MINISTERIO DE OBRAS PÚBLICAS Y TRANSPORTES
CONSEJO TÉCNICO DE AVIACIÓN CIVIL
AUDITORÍA INTERNA

INFORME № AI-07-2023

DIAGNÓSTICO SOBRE EL ALCANCE Y EFECTIVIDAD EN LA ENTREGA DE SERVICIOS ESPECIALIZADOS DEL CENTRO DE DATOS DE LA DGAC BRINDADO POR PARTE DE MARTINEXA Y OTROS TÓPICOS RELACIONADOS

NOVIEMBRE, 2023

ÍNDICE

ABREVIATURAS

Abreviatura	Significado
CGR	Contraloría General de la República
TI	Tecnologías de Información
LGCI	Ley General de Control Interno
SICOP	Sistema Integral de Compras Públicas
MICITT	Ministerio de Ciencias, Innovación, Tecnológica y Telecomunicaciones
MOPT	Ministerio de Obras Públicas y Transporte
PETIC	Plan Estratégico de Tecnologías de Información y Comunicación
SLAs	Acuerdos de Nivel de Servicio (siglas en inglés)

RESUMEN EJECUTIVO

¿Cuál fue el objetivo del estudio?

Realizar un diagnóstico sobre el alcance y efectividad en la entrega de servicios especializados del Centro de Datos de la DGAC brindado por parte de Martinexa.

¿Por qué se justificó el estudio?

Estudio especial de auditoría, con fundamento en las competencias conferidas a las auditorías internas en el artículo 22 de la Ley General de Control Interno y en cumplimiento del Plan Anual de Trabajo del año 2023 de esta Auditoría Interna.

¿Cuáles fueron los principales hallazgos?

Los principales hallazgos identificados comprenden:

a. Riesgo de integridad de la información migrada de la DGAC
b. Protocolo de destrucción de datos luego de la migración
c. Procedimiento de migración al rescindir contratos de
d. Plan de recuperación de desastres
e. Acuerdos de confidencialidad
f. Controles de seguridad de activos de tipo portátiles
g. Instalación de licencias de antivirus
h. Sistema de registro de bitácoras de actividades en la plataforma
i. Sistema de seguridad de control de acceso a la red
j. Falta de documentación formal para comprobación de hallazgos
k. Visión de la estrategia tecnológica de la DGAC

¿Qué esperamos de la Administración?

La aceptación e implementación de las recomendaciones tienen como propósito robustecer las prácticas que se llevan a cabo en temas de gestión y control en la ejecución de los servicios especializados para el Centro de Datos de la DGAC.

También se espera que la Administración tome medidas proactivas y eficientes para transformar la Unidad de TI en un centro de apoyo estratégico y soporte para la Institución.

I. INTRODUCCIÓN

1.1.- NATURALEZA DEL ESTUDIO

Con base en los resultados del estudio vinculante con el informe AI-01-2023 "DIAGNÓSTICO SOBRE LA SITUACIÓN ACTUAL DE LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL (DGAC) RESPECTO A LA CONTRATACIÓN DE SERVICIOS ESPECIALIZADOS PARA LA GESTIÓN, CONTROL Y OPERACIÓN DEL CENTRO DE DATOS DE LA INSTITUCIÓN", la Auditoría Interna requiere reforzar los criterios técnicos y análisis realizados con un estudio complementario sobre el alcance y efectividad en la entrega de servicios especializados vinculantes con el estudio.

Lo anterior con el fin de continuar brindando los servicios de asesorías o advertencias a la administración, por acciones que puedan poner en riesgo la continuidad del servicio de la institución y la utilización eficiente, efectiva y económica de los recursos; todo en apego a lo establecido en el marco jurídico y administrativo que nos rige.

1.2.-JUSTIFICACIÓN

Estudio especial de auditoría, con fundamento en las competencias conferidas a las auditorías internas en el artículo 22 de la Ley General de Control Interno y en cumplimiento del Plan Anual de Trabajo del año 2020 de esta Auditoría Interna.

1.3.-OBJETIVOS

1.3.1.- Objetivo general

Realizar un diagnóstico sobre el alcance y efectividad en la entrega de servicios especializados del Centro de Datos de la DGAC brindado por parte de la empresa Martinexa.

1.3.2.- Objetivos específicos

1. Realizar un diagnóstico sobre el alcance funcional de la plataforma tecnológica del Centro de Datos principal y alterno de la DGAC.
2. Realizar un diagnóstico sobre el alcance y efectividad de los servicios de seguridad de la información en la operación del Centro de Datos de la DGAC.

3. Realizar un análisis del proceso de gestión y control de la entrega de los servicios especializados de Martinexa por parte de la Función de TI de la DGAC.
4. Identificar la visión institucional en relación con la estrategia y la entrega de servicios tecnológicos.

1.4.- ALCANCE

El estudio de auditoría se enfocará en verificar el alcance y efectividad en la puesta en ejecución de los aspectos técnicos pactados por la administración activa en la contratación de servicios administrados para centro de datos principal, procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos y otros aspectos vinculantes para la DGAC, así como el cumplimiento de las métricas de desempeño, continuidad y aseguramiento del servicio, para determinar eventuales desviaciones, incumplimientos, brechas y oportunidades de mejora.

El estudio rige desde enero del 2022, con fecha de corte hasta el 31 de agosto del 2023. Se consultó documentación generada durante el año el curso hasta la fecha de corte para la ejecución de los procedimientos del estudio, facilitada por la Unidad de Tecnologías de Información, la Gerencia General y la Auditoría Interna del CETAC.

1.5.- METODOLOGÍA

En la realización de esta auditoría se aplicarán técnicas verbales, documentales, entrevistas; así como prácticas usuales para este tipo de estudios, dentro de ellas, el síntoma y la síntesis, con el fin de obtener el respaldo adecuado de los hallazgos encontrados.

1.6.- TIPO DE AUDITORÍA

Auditoría especial.

1.7.- NORMATIVA ADMINISTRATIVA, LEGAL Y TÉCNICA

a. Ley General de Control Interno, Ley № 8292 del 31 de julio de 20021.
b. Ley General de la Administración Pública; Ley № 6727 de 02 de mayo de 1978 y sus reformas
c. Ley de Administración Financiera de la República y Presupuestos Públicos, № 8131 del 18 de setiembre del 2001 y sus reformas.

d. Las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, (Resolución R-DC-119-2009 del 16 de diciembre del 2009), publicado en “La Gaceta” №28 del 10 de febrero de 2010.
e. Las “Normas Generales de Auditoria para el Sector Público”, R-DC-64-2014, publicadas en “La Gaceta” N° 184 del 25/09/2014 que rigen a partir del 01 de enero de 2015.
f. Procedimientos del Sistema de Gestión de la Auditoría Interna y la DGAC.
g. Otra normativa interna o externa que resulte aplicable.

Asimismo, en la tramitación del presente estudio se deberá observar lo estipulado en la Ley General de Control Interno, № 8292, específicamente en los siguientes artículos:

> “Artículo 37.-**Informes dirigidos al jerarca.** Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.
>
> Artículo 38.-**Planteamiento de conflictos ante la Contraloría General de la República.** Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.
>
> La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de

treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

Artículo 39.-**Causales de responsabilidad administrativa.** El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios.

El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable.

Asimismo, cabrá responsabilidad administrativa contra el jerarca que injustificadamente no asigne los recursos a la auditoría interna en los términos del artículo 27 de esta Ley.

Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente.

El jerarca, los titulares subordinados y los demás funcionarios públicos también incurrirán en responsabilidad administrativa y civil, cuando corresponda, por obstaculizar o retrasar el cumplimiento de las potestades del auditor, el subauditor y los demás funcionarios de la auditoría interna, establecidas en esta Ley.

> Cuando se trate de actos u omisiones de órganos colegiados, la responsabilidad será atribuida a todos sus integrantes, salvo que conste, de manera expresa, el voto negativo."

1.8.- CUMPLIMIENTO CON NORMAS GENERALES DE AUDITORÍA

El estudio se ejecutó de conformidad con las "Normas Generales de Auditoría para el Sector Público" (R-DC-64-2014) y las "Normas para el Ejercicio de la Auditoría Interna en sector Público".

1.9.- LIMITACIONES

a. La Función de Tecnologías de Información de la DGAC no cuenta con un expediente que centralice la documentación del proyecto desde su conceptualización y planificación institucional, por lo que puede faltar información durante el desarrollo de este estudio por debilidades en el sistema de control de la función y la gestión documental.
b. El Director General de la DGAC ha priorizado labores internas para la identificación y robustecimiento de los procesos, lineamientos y cultura organizacional en la Institución, incluyendo al área de Tecnologías de Información; sin embargo, a la fecha de corte de este estudio, no se ha realizado un análisis sobre el alcance, capacidades y expectativas estratégicas con la ejecución del Centro de Datos y los requerimientos y oportunidades de la DGAC.

1.10.- GENERALIDADES DEL ESTUDIO

Desde el 2019, por medio del informe № AI-14-2019, la Auditoría Interna del CETAC emitió la alerta relacionada con la finalización de la contratación de servicios especializados del Consorcio CODISA, CMA, BCNetwork y Fusionet, que presentaba un riesgo alto, ya que existía el riesgo "de no contar con un centro de datos suficiente y en un tiempo prudente para finalizar el contrato con el Consorcio", y se emitió como recomendación a la persona encargada de la Unidad de Tecnologías de Información: "Establecer, con la máxima prioridad, la estrategia para la eventual finalización de los servicios contratados, y los lineamientos para la negociar con un nuevo centro de datos, si aplica y es de interés de la Institución, ya sea por un centro de datos propio o tercerizado".

En diciembre del 2022, la Unidad de Tecnologías de Información había comentado en reunión de trabajo que el trabajo de implementación de la infraestructura tecnológica de la DGAC, tanto el centro de datos principal

(implementado en ADN Data Center) como su sitio alterno (implementado en las oficinas centrales de la DGAC), estaba finalizado, incluyendo la habilitación de servicios digitales y acceso a sistemas. A la fecha de corte de este estudio, la entrega del servicio especializado en producción se ha ejecutado exitosamente por 06 meses.

El alcance de la contratación del servicio administrado incluye la implementación y soporte de los activos tecnológicos sustantivos de la DGAC, infocomunicaciones y servicios públicos vinculantes, administración y control de ambientes productivos y de pruebas en centro de datos, seguridad y continuidad, soporte técnico y mantenimiento de la plataforma. Según la Función de TI, el servicio adquirido cuenta con mayor valor agregado a la Institución tanto en alcance de la contratación como en los servicios administrados vinculantes, reduciendo, además su riesgo en materia de fiscalización de contrato y SLAs y gestión de la infraestructura tecnológica.

1.11.- COMUNICACIÓN DE RESULTADOS

En atención a lo señalado en la Norma № 205 (Comunicación de resultados) de las Normas Generales de Auditoría para el Sector Público, el 01 de noviembre del año en curso se remitió nota, AI-291-2023, con el fin convocar a la conferencia final con el propósito de atender, escuchar y valorar opiniones, discrepancias y aportes que puedan surgir de los resultados finales que obtuvimos durante el estudio. Este ejercicio se llevó a cabo el 09 de noviembre del 2023 por medio de la plataforma Microsoft Teams, con la presencia, por parte de la Administración de:

- Sr. Fernando José Naranjo Elizondo, Director General de Aviación Civil
- Sr. Luis Eduardo Miranda Muñoz, Subdirector General de Aviación Civil
- Sr Jorge Gustavo Oses Rodríguez, Funcionario representante de la Unidad de Tecnologías de Información

Por parte de la Auditoría Interna participaron:

- Sr. Oscar Serrano Madrigal, Auditor General
- Sra. Maribel Muñoz Arrieta, Sub Auditora
- Sr. Jonathan Escalante Jiménez, Auditor de TI
- Sr. Damián Calvo de León, Auditor TI (externo)
- Sr. Francisco Hernández Chavarría, Auditor TI (externo)

Durante ese ejercicio no se presentaron observaciones que hicieran necesario introducir cambios en el informe.

II. COMENTARIOS

Considerando los resultados de la evaluación de control interno realizada por la Auditoría Interna a percepción de los auditados y con criterios establecidos por la misma Auditoría; encontramos que el sistema de control interno que prevalece es: malo.

A partir de estos resultados se realizaron las pruebas correspondientes, complementario a los hallazgos ya documentados en el informe AI-01-2023, resultando lo que se detalla a continuación:

2.1.- HALLAZGO 1 RIESGO DE INTEGRIDAD DE LA INFORMACIÓN MIGRADA DE LA DGAC

Durante la auditoría de sistemas de tecnología de la información, se identificó un riesgo significativo relacionado con la integridad de la información migrada del Centro de Datos de CODISA al Centro de Datos de ADN (gestionado por Martinexa). Este riesgo se originó debido al transporte de los datos en un dispositivo NAS en un vehículo sin las debidas precauciones de seguridad.

Se identifican debilidades en el sistema de control interno Institucional a causa de la falta de un protocolo de transporte seguro y la ausencia de medidas adecuadas para proteger los datos migrados durante el trayecto.

Esta situación puede haber materializado la pérdida o corrupción de datos críticos durante la migración, lo que podría resultar en la falta de disponibilidad o integridad de la información necesaria para las operaciones de la DGAC.

El criterio para evaluar esta condición es la adecuada protección de la integridad de la información durante el proceso de migración de datos. Esto incluye asegurarse de que los datos no se vean comprometidos ni sufran pérdidas o daños durante el transporte.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI “Seguridad y Ciberseguridad”, se indica:

> “La Unidad de TI debe 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 en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información."

2.2.- HALLAZGO 2 PROTOCOLO DE DESTRUCCIÓN DE DATOS LUEGO DE LA MIGRACIÓN

Se ha identificado una deficiencia en el proceso de migración de datos relacionada con la validación de la destrucción de datos en el Centro de Datos de CODISA después de la migración. El personal de TI de la DGAC no ha realizado una verificación adecuada para asegurar que los datos se hayan destruido de manera segura y permanente.

Esta condición evidencia debilidades en el sistema de control interno de TI a causa de la falta de un proceso de validación sólido y documentado para la destrucción de datos en el Centro de Datos de origen después de la migración.

Esta situación puede haber materializado la persistencia de datos sensibles o confidenciales en el Centro de Datos de origen, lo que podría exponer a la organización a riesgos de seguridad de la información, incluyendo el acceso no autorizado o la divulgación de datos críticos.

El criterio para evaluar esta condición es la verificación de que todos los datos críticos y sensibles se han eliminado de manera segura y permanente del Centro de Datos de CODISA después de la migración.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI "Seguridad y Ciberseguridad", se indica:

> "La Unidad de TI debe incorporar prácticas de valoración para el aseguramiento sobre la entrega de servicios y el uso óptimo de los recursos tecnológicos instalados para apoyar a la institución en la continuidad de sus operaciones, salvaguarda y protección de la información y activos asociados y la

implementación de iniciativas para el logro de los objetivos institucionales."

2.3.- HALLAZGO 3 PROCEDIMIENTO DE MIGRACIÓN AL RESCINDIR CONTRATOS DE TI

Se ha identificado una deficiencia en el cartel de contratación, ya que no detalla el proceso de migración de datos que debe seguirse en caso de rescisión del contrato de servicios. La falta de información específica sobre el proceso de migración podría representar un riesgo importante para la DGAC.

Esta condición se materializa a causa de una falta de una política o normativa que exija que el cartel de contratación incluya detalles sobre el proceso de migración de datos al rescindir el servicio.

El efecto potencial de esta situación es la falta de claridad y procedimientos establecidos para la migración de datos en caso de terminación del contrato de servicios. Esto podría resultar en la pérdida de datos críticos o en una migración inadecuada que afecte la continuidad de la Institución.

El criterio para evaluar esta condición es la inclusión de información detallada y clara en el cartel de contratación que describa el procedimiento a seguir para la migración de datos en caso de rescisión del contrato de servicios

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI "Seguridad y Ciberseguridad", se indica:

"Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución."

2.4.- HALLAZGO 4 PLAN DE RECUPERACIÓN DE DESASTRES

Durante la auditoría de sistemas de tecnología de la información, se ha identificado una deficiencia en la ejecución del plan de implementación. No se ha

encontrado evidencia de que se hayan ejecutado las pruebas y actividades planificadas del plan de implementación, lo que representa un riesgo alto para la continuidad de los servicios en caso de fallos.

Esta condición evidencia una deficiencia en el control interno para la adquisición de los servicios contratados, la cual puede darse por la falta de seguimiento adecuado al plan de implementación, posiblemente debido a la falta de tiempo o priorización incorrecta de tareas.

El efecto potencial de esta situación es la falta de conocimiento sobre la funcionalidad y la capacidad de recuperación de los servicios en caso de fallos o interrupciones. Esto podría resultar en una respuesta deficiente a incidentes y una prolongación en la restauración de los servicios.

El criterio para evaluar esta condición es la ejecución adecuada y completa del plan de implementación, incluyendo las pruebas y actividades planificadas para garantizar la operación y disponibilidad de los servicios.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado X “Desarrollo, Implementación y Mantenimiento de Sistema de Información”, se indica

> “La Unidad de TI debe aplicar las prácticas de aseguramiento del cumplimiento contractual y las prácticas de calidad asociadas para los casos en utilice soluciones desarrolladas y/o implementadas por proveedores externos.”

2.5.- HALLAZGO 5 ACUERDOS DE CONFIDENCIALIDAD

Se ha identificado una deficiencia en los procesos de contratación, ya que no se ha encontrado evidencia de que la DGAC exija al proveedor de servicios del Centro de Datos los diferentes acuerdos de confidencialidad necesarios. La falta de estos acuerdos podría representar un riesgo significativo para la protección de la información confidencial y sensible.

Esto continúa evidenciando una debilidad con respecto al seguimiento de la ejecución de las actividades vinculantes con la entrega de servicios de TI. La causa de este hallazgo se da por una ausencia de políticas o procedimientos establecidos

que exijan la inclusión de acuerdos de confidencialidad en los contratos con proveedores.

El efecto potencial de esta situación es la falta de protección legal y contractual de la información confidencial y sensible que se confía al proveedor de servicios de Centro de Datos. Esto podría resultar en la divulgación no autorizada o el uso indebido de datos críticos.

El criterio para evaluar esta condición es la inclusión de acuerdos de confidencialidad adecuados y necesarios en los contratos con los proveedores de servicios del Centro de Datos, especialmente cuando se trata de la gestión de datos sensibles.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI “Seguridad y Ciberseguridad”, se indica:

> “La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, 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.”

2.6.- HALLAZGO 6 CONTROLES DE SEGURIDAD DE ACTIVOS DE TIPO PORTÁTILES

Se ha identificado una deficiencia en los controles de seguridad para los dispositivos tipo portátiles (como, por ejemplo, *laptops*) utilizados en la DGAC. Los dispositivos carecen de medidas adecuadas de protección, como la encriptación, lo que representa un riesgo significativo de filtrado de información en caso de robo o pérdida.

La causa de este hallazgo tiene relación con la falta de políticas y procedimientos claros relacionados con la seguridad de los dispositivos móviles y la falta de conciencia sobre los riesgos asociados con la pérdida o el robo de *laptops*.

El efecto potencial de esta situación es la exposición de información confidencial y sensible en caso de que un dispositivo sea robado o se pierda. Esto podría resultar en la divulgación no autorizada de datos críticos y daños a la reputación de la organización.

El criterio para evaluar esta condición es la implementación de controles de seguridad adecuados en los dispositivos tipo *laptops*, incluyendo la encriptación de datos, para proteger la información confidencial y sensible.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI "Seguridad y Ciberseguridad", se indica:

> "La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, 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."

2.7.- HALLAZGO 7 INSTALACIÓN DE LICENCIAS DE ANTIVIRUS

Se ha identificado una deficiencia en la instalación de aproximadamente el 10% de los equipos de usuarios finales de la DGAC. Estos equipos aún no han sido desplegados y configurados, lo que podría resultar en un retraso en la detección o mitigación oportuna de amenazas de seguridad y virus.

La causa de este hallazgo está vinculada con una falta de disponibilidad del talento humano o una planificación de actividades de soporte inadecuada.

El efecto potencial de esta situación es la falta de visibilidad y control sobre el comportamiento de aproximadamente el 10% de los equipos de usuarios finales. Esto podría dar lugar a una mayor exposición a amenazas de seguridad, ya que los equipos no están debidamente monitoreados ni protegidos.

El criterio para evaluar esta condición es la instalación completa y oportuna de todos los equipos de usuarios finales, asegurando que estén debidamente configurados y protegidos contra amenazas de seguridad.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI "Seguridad y Ciberseguridad", se indica:

> "La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados."

2.8.- HALLAZGO 8 SISTEMA DE REGISTRO DE BITÁCORAS DE ACTIVIDADES EN LA PLATAFORMA

Se ha identificado una deficiencia en la infraestructura de monitoreo y seguridad de la organización, ya que no se ha instalado un *Syslog Server* que permita tener una visión completa de las actividades y movimientos de los usuarios, tanto del equipo de TI de la DGAC, como del proveedor de servicios.

Este hallazgo tiene relación con la falta de priorización de tener un sistema de monitoreo integral de usuarios en la DGAC.

Como consecuencia de esta causa, se puede materializar la falta de visibilidad y capacidad para detectar eventos y actividades sospechosas o anómalas en la red y los sistemas de la organización. Esto podría aumentar el riesgo de incidentes de seguridad no detectados.

El criterio para evaluar esta condición es la instalación de un *Syslog Server* capaz de recopilar, almacenar y analizar registros de actividad de todos los sistemas, redes y usuarios relevantes, proporcionando una visión integral de lo que está sucediendo en la organización.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI "Seguridad y Ciberseguridad", se indica:

> "La Unidad de TI debe 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 en las que se almacena, procesa y transmite información […]"

2.9.- HALLAZGO 9 SISTEMA DE SEGURIDAD DE CONTROL DE ACCESO A LA RED

Se ha identificado una deficiencia en la infraestructura de seguridad de la DGAC, ya que no se ha implementado un Sistema de Control de Acceso a la Red (NAC, por sus siglas en inglés). La falta de NAC podría aumentar el riesgo de que dispositivos no autorizados se conecten a la red de la organización.

Este hallazgo tiene relación con la falta de priorización de una plataforma de gestión de un *NAC* y la falta de una política de seguridad clara al respecto.

Como consecuencia de esta causa, se puede materializar la exposición a riesgos de seguridad, como la conexión de dispositivos no autorizados, la propagación de *malware*[1] y la falta de visibilidad y control sobre la red.

El criterio para evaluar esta condición es la implementación de un Sistema NAC que permita controlar y autorizar el acceso a la red, asegurando que solo los dispositivos autorizados y en cumplimiento con las políticas de seguridad puedan conectarse.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XI "Seguridad y Ciberseguridad", se indica:

> "La Unidad de TI debe 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 en las que se almacena, procesa y transmite información […]"

[1] El malware, programa maligno, hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo. Se podría decir que el malware Troyano es el más popular de todos e incluso, a veces por confusión, se dice que los Troyanos son un tipo de gusano informático.

2.10.- HALLAZGO 10 FALTA DE DOCUMENTACIÓN FORMAL PARA COMPROBACIÓN DE HALLAZGOS

Se ha identificado una deficiencia en la disponibilidad de documentación formal por parte del personal de TI de la DGAC sobre su gestión operativa, administración de su sistema de control, entrega de servicios y cumplimiento normativo, de gestión y gobierno de TI. Esta documentación es necesaria para la comprobación de ciertos hallazgos y que no ha sido proporcionada, lo que afecta la capacidad de llevar a cabo una auditoría completa y precisa.

La causa de este hallazgo tiene relación con la falta de un proceso establecido para documentar y presentar la información requerida durante una auditoría, la falta de conciencia sobre la importancia de proporcionar documentación adecuada, y la falta de recursos asignados para la gestión de la documentación.

El efecto potencial de esta situación es la limitación en la capacidad de los auditores para verificar la precisión de ciertos hallazgos y evaluar adecuadamente el estado de los controles de seguridad y las prácticas de TI de la DGAC.

El criterio para evaluar esta condición es la disponibilidad de documentación formal que respalde la comprobación de hallazgos y permita una auditoría efectiva.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado XIV “Aseguramiento”, se indica:

> “La institución debe disponer de prácticas formales que permitan la valoración de la disponibilidad y adecuada aplicación de un sistema de control interno para el uso eficiente de los recursos tecnológicos de la institución para lograr mantener la continuidad de las operaciones, salvaguarda y protección de la información y los activos asociados a su captura, procesamiento, consulta, almacenamiento y transferencia y la gestión apropiada de los riesgos asociados.
>
> […]
>
> La institución debe estar comprometida en la aplicación de buenas prácticas y seguimiento en la gestión de las TI estableciendo criterios efectivos para el

cumplimiento de regulaciones internas y externas, así como disposiciones contractuales.

La Unidad de TI debe incorporar prácticas de valoración para el aseguramiento sobre la entrega de servicios y el uso óptimo de los recursos tecnológicos instalados para apoyar a la institución en la continuidad de sus operaciones, salvaguarda y protección de la información y activos asociados y la implementación de iniciativas para el logro de los objetivos institucionales."

2.11.- HALLAZGO 11 VISIÓN DE LA ESTRATEGIA TECNOLÓGICA DE LA DGAC

Complementario al hallazgo № 3: "Falta de alineación entre la Estrategia Institucional, la Operación Sustantiva y el Área de TI" del informe AI-01-2023, en reuniones de trabajo con el área de TI y la Dirección General de la DGAC, se les consultó sobre su participación en la identificación de necesidades y oportunidades de cara a transformación digital y robustecimiento tecnológico de la Institución.

Con base en la realimentación de ambas áreas, se identificó que no se cuenta con una estrategia formal que precise la arquitectura institucional alineada a la realidad actual del alcance de los servicios de TI utilizados por la DGAC, ni de una visión sobre la transformación tecnológica Institucional basada en las oportunidades y necesidades que tanto las áreas usuarias como las tendencias relacionadas con la industria aeronáutica pueden aprovechar para optimizar y robustecer sus procesos, entrega de servicios y valor público.

Además, el área de TI comentó en reunión de trabajo que no cuentan con una estrategia formal que les permita establecer los procedimientos y lineamientos para la evaluación del desempeño de la plataforma tecnológica, la evaluación interna del cumplimiento del alance de los servicios administrados del Centro de Datos, el desempeño por control cruzado de la ejecución contractual, la evaluación del cumplimiento de las necesidades de las áreas funcionales Institucionales y el robustecimiento tanto del control interno como el cumplimiento normativo para la gestión de TI.

Esta condición se materializa al no contar con una estrategia multidisciplinaria (tanto operativa como administrativa, estratégica y de soporte

Institucional) que permita articular la formalización de la arquitectura institucional actual y la visión tecnológica basada en la identificación de necesidades, oportunidades y la priorización de atención en materia de tecnologías de información para la DGAC, que, además, permita evaluar de forma ordenada y objetiva el desempeño de la plataforma tecnológica actual, la planificación de crecimiento y capacidad, la planificación de transformación digital y cumplimiento normativo.

La falta de alineación entre las áreas estratégicas, sustantivas y la función de tecnologías de información, de cara a la gestión y control de la función del TI y la visión de transformación digital y cumplimiento normativo, pone a la Organización en riesgo de que se materialicen pérdidas de oportunidades de atender requerimientos y necesidades que las diferentes áreas de la Institución tienen, el uso inapropiado de recursos públicos y activos tecnológicos, la resistencia en la adopción y aprovechamiento de herramientas tecnológicas que robustezcan los servicios brindados por la Institución, tanto a clientes internos como externos, incumplimientos en las normas de gestión y gobierno de TI, y la planificación presente y futura de recursos institucionales tangibles e intangibles para la transformación digital de la DGAC.

En las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado I “Gobernanza”, se indica

> *“La institución debe disponer de un marco orientador que permita la definición de la acción institucional con un enfoque de valor público. Asimismo, debe considerar en la estrategia institucional la incorporación de iniciativas habilitadas por tecnologías de información.”*

Además, en las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de Información del MICITT, en el apartado II “Gestión de TI”, se indica

> “La institución debe implementar y mantener prácticas de gestión de las TI, que defina formalmente los siguientes componentes para la entrega de servicios al nivel de tecnologías de información en alineación con el marco estratégico y el modelo de arquitectura empresarial:
>
> […]

3. Servicios, formalmente establecidos a través de un catálogo y las relaciones de acuerdos con las unidades funcionales, de forma tal que se pueda administrar adecuadamente la infraestructura tecnológica instalada en la organización para asegurar la continuidad de las operaciones institucionales, el resguardo de la información, el cumplimiento regulatorio y la mejora continua hacia el logro de los objetivos institucionales.

4. Investigación sobre tecnologías emergentes que permitan a través de su eventual incorporación, la innovación y mejora continua al nivel institucional para el logro de los objetivos y la entrega de valor público."

III. CONCLUSIONES

De acuerdo con los resultados del estudio, se tiene que:

1. Basado en las pruebas recopiladas, se concluye que existió un riesgo real en la integridad de la información trasladada durante el proceso de migración de datos debido a la falta de medidas de seguridad adecuadas durante el transporte **(Comentario 2.1).**

2. Complementario al hallazgo 1, existe un riesgo significativo en la validación de la destrucción de datos luego de la migración debido a la falta de un proceso formal y una verificación adecuada **(Comentario 2.2).**

3. Existe además un riesgo significativo debido a la falta de detalle en el cartel de contratación con respecto al proceso de migración de datos al rescindir el servicio **(Comentario 2.3).**

4. Existe un riesgo alto debido a la falta de ejecución del plan de implementación, lo que pone en peligro la capacidad de la organización para mantener la operación y disponibilidad de los servicios ante fallos **(Comentario 2.4).**

5. Existe un riesgo significativo debido a la falta de exigencia de acuerdos de confidencialidad en los contratos con proveedores de servicios del Centro de datos **(Comentario 2.5)**

6. Igualmente, existe un riesgo significativo debido a la falta de controles de seguridad en los dispositivos tipo portátiles, lo que pone en peligro la confidencialidad de la información **(Comentario 2.6).**

7. Además, existe un riesgo significativo debido a la falta de instalación de aproximadamente el 10% de los equipos de usuarios finales, lo que podría comprometer la seguridad de la DGAC **(Comentario 2.7)**.

8. Existe un riesgo significativo debido a la falta de instalación de un *Syslog Server* para monitoreo de acceso a usuarios integral, lo que podría comprometer la seguridad de la organización **(Comentario 2.8)**.

9. Complementario al hallazgo 8, existe un riesgo significativo debido a la falta de implementación de un Sistema *NAC* para el control de acceso a la red, lo que podría comprometer la seguridad de la organización **(Comentario 2.9).**

10. Existe un riesgo significativo debido a la falta de documentación formal para la comprobación de ciertos hallazgos **(Comentario 2.10).**

11. La DGAC no cuenta con una estrategia que alinee la estrategia institucional, la práctica operativa sustantiva y la Función de TI para articular la integración de requerimientos y necesidades en materia tecnológica a nivel institucional, la valoración de las capacidades y desempeño de la plataforma, y la adopción de prácticas de gestión y gobierno de TI **(Comentario 2.11).**

IV. RECOMENDACIONES

A la Dirección General de Aviación Civil

1. Aprobar el Informe y ordenar la implementación de las recomendaciones incluidas en el mismo.

2. Articular los esfuerzos para la constitución de un plan de acción que establezca una estrategia de definición de arquitectura institucional, entrega de servicios de TI y la formalización de iniciativas de carácter tecnológico para su ejecución, con sus respectivos procesos y prácticas de gestión y evaluación **(Conclusión 11).**

A la Unidad de Tecnologías de Información

3. Establecer un protocolo de migración de información seguro que incluya medidas de seguridad física y lógica para garantizar la protección de los datos durante el proceso de traslado de estos **(Conclusión 1)**.

4. Documentar detalladamente el proceso de migración, incluyendo la cadena de custodia de los dispositivos de almacenamiento utilizados durante el transporte **(Conclusión 1)**.

5. Proporcionar capacitación al equipo de TI de la DGAC sobre las mejores prácticas para la migración segura de datos y la gestión de riesgos asociados **(Conclusión 1)**.

6. Como oportunidad de mejora, realizar copias de respaldo de los datos antes de la migración y verificar la integridad de estas antes y después del transporte **(Conclusión 1)**.

7. Implementar políticas y procedimientos claros para el manejo seguro y la destrucción de datos sensibles de acuerdo con las normativas y estándares de seguridad de la información **(Conclusión 2)**.

8. Proporcionar capacitación al personal sobre las mejores prácticas para la destrucción segura de datos **(Conclusión 2)**.

9. Como oportunidad de mejora, establecer un proceso documentado y formal para la destrucción de datos en el centro de datos de origen después de la migración, incluyendo un registro detallado de los datos destruidos **(Conclusión 2)**.

10. Como oportunidad de mejora, realizar una verificación exhaustiva de la destrucción de datos mediante la revisión de registros y auditorías regulares **(Conclusión 2)**.

11. Establecer una política que exija que todos los contratos de servicios, especialmente aquellos relacionados con la gestión de datos, incluyan información detallada sobre la migración de datos al finalizar el contrato **(Conclusión 3)**.

12. Como oportunidad de mejora, desarrollar los carteles de contratación que incluya información detallada sobre el proceso de migración de datos en caso de rescisión del contrato; esto debe incluir plazos, responsabilidades y procedimientos claros **(Conclusión 3).**

13. Se recomienda tomar las siguientes medidas para mitigar este riesgo:

a. Programar y ejecutar de manera inmediata las pruebas y actividades planificadas del plan de implementación para garantizar la funcionalidad y la capacidad de recuperación de los servicios.

b. Establecer un proceso de seguimiento y documentación riguroso para el plan de implementación, que incluya registros de resultados de pruebas y actividades realizadas.

c. Procurar los recursos necesarios y priorizar adecuadamente la ejecución del plan de implementación.

d. Realizar inspecciones regulares para verificar el cumplimiento del plan de implementación y la ejecución de pruebas **(Conclusión 4)**.

14. Identificar los tipos de acuerdos de confidencialidad necesarios según el tipo de información que se compartirá con el proveedor, como acuerdos de no divulgación (NDA), acuerdos de procesamiento de datos (DPA) y

acuerdos de confidencialidad y seguridad de la información **(Conclusión 5).**

15. Capacitar al personal sobre la importancia de los acuerdos de confidencialidad y cómo incluirlos en los contratos **(Conclusión 5)**.

16. Implementar la encriptación de datos en todos los dispositivos tipo laptops utilizados en la organización. Esto incluye la encriptación del disco duro o el uso de soluciones de gestión de dispositivos móviles (MDM) que permitan el cifrado de datos **(Conclusión 6)**.

17. Establecer políticas claras de seguridad de dispositivos móviles que incluyan la encriptación como requisito obligatorio **(Conclusión 6)**.

18. Realizar capacitación y concienciación para el personal sobre las mejores prácticas de seguridad en dispositivos móviles y los riesgos asociados con la pérdida o el robo de dispositivos móviles **(Conclusión 6)**.

19. Establecer procedimientos de respuesta a incidentes en caso de pérdida o robo de dispositivos, que incluyan la notificación oportuna y la desactivación remota de datos **(Conclusión 6)**.

20. Se recomienda tomar las siguientes acciones:

a. Priorizar y acelerar la implementación de los equipos restantes para completar el despliegue de usuarios finales.

b. Implementar medidas temporales de seguridad en los equipos no instalados, como políticas de acceso restringido y controles de seguridad adicionales.

c. Realizar un seguimiento continuo de la instalación y configuración de los equipos, asegurándose de que estén debidamente actualizados y protegidos contra amenazas de seguridad.

d. Establecer un proceso de revisión y auditoría para garantizar que todos los equipos estén debidamente instalados y configurados **(Conclusión 7)**.

21. Implementar un *Syslog Server* que sea capaz de recopilar y analizar registros de actividad de todos los movimientos de los usuarios en los sistemas, redes y servidores **(Conclusión 8)**.

22. Configurar alertas y notificaciones para eventos de seguridad críticos o inusuales **(Conclusión 8)**.

23. Realizar capacitación para el personal de TI y de seguridad en la interpretación de registros y eventos del *Syslog Server* **(Conclusión 8)**.

24. Establecer políticas y procedimientos para el uso efectivo del *Syslog Server* en la detección y respuesta a incidentes de seguridad **(Conclusión 8)**.

25. Implementar un Sistema *NAC* que permita controlar y autorizar el acceso de dispositivos a la red, verificando su cumplimiento con las políticas de seguridad **(Conclusión 9)**.

26. Definir políticas de seguridad claras que establezcan los requisitos para la conexión a la red, como la autenticación, la segmentación y la detección de amenazas **(Conclusión 9)**.

27. Realizar una evaluación de riesgos para identificar y documentar las amenazas y vulnerabilidades en la red que podrían mitigarse con un *NAC* **(Conclusión 9)**.

28. Capacitar al personal de TI y de seguridad en la configuración y operación del Sistema *NAC* **(Conclusión 9)**.

29. Realizar pruebas y simulacros para evaluar la efectividad del Sistema *NAC* en la detección y respuesta a eventos de seguridad **(Conclusión 9)**.

30. Establecer un proceso formal para la gestión de documentación relacionada con la auditoría, que incluya la identificación, recopilación y presentación de la documentación requerida **(Conclusión 10)**.

31. Designar un responsable o un equipo encargado de coordinar la entrega de documentación durante una auditoría y asegurarse de que se satisfagan las solicitudes de manera oportuna **(Conclusión 10)**.

32. Sensibilizar al personal de TI sobre la importancia de proporcionar documentación adecuada durante una auditoría y la necesidad de colaborar con los auditores **(Conclusión 10)**.

33. Realizar revisiones periódicas para evaluar el estado de la documentación y asegurarse de que esté actualizada y completa **(Conclusión 10)**.

34. Implementar herramientas y sistemas de gestión de documentos que faciliten la búsqueda y entrega eficiente de documentación requerida **(Conclusión 10)**.