel Oduber (IATA[7]:LIR) y Juan Santamaría (IATA:SJO), se lleva a cabo mediante las figuras de concesionario y gestión interesada respectivamente. El gestor interesado de SJO es Aeris Holding Costa Rica, S.A parte del grupo brasileño CCR y el concesionario de la terminal de LIR es CORIPORT.

1.16. Por otro lado, la gestión de los servicios de navegación aérea corresponde a la Corporación Centroamericana de Servicios de Navegación Aérea (COCESNA), la cual es un organismo internacional de integración centroamericana, de servicio público, sin fines de lucro, con estatus legal y autonomía financiera.

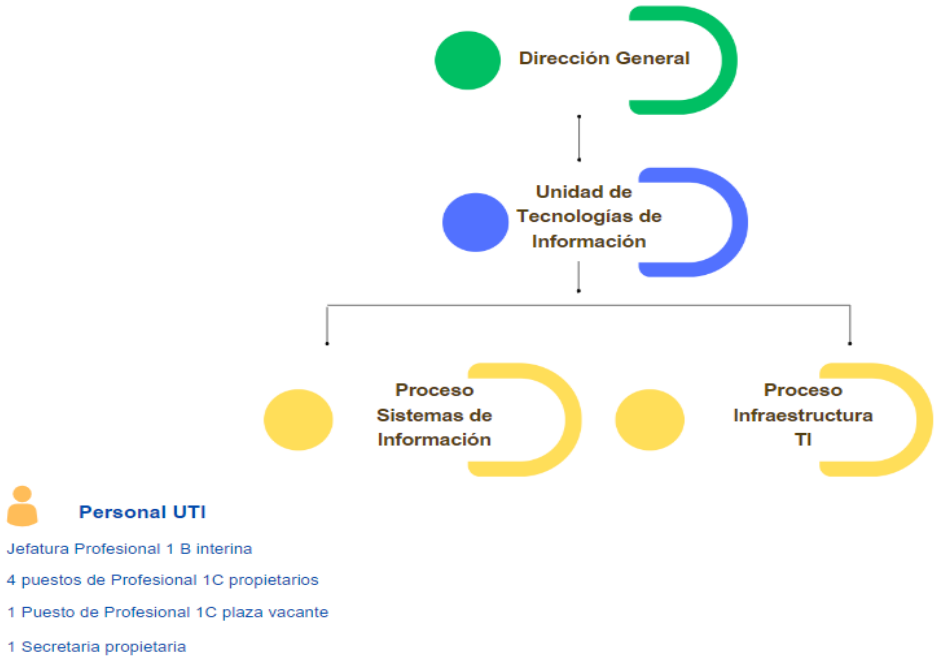
1.17. Dentro de la estructura del CETAC y la DGAC se cuenta con la Unidad de Tecnologías de Información (UTI), la cual según se observa en la imagen N.°1, tienen asignados los procesos de Sistemas de Información e Infraestructura de TI.

1.18. Cabe indicar que los servicios sobre los sistemas e infraestructura tecnológica, que facilitan el proceso de uso del espacio aéreo como sistemas de radar, sistema de planes de vuelo, o sistema de radiocomunicación, están a cargo de COCESNA. A la Unidad de Administración del Espacio Aéreo de la DGAC le corresponde supervisar, regular y controlar las infraestructuras, soporte de comunicaciones, navegación y vigilancia del Sistema de Navegación Aérea, dentro del territorio nacional.

---

[7] Asociación Internacional de Transporte Aéreo (Siglas en inglés: International Air Transport Association).

Imagen 1: Conformación de la Unidad de Tecnologías de Información (UTI)



Fuente: Elaboración propia con base en oficio N.° DGAC-UPI-OF-189-2022 del 22 de noviembre de 2022

MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA

1.19. Durante la ejecución de la auditoría, la DGAC informó que con respecto a las vulnerabilidades reportadas por la Contraloría General[8] sobre la revisión de componentes externos y configuraciones del Aeropuerto Juan Santamaría, esta entidad remitió los ajustes efectuados para subsanar las debilidades reportadas[9].

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.20. Mediante oficio N.° 07863 (DFOE-CIU-0245) del 16 de junio de 2023, se remitió el borrador del informe, con el propósito de que se formularan las observaciones que se estimaran pertinentes sobre el documento, a más tardar el 23 de junio de 2023. .

[8] Oficio N.° DFOE-CIU-0095 relacionado con el oficio con insumos N.° DFOE-CIU-OI-00002-2023 relacionados con riesgos sobre ciberseguridad institucional, del 21 de marzo de 2023.

[9] Oficios N^{os}. GO-TI-23-389 y GO-LE-23-461 del 09 de mayo y 01 de junio de 2023, respectivamente.

1.21. Asimismo, los resultados de la auditoría se comunicaron el 20 de junio de 2023, en sesión presencial en las instalaciones de Aviación Civil, con la participación de los funcionarios Fernando Naranjo, Director General de Aviación Civil; Allan Monge Hernández, Jefe Unidad de Tecnologías de información; Oscar Serrano Madrigal, Auditor Interno; Maribel Muñoz Arrieta, SubAuditora Interna; Jonathan Escalante Jiménez, Auditor Interno de TI; Alexander Sánchez Mora, Jefe a.i. Departamento de Aeropuertos; Silvia Solano Solís, Jefe de despacho de la Dirección General de Aviación Civil; Mauricio Garbanzo Calvo, Fiscalizador de Mantenimiento del Órgano Fiscalizador del Aeropuerto Juan Santamaría; Karla Cascante Ureña, Gerente de Proyecto del Contrato de Concesión Aeropuerto Daniel Oduber.Durante dicha sesión se efectuaron las observaciones al borrador, las cuales se consignaron en el Acta de comunicación y se consideraron en lo correspondiente.

1.22. De acuerdo a lo anterior, mediante oficio N.° DGAC-DG-OF-1273 del 20 de junio de 2023, el Licenciado Fernando Naranjo Elizondo, Director General de Aviación Civil informó al Órgano Contralor, no tener observaciones al contenido del referido borrador.

SIGLAS Y ABREVIATURAS

1.23. 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	Significado
BIA	Análisis de Impacto en el Negocio (Siglas en inglés:Business Impact Analysis)
CETAC	Consejo Técnico de Aviación Civil
CGR	Contraloría General de la República
COCESNA	Corporación Centroamericana de Servicios de Navegación Aérea
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DGAC	Dirección General de Aviación Civil
IATA	Asociación Internacional de Transporte Aéreo (Siglas en inglés: International Air Transport Association)
LGCI	Ley General de Control Interno
LIR	Aeropuerto Internacional de Liberia
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
OACI	Organización de Aviación Civil Internacional
OFGI	Órgano Fiscalizador de la Gestión Interesada del Aeropuerto Juan Santamaría
SJO	Aeropuerto Internacional Juan Santamaría
SGSI	Sistema de Gestión de la Seguridad de la Información
UTI	Unidad de Tecnologías de Información

2. RESULTADOS

ESTRATEGIA Y ESTRUCTURA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

2.1. La estrategia y estructura para la gestión de la seguridad de la información es de vital relevancia, ya que permite tener una base sólida para la implementación de los mecanismos de control pertinentes y oportunos, conforme a procesos críticos y sustantivos de la Dirección General de Aviación Civil (DGAC).

2.2. Por otra parte tanto la seguridad de la información como los mecanismos para atender la ciberseguridad, son aspectos transversales a toda la institución y no solamente por las áreas técnicas de tecnologías de información, además requieren del apoyo jerárquico institucional y asignación de recursos; todo ello, para poder ser gestionados y atendidos integralmente.

2.3. Al respecto, la DGAC actualmente cuenta con una contratación con una empresa, que le provee y administra los servicios de infraestructura tecnológica con base en buenas prácticas de la industria, que considera mecanismos de control sobre las principales plataformas tecnológicas que soportan los procesos de la institución.

2.4. No obstante, según se detalla en los siguientes párrafos, se identificaron debilidades relacionadas con aspectos relacionados con el sistema de gestión de la seguridad de la información, estructura de TI y mecanismos de coordinación con entes que le brindan servicios y soporte a procesos críticos.

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

2.5. Se determinó que la DGAC no cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI), lo cual se evidencia en las siguientes debilidades técnicas y de gestión:

- La Política de Seguridad de la Información N.° ID-001 y la Política de usos aceptable y prevención de software malicioso procedente para la gestión de seguridad de la Información N.° ID-008, no han sido formalmente aprobadas por la DGAC y por tanto tampoco se han comunicado al personal.
- Se carece de procedimientos y políticas para proteger la confidencialidad, autenticidad, privacidad e integridad de la información de los sistemas.
- La DGAC en el mes de marzo del año en curso, definió los procesos críticos y el inventario de sus sistemas de información, sin embargo no ha realizado una clasificación de sus activos tecnológicos según los criterios de confidencialidad, integridad y disponibilidad.

- La información institucional no se ha clasificado según su valor, criticidad y sensibilidad a la divulgación o modificación no autorizada, que asegure que dicha información recibe un nivel de protección apropiado, de acuerdo con su importancia para la Institución.
- Falta de un plan de capacitación y actualización para el personal encargado en seguridad de la información y ciberseguridad.
- No se cuenta con un plan integrado con acciones concretas tendientes a la sensibilización o concientización de los funcionarios en materia de seguridad de la información a nivel institucional.
- Ausencia de acuerdos de confidencialidad o no divulgación para la protección de la información institucional.
- Ausencia de lineamientos sobre los roles y responsabilidades para los encargados de la Unidad de Tecnologías de Información (UTI), así como de la seguridad de la información.
- Débil gestión en el seguimiento del servicio entregado por el proveedor de servicios administrados para mejorar la atención de la plataforma de red de datos, comunicaciones unificadas, seguridad del portal web, servicios informáticos, y gestión de dispositivos para la Dirección. Al respecto, se identificó que existen recomendaciones[10] dadas por la empresa contratista que aún no han sido atendidas por la DGAC.

2.6. De conformidad con el artículo 15 de la Ley General de Control Interno N.° 8292, la DGAC debe tener actividades de control que permitan documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.

2.7. Así también como sana práctica, la norma ISO 27001[11], indica que es responsabilidad de la alta dirección establecer una política de seguridad de la información que sea adecuada para el propósito de la organización; que incluya objetivos y un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la información, así como un compromiso de mejora continua del sistema de gestión de seguridad de la información; y que dicha política debe estar disponible y ser comunicada tanto a la organización como a las partes interesadas.

2.8. Además el objetivo A.7.2.2 de la citada norma ISO 27001, establece en cuanto a la concientización de la seguridad de la información, que todos los empleados de la institución, y cuando sea pertinente, los contratistas, deben recibir educación, formación y toma de conciencia y actualización periódica de las políticas y procedimientos de la organización cuando sea pertinente para su función laboral.

---

[10] Informes mensuales de febrero y marzo.

[11] Norma internacional del marco de trabajo de para los Sistemas de Gestión de la seguridad de la Información (SGSI)

2.9. Por su parte, el Proceso XI de las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información[12] estipulan que la institución debe tener y aplicar en forma consistente, una estructura formal a nivel institucional, que permita establecer las acciones para administrar la seguridad de la información y ciberseguridad, debidamente respaldada con la política de seguridad de la información y ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados. Además, se debe establecer un plan efectivo de capacitación y actualización tecnológica para los funcionarios, considerando la participación o involucramiento de los usuarios finales, responsables de los diferentes procesos y servicios institucionales.

2.10. Asimismo, en cuanto a la contratación y adquisición de bienes y servicios tecnológicos, el proceso VIII de las citadas normas técnicas, señala que es relevante que la UTI disponga y aplique en forma consistente prácticas para la supervisión y evaluación a través de pruebas de aceptación y valoración del cumplimiento contractual en cuanto al servicio y desempeño en la implementación, configuración y administración de los recursos tecnológicos contratados a terceros.

2.11. Las aspectos antes señalados obedecen a la falta de concientización y capacitación sobre seguridad de la información entre el personal, así como de un mayor apoyo por parte del nivel gerencial en la gestión de recursos necesarios para establecer las medidas que permitan contar con un SGSI institucional robusto.

2.12. Lo indicado, expone a la DGAC a diversos riesgos y amenazas como accesos no autorizados a información sensible, pérdida o alteración de datos, interrupción o afectación de servicios críticos, robo de información confidencial; así como omitir el cumplimiento de normativa relacionada con la protección de datos.

Debilidades en la estructura y estrategia de las tecnologías de información

2.13. Las tecnologías de información contribuyen de manera importante al cumplimiento de los objetivos de la institución, dando soporte y apoyo a los procesos institucionales, además de mejorar la productividad de estos, optimizando recursos y dando como resultado un flujo más eficiente. Al respecto, se evidenció que la DGAC cuenta con una estructura débil para atender oportuna y eficazmente las necesidades en temas de tecnologías y seguridad de la información.

2.14. En ese sentido, se determinó que no existe una gestión de valoración de riesgos sobre Tecnologías de Información, que considere los riesgos existentes en la estructura de la UTI, la suficiencia y competencia del personal, con el fin de priorizar la ejecución de sus funciones y poder atender a la DGAC, los aeropuertos y dar seguimiento a las contrataciones de los servicios dados por proveedores externos. A su vez, toma

[12] Emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, actualizadas en 2022.

relevancia que desde abril de 2022, no se cuenta con un nombramiento oficial de la jefatura que guíe el accionar de esta Unidad.

2.15. Cabe indicar que en el 2010 se creó un Comité Gerencial de Tecnología denominado CITI, conformado por representantes de los diferentes departamentos, con el fin de establecer prioridades y asignar recursos para proyectos de TI teniendo una perspectiva más amplia de los objetivos y necesidades de la institución; no obstante solo se cuenta con evidencia de que se reunieron una única vez en el 2020, por lo que no se cumplió el objetivo para el cual fue creado dicho Comité.

2.16. En cuanto al direccionamiento estratégico, se evidenció que durante los periodos 2021-2022 la UTI no contaba con un plan estratégico de Tecnologías de Información debidamente formalizado. Al respecto se evidenció que fue hasta febrero de 2023 que se aprobó el citado plan.

2.17. La DGAC tampoco ha implementado las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), que orienten los procesos requeridos para brindar de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos, de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo.

2.18. Al respecto, en el Proceso VI de las citadas Normas Técnicas, se indica que la Unidad de TI debe constituirse con funcionarios que dispongan de un perfil técnico de acuerdo con sus responsabilidades, así como habilidades de gestión y administrativas que permitan realizar actividades requeridas para asegurar la gobernanza de las TI.

2.19. Además en el Proceso IV de dichas normas, se señala que la institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el marco normativo que le resulte aplicable. A su vez, la Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución.

2.20. Las situaciones señaladas se deben a que no se efectúa un análisis de riesgos de forma integral que considere la estructura de tecnologías de información de la DGAC; así como al poco involucramiento y apoyo de la alta gerencia y ausencia de mecanismos por parte de los jerarcas para establecer prioridades y asignar recursos para la gestión de TI.

2.21. La existencia de una estructura débil en la UTI conlleva riesgos para mantener y administrar la infraestructura tecnológica de forma óptima; además de atender la exposición de vulnerabilidades y ataques de seguridad de forma eficiente y

eficaz.También, se pueden presentar dificultades para implementar nuevas tecnologías que atiendan las necesidades actuales requeridas por la DGAC, problemas en la atención de soporte y resolución de problemas e incidentes. Todo lo anterior puede afectar el cumplimiento de los objetivos institucionales y de la prestación de los servicios de forma continua.

Debilidades en los mecanismos de control y coordinación con COCESNA

2.22. La gestión de los servicios de navegación aérea en el país los brinda la Corporación Centroamericana de Servicios de Navegación Aérea (COCESNA), organismo internacional de integración centroamericana, de servicio público, conformado por los representantes de los Estados signatarios de su Convenio Constitutivo; incluido Costa Rica. La Corporación goza de los derechos exclusivos sobre la prestación de servicios de tránsito aéreo, de telecomunicaciones aeronáuticas y de radioayudas en los territorios de los Estados Miembros y sus operaciones se basan fundamentalmente en las Normas y Métodos recomendados por la Organización de Aviación Civil Internacional (OACI).

2.23. Al respecto, se determinó que la UTI no tiene injerencia, ni realiza coordinación alguna sobre las funciones que ejerce COCESNA respecto de los sistemas de información utilizados por la Corporación. Tampoco se evidenció que la DGAC cuente con controles que le permitan dar un seguimiento a la seguridad de los sistemas de información y procesos críticos asignados a COCESNA.

2.24. De conformidad con el artículo 10, incisos vi y xii de la Ley General de Aviación Civil N.° 5150, entre las atribuciones del CETAC está vigilar el cumplimiento de las obligaciones contraídas por el gobierno con motivo de tratados, convenciones o convenios internacionales sobre aviación civil. Además que como organismo técnico le corresponde toda la supervisión de la actividad aeronáutica del país.

2.25. Además, la Norma 4.1 de las Normas de Control Interno para el Sector Público señala como parte de las competencias del jerarca y los titulares subordinados, diseñar, adoptar y evaluar, las actividades de control pertinentes en todos los niveles de la institución, incluyendo las políticas, procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. En ese sentido, la gestión institucional y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas.

2.26. Así también, mediante Dictamen 014 del 16 de enero de 2014, la Procuraduría General de la República[13], indicó lo siguiente: *"Puesto que los aeropuertos nacionales e internacionales están a cargo de la Dirección General de Aviación Civil, esta debe poder ejercer control y fiscalización sobre quienes ejercen actividades en las instalaciones*

[13] Dictamen 014 del 16 de enero de 2014.

aeroportuarias, aun cuando no sean sus funcionarios. Para lo cual puede adoptar medidas para que las actividades que estas personas desarrollan se presten en consonancia con normas técnicas y se garantice la seguridad en los aeropuertos, lo que implica un poder de verificar el cumplimiento de las medidas adoptadas."

2.27. La Administración omite el establecimiento de controles sobre la seguridad de la información gestionada por COCESNA, justificado[14] en que no tiene ningún control sobre sus funciones, al corresponder a una persona jurídica de derecho internacional, con responsabilidades asignadas mediante un Convenio Internacional, sin considerar que al CETAC le corresponde toda la supervisión de la actividad aeronáutica del país.

2.28. La situaciones descritas, conllevan a que la DGAC no cuente con información precisa y oportuna para la toma de decisiones; pues se desconoce cómo están incidiendo las funciones asignadas a COCESNA mediante el convenio suscrito con dicho ente, en cuanto al manejo y seguridad de los sistemas de información de los procesos críticos de Aviación Civil, así como los mecanismos de alerta, contingencia y prevención definidos ante eventuales ciberataques.

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

2.29. El gobierno de la seguridad de la información comprende impulsores de valor específicos como la confidencialidad, integridad y disponibilidad de la información, la continuidad de los servicios y la protección de los activos de la información. La ausencia de una estrategia en esta temática, reduce la capacidad de una organización para mitigar el riesgo y aprovechar las oportunidades de las tecnologías de información en el mejoramiento del proceso de negocio.

2.30. En atención a lo anterior, la DGAC ha ejecutado acciones tales como la formalización de la Comisión de Continuidad de Negocio que se encarga del análisis y elaboración del plan de continuidad de los servicios en caso de presentarse una afectación en las plataformas digitales. Adicionalmente, la Dirección cuenta con una contratación que le provee y administra los servicios de infraestructura tecnológica con base en buenas prácticas de la industria, considerando la seguridad perimetral, la hiperconvergencia y la gestión de respaldos. No obstante, se identificaron debilidades relacionadas con la disponibilidad, integridad y confidencialidad de la seguridad de la información de los servicios críticos institucionales, las cuales se detallan seguidamente.

[14] Oficio N.° DGAC-DG-OF-0768-2023 del 20 de abril de 2023.

Debilidades relacionadas con la continuidad del negocio y su impacto en la disponibilidad de la información de los servicios críticos de la DGAC

2.31. Se determinó que la DGAC no ha desarrollado la política de continuidad de negocio, el análisis de impacto de negocio (BIA), el plan para la recuperación ante desastres (DRP), y el plan de continuidad de negocio institucional que le permita direccionar los esfuerzos aislados que han ejecutado los diferentes actores involucrados.

2.32. En esa línea, no existe una vinculación de la documentación que se genera para gestionar la continuidad del negocio y la recuperación ante desastres en los aeropuertos Juan Santamaría (SJO) y Daniel Oduber Quirós (LIR) con la gestión de la continuidad institucional de la DGAC.

2.33. Por su parte, el Aeropuerto Juan Santamaría (SJO) cuenta con una serie de procedimientos para gestionar la continuidad del negocio y la recuperación ante desastres, los cuales involucran alternativas manuales para mantener el servicio que se brinda a la ciudadanía, sin embargo, esta documentación se encuentra aislada y no ha sido integrada en documentos que permitan su formalización y utilización oportuna.

2.34. Además, el aeropuerto Daniel Oduber Quirós (LIR), cuenta con dos documentos formales orientados a gestionar la continuidad del negocio y la recuperación ante desastres, no obstante, su enfoque está relacionado con las amenazas tradicionales físicas como terrorismo, terremotos y otros que impactan la vida del ser humano, por lo tanto, carecen de la gestión de amenazas relacionadas con la seguridad de información o ciberseguridad.

2.35. Adicionalmente, la revisión de la documentación sobre continuidad de negocio de ambos aeropuertos permitió determinar que no se han ejecutado pruebas integrales de los planes de continuidad considerando amenazas o vulnerabilidades relacionadas con la seguridad de la información o la ciberseguridad.

2.36. Por su parte, si bien, la DGAC manifestó[15] que se encuentra en el proceso de contratar una asesoría para la elaboración de estos documentos, es relevante señalar que a la fecha no se han ejecutado las acciones suficientes para coordinar la continuidad del negocio de forma integral con los actores involucrados, tal como se muestra en la imagen 2 y velar por la protección de los activos, la viabilidad de la organización y la continuidad de los servicios críticos a su cargo.

[15] Oficio N.° DGAC-DG-OF-0768-2023 (8894) del 21 de abril de 2023 y Minuta DGAC-DFA-MIN-CN-2023-01 del 31 de enero de 2023.

Imagen N.° 2: Actores que intervienen en la continuidad de negocio de la DGAC

Fuente: Elaboración propia con información suministrada durante la auditoría

2.37. El artículo 4 de la Ley General de la Administración Pública N.° 6227 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, su eficiencia, su 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.

2.38. Asimismo, la Norma 5.7.4 de Control Interno para el Sector Público señala, que se deben instaurar los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.

2.39. Por su parte, como sana práctica, en la norma DSS04 Gestionar la Continuidad[16], 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.

2.40. Además, en las prácticas establecidas en la NIST 800-53[17] se detalla que las organizaciones deben identificar los activos críticos como parte del análisis de criticidad, planificación de la continuidad del negocio o análisis de impacto en el negocio, lo anterior les permite emplear controles adicionales (más allá de los controles rutinarios implementados) que coadyuven en asegurar que la misión organizacional y las funciones continúen durante las operaciones de contingencia, asimismo, la identificación de los activos críticos facilita la priorización de los recursos de la organización.

2.41. Las situaciones evidenciadas se deben a la falta de compromiso o conocimiento por parte de la alta gerencia para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del sistema de gestión de la continuidad del negocio que integre a toda la institución.

2.42. Las debilidades asociadas a la planificación de la continuidad del negocio, atentan contra la disponibilidad, integridad y confidencialidad de los sistemas críticos y los procesos de negocio vinculados a éstos; con el consecuente riesgo de afectación a la oportuna prestación de los servicios de la DGAC y su interacción con los diferentes actores. Lo anterior con el agravante que ello implica debido a su impacto en la actividad aeronáutica del país, la cual también está ligada al desarrollo de las regiones, crecimiento económico, generación de empleos y la facilitación del comercio internacional y el turismo.

Debilidades en la gestión de la ciberseguridad para garantizar la protección de los servicios críticos de la DGAC

2.43. Con respecto a la ciberseguridad y seguridad de la información, se identificó que la DGAC tiene oportunidades de mejora que pueden comprometer la integridad, disponibilidad y confidencialidad de la información de la institución. En ese sentido, la Contraloría General remitió los oficios N.° DFOE-CIU-0095 del 31 de marzo de 2023 y N.° DFOE-CIU-0206 del 19 de mayo de 2023, con carácter de acceso restringido, en los cuales se detallaron los aspectos técnicos y riesgos identificados, considerando su clasificación CVSS[18], CWE[19], CVE[20]; así como las recomendaciones tanto para la DGAC, Aeropuerto Daniel Oduber y Aeropuerto Juan Santamaría.

---

16 COBIT 5 de ISACA
17 CP-2 Plan de Contingencias, inciso 8 del Instituto Nacional de Estándares y Tecnología.
18 Marco abierto de la NIST (National Institute of Standards and Technology /U.S Department of Commerce)
19 Common Weakness Enumeration (CWE) es una lista desarrollada por la comunidad de tipos de debilidades de software y hardware.
20 Common Vulnerabilities and Exposures (CVE), lista de información registrada sobre vulnerabilidades de seguridad conocidas.

2.44. A partir de las vulnerabilidades reportadas, la Administración determinó algunos ajustes que pueden ser realizados por parte de la DGAC[21], sin embargo aún no se habían establecido fechas y responsables para su cumplimiento. Por su parte, sobre las vulnerabilidades del Aeropuerto Juan Santamaría (SJO) la administración remitió los ajustes efectuados[22], y en el caso del Aeropuerto Daniel Oduber (LIR) la detección de vulnerabilidades se reportó en el mes de mayo, y las acciones para su remediación fueron remitidas el 19 de junio de 2023[23].

2.45. Por otra parte, se revisó el sistema de administración de usuarios[24], que almacena información acerca de las cuentas de usuario, como nombres, contraseñas, números de teléfono y permite que otros usuarios autorizados de la misma red tengan acceso a dicha información. Al respecto, se identificó que de las 676 cuentas de usuario creadas, existen 52 cuentas de funcionarios que ya no laboran para la institución, 9 cuentas con inconsistencias en el nombre asociado y 167 cuentas de usuarios genéricos de los cuales no se tiene certeza de su pertinencia[25].

Imagen N.° 3: Resultados de la revisión de las cuentas en el sistema de administración de usuarios

Fuente: Elaboración propia con información de los resultados de las pruebas

[21] Oficio N.° DGAC-TI-OF-044-2023 remitido por la UTI-DGAC el 28 de marzo de 2023.
[22] Oficio N.° GO-TI-23-389 del 09 de mayo de 2023.
[23] Oficio N. ° DGAC-DG-OF-1251-2023 del 19 de junio de 2023.
[24] Base de datos y un conjunto de servicios que conecta a usuarios con los recursos de red, y que proporciona los métodos para almacenar datos de directorio y poner dichos datos a disposición de los usuarios y administradores de la red.
[25] Información suministrada mediante oficios N^{os} DGAC-TI-OF-047-2023 y DGAC-DFA-RH-OF-0630-2023, del 11 y 13 de abril de 2023 respectivamente.

2.46. Adicionalmente, se determinó que la DGAC no cuenta con el mecanismo de autenticación multifactor 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.

2.47. Por su parte, la DGAC cuenta con una adecuada gestión de respaldos como parte de la contratación del centro de datos principal, procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos, solución de telefonía sobre IP, servicio de seguridad y gestión de dispositivos.

2.48. No obstante lo anterior, el análisis del proceso integral de restauración y respaldo permitió determinar que a la fecha la UTI no ha implementado las recomendaciones que remite el proveedor en sus informes mensuales. Tampoco ha continuado con la ejecución de respaldos fuera de línea, ni realiza pruebas de los respaldos que permitan garantizar que esos respaldos funcionan correctamente y que se cuenta con el conocimiento necesario para restablecer los sistemas; y no utiliza los mecanismos de cifrado en la generación de respaldos para proteger la información y prevenir riesgos relacionados con seguridad de la información de la DGAC.

2.49. Además, se evidenció que el centro de datos alterno presenta debilidades en la seguridad física relacionadas con la falta de controles para el acceso a áreas restringidas como el cuarto de monitoreo y el cuarto de telecomunicaciones donde está la UPS, así como debilidades en la colocación y actualización de las cámaras del monitoreo, el uso y mantenimiento de los aires acondicionados, y la protección automática contra incendios[26]

2.50. Por otra parte, se identificaron debilidades relacionadas con la actualización manual de software en los equipos de las personas funcionarias, y que el servicio de actualizaciones masivas de la infraestructura de TI se encuentra inhabilitado en el dominio de la DGAC, por lo tanto, la UTI no cuenta con visualización de alertas sobre el estado actual de estos equipos.

2.51. Además, la UTI no ha realizado los esfuerzos de coordinación con el respectivo proveedor para completar la instalación del antivirus pendientes, situación que fue comunicada por el proveedor en los informes mensuales de febrero y marzo de 2023; cabe señalar que las rondas de instalación física finalizaron en diciembre de 2022.

2.52. Sobre las situaciones antes expuestas, el Código Nacional de Tecnologías Digitales del MICITT establece como una mejor práctica el deber de administrar la infraestructura desarrollando procedimientos para la actualización frecuente de firmware, controladores y parches del sistema operativo, aplicaciones y dispositivos, y que el desarrollo de la ciberseguridad en la infraestructura tecnológica debe de contar con un inventario de software oficial y actualizado periódicamente.

[26] PE-3 sobre control de acceso físico, apartado 3.11 sobre protección física y ambiental de la NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

2.53. Además, en el mismo cuerpo normativo se señala que el acceso a los activos físicos y lógicos e instalaciones asociadas debe estar limitado a los usuarios, procesos y dispositivos autorizados, y que los mecanismos de autenticación deben garantizar la veracidad de la identidad del usuario y seguir las mejores prácticas para prevenir el mal uso o el abuso por parte de usuarios o sistemas no autorizados. Asimismo, sugiere el uso de mecanismos de cifrado para proteger la información de acceso restringido, así como la validación, filtrado y codificación de la información recibida por las aplicaciones, para prevenir los riesgos relacionados con la posible captura de información de la institución.

2.54. En cuanto a la ejecución de pruebas de los respaldos, en las mejores prácticas[27] se establece que las copias de respaldo de la información del software y de las imágenes del sistema, deben ser probadas y analizadas periódicamente de acuerdo con una política acordada de respaldo.

2.55. Asimismo, en las mejores prácticas del Instituto Nacional de Estándares y Tecnología, contenidas en la NIST 800-53[28], se establece que las organizaciones necesitan asegurarse de que la información de respaldo se pueda recuperar de manera confiable. La confiabilidad se refiere a los sistemas y componentes del sistema donde se encuentra la información de respaldo, y las operaciones utilizadas para recuperar la información, así como la integridad de la información que está siendo recuperada.

2.56. Con respecto al cifrado de respaldos, se debe[29] considerar que el cifrado o enmascaramiento de los datos debe ejecutarse de conformidad con una política relacionada con el control de acceso a la información de la organización. Asimismo, en las mejores prácticas contenidas en la citada NIST 800-53, se establece que se deben implementar mecanismos criptográficos para evitar la divulgación no autorizada y modificación de la información de respaldo definida por la organización; la protección se aplica a la información de copia de seguridad del sistema, almacenada tanto en el servidor principal como en el alternativo.

2.57. En el mismo marco de mejores prácticas se recomienda el establecimiento de procedimientos para facilitar la implementación de la política de control de acceso y los controles asociados, considerando que el control del acceso físico brinda seguridad física adicional para las áreas donde hay una concentración de componentes del sistema que pueden impactar en la confidencialidad, integridad y disponibilidad de la información.

2.58. Las debilidades identificadas obedecen a la ausencia de mecanismos para monitorear e identificar posibles riesgos y vulnerabilidades que les permitan tomar decisiones oportunas sobre la aplicación de parches de seguridad, mejoras en la configuración, actualización de equipos y sistemas, entre otros. Ahora bien, las debilidades encontradas con respecto a la seguridad lógica, obedecen a que la DGAC no ha definido las medidas específicas para gestionar los riesgos.

---

[27] Inciso A.12.3.1 de la ISO 27001:2022.
[28] Security and Privacy Controls for Information Systems and Organizations.
[29] Inciso 8.11 de la ISO 27001:2022.

2.59. También se debe a que la DGAC no ha implementado una política de seguridad de la información ni procedimientos formales para proteger la confidencialidad, integridad y disponibilidad de la información contenida en sus sistemas y plataformas, considerando normas para la creación, modificación y eliminación de los usuarios en coordinación con la Unidad de Recursos Humanos, así como la gestión de los respaldos de la información y los métodos de autenticación. Además, existe una dependencia de los proveedores, ya que el personal de la UTI no ha logrado asimilar el conocimiento y dominio necesario del sistema de administración de usuarios y de las herramientas para la administración de los servicios contratados.

2.60. Las debilidades no corregidas pueden ser aprovechadas por la ciberdelincuencia y vulneran la institución al ser susceptible de accesos no autorizados, pérdida o modificación de información, degradación parcial o total de los servicios; adicionalmente, la ausencia de respaldos fuera de línea impacta en la capacidad de la DGAC para mantener o reanudar rápidamente las funciones críticas después de un posible evento disruptivo.

2.61. Además, si no se corrigen las debilidades evidenciadas la institución puede ser susceptible a fallos de seguridad o vulnerabilidades que pueden ser aprovechadas para intentar acceder a los sistemas y obtener o secuestrar información sensible o confidencial de la institución; lo cual se agrava si se consideran las debilidades identificadas en el área de respaldos y restauración.

3. CONCLUSIÓN

3.1. Con respecto al cumplimiento del objetivo de la auditoría, el cual consistió en determinar si la seguridad de información de los sistemas críticos del CETAC responden al marco regulatorio y buenas prácticas aplicables, se determinó que cumple con ello de forma parcial, ya que si bien ese Consejo ha realizado acciones, estas son escasas y no se han desarrollado de manera integral.

3.2. La ausencia de un Sistema de Gestión de la Seguridad de la Información, de una gestión para la identificación de riesgos y la falta de políticas institucionales en esta materia, evidencian que la DGAC cuenta con una débil estrategia y estructura para la gestión y seguridad de la información y ciberseguridad. Lo indicado evidencia la necesidad de promover el fortalecimiento de la UTI y la comprensión, a nivel institucional, sobre la seguridad de la información, incluyendo lo relativo a ciberseguridad, como una responsabilidad compartida por todas las personas funcionarias y no como una función exclusiva de la UTI.

3.3. Además las debilidades identificadas respecto de la seguridad de la información y ciberseguridad donde se evidencia la falta de un Sistema de Gestión de la Continuidad del Negocio, vulnerabilidades en la infraestructura, debilidades en la gestión de respaldos,

actualizaciones de software y gestión de antivirus, ponen en riesgo la confidencialidad, integridad y disponibilidad de la información, al ser susceptible de accesos no autorizados, pérdida o modificación de información, degradación parcial o total de los servicios.

3.4. De conformidad con lo anterior, es relevante que la Administración impulse acciones oportunas y pertinentes para la gobernanza de las tecnologías de información que promuevan la incorporación de prácticas de seguridad de la información y ciberseguridad como un componente transversal de los procesos y cultura institucional, de forma tal que se cuente con una mejor preparación ante intentos de ciberataques o cualquier otro evento que atente contra la seguridad y continuidad de sus servicios.

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, N.° 8292, 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 FERNANDO NARANJO ELIZONDO, DIRECTOR GENERAL DE AVIACIÓN CIVIL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Elaborar, oficializar, divulgar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) que incluya al menos los siguientes aspectos:

a) Política de seguridad de la información institucional aprobada y divulgada.
b) Clasificación de activos tecnológicos institucionales según confidencialidad, integridad y disponibilidad.
c) Clasificación de información de acuerdo a su valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

d) Plan de capacitación y actualización para el personal encargado en seguridad de la información y ciberseguridad.
e) Plan integrado de campañas de concientización sobre la seguridad de la información.
f) Establecimiento formal de los roles y responsabilidades para cada uno de los encargados del área de TI, así como de la seguridad de la información.
g) Procedimiento para el establecimiento de acuerdos de confidencialidad o no divulgación.
h) Procedimiento para el seguimiento oportuno de los servicios brindados por los diferentes proveedores de servicios de tecnologías de información, que incluya la definición de responsables, establecimiento de plazos y la atención de las recomendaciones dadas por cada proveedor.
i) Mecanismos para la prueba y mejora continua del SGSI.

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación en la que conste la elaboración oficialización y divulgación del SGSI a más tardar el 5 de julio de 2024.
ii) Informes bimensuales, a más tardar el 5 de febrero de 2024, 5 de abril de 2024 y 5 de junio 2024, donde se haga constar el avance respecto a la implementación del citado Sistema. (Ver párrafos del 2.5 al 2.12)

4.5. Realizar un análisis de riesgos integral y definir la estrategia para administrar los riesgos identificados en dicho análisis, que considere la estructura de tecnologías de información e incluya, entre otros, los siguientes aspectos identificados en el hallazgo:

a) Suficiencia y competencias del personal de TI.
b) Definición de roles y funciones definidas para cada uno de los miembros de TI.
c) Identificación de riesgos de seguridad de la información y ciberseguridad.
d) Implementación de las normas técnicas para la gestión y el control de las tecnologías de información del MICITT.
e) Desfase de planificación estratégica de TI.
f) Pertinencia de la activación del Comité Gerencial de Tecnología denominado CITI

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación donde se haga constar que se realizó el análisis de riesgos y la definición de la estrategia para administrar dichos riesgos, a más tardar el 18 de septiembre de 2023.
ii) Una certificación en la que se evidencien las acciones implementadas, de acuerdo a la estrategia definida, a más tardar el 20 de noviembre de 2023. (Ver párrafos del 2.13 al 2.21)

4.6. Definir, oficializar, divulgar e implementar un mecanismo de coordinación para el seguimiento y control de las funciones asignadas a COCESNA de conformidad con lo establecido en el Convenio de cooperación suscrito entre ambas partes, en lo que respecta al resguardo de la información crítica y los sistemas de información críticos que gestiona dicha entidad.

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación donde se haga constar que se definió, oficializó y divulgó el citado mecanismo, a más tardar el 31 de agosto de 2023.

ii) Una certificación donde se haga constar que se implementó el mecanismo, a más tardar el 31 de octubre de 2023. (Ver párrafos del 2.22 al 2.28)

4.7. Elaborar, aprobar y divulgar el Sistema de Gestión de la Continuidad del Negocio de la DGAC, que contemple al menos lo siguiente:

a) La política de continuidad de negocio.
b) El plan de continuidad de negocio (PCN).
c) El plan de recuperación de desastre (DRP).
d) El análisis de impacto de negocio (BIA).
e) Medidas de coordinación entre los actores involucrados en la continuidad de negocio de la DGAC, que considere la alineación entre los planes de continuidad de negocio de los aeropuertos con el Sistema de Gestión de Continuidad de la institución y la capacidad de preparación y respuesta efectiva en caso de ciberataque.
f) Las pruebas integrales

Para dar cumplimiento a esta disposición, deberá remitirse al al Órgano Contralor:

i) Informes semestrales en los que se haga constar el avance en la elaboración del Sistema de Gestión de la Continuidad del Negocio, en las siguientes fechas: 27 de noviembre de 2023, 29 de febrero de 2024 y 24 de mayo de 2024.
ii) Certificación en la que se haga constar que se elaboró, aprobó y divulgó el Sistema de Gestión de la Continuidad del Negocio solicitado a más tardar el 01 de julio de 2024.
iii)Certificación en la que se haga constar que se realizó las pruebas del Sistema de Gestión de la Continuidad del Negocio a más tardar el 01 de agosto de 2024 (Ver párrafos del 2.31 al 2.42).

4.8. Con respecto a la identificación de vulnerabilidades sobre seguridad de la información, se requiere lo siguiente:

a) Elaborar, aprobar e implementar un plan de remediación de las vulnerabilidades sobre seguridad de la información comunicadas mediante los oficio N.º DFOE-CIU-0095 del

31 de marzo, considerando al menos la priorización de las acciones requeridas para subsanar las debilidades identificadas y los planes de mitigación cuando corresponda, así como los plazos de ejecución, los responsables y los mecanismos para supervisar el avance en dicha remediación.

b) Elaborar, aprobar e implementar mecanismos de control para monitorear e identificar posibles riesgos y vulnerabilidades de la infraestructura de la DGAC, que permita tomar decisiones oportunas para reducir el impacto de estos riesgos en los procesos del negocio, considerando al menos las acciones, responsables, informes requeridos y su periodicidad.

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación en la cual se haga constar que se elaboró y aprobó el plan de remediación solicitado, a más tardar el 4 de agosto de 2023.

ii) Una certificación donde se haga constar que se elaboraron y aprobaron los mecanismos de control solicitados, a más tardar el 31 de agosto de 2023.

iii) Una certificación en la cual se haga constar la implementación del plan de remediación, a más tardar el 31 de octubre de 2023.

iv) Una certificación donde se haga constar el avance en la implementación de los mecanismos de control, a más tardar el 22 de diciembre de 2023.(Ver párrafos del 2.43 y 2.44)

A LA LICENCIADA SYLVIA JIMÉNEZ CASCANTE, COORDINADORA DEL DEPARTAMENTO DE AEROPUERTOS DE LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.9. En cuanto a continuidad del negocio de los aeropuertos, efectuar lo siguiente:

a) Elaborar, oficializar, divulgar, implementar y realizar las pruebas del Plan de Continuidad de Negocio y el Plan de recuperación de desastre del Aeropuerto Juan Santamaría.

b) Incorporar, oficializar, divulgar, implementar y realizar las pruebas, en los planes de continuidad del negocio y recuperación de desastre del Aeropuerto Daniel Oduber, lo relacionado a la gestión de amenazas de la seguridad de información o ciberseguridad, para una capacidad de preparación y respuesta efectiva en caso de ciberataques.

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Informes semestrales en los que se haga constar el avance en la elaboración del Plan de Continuidad de Negocio y del Plan de recuperación de desastre del Aeropuerto Juan Santamaría en las siguientes fechas: 29 de setiembre de 2023 y 22 de diciembre de 2023.
ii) Una certificación en la que se haga constar que se elaboró, oficializó y divulgó el Plan de Continuidad de Negocio y el Plan de recuperación de desastre del Aeropuerto Juan Santamaría, a más tardar el 16 de febrero de 2024.
iii) Una certificación en la que se haga constar que se incorporó, oficializó y divulgó los respectivos planes sobre la gestión de amenazas de la seguridad de información o ciberseguridad del Aeropuerto Daniel Oduber, a más tardar el 13 de octubre de 2023.
iv) Certificación en la que se haga constar que se realizaron las pruebas del plan de continuidad y plan de recuperación de desastres, a más tardar el 26 de enero de 2024 para el Aeropuerto Daniel Oduber, y a más tardar el 15 de marzo de 2024 para el Aeropuerto Juan Santamaría.(Ver párrafos del 2.31 al 2.42)

AL LICENCIADO ALLAN MONGE HERNÁNDEZ, JEFE DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.10. Elaborar e implementar un cronograma en coordinación con el proveedor de la contratación de servicios administrados para mejorar la atención de los servicios informáticos, plataforma de red de datos, comunicaciones unificadas, seguridad del portal web y gestión de dispositivos para la DGAC, con el fin de atender las recomendaciones brindadas en los informes mensuales vigentes que emite el proveedor. El cronograma debe incluir al menos los siguientes aspectos:

a) Definición de responsables
b) Establecimiento de plazos
c) Detalle de las acciones a llevar a cabo
d) Valoración de riesgos asociados a la no ejecución de las recomendaciones dadas por el proveedor en los informes mensuales.

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación donde se haga constar que se elaboró el cronograma solicitado, a más tardar el 3 de agosto de 2023.

ii) Una certificación donde se haga constar que se implementó el cronograma, a más tardar el 14 de setiembre 2023. (Ver párrafos del 2.45 al 2.61)

4.11. Definir e implementar controles para prevenir, detectar y corregir las debilidades de la seguridad de la información detalladas en este informe, considerando al menos:

a) Asignación de roles y perfiles del sistema de administración de usuarios de conformidad con la segregación de funciones y el principio del mínimo privilegio
b) Depuración de usuarios genéricos, en el sistema de administración de usuarios, con base en su pertinencia y utilidad.
c) Gestión de los respaldos.
d) Debilidades en la seguridad física.
e) Actualizaciones del software
f) Gestión del antivirus

Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Una certificación donde se haga constar que se definieron los controles solicitados a más tardar el 29 de septiembre de 2023.
ii) Una certificación donde se haga constar que se corrigió la asignación de roles y perfiles y se depuró los usuarios genéricos del sistema de administración de usuarios, a más tardar el 29 de septiembre de 2023.
iii) Una certificación donde se haga constar el avance en la implementación de los controles solicitados a más tardar el 22 de diciembre de 2023. (Ver párrafos del 2.45 al 2.61)

A LA LICENCIADA SANDRA LÓPEZ MADRIGAL, JEFE DE UNIDAD GESTIÓN INSTITUCIONAL DE RECURSOS HUMANOS O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.12. Definir e implementar los mecanismos de control para que se comunique a la UTI de manera oportuna los ingresos, salidas, permisos y muerte de los funcionarios de la DGAC, con el fin de actualizar el sistema de administración de usuarios que administra la UTI.

Para dar cumplimiento a esta disposición,deberá remitirse al Órgano Contralor:

i) Una certificación donde se haga constar que definieron los mecanismos de control, a más tardar el 3 de agosto de 2023.
ii) Una certificación donde se haga constar que se implementaron los mecanismos de control, a más tardar el 4 de setiembre de 2023. (ver párrafo 2.45).

Firmamos a los 28 días del mes de junio del 2023, San José, Costa Rica.

Marcela Aragón Sandoval **Gerente de Área**	Angie Mora Chacón **Asistente Técnico**
Grettel K. Camacho Aguilar **Coordinadora**	Wilmer I. Ramírez Alpízar **Colaborador**

CGR | Firmado digitalmente
Valide las firmas digitales

MRR/vas

G: 2022003213-1