

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

INFORME Nº AI-14-2019

EVALUACIÓN DEL CENTRO DE DATOS PRINCIPAL Y  
SERVICIOS ASOCIADOS IMPLEMENTADO EN LA  
DIRECCIÓN GENERAL DE AVIACIÓN CIVIL

DICIEMBRE, 2019

**ÍNDICE**

Índice .....	2
Índice de cuadros y gráficos .....	4
Abreviaturas.....	4
<b>RESUMEN EJECUTIVO</b> .....	5
<b>I. INTRODUCCIÓN</b> .....	7
1.1.- NATURALEZA DEL ESTUDIO .....	7
1.2.- JUSTIFICACIÓN .....	7
1.3.- OBJETIVOS .....	7
<b>1.3.1.- Objetivo general</b> .....	7
<b>1.3.2.- Objetivos específicos</b> .....	8
1.4.- ALCANCE.....	9
1.5.- METODOLOGÍA.....	9
1.6.- TIPO DE AUDITORÍA.....	9
1.7.- NORMATIVA ADMINISTRATIVA, LEGAL Y TÉCNICA.....	9
1.8.- CUMPLIMIENTO CON NORMAS GENERALES DE AUDITORÍA .....	12
1.9.- LIMITACIONES .....	12
1.10.- GENERALIDADES DEL ESTUDIO .....	12
1.11.- COMUNICACIÓN DE RESULTADOS .....	19
<b>II. COMENTARIOS</b> .....	20
2.1.- Hallazgo 1 Debilidades en el control de la ejecución del proyecto .....	20
2.2.- Hallazgo 2 Incumplimiento de Condiciones específicas del cartel en temas de capacitación.....	22
2.3.- Hallazgo 3 Incumplimiento de Condiciones específicas del cartel en temas de Enlaces con sede regional.....	25
2.4.- Hallazgo 4 Incumplimiento de especificaciones técnicas en dispositivo implementados .....	27
2.5.- Hallazgo 5 Incumplimiento en la revisión del estado de salud de la central telefónica IP y administración y gestión de las operaciones de mantenimiento diario de configuración del servicio de telefonía IP .....	30
2.6.- Hallazgo 6 Caída en la disponibilidad del equipo ubicado en el centro de datos principal redujo el porcentaje de disponibilidad del servicio administrado del centro de datos correspondiente al mes de mayo del 2019 por abajo del porcentaje mínimo solicitado. ....	31
2.7.- Hallazgo 7 No ejecución de multa por incumplimiento en el nivel del servicio administrado del centro de datos correspondiente al mes de mayo del 2019.....	32
2.8.- Hallazgo 8 Riesgos para la finalización de los servicios.....	33

2.9.- Hallazgo 9 Riesgos asociados a la Gestión del área de Tecnologías de Información y la operación y funcionamiento del centro de datos de DGAC. ....	34
2.10.- Hallazgo 10 Control interno insuficiente para mitigar los riesgos identificados para la Gestión del área de Tecnologías de Información y la operación y funcionamiento del centro de datos de DGAC. ....	42
2.11.- Hallazgo 11 Nivel de satisfacción de los usuarios de la DGAC de cara a la Unidad de Tecnologías de Información. ....	47
<b>III. CONCLUSIONES</b> .....	<b>51</b>
<b>IV. RECOMENDACIONES</b> .....	<b>53</b>

---

**ÍNDICE DE CUADROS Y GRÁFICOS**

Tabla 1 Roles de las empresas que integran el Consorcio .....	15
Tabla 2 Riesgos no aceptados identificados de la gestión de TI de la DGAC .....	35
Tabla 3 Riesgos aceptados identificados de la gestión de TI de la DGAC .....	36
Tabla 4 Riesgos no cuantificados .....	38
Tabla 5 Riesgos identificados de la gestión del Centro de Datos objeto del estudio .....	38
Tabla 6 Valoración de Riesgos y Controles Internos .....	44
Figura 1 Ámbito del proyecto implementado .....	17
Figura 2 Fotografías de gabinete de servidores en CODISA Data Center (frontal y posterior) .....	18
Figura 3 Especificaciones técnicas de servidor.....	27
Figura 4 Especificaciones técnicas de servidor (II parte) .....	28
Figura 5 Especificaciones técnicas de router Oficinas Centrales y Datacenter .....	28
Figura 6 Especificaciones técnicas de router Oficinas Regionales.....	29
Figura 7 Especificaciones técnicas de switch Oficinas Regionales .....	29
Figura 8 Especificaciones técnicas de switch Oficinas Centrales y Datacenter.....	30

**ABREVIATURAS**

<b>Abreviatura</b>	<b>Significado</b>
CGR	Contraloría General de la República
IP	Internet Protocol
TI	Tecnologías de Información
LGCI	Ley General de Control
SICOP	Sistema Integral de Compras Públicas
COSO	Committee of Sponsoring Organizations of the Treadway Commission (siglas en inglés)
COBIT	Control Objectives for Information and Related Technology (siglas en inglés)

## **RESUMEN EJECUTIVO**

### **¿Cuál fue el objetivo del estudio?**

Verificar el 100% del cumplimiento en la implementación y puesta en ejecución de los aspectos técnicos pactados por la administración activa en la Licitación Pública 2017LN-000001-0006600001 denominada “Contratación de Servicios Administrados para Centro de Datos principal, procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos y telefonía sobre IP para la DGAC”, para determinar eventuales desviaciones, cumplimientos, brechas y oportunidades de mejora; realizar un inventario de la información y evaluar la razonabilidad de los pagos efectuados a la fecha; todo en apego a la normativa que le rige.

### **¿Por qué se justificó el estudio?**

La Dirección General de Aviación Civil –DGAC– implementó entre finales del 2017 y 2018, a través de servicios administrados con un proveedor comercial, y por un plazo de 48 meses, un centro de datos principal: procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos y una solución de telefonía sobre IP. Los términos del cartel, aclaraciones, oferta, contrato y otros documentos están disponibles en el sitio web SICOP en la dirección <https://www.sicop.go.cr/index.jsp> con el número de procedimiento 2017LN-000001-0006600001.

Debido a lo anterior, la Auditoría Interna programó, en el Plan Anual de Trabajo 2019, llevar a cabo un estudio con el propósito de verificar el cumplimiento en la implementación y puesta en ejecución de los aspectos técnicos definidos en el respectivo contrato, y determinar eventuales desviaciones, brechas y/u oportunidades de mejora; todo en apego a la normativa que le rige.

### **¿Cuáles fueron los principales hallazgos?**

Los principales hallazgos identificados comprenden:

- a. Las prácticas que se llevan a cabo la gestión y control del proyecto muestran debilidades para realizar una correcta administración de servicios y ejecución contractual de cara al desarrollo de esta licitación.
- b. La falta de una diligencia robusta y efectiva para validar y atender debidamente incumplimientos vinculantes con capacitaciones, plataforma

- de comunicaciones, y dispositivos tecnológicos entregados y en proceso de implementación.
- c. Debilidades en la validación y debido seguimiento para certificar que los equipos entregados e implementados están alineados con los requerimientos solicitados a nivel cartelario.
  - d. Debilidades en la validación de la entrega de servicios administrados de forma proactiva y atendiendo los requerimientos contractuales, del personal e Institucionales, con sus debidos procedimientos, cuando aplique.
  - e. Debilidades en la identificación del catálogo de riesgos y controles internos para la Gestión General de Tecnologías de Información trasiega.
  - f. Una imagen deficiente de la prestación de servicios de Tecnologías de Información a nivel interno en la Institución, así como la alineación estratégica del área con la Institución y su personal.

### **¿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 proyectos y necesidades usuarias, así como la debida diligencia a la correcta aceptación a satisfacción de servicios brindados por terceros, además de los mecanismos de intervención que apliquen.

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, los tomadores de decisiones y la ciudadanía vinculante.

## **I. INTRODUCCIÓN**

### **1.1.- NATURALEZA DEL ESTUDIO**

Evaluar el proceso de ejecución contractual de la Licitación Pública 2017LN-000001-0006600001 para determinar cumplimientos, eventuales incumplimientos, brechas, oportunidades de mejora, identificar riesgos y evaluar la razonabilidad de los pagos efectuados a la fecha desde su implementación, es de vital importancia para constatar que los fondos públicos comprometidos en este contrato son razonables y se ajusta a lo contratado.

### **1.2.- JUSTIFICACIÓN**

De conformidad con el Artículo 22, inciso c) de la Ley General de Control (LGCI) Interno, Ley No 8292, le corresponde a la Auditoría Interna, en cumplimiento de sus funciones, realizar estudios que contribuyan a que se alcancen los objetivos institucionales.

La Dirección General de Aviación Civil –DGAC– implementó entre finales del 2017 y 2018, a través de servicios administrados con un proveedor comercial, y por un plazo de 48 meses, un centro de datos principal: procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos y una solución de telefonía sobre IP. Los términos del cartel, aclaraciones, oferta, contrato y otros documentos están disponibles en el sitio web SICOP en la dirección <https://www.sicop.go.cr/index.jsp> con el número de procedimiento 2017LN-000001-0006600001.

Debido a lo anterior, la Auditoría Interna programó, en el Plan Anual de Trabajo 2019, llevar a cabo un estudio con el propósito de verificar el cumplimiento en la implementación y puesta en ejecución de los aspectos técnicos definidos en el respectivo contrato<sup>1</sup>, y determinar eventuales desviaciones, brechas y/u oportunidades de mejora; todo en apego a la normativa que le rige.

### **1.3.- OBJETIVOS**

#### **1.3.1.- Objetivo general**

---

<sup>1</sup> Entiéndase por contrato, el cartel, las aclaraciones, la oferta adjudicada, el contrato y otros relacionados disponibles en SICOP.

Evaluar el 100% de los aspectos técnicos del contrato derivado de la Licitación Pública 2017LN-000001-0006600001, denominada “Contratación de Servicios Administrados para Centro de Datos principal, procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos y telefonía sobre IP para la DGAC”.

**1.3.2.- Objetivos específicos**

1. Identificar el alcance de la licitación de los servicios brindados por el consorcio CODISA, CMA, BCNetwork, Fusionet.
2. Determinar aspectos técnicos que se cumplen: Se debe documentar la evidencia respectiva; suficiente y competente para cada caso que se determine cumplimiento.
3. Determinar aspectos técnicos que se incumplen: Se debe determinar la evidencia respectiva; suficiente y competente para cada aspecto técnico que se determine incumplido; identificar la causa y el impacto o efecto; tanto en el funcionamiento del centro de datos como en los fondos públicos respectivos.
4. Determinar brechas por ajuste al funcionamiento: Determinar la existencia de brechas -si las hay- su causa y efecto respectivo; tanto en el funcionamiento como en los fondos públicos.
5. Realizar un inventario de la información que se guarda/custodia en el centro de datos/data center.
6. Evaluar la razonabilidad de los pagos efectuados 2018 a la fecha; desde el inicio de la Contratación.
7. Identificar oportunidades de mejora para el citado Centro de Datos.
8. Identificar los riesgos asociados a la operación y funcionamiento del centro de datos de la DGAC, a partir de las debilidades del sistema de control interno.
9. Otros aspectos a criterio del Contratista.
  - a. Identificar el alcance de la licitación de los servicios brindados por el consorcio CODISA, CMA, BCNetwork, Fusionet.

- b. Realizar una evaluación general de riesgos y Controles Internos asociados a la Gestión de Tecnologías de Información de la DGAC.
- c. Identificar el nivel de satisfacción de los usuarios Institucionales relacionado con el soporte, herramientas tecnológicas, capacitaciones, proyectos relacionados con TI y la Unidad de TI Institucional en General, además de la percepción de la calidad de la plataforma tecnológica brindada por servicios administrados.

#### **1.4.- ALCANCE**

El estudio de auditoría se enfocó en verificar el total cumplimiento en la implementación y puesta en ejecución de los aspectos técnicos pactados por la administración activa en la Licitación Pública 2017LN-000001-0006600001 denominada “Contratación de Servicios Administrados para Centro de Datos principal, procesamiento, almacenamiento, respaldo de datos, plataforma de red de datos y telefonía sobre IP para la DGAC”, para determinar eventuales desviaciones, cumplimientos, brechas y oportunidades de mejora; realizar un inventario de la información y evaluar la razonabilidad de los pagos efectuados a la fecha; todo en apego a la normativa que le rige.

El estudio rige desde 11 de noviembre del 2017 (fecha de adjudicación en firme de la licitación pública mencionada anteriormente), con fecha de corte hasta el 1 de noviembre del 2019.

#### **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. Contrato de la Licitación Pública 2017LN-000001-0006600001.
- b. Ley de Contratación Administrativa; Ley Nº 7494 y sus reformas.

- c. Las “Normas Generales de Auditoría para el Sector Público”, R-DC-64-2014, publicadas en “La Gaceta” Nº 184 del 25/09/2014 que rigen a partir del 01 de enero de 2015.
- d. Normas técnicas para la gestión y el control de las Tecnologías de Información (N2-2007-CO-DFOE). Aprobadas mediante Resolución del Despacho de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007. Publicada en La Gaceta Nro.119 del 21 de junio, 2007.
- e. Control de Objetivos para Tecnologías de Información y Relacionadas (COBIT ver.5).
- f. Marco de referencia para la implementación, gestión y control sistema de control interno COSO.
- g. ISO 27001 – Sistemas de Gestión de la Seguridad de la Información.

Asimismo, en la tramitación del presente estudio se deberá observar lo estipulado en la Ley General de Control Interno, N° 8292, específicamente en los siguientes artículos:

Artículo 37. –**Informes dirigidos al jefarcarca**. Cuando el informe de auditoría esté dirigido al jefarcarca, 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 jefarcarca 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” (R-DC-119-2009).

### **1.9.- LIMITACIONES**

- a. La Unidad de Tecnologías de Información no entregó un expediente de gestión interna de la ejecución de la contratación objeto de este estudio, sino una serie de documentos relacionados sin un orden definido; las evidencias que respaldan los hallazgos por tanto se sustentan con la documentación entregada.

### **1.10.- GENERALIDADES DEL ESTUDIO**

Con respecto al alcance y planificación de la ejecución de la Licitación:

- a. El propósito de la contratación surge de la necesidad de realizar una actualización tecnológica del centro de datos de la DGAC, reemplazando los equipos de la infraestructura tecnológica Institucional ya obsoletos, la modernización de la plataforma de telefonía sobre IP, y la implementación de una línea redundante entre el centro de datos y las sedes regionales que la Institución soporta y fiscaliza.
- b. La adjudicación del contrato se dio al Consorcio compuesto por CODISA, CMA, BCNetwork y Fusionet.
- c. El objeto de la contratación es la entrega por medio de servicios administrados de la gestión, monitoreo, soporte y mantenimiento de los siguientes componentes:

- i. La entrega de los equipos físicos que componen la plataforma física tecnológica y los ambientes virtuales para soportar la plataforma de sistemas, servicios y bases de datos de la DGAC, implementado en un centro de datos externo a la Institución gestionado por CODISA, el cual se refiere en adelante como centro de datos principal.
- ii. La infraestructura de enlace de datos entre las oficinas centrales y regionales de la DGAC con su centro de datos principal.
- iii. La plataforma de seguridad física y lógica de los equipos de procesamiento del centro de datos (seguridad perimetral).
- iv. La plataforma de telefonía IP.
- d. El ámbito de la contratación corresponde a la implementación y habilitación de los activos tecnológicos, tanto en el centro de datos principal como en las oficinas centrales de la DGAC y sus centros regionales:
  - i. Aeropuerto Tobías Bolaños
  - ii. Hangar en el Aeropuerto Tobías Bolaños
  - iii. Aeropuerto Daniel Oduber
  - iv. Torre de Control del Aeropuerto Daniel Oduber
  - v. Edificio Radar ATC del Aeropuerto Juan Santamaría
  - vi. Aeropuerto Juan Santamaría
  - vii. Edificio OFGI del Aeropuerto Juan Santamaría
  - viii. Aeropuerto de Limón
- e. Se planificó el período de implementación de la plataforma tecnológica para 6 meses.
- f. CMA es el encargado del soporte técnico especializado para la DGAC, con la responsabilidad de atender y resolver cualquier incidente que reporte la Institución de cara a la plataforma tecnológica física, ambientes virtuales, enlaces de datos, seguridad y telefonía IP; las empresas miembros del consorcio complementan el soporte según su especialidad.
- g. Según la orden de compra № 2087, el costo anual de la adjudicación es de \$933,311.20 dólares de los Estados Unidos (USD), a 10 meses (el primer año).
  - i. Por el tipo de cambio utilizado en la orden de compra (₡606.45) y el monto para financiar el diferencial cambiario, se establece el costo del proyecto en ₡598,887,130.82

Con respecto a la ejecución e implementación de la plataforma tecnológica objeto de la contratación:

- a. El período de implementación estaba planeado para 6 meses, y por razones de entrega de equipos y estabilización de la plataforma se alargó a 9 meses.
- b. A nivel cartelario, quedan pendiente de cumplirse las siguientes especificaciones:
  - i. Enlace de fibra óptica para el Aeropuerto de Limón (actualmente opera con una conexión por enlace inalámbrico); su cumplimiento depende de la gestión realizada con el responsable de los postes de tendido en la zona (ICE) para que faciliten la instalación de la fibra.
  - ii. Ejecución de capacitaciones especializadas; su cumplimiento depende de la asignación de personal para la recepción de los cursos, los cuales tienen requisitos previos que deben ser cumplidos por los participantes.
- c. Durante la ejecución de la etapa de implementación, se materializaron imprevistos que generaron complicaciones de cara a la certificación y pruebas de la plataforma implementada, esto a raíz de que la Institución no facilitó las condiciones para realizar trabajos de cambio de los activos fuera de horarios de oficina, ni se contaba con espacios idóneos ni seguros para la instalación de equipos en sedes regionales.
- d. También, por la estrategia de migración del ambiente virtual de producción del centro de datos de la DGAC (sistemas, servicios, herramientas y bases de datos), se requirió un período de gracia que permitiera al consorcio estabilizar la plataforma tecnológica en el centro de datos principal.

Con respecto a la aceptación por parte de la DGAC e inicio de los servicios administrados:

- a. El personal de la Dirección de Tecnologías de Información de DGAC asignado al proyecto revisó la entrega de equipos tanto en las oficinas centrales como en el centro de datos de CODISA y de las sedes regionales.
- b. El cierre de la etapa de implementación fue recibida a satisfacción por el personal de TI de la DGAC, aceptando las tareas no finalizadas como “pendientes no imputables al contratista”, iniciando la etapa de servicios administrados a partir de agosto del 2018.
- c. Actualmente, la etapa de ejecución de los servicios administrados cumplió su primer año, el cual ha sido prorrogado por un segundo más (hasta agosto del 2020); esta etapa no es fiscalizada de forma efectiva por el área de Tecnologías de Información de la DGAC, ni se tiene la trazabilidad

documentada para corroborar el cumplimiento de los Acuerdos de Nivel de Servicio por parte del consorcio de cara a incidentes.

- d. Se indicó además que, por falta de condiciones de seguridad perimetral en algunas sedes regionales, los equipos de enlace de datos están expuestos a un uso indebido por parte de funcionarios internos, ya sea por la conexión de activos tecnológicos no autorizados, o por daños materiales a los componentes.
- e. También existen posiciones encontradas entre los incidentes que requieren atención por parte de la Dirección de TI Institucional y aquellos que son responsabilidad dentro del ámbito de la contratación del Consorcio, lo que aumenta el tiempo de atención e incrementa la dificultad de resolución de los incidentes que se materializan.
- f. Además, no se identifica evidencia que sustente que la DGAC realiza el debido seguimiento en tiempo real de la plataforma tecnológica, pese a que CODISA/CMA les dio acceso a un Cuadro de Mando (Dashboard) Web para monitorearla, a causa de la falta de disponibilidad del personal fiscalizador de la Unidad de TI.

Con respecto al alcance de los servicios administrados ofrecidos por el Consorcio:

- a. El costo mensual del proyecto es de \$93,331,12 USD.
  - i. El costo de la primera prórroga vigente es de \$1.119.973,44 USD.
  - ii. Hasta este momento, se ha pagado al Consorcio la suma de \$1.306.635,68 USD, al mes de octubre del 2019.
- b. La persona responsable de la aceptación y aprobación de pago es Malou Guzmán, jefa del área de Tecnologías de Información.
- c. Como parte de los servicios administrados de la plataforma tecnológica ya en producción, el ámbito de acción de cada integrante del consorcio se describe a continuación:

**Tabla Nº 1**  
**Roles de las empresas que integran el Consorcio**

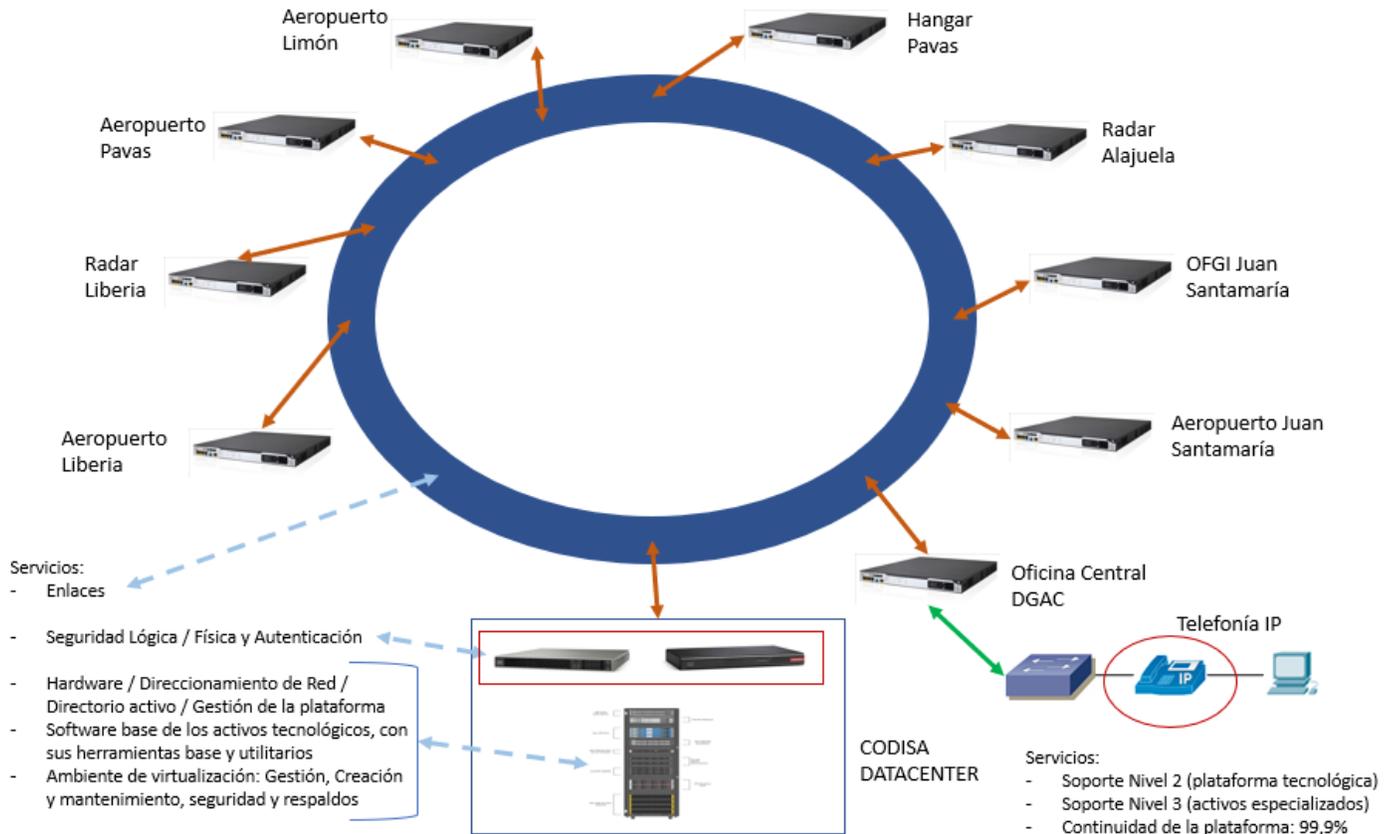
Nombre	Rol	Responsabilidad	Ámbito de trabajo
<b>CODISA</b>	Responsable de la contratación / Administrador del Centro de Datos	Administrar el ambiente físico de la plataforma de centro de datos y enlaces de datos.	Oficinas Centrales, Centro de Datos

<b>Nombre</b>	<b>Rol</b>	<b>Responsabilidad</b>	<b>Ámbito de trabajo</b>
<b>CMA</b>	Integrador de la plataforma física / Mesa de ayuda	Administrar los activos físicos y ambientes virtuales; dar atención a incidentes de la DGAC	Oficinas Centrales, Centro de Datos, Sedes Regionales
<b>BC Network</b>	Telefonía IP	Administrar la configuración de la plataforma de telefonía IP y el soporte de los equipos	Oficinas Centrales, Sedes Regionales
<b>Fusionet</b>	Perimetral / Seguridad	Administrar la configuración de la plataforma de seguridad perimetral físico / virtual de los enlaces de datos	Oficinas Centrales, Centro de Datos, Sedes Regionales

**Fuente:** elaboración propia con insumos del Consorcio.

- d. Los servicios por parte de los diferentes integrantes del Consorcio se encuentran vigente, dentro del ámbito de cada uno, y su participación para la atención de incidentes y mantenimiento es administrado por CMA como responsable de la mesa de ayuda.
- e. Desde el momento que inicia la etapa de servicios administrados hasta agosto del 2019, la Dirección de Tecnologías de Información ha recibido a satisfacción los servicios ofrecidos por el Consorcio.
- f. A continuación, se representa el alcance de los servicios otorgados a la DGAC, con base en los entregables ofertados y entregados por parte del Consorcio objeto de esta licitación, y aceptado por parte del área de Tecnologías de Información:

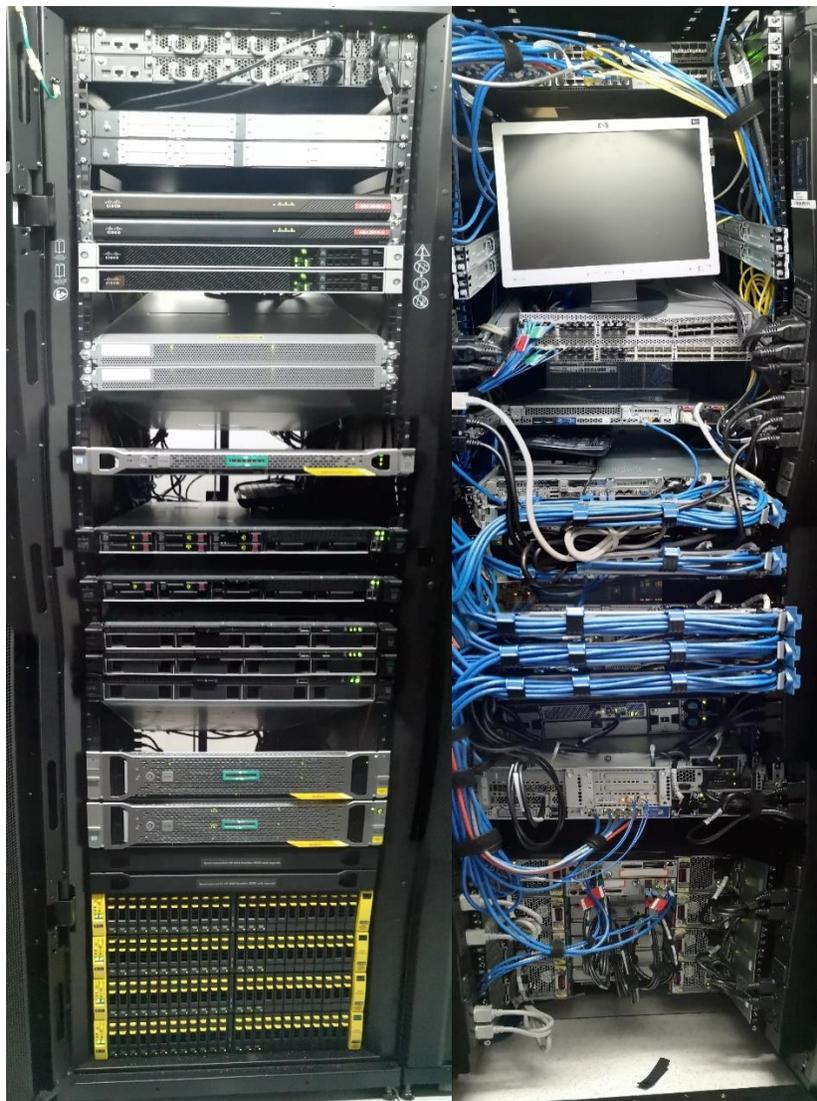
**Figura Nº 1**  
**Ámbito del proyecto implementado**



**Fuente:** elaboración propia con insumos del Consorcio.

- g. A continuación, se presentan las imágenes de los equipos instalados en el centro de datos (frontal y posterior):

**Figura No 2**  
**Fotografías de gabinete de servidores en CODISA Data Center (frontal y posterior)**



Fuente: Codisa Datacenter, 2019.

### **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 04 de diciembre del año en curso se remitieron notas 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 diciembre en la sala de reuniones de la Auditoría Interna, con la presencia, por parte de la Administración de Álvaro Vargas Segura, Director General de Aviación Civil, Malou Guzmán Quesada, Jefe de la Unidad de Tecnologías de Información, Rafael Eduardo Hidalgo Fonseca, de la Unidad de Planificación, por parte del equipo contratado para llevar a cabo el estudio asistieron, Damián Calvo de León, Benjamín Calvo de León y Francisco Hernández Chavarría. En esa oportunidad la administración presentó algunas observaciones verbales, las cuales no generaron cambios a los hallazgos detectados.

## **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, resultando lo que se detalla a continuación:

### **2.1.- HALLAZGO 1 DEBILIDADES EN EL CONTROL DE LA EJECUCIÓN DEL PROYECTO**

Al iniciar el estudio y solicitar la documentación relacionada con la ejecución de las actividades de la licitación contratada, la Unidad de TI entregó archivos de consulta del proyecto sin un orden formal (ya fuese por etapa del proyecto, por tipo de documento, por actividad vinculante, u otra forma de gestión), que además dificulta la trazabilidad secuencial de las tareas realizadas y el seguimiento y control de los servicios otorgados por el contratista.

Además, se identificaron los siguientes puntos que representan una brecha<sup>2</sup> por ajuste al funcionamiento de la plataforma tecnológica, sin que se presente la debida documentación que evidencie una gestión formal de cambio:

1. Se implementó en el centro de datos de CODISA equipos tecnológicos (servidores, solución de respaldo y almacenamiento) de Generación 10. El contratista indicó que se adquirieron para brindar a la Institución una plataforma “estado del arte” en su última generación liberada.
2. Se incrementó el ancho de banda de los enlaces al edificio central y sedes regionales al doble de lo solicitado. El contratista indicó que se brindó este cambio para dar mayor estabilidad y respuesta a la plataforma y realizar pruebas de desempeño, pero no se han regresado a su estado original.
3. El almacenamiento total de la solución virtualizada consume más espacio del ofertado a nivel cartelario, lo cual el contratista gestiona como parte del espacio habilitado para servicios complementarios de gestión de la plataforma sin alterar su capacidad instalada ni sus funciones.

Esto evidencia una debilidad con respecto al monitoreo y control de seguimiento de la ejecución de las actividades vinculantes al alcance objeto de la

---

<sup>2</sup> Esta brecha no ha implicado un aumento en el costo mensual del servicio administrado.

contratación, así como la debida diligencia al estado de cumplimiento de requerimientos conforme fueron desarrollados y presentados.

La ausencia de un expediente formal de ejecución del proyecto, además de la falta de mecanismos robustos para su debida gestión y control, limita la capacidad de certificar el cumplimiento de actividades de gestión relacionadas con la planificación, ejecución, monitoreo y control y cierre del proyecto, dificulta la trazabilidad de atrasos, causas de incumplimientos, subsanes, adendas a contrato, acuerdos y compromisos, entre otro; además de dificultar la transparencia en el cumplimiento del objeto de la contratación.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, en el Capítulo V: *Seguimiento*, definen, con respecto a la gestión de proyectos:

*"5.1 Gestión de proyectos: La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.*

Además, las mismas Normas, en el Capítulo III: *Implementación de tecnologías de información*, definen, con respecto a la ejecución de proyectos:

*3.1 Consideraciones generales de la implementación de TI:  
[...]*

*h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos."*

Las Normas de Control Interno para el Sector Público, emitidas por la CGR, en la norma 4.5: *Garantía de eficiencia y eficacia de las operaciones*, específicamente en la subnorma 4.5.2, establece:

*"Gestión de proyectos. El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la*

*correcta planificación y gestión de los proyectos que la institución emprenda...*

*[...]*

*b. La designación de un responsable del proyecto con competencias idóneas para que ejecute las labores de planear, organizar, dirigir, controlar y documentar el proyecto."*

Como parte del control a seguir, las Normas de Control Interno para el Sector Público, emitidas por la CGR, en lo que compete a la gestión documental señala:

*"5.4 Gestión documental El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales."*

## **2.2.- HALLAZGO 2 INCUMPLIMIENTO DE CONDICIONES ESPECÍFICAS DEL CARTEL EN TEMAS DE CAPACITACIÓN**

Al revisar la documentación relacionada con el informe de implementación de los servicios contratados en oficinas centrales y regionales de la DGAC, se identifica que se encuentran pendientes cursos formales de la plataforma de cara a las capacitaciones solicitadas a nivel cartelario.

En reuniones de trabajo separadas con el personal del Consorcio y el personal de la Unidad de TI de la DGAC, se llega al consenso de lo mencionado a continuación:

*"Debido a la limitación de recurso humano de la Unidad de Tecnologías de Información que debe apoyar y/o participar en diferentes actividades del proyecto, no se han logrado impartir los siguientes cursos de capacitación:*

*a. VMware vRealize Operations Manager: Install, Configure, Manage*

*b. Administración MS Windows Server DataCenter 2012 R2*

*c. Administración MS SQL Server Standard”<sup>3</sup>*

Estos cursos tienen como requisito cursos de certificación formal, los cuales fueron otorgados a personal de la Unidad de TI de la DGAC que ya no labora en la Institución, por lo cual, para solventar el requisito:

- Se requiere realizar un desembolso adicional a lo ya pagado al Consorcio para habilitar de nuevo los cursos ya ofrecidos, o;
- Contratar servicios externos que brinden al personal designado de la Unidad de TI los cursos formales requisito para continuar con la oferta de capacitaciones.

Complementario a la capacitación, no se cuenta con evidencia que sustente que las siguientes sesiones fueron ejecutadas; estas actividades identificadas se encuentran como “pendientes” en el informe de implementación en cuestión:

*“El estado de ejecución de las sesiones de transferencia de conocimiento requeridas en el Cartel de Licitación es el siguiente:*

*[...]*

*b. Diseño de ambiente de comunicaciones LAN, WAN, Wireless.*

*Estado: Se impartirá en el mes de septiembre.*

*[...]*

*e. Software de Gestión y Monitoreo*

*Estado: Se impartirá en el mes de septiembre.*

*f. Software de antivirus a nivel de servidores y cliente.*

*Estado: Se impartirá en el mes de septiembre.*

*[...]”<sup>4</sup>*

Estos requerimientos pendientes se deben no solo a que el personal no puede disponer del tiempo dentro de sus horarios para atender debidamente los

---

<sup>3</sup> Fuente: Informe de implementación de los servicios contratados en oficinas centrales y regionales de la Dirección General de Aviación Civil, Agosto 2018. Elaborado por el Consorcio contratado.

<sup>4</sup> Fuente: Informe de implementación de los servicios contratados en oficinas centrales y regionales de la Dirección General de Aviación Civil, Agosto 2018. Elaborado por el Consorcio contratado.

cursos, sino además porque no se facilita la disponibilidad del personal en horarios fuera del definido para la Unidad.

La falta de coordinación para formalizar la ejecución de las capacitaciones y cursos pendientes, además de la no disponibilidad o disposición del personal de TI para cumplir con estas tareas fuera de horario de oficina, hace que el requisito quede en un estado de “pendiente” sin responsabilidad para el contratista, y que en un momento de terminación de contrato, el costo de oportunidad de no ser capacitados se materialice (tanto material como económicamente), sin un reconocimiento o reembolso para la Institución.

A nivel cartelario, en la tercera parte: *Condiciones Específicas*, sección 12: *Transferencia de conocimiento*, se establece:

“[...]

*f.) Adicionalmente, el contratista deberá brindar una capacitación formal en la plataforma VMWare solicitada en este cartel, basado en los siguientes alcances:*

*1. Curso de “Administración del Software de Virtualización VMWare”, en su última versión disponible, para tres personas.*

[...]

*g.) El contratista deberá brindar una capacitación formal en la plataforma Microsoft Windows Server DataCenter 2012 R2 solicitada en este cartel, basado en los siguientes alcances:*

*1. Curso de “Administración Microsoft Windows Server DataCenter 2012 R2 que incluya la instalación, configuración y administración de roles como DNS, DHCP, Active Directory y IIS”, en su última versión disponible, para dos personas.*

[...]

*h.) El contratista deberá brindar una capacitación formal en la plataforma SQL Server Standard solicitada en este cartel, basado en los siguientes alcances:*

*1. Curso de “Administración SQL Server Standard”, en su última versión disponible, para tres personas.*

[...]”

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, definen, con respecto a la gestión de proyectos:

*"5.1 Gestión de proyectos: La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos."*

*"3.1 Consideraciones generales de la implementación de TI:  
[...]*

*h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos."*

Además, la Ley de Contratación Administrativa establece:

*"Artículo 4°-Principios de eficacia y eficiencia. Todos los actos relativos a la actividad de contratación administrativa deberán estar orientados al cumplimiento de los fines, las metas y los objetivos de la administración, con el propósito de garantizar la efectiva satisfacción del interés general, a partir de un uso eficiente de los recursos institucionales".*

### **2.3.- HALLAZGO 3 INCUMPLIMIENTO DE CONDICIONES ESPECÍFICAS DEL CARTEL EN TEMAS DE ENLACES CON SEDE REGIONAL**

Al revisar la documentación relacionada con el informe de implementación de los servicios contratados en oficinas centrales y regionales de la Dirección General de Aviación Civil, se identifica que de cara a la implementación del enlace de datos a la sede regional Aeropuerto de Limón:

*"El enlace de comunicaciones redundante en capa 2 a 8 Mbps se encuentra activo y en operación de forma inalámbrica. Esta solución temporal cuenta con el visto bueno de la señora Malou Guzmán, Administradora del Contrato por parte de la DGAC.*

*Lo anterior, debido a que el ICE debe gestionar a lo interno la Solicitud de mejoras #078-2018 que le*

*permitirán a El Consorcio instalar la fibra óptica a la altura requerida.”<sup>5</sup>*

A la fecha de corte de este informe, no se ha solventado la situación relacionada con la integración del Aeropuerto de Limón con la infraestructura de redes gestionada por servicios administrados para la Institución, como se indica en la segunda parte: *Especificaciones Técnicas*, sección E: *Enlaces de Comunicación*.

Si bien se requiere la intervención de un tercero fuera del ámbito de los actores de la ejecución contractual, no se cuenta con evidencia de la debida diligencia relacionada con la atención y resolución de esta situación “temporal”.

La falta de atención de este requerimiento puede materializar el riesgo de un enlace deficiente para la sede regional, sin responsabilidad para el contratista, y sin un reconocimiento o reembolso para la Institución.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, definen, con respecto a la gestión de proyectos:

*“5.1 Gestión de proyectos: La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.”*

*“3.1 Consideraciones generales de la implementación de TI:  
[...]*

*h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.”*

---

<sup>5</sup> Fuente: Informe de implementación de los servicios contratados en oficinas centrales y regionales de la Dirección General de Aviación Civil, Agosto 2018. Elaborado por el Consorcio contratado.

## **2.4.- HALLAZGO 4 INCUMPLIMIENTO DE ESPECIFICACIONES TÉCNICAS EN DISPOSITIVO IMPLEMENTADOS**

Al realizar pruebas de revisión de las actas de recibido conforme de los equipos por el departamento de Tecnologías de Información de la DGAC, se realiza una comparación entre las características mencionadas en el cartel y las especificaciones técnicas de los equipos implementados, y se detectaron los siguientes incumplimientos:

### **2.4.1 DEFICIENCIA DE MEMORIA CACHÉ EN DISPOSITIVO DE TIPO “SERVIDOR” “HP DL360”, SERVIDOR DE GESTIÓN**

Según la ficha técnica oficial del fabricante, documento anexo “HP DL360 QuickSpecs.pdf”, página 6 en el cuadro de comparación de capacidades de los procesadores se especifica lo siguiente:

**Figura No 3**  
**Especificaciones técnicas de servidor**

Intel Xeon Models	Frequency	Cores	L3 Cache	Power	UPI	DDR4 MT/s	Max Memory per socket
Gold 5118	2.3 GHz	12	16.50 MB	105W	2 @ 10.4 GT/s	2400 MT/s	768 GB

Fuente: Hewlett Packard Enterprise. <http://www.hpe.com/>

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección II: *Especificaciones técnicas*, inciso b.8.1 que el producto de tipo “servidor”, debe contar con al menos dos (2) procesadores Intel E5-2650v4 12-Core o superior. Cada procesador debe incluir al menos 30MB de memoria cache. Según la ficha técnica del producto “HP DL360” el equipo de serie, con el procesador actualmente configurado “Intel® Gold 5118 CPU” cuenta solamente con 16.50 MB de memoria caché.

### **2.4.2 DEFICIENCIA DE MEMORIA CACHÉ EN DISPOSITIVO DE TIPO “SERVIDOR” “HP DL360”, SERVIDOR DE PROCESAMIENTO**

Según la ficha técnica oficial del fabricante, documento anexo “HP DL360 QuickSpecs.pdf”, página 6 en el cuadro de comparación de capacidades de los procesadores se especifica lo siguiente:

**Figura No 4**  
**Especificaciones técnicas de servidor (II parte)**

Intel Xeon Models	Frequency	Cores	L3 Cache	Power	UPI	DDR4 MT/s	Max Memory per socket
Gold 6140M	2.3 GHz	18	24.75 MB	140W	2 @ 10.4 GT/s	2666 MT/s	1.5 TB
Gold 6140	2.3 GHz	18	24.75 MB	140W	2 @ 10.4 GT/s	2666 MT/s	768 GB

Fuente: Hewlett Packard Enterprise. <http://www.hpe.com/>

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección II: *Especificaciones técnicas*, inciso b.6.3.1 que el producto de tipo “servidor”, debe contar con al menos dos (2) procesadores Intel E5-2690v4 14-Core o superior. Cada procesador debe incluir al menos 35MB de memoria cache. Según la ficha técnica del producto “HP DL360” el equipo de serie, con el procesador actualmente configurado “Intel® Gold 6140 CPU” cuenta solamente con 24.75 MB de memoria caché.

#### 2.4.3 DEFICIENCIA DE MEMORIA FLASH Y MEMORIA RAM EN DISPOSITIVOS DE TIPO “ROUTER” “HP MSR3024” PARA OFICINAS CENTRALES Y DATACENTER

Según la ficha técnica oficial del fabricante, documento anexo “HP MSR300 QuickSpecs.pdf”, página 40 en el apartado “Memory and Processor”, especifica lo siguiente:

**Figura No 5**  
**Especificaciones técnicas de router Oficinas Centrales y Datacenter**

<b>Memory and processor</b> RISC, 4 cores @ 1 GHz, 256 MB flash capacity, 2 GB DDR3 SDRAM
---

Fuente: Hewlett Packard Enterprise. <http://www.hpe.com/>

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección II (Especificaciones técnicas), los incisos b.12.8.h y d.1.9.1.i que el producto de tipo “router”, debe contar con al menos 2 GB de memoria flash y 4 GB de memoria RAM. Según la ficha técnica del producto “HP MSR3024” el equipo de serie, cuenta solamente con 256 MB de memoria Flash y 2 GB de memoria RAM.

#### 2.4.4 DEFICIENCIA DE MEMORIA FLASH DISPOSITIVO DE TIPO “ROUTER” “HP MSR3024” PARA LAS OFICINAS REGIONALES

Según la ficha técnica oficial del fabricante, documento anexo “HP MSR300 QuickSpecs.pdf”, página 40 en el apartado “Memory and Processor”, especifica lo siguiente:

##### Figura № 6 Especificaciones Técnicas de Router Oficinas Regionales

**Memory and processor** RISC, 4 cores @ 1 GHz, 256 MB flash capacity, 2 GB DDR3 SDRAM

Fuente: Hewlett Packard Enterprise. <http://www.hpe.com/>

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección II (Especificaciones técnicas), el inciso c.1.10.1.f.v que el producto de tipo “router”, debe contar con al menos 1 GB de memoria flash y 2 GB de memoria RAM. Según la ficha técnica del producto “HP MSR3024” el equipo de serie, cuenta solamente con 256 MB de memoria Flash y 2 GB de memoria RAM.

#### 2.4.5 DEFICIENCIA DE MEMORIA FLASH Y MEMORIA RAM AL DISPOSITIVO DE TIPO “SWITCH” “HP 5130” PARA OFICINAS REGIONALES

Según la ficha técnica oficial del fabricante, documento anexo “HP 5130 QuickSpecs.pdf”, página 30 en el apartado “Memory and Processor”, especifica lo siguiente:

##### Figura 7 Especificaciones técnicas de switch Oficinas Regionales

**Memory and processor** 1 GB SDRAM, 512 MB flash; packet buffer size: 3 MB

Fuente: Hewlett Packard Enterprise. <http://www.hpe.com/>

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección II (Especificaciones técnicas), en los incisos c.1.9.2.e.vi y c.1.9.2.e.vii que el producto de tipo “switch”, debe contar con al menos 2 GB de memoria flash y 4 GB de memoria RAM. Según la ficha técnica del producto “HP 5130” el equipo de serie cuenta solamente con 512 MB de memoria Flash y 1 GB de memoria RAM.

#### 2.4.6 DEFICIENCIA DE MEMORIA FLASH Y MEMORIA RAM AL DISPOSITIVO DE TIPO “SWITCH” “HP 5700” PARA OFICINAS CENTRALES Y DATACENTER

Según la ficha técnica oficial del fabricante, documento anexo “HP 5700 QuickSpecs.pdf”, página 17 en el apartado “Memory and Processor”, especifica lo siguiente:

**Figura № 8**  
**Especificaciones técnicas de switch Oficinas Centrales y Datacenter**

<b>Memory and processor</b> 512 MB flash; Packet buffer size: 9 MB, 2 GB SDRAM
--

Fuente: Hewlett Packard Enterprise. <http://www.hpe.com/>

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección II (Especificaciones técnicas), en los incisos b.12.9.e.vi y b.12.9.e.vii que el producto de tipo “switch”, debe contar con al menos 2 GB de memoria flash y 4 GB de memoria RAM. Según la ficha técnica del producto “HP 5700” el equipo de serie cuenta solamente con 512 MB de memoria Flash y 2 GB de memoria RAM.

Esto refleja una debilidad en la correspondiente diligencia por parte del responsable de la validación, durante la entrega de equipo, para su aceptación, sin la debida evidencia aclaratoria en los subsanes u otros documentos aportados por el departamento.

En general, una capacidad menor en memoria RAM puede implicar que el rendimiento de los servicios de procesamiento de los servidores se vea impactado negativamente en lapsos de alta demanda por parte de los usuarios en la que el faltante afecte directamente la calidad del servicio; además, una capacidad menor de memoria Flash puede implicar que la configuración base y el sistema operativo gestor de los activos tecnológicos no funcionen debidamente cuando una actualización importante y de gran tamaño se instale, o que se pierda información o se sobrescriba cuando el equipo se quede sin capacidad de almacenamiento.

#### 2.5.- HALLAZGO 5 INCUMPLIMIENTO EN LA REVISIÓN DEL ESTADO DE SALUD DE LA CENTRAL TELEFÓNICA IP Y ADMINISTRACIÓN Y GESTIÓN DE LAS OPERACIONES DE MANTENIMIENTO DIARIO DE CONFIGURACIÓN DEL SERVICIO DE TELEFONÍA IP

Por medio de una sesión de trabajo de verificación de supervisión de servicios con el consorcio adjudicado, el representante del equipo encargado del

servicio de telefonía IP confirmó que no se realizan actividades más allá de la actualización periódica de los dispositivos involucrados en dicho servicio y la resolución de solicitudes de asistencia tramitadas a través de la mesa de ayuda.

El consorcio adjudicatario, a pesar de contar con una herramienta de gestión y monitoreo de la plataforma de telefonía IP, no realiza las actividades diarias de mantenimiento diario de dicha plataforma.

Esto puede provocar que el servicio de telefonía IP implementado se degrade debido a alertas o errores no visualizadas por parte del consorcio responsable, afectando las comunicaciones telefónicas de los funcionarios de la DGAC en todas sus sedes.

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección III “Condiciones específicas”, el inciso 7.i y 7.iii, que el adjudicatario debe administrar y gestionar las operaciones de mantenimiento diario de la configuración del servicio de telefonía IP y realizar revisiones del estado de salud de la central telefónica IP.

**2.6.- HALLAZGO 6 CAÍDA EN LA DISPONIBILIDAD DEL EQUIPO UBICADO EN EL CENTRO DE DATOS PRINCIPAL REDUJO EL PORCENTAJE DE DISPONIBILIDAD DEL SERVICIO ADMINISTRADO DEL CENTRO DE DATOS CORRESPONDIENTE AL MES DE MAYO DEL 2019 POR ABAJO DEL PORCENTAJE MÍNIMO SOLICITADO**

Por medio de una revisión de los reportes mensuales correspondientes a los servicios brindados por el consorcio, se validó el nivel de disponibilidad de la plataforma tecnológica en el centro de datos principal.

Se identificó que, en el día 30 de mayo del 2019, hubo una falla en el sistema de aire acondicionado de la *suite* en la que se ubica el equipo del centro de datos principal en Codisa, la cual generó un sobrecalentamiento en los equipos resultando en un apagado automático a las 5:17 a.m.; una vez resuelto el problema, dichos equipos no fueron encendidos en su totalidad hasta las 8:40 a.m.

Esta afectación provocó que los sistemas y servicios dependientes de la plataforma tecnológica del centro de datos no estuvieran disponibles para los funcionarios de la DGAC en todas sus sedes por 3 horas y 23 minutos

aproximadamente, lo cual pudo haber impactado las funciones Institucionales directa o indirectamente.

La pérdida de la plataforma tecnológica del centro de datos principal puede materializar la falta de disponibilidad para atender los requerimientos funcionales y estratégicos de la Institución, pérdida de información, datos erróneos o desactualizados, o retrasos en la entrega de servicios, lo que puede generar daños tanto en imagen Institucional, confianza en los procesos y la materialización de penalizaciones económicas, entre otros.

Se realiza además un cálculo de disponibilidad para el mes correspondiente y se determinó una disponibilidad de aproximadamente 99.535%. Sobre esta alerta, en el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección III "*Condiciones específicas*", inciso 9.b, que la disponibilidad mensual del servicio administrado de centro de datos debe ser de un 99.9% mensual, correspondientes a solo 43 minutos de baja mensuales como máximo.

### **2.7.- HALLAZGO 7 NO EJECUCIÓN DE MULTA POR INCUMPLIMIENTO EN EL NIVEL DEL SERVICIO ADMINISTRADO DEL CENTRO DE DATOS CORRESPONDIENTE AL MES DE MAYO DEL 2019**

Por medio de una revisión de los reportes mensuales correspondientes a los servicios brindados por el consorcio adjudicatario y las facturas y desembolsos correspondientes al servicio, se validó si se realizó una penalización por el incumplimiento del nivel de servicio de la caída del centro de datos descrita en el hallazgo anterior.

De esta revisión, no se encontró evidencia de un trámite de multa correspondiente al incumplimiento de la disponibilidad del servicio administrado de centro de datos, el cual está definido a nivel cartelario.

El departamento de Tecnologías de Información no verificó el cumplimiento de los acuerdos de nivel de servicio correspondientes, con base en el reporte mensual suministrado por el consorcio adjudicatario, para validar la entrega de los servicios administrados contratados

Esto implicó que la Dirección General de Aviación Civil desembolsó la totalidad del monto correspondiente a la cuota mensual del servicio proporcionado, aun cuando el consorcio adjudicatario no cumplió a cabalidad con la disponibilidad del servicio de centro de datos, resultando en la omisión de la multa

correspondiente. Esta materialización de riesgo hace que se pierda la noción del servicio brindado y el desembolso de recursos económicos por un servicio deficiente.

En el cartel de contratación 2018CD-000080-0006600001, se especifica en la sección III "Condiciones específicas", el inciso 9.d.ii que el no cumplimiento de la disponibilidad mensual de un 99.9% del servicio administrado de centro de datos implica una multa del 5% de la cuota mensual, equivalente a \$4 666,56 dólares de los Estados Unidos.

## **2.8.- HALLAZGO 8 RIESGOS PARA LA FINALIZACIÓN DE LOS SERVICIOS**

Según la cláusula 10: *Finalización de los servicios* de la tercera parte: *Condiciones Específicas* del cartel de licitación:

*"Seis meses antes de finalizar el plazo del contrato, la DGAC notificará al contratista si amplía el plazo o finiquita el contrato.*

*En caso de no continuar con el servicio, el contratista:*

- Debe entregar copia de la información, copia de las máquinas virtuales y resumen de la configuración del ambiente productivo a nivel de comunicaciones y centro de datos en un plazo de una semana calendario al nuevo contratista seleccionado por la administración.*
- Eliminará toda la información que sea propiedad de la DGAC, incluyendo el formateo a bajo nivel de los medios de almacenamiento, tareas a realizar previa autorización por escrito y constatada por parte de la Unidad de Tecnologías de Información de la DGAC, una vez comprobado el pase de información a la nueva plataforma."*

En reunión de trabajo con el contratista, se aclaró que el cartel de licitación no estableció requerimientos relacionados con la implementación y puesta en producción de un nuevo centro de datos con un contratista diferente; además, los activos tecnológicos son propiedad del consorcio, incluyendo el equipo instalado en las sedes regionales, y que estos equipos no serán entregados a la DGAC al finalizar los servicios.

También existe la incertidumbre de si se finaliza el contrato, exista la obligación de indemnizar al Consorcio por los meses que no se ejecuten de cara a la ampliación del contrato que se encuentre vigente.

Esto expone que la Administración no contó con el asesoramiento o el criterio experto para definir las condiciones adecuadas para finalizar el contrato, velando por los intereses de la Institución y del interés público a la inversión realizada.

Esto representa esfuerzos importantes para establecer una estrategia de finalización de contrato e implementación de un nuevo centro de datos, ya que implica además la preparación e instalación del equipo necesario para la comunicación, redes de datos, seguridad, procesamiento y almacenamiento, tanto en oficinas centrales como sedes regionales, y esta estrategia debe estar lista seis meses antes de finalizar los servicios.

Esta condición puede generar riesgos de no contar con un centro de datos suficiente y en un tiempo prudente para finalizar el contrato con el Consorcio, además de incrementar la inversión necesaria (ya sea por compra de equipo o por contratación por licitación pública) para mantener la plataforma tecnológica y de comunicaciones en condiciones óptimas (o suficientes, de ser el caso), y por tanto la Institución no tenga la plataforma necesaria para realizar sus funciones efectiva y eficientemente.

### **2.9.- HALLAZGO 9 RIESGOS ASOCIADOS A LA GESTIÓN DEL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y LA OPERACIÓN Y FUNCIONAMIENTO DEL CENTRO DE DATOS DE DGAC**

Con base en el estándar ISO 27001:2013 y el marco de COBIT 5, se identificaron riesgos asociados con la gestión del área de Tecnologías de Información institucional; y con base en los criterios de riesgo del Anexo 6: “*Metodología de Gestión de Riesgo según SEVRI del Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) de la DGAC*”, y en conjunto con el personal de TI institucional, se validaron y cuantificaron los riesgos inventariados, basados además en la percepción del personal de la Unidad de Informática.

A continuación, se listan los riesgos vinculantes a la gestión de TI institucional, separados por riesgos *aceptados* y *no aceptados*, y agrupados por rango de aceptabilidad, tipo e identificación:

**Tabla No No 2**  
**Riesgos no aceptados identificados de la gestión de TI de la DGAC**

**Riesgos no aceptados:**

<b>Riesgos Altos</b>	<b>Categoría</b>	<b>Probabilidad</b>	<b>Magnitud</b>	<b>Criticidad</b>
Falta de respaldo Institucional a la función de TI	Entorno	5	5	25
Disponibilidad insuficiente del personal para atender las necesidades Institucionales	Proceso	5	5	25
Recursos materiales (equipo, infraestructura, herramientas, transporte, entre otros) insuficientes para atender las necesidades Institucionales	Proceso	5	5	25
Fuga del personal	Proceso	5	4	20
Personal Institucional insuficiente para atender los servicios de TI	Proceso	5	4	20
Adquisición o desarrollo de tecnología sin la participación de TI	Proceso	4	4	16
Nivel de especialización insuficiente para atender los servicios de TI	Proceso	4	4	16
<b>Riesgos Serios</b>	<b>Categoría</b>	<b>Probabilidad</b>	<b>Magnitud</b>	<b>Criticidad</b>
No acceso a infraestructura del centro de datos por fallas en servidores	Proceso	3	4	12
Accesos no autorizados por falta de seguridad lógica en el perímetro externo	Proceso	3	4	12
Debilidades en el monitoreo de la plataforma tecnológica	Información para la toma de decisiones	3	4	12
Fallas en el diseño y requisitos de la plataforma tecnológica	Proceso	3	4	12
Capacidad para la atención de usuarios insuficiente	Proceso	3	4	12
Capacidad de la contraparte técnica insuficiente	Proceso	3	4	12
Debilidades con la ejecución de tareas críticas de TIC soportadas por terceros	Proceso	3	4	12
Cambios en el alcance del servicio / prioridades Institucionales	Entorno	3	4	12
Insatisfacción de los usuarios por el servicio brindado	Entorno	3	4	12

Pérdida de servicios en la infraestructura de sistemas por modificaciones/actualizaciones a la plataforma tecnológica	Proceso	2	5	10
---	---------	---	---	----

**Fuente:** elaboración propia con insumos de la Unidad de Informática de la DGAC.

**Tabla No 3**  
**Riesgos aceptados identificados de la gestión de TI de la DGAC**

**Riesgos aceptados:**

<b>Riesgos Moderados</b>	<b>Categoría</b>	<b>Probabilidad</b>	<b>Magnitud</b>	<b>Criticidad</b>
Infraestructura tecnológica insuficiente	Proceso	3	3	9
Debilidades en la adquisición de insumos para la evaluación de la ejecución del servicio asociado	Información para la toma de decisiones	3	3	9
Incumplimiento de los lineamientos establecidos a nivel contractual	Entorno	3	3	9
Capacidad de gestión del servicio insuficiente	Proceso	3	3	9
Entrega tardía de servicios y/o productos	Proceso	3	3	9
Debilidades para la autenticación de programas / instalación de equipo ilegal	Proceso	3	3	9
Capacitaciones insuficientes	Proceso	3	3	9
Defectos o incidentes reportados del sistema desatendidos	Proceso	2	4	8
No acceso a infraestructura del centro de datos debido a fallas en enlaces de comunicación	Proceso	2	4	8
No acceso a infraestructura del centro de datos por fallas en el equipo perimetral de seguridad	Proceso	2	4	8
Fallas en la plataforma de virtualización y ambientes	Proceso	2	4	8
Fallas en la Plataforma Tecnológica que soporta los activos de apoyo Institucional (fuera del centro de datos)	Proceso	2	4	8
Falla de los equipos para usuarios finales	Proceso	2	4	8
Incompatibilidad tecnológica con la plataforma Institucional	Proceso	2	3	6
Interrupciones en el uso de la plataforma	Proceso	2	3	6

Riesgos Moderados	Categoría	Probabilidad	Magnitud	Criticidad
Información incompleta o errónea para realizar las labores Institucionales	Información para la toma de decisiones	2	3	6
Atraso en el procesamiento de la información en los sistemas	Proceso	2	3	6
No contar con la información precisa, oportuna y correcta	Información para la toma de decisiones	2	3	6
Fallas en la continuidad y seguridad del servicio	Proceso	2	3	6
Fallas en la plataforma de seguridad física	Proceso	2	3	6
Pérdida de información irrecuperable	Información para la toma de decisiones	2	3	6
Gestión insuficiente de respaldos	Proceso	2	3	6
Ausencia de seguimiento oportuno del cumplimiento contractual	Gestión de proyectos	2	3	6
Carencia de información adecuada para el proceso de Mantenimiento	Proceso	2	3	6
Incumplimiento de Acuerdos de Nivel de Servicio (SLAs)	Proceso	2	3	6
Cancelación del contrato	Entorno	2	3	6
Renuncia del contratista	Proceso	1	5	5
Riesgos Bajos	Categoría	Probabilidad	Magnitud	Criticidad
Falla en los equipos de la plataforma de VoIP	Proceso	2	2	4
Fallas en la plataforma de seguridad lógica	Proceso	2	2	4
Pérdida de competitividad	Entorno	2	2	4
Obsolescencia tecnológica	Proceso	2	2	4
Cambios en el Marco Jurídico externo vigente	Entorno	1	4	4
Recursos presupuestarios insuficientes	Proceso	1	3	3
Cambios en el Marco Normativo interno vigente	Entorno	1	3	3
Brechas de cumplimiento normativo/jurídico	Entorno	1	3	3

Fuente: elaboración propia con insumos de la Unidad de Informática de la DGAC.

Del ejercicio que se realizó, el personal del área de Tecnologías de Información de la DGAC no cuantificó los siguientes riesgos, con su respectiva justificante:

**Tabla No 4**  
**Riesgos no cuantificados**

Riesgo	Categoría	Observaciones
Falta de experiencia del equipo responsable del servicio	Proceso	Dificultades para medir el nivel de experiencia
Desatención de recomendaciones de mejora	Proceso	No hay apertura para la propuesta de mejoras
Inadecuado mantenimiento preventivo	Proceso	Medición del nivel de disponibilidad y calidad del servicio
Incumplimiento de las expectativas del proyecto	Entorno	Expectativas regidas por la Administración Superior

**Fuente:** elaboración propia con insumos de la Unidad de Informática de la DGAC.

Del análisis anterior, se desprenden los siguientes riesgos potenciales no aceptados que son vinculantes a la operación y funcionamiento del centro de datos de la DGAC:

**Tabla No 5**  
**Riesgos identificados de la gestión del Centro de Datos objeto del estudio**

	Riesgos	Categoría	Probabilidad	Magnitud	Criticidad	Tipo de Aceptabilidad
1	Falta de respaldo Institucional a la función de TI	Entorno	5	5	25	Alto
2	Recursos materiales (equipo, infraestructura, herramientas, transporte, entre otros) insuficientes para atender las necesidades Institucionales	Proceso	5	5	25	Alto
3	Disponibilidad insuficiente del personal para atender las necesidades Institucionales	Proceso	5	5	25	Alto
4	Fuga del personal	Proceso	5	4	20	Alto
5	Personal Institucional insuficiente para atender los servicios de TI	Proceso	5	4	20	Alto
6	Nivel de especialización insuficiente para atender los servicios de TI	Proceso	4	4	16	Alto

	Riesgos	Categoría	Probabilidad	Magnitud	Criticidad	Tipo de Aceptabilidad
7	Adquisición o desarrollo de tecnología sin la participación de TI	Proceso	4	4	16	Alto
8	No acceso a infraestructura del centro de datos por fallas en servidores	Proceso	3	4	12	Serio
9	Accesos no autorizados por falta de seguridad lógica en el perímetro externo	Proceso	3	4	12	Serio
10	Debilidades en el monitoreo de la plataforma tecnológica	Información para la toma de decisiones	3	4	12	Serio
11	Fallas en el diseño y requisitos de la plataforma tecnológica	Proceso	3	4	12	Serio
12	Capacidad para la atención de usuarios insuficiente	Proceso	3	4	12	Serio
13	Capacidad de la contraparte técnica insuficiente	Proceso	3	4	12	Serio
14	Debilidades con la ejecución de tareas críticas de TIC soportadas por terceros	Proceso	3	4	12	Serio
15	Cambios en el alcance del servicio / prioridades Institucionales	Entorno	3	4	12	Serio
16	Insatisfacción de los usuarios por el servicio brindado	Entorno	3	4	12	Serio
17	Pérdida de servicios en la infraestructura de sistemas por modificaciones/actualizaciones a la plataforma tecnológica	Proceso	2	5	10	Serio

**Fuente:** elaboración propia con insumos de la Unidad de Informática de la DGAC.

La Unidad de Tecnologías de Información de la DGAC no cuenta con un inventario de riesgos asociados a la gestión de TI Institucional, por lo que se implementó un instrumento propio del equipo ejecutor de este estudio para realizar la evaluación de los mismos, con base en la metodología de gestión de riesgos del PETIC.

Estos riesgos no se encuentran documentados como parte del alcance de revisión y control del Sistema Estratégico de Valoración del Riesgo Institucional (SEVRI), lo que denota una gestión débil de riesgos vinculantes a la gestión de TI.

Su falta de gestión puede materializar impactos catastróficos para la DGAC en temas de eficiencia y efectividad, confianza en los procesos y la plataforma tecnológica, y en el cumplimiento de la correcta rendición de cuentas, alineada con los requerimientos relacionados del sistema público costarricense.

Los resultados anteriores se cuantificaron a partir de los criterios definidos como parte de la metodología de riesgos definida en el anexo 6 del PETIC, desarrollado por el personal Unidad de Tecnologías de Información, los cuales se detallan a continuación:

***Estructura de Riesgos***

*La identificación de riesgos del SEVRI, [es] realizada utilizando las siguientes categorías para la estructura de riesgos:*

***Entorno:*** *desastres naturales, decisiones políticas o gubernamentales, disponibilidad de capital o recursos, energía, legal y fiscal, entorno económico - social, regulación y sensibilidad.*

***Proceso:*** *acceso, autoridad, capital de conocimiento, credibilidad, fraude, infraestructura, liderazgo, liquidez, operación, oportunidad, recursos humanos, reputación, salud ocupacional, satisfacción al usuario, uso no autorizado.*

***Información para la toma de decisiones:*** *alineación con la estrategia, asignación de recursos, contingencia, disponibilidad de información, enlaces de comunicación, evaluación del entorno, medición de resultados y veracidad de información.*

***Gestión de Proyectos:*** *afectación de servicios públicos, aplicación de metodologías de desarrollo, condiciones de calidad, cultura informática (TI), dirección del proyecto, diseño del proyecto, estudios requeridos, fiscalización y supervisión de proyectos, gestión de adquisición del derecho de vía, gestión de interesados, gestión de proyectos, infraestructura tecnológica (TI),*

**INFORME AI-14-2019**

*interpretación de los términos del proyecto (TI), mejores prácticas, modificaciones en alcance, tiempo, costo y calidad (TI), obligaciones del contratista, permisos requeridos, proceso de planeación de proyectos, quiebra del proveedor (TI), requerimientos incompletos (TI), resistencia al cambio (TI), rotación de recursos humanos (TI), soporte de atención (TI) y vinculación entre diferentes sistemas (TI).*

Asimismo, se establecen los siguientes criterios:

**Criterios de probabilidad**

CRITERIOS DE PROBABILIDAD	N°	Categoría	Descripción
	5	Constante	Se espera que se presente reiteradamente
	4	Probable	Se espera que ocurra en la mayoría de las circunstancias
	3	Ocasional	Se espera que ocurra en algunos casos
	2	Inusual	Aunque no se espera que suceda, puede ocurrir en algún momento
	1	Remoto	Puede ocurrir sólo en circunstancias excepcionales

**Criterios de magnitud**

Criterio de Magnitud	No.	Categoría	Descripción
	5	Catastrófico	Impactos de orden Financiero y de Vidas humanas en Seguridad Aeronáutica como de Proyectos de Infraestructura, que resulten DESASTROSOS
	4	Mayor	Impactos de orden Financiero y de Vidas humanas en Seguridad Aeronáutica como de Proyectos de Infraestructura, que resulten SIGNIFICATIVOS
	3	Moderado	Impactos de orden Financiero y de Vidas humanas en Seguridad Aeronáutica como de Proyectos de Infraestructura, que resulten CONSIDERABLES
	2	Menor	Impactos de orden Financiero y de Vidas humanas en Seguridad Aeronáutica como de Proyectos de Infraestructura, que resulten BAJOS
	1	Insignificante	Impactos de orden Financiero y de Vidas humanas en Seguridad Aeronáutica como de Proyectos de Infraestructura, que resulten MÍNIMOS

**Parámetros de aceptabilidad**

El nivel de riesgo se determinará valorando con estimaciones la probabilidad de ocurrencia y la magnitud de la consecuencia esperada de los eventos que conforman los riesgos, con base en los siguientes parámetros:

- *Serán considerados aceptables los riesgos que han sido calificados con un nivel de Bajo (rango de 1 - 4) y Moderado (rango de 5 - 9).*
- *No podrá considerarse aceptables los riesgos que han sido calificados con un nivel Serio (rango 10 - 15) y Alto (rango 16 - 25).*

Los rangos de aceptabilidad del riesgo se observan en la siguiente tabla:

**Rangos de Aceptabilidad de Riesgos**

Rango de aceptabilidad	Tipo	Identificación
16 - 25	Alto	
10 - 15	Serio	
5 - 9	Moderado	
1 - 4	Bajo	

**2.10.- HALLAZGO 10 CONTROL INTERNO INSUFICIENTE PARA MITIGAR LOS RIESGOS IDENTIFICADOS PARA LA GESTIÓN DEL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y LA OPERACIÓN Y FUNCIONAMIENTO DEL CENTRO DE DATOS DE DGAC.**

Con base en el estándar COSO del ISACA, y en conjunto con el personal de la Unidad de Informática de la DGAC, se realizó una evaluación de los Controles Internos de Gestión de TI; estos controles fueron calificados a percepción del personal de la unidad.

De acuerdo con el análisis de resultados de la valoración de control interno, se concluye que el SCI tiene un nivel "En Proceso", lo que significa que el área de Tecnologías de Información de la DGAC se encuentra en una etapa transitoria inicial entre ser una unidad reactiva ante necesidades de la Institución, a desarrollar instrumentos de gestión y procedimientos formales para la atención ordenada de requerimientos en temas tecnológicos.

Es importante recalcar que esta etapa inicial no significa que el área de Tecnologías de Información está en un proceso de transformación para ser una

unidad de gestión efectiva, sino que está integrando los controles y adoptando prácticas suficientes para responder correctamente ante requerimientos de la Institución.

A continuación, se describen los principales hallazgos identificados con la ejecución del estudio de Control Interno por componente, para la gestión de TI Institucional:

### **Entorno de control**

- a. Tiene debilidades sustantivas con respecto a la gestión de activos tecnológicos, relaciones con terceros, documentación de controles generales y en un marco normativo formal interno de TI.
- b. Tiene debilidades graves en temas de conflictos de intereses, un plan global de seguridad en TI, política de software seguro, y estructura organizacional.

### **Evaluación de riesgos**

- a. Tiene debilidades sustantivas en identificación y análisis de riesgos.
- b. No cuenta con un Plan de Continuidad de Negocio.

### **Actividades de Control – Seguridad de los Sistemas de Información**

- a. Tiene debilidades en temas de gestión de usuarios (creación, deshabilitación y eliminación).
- b. Tiene debilidades en el uso de canales formales de atención de incidentes (mesa de ayuda).
- c. Tiene debilidades sustantivas en adopción de mejores prácticas en seguridad y en evaluación de la efectividad de los controles.
- d. Tiene debilidades graves en la creación de perfiles de usuarios en los sistemas.
- e. No cuenta con controles relacionados con la gestión de la seguridad, segregación de funciones, certificaciones, pistas de auditoría, marco normativo, custodia de activos o desarrollo y control de planes de Contingencia.

### **Actividades de Control – Administración de Cambios**

- a. Tiene debilidades en la gestión y fiscalización de la administración de cambios, trazabilidad y seguimientos con usuarios.

- b. Tiene debilidades sustantivas en el control de cambios implementados y actualización documental.
- c. No cuenta con lineamientos para cambios de emergencia o lineamientos de desarrollo seguro.

### Actividades de Control – Desarrollo de Sistemas

- a. Tiene debilidades con respecto a requerimientos de desarrollo, integración de componentes de seguridad, cumplimiento de requerimientos funcionales, gobierno de los sistemas, actualizaciones y seguimiento con usuarios.
- b. No cuenta con controles de gestión de especificaciones técnicas o funcionales, aseguramiento de la calidad ni planes ordenados de desarrollo, pruebas, liberación y mantenimiento de sistemas.

### Información y Comunicación

- a. No cuenta con estrategias de divulgación y comunicación de normativas internas de TI, clasificación de información ni canales de comunicación entre usuarios y el área para incidentes de fraude.

### Supervisión y monitoreo

- a. No se cuenta con controles para la atención de recomendaciones de auditoría.

A continuación, se presentan las debilidades de control interno relevantes relacionados con la gestión del Centro de Datos Institucional:

**Tabla Nº 6**  
**Valoración de Riesgos y Controles Internos**

Debilidad en Control Interno	Riesgo Asociado	Criterio
Debilidades con respecto a la validación de la entrega de servicios tecnológicos con terceros, donde se definan las directrices con relación a los acuerdos de niveles de servicio, el seguimiento y la evaluación de los proveedores.	No acceso a infraestructura del centro de datos por fallas en servidores	El control se mantiene implementado y en ejecución en casos excepcionales
Falta de seguimiento oportuno y efectivo de la política de administración y control de cambios	Pérdida de servicios en la infraestructura de sistemas por	El control se mantiene implementado y en

**INFORME AI-14-2019**

Debilidad en Control Interno	Riesgo Asociado	Criterio
	modificaciones/actualizaciones a la plataforma tecnológica	ejecución en caso importantes
No se certifica la política de acceso lógico para el ingreso a los sistemas de información y la configuración, alineado a estándares de buenas prácticas	Accesos no autorizados por falta de seguridad lógica en el perímetro externo	El control se mantiene implementado y en ejecución en casos excepcionales
No se realizan actividades de certificación continua relacionadas con la implementación de la seguridad de la información	Debilidades en el monitoreo de la plataforma tecnológica	El control se mantiene implementado y en ejecución en casos excepcionales
No se asegura que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable	Fallas en el diseño y requisitos de la plataforma tecnológica	El control se mantiene implementado y en ejecución en caso importantes
La estructura organizacional del área de T.I. no es suficientemente robusta para atender las necesidades del negocio	Capacidad para la atención de usuarios insuficiente	El control existe pero no se ejecuta
El personal del área de T.I. tiene brechas relacionadas con la experiencia y habilidades necesarias para realizar su trabajo	Capacidad de la contraparte técnica insuficiente	El control se mantiene implementado y en ejecución en la mayoría de los casos
No se dispone de un procedimiento robusto de contratación de servicios tecnológicos con terceros, donde se definan las directrices con relación a los acuerdos de niveles de servicio, el seguimiento y la evaluación de los proveedores	Debilidades con la ejecución de tareas críticas de TIC soportadas por terceros	El control se mantiene implementado y en ejecución en casos excepcionales
No se cuenta con manuales, normas, políticas o procedimientos efectivos para el proceso de Gestión de T.I.	Adquisición o desarrollo de tecnología sin la participación de TI	El control se mantiene implementado y en ejecución en casos excepcionales
No se cuenta con un Plan Estratégico de TI debidamente alineado con el de la organización	Cambios en el alcance del servicio / prioridades Institucionales	El control se mantiene implementado y en ejecución en caso importantes
La estructura organizacional del área de T.I. no es suficientemente robusta para atender las necesidades del negocio	Insatisfacción de los usuarios por el servicio brindado	El control existe pero no se ejecuta
La organización no cuenta con un Plan de Continuidad de Negocio que incluya el plan de contingencia ante no disponibilidad de servicios de T.I.	Personal Institucional insuficiente para atender los servicios de TI	No existe el control

Debilidad en Control Interno	Riesgo Asociado	Criterio
El personal del área de T.I. tiene brechas relacionadas con la experiencia y habilidades necesarias para realizar su trabajo	Nivel de especialización insuficiente para atender los servicios de TI	El control se mantiene implementado y en ejecución en la mayoría de los casos
La estructura organizacional del área de T.I. no es suficientemente robusta para atender las necesidades del negocio	Disponibilidad insuficiente del personal para atender las necesidades Institucionales	El control existe pero no se ejecuta
No se realizan análisis de impacto, justificación costo/beneficio y administración de requerimientos en toda la plataforma de sistemas de la Institución	Recursos materiales (equipo, infraestructura, herramientas, transporte, entre otros) insuficientes para atender las necesidades Institucionales	El control se mantiene implementado y en ejecución en caso importantes
No están definidos los principios y valores que incluya el tratamiento de conflictos de interés y de seguridad de la información en el proceso de Gestión de T.I.	Fuga del personal	El control existe pero no se ejecuta
No se cuenta con manuales, normas, políticas o procedimientos efectivos para el proceso de Gestión de T.I.	Falta de respaldo Institucional a la función de TI	El control se mantiene implementado y en ejecución en casos excepcionales

**Fuente:** elaboración propia con insumos de la Unidad de Informática de la DGAC.

Estos controles no se ven reflejados en el Sistema propio del área, lo que denota una gestión débil del sistema de control interno vinculante a la gestión de TI.

La Unidad de Tecnologías de Información de la DGAC no cuenta con un inventario de controles internos asociados a la gestión de TI Institucional, por lo que se implementó un instrumento propio del equipo executor de este estudio para realizar la evaluación de los mismos, con base en la metodología de la iniciativa COSO del ISACA.

Las debilidades en el Sistema de Control Interno de TI hacen que la mitigación, manejo proactivo y atención de incidentes sea más compleja, costosa e ineficiente, lo que además puede impactar en los procesos, recursos, capacidades e imagen de la Institución.

Para este estudio, se establecieron los siguientes criterios de respuesta para cada elemento de control interno:

- 5: Siempre - el control se mantiene implementado y en ejecución en todo momento
- 4: Casi siempre - el control se mantiene implementado y en ejecución en la mayoría de los casos
- 3: Algunas veces - el control se mantiene implementado y en ejecución en caso importantes
- 2: Casi nunca - el control se mantiene implementado y en ejecución en casos excepcionales
- 1: Nunca - el control existe pero no se ejecuta
- 0: Ausente - No existe el control
- N/A: No aplica este control

### **2.11.- HALLAZGO 11 NIVEL DE SATISFACCIÓN DE LOS USUARIOS DE LA DGAC DE CARA A LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN**

Para identificar el nivel de satisfacción del personal de la DGAC, se realizó una encuesta por medio de entrevistas individuales a 30 personas funcionarias de la Institución, de diferentes áreas y nivel de puesto dentro del respectivo organigrama funcional.

Los funcionarios participantes de la encuesta fueron escogidos usando los siguientes criterios cualitativos:

- Capacidad de toma de decisiones en el área que representan.
- Usuario continuo de los servicios ofrecidos por el área de TI de la DGAC.
- Involucrado en proyectos de TI Institucionales.
- Con conocimiento de las funciones y sistemas que utilizan en el área de representan.
- Con capacidad de emitir un criterio sobre su percepción de la efectividad, eficiencia y satisfacción que recibe por parte de la función de TI de la DGAC.

Esta encuesta está basada en los lineamientos de gestión de Tecnologías de Información de la Norma de Control Interno para el Sector Público, Normas técnicas para la gestión y el control de las Tecnologías de Información, Marco de Gestión de Control Interno COSO, y el Marco de Gobierno de Tecnologías de Información COBIT 5.

Con base en la ejecución de la encuesta y las respuestas obtenidas, a continuación, se describen los resultados del nivel de satisfacción de los usuarios de la DGAC, de cara a los servicios de TI:

*Con respecto al soporte técnico:*

- El 67% del personal Institucional considera que no existen canales suficientes para solicitar atención por parte de TI.
- El 73% del personal Institucional considera que no puede dar su opinión para priorizar atenciones por parte de TI.
- El 63% del personal Institucional no recibe una resolución oportuna por parte de TI.
- El 77% del personal Institucional no recibe información sobre el estado de resolución de sus solicitudes.
- El 50% del personal Institucional considera que la Unidad de TI no da seguimiento o resuelve sus solicitudes completamente.
- El 67% del personal Institucional considera que el personal de TI no es suficientemente capaz o conocedor para atender incidentes.
- El 97% del personal Institucional considera que TI no es proactivo ni oportuno en reducir cantidad y severidad de incidentes.

*Con respecto a las herramientas tecnológicas disponibles:*

- El 70% del personal Institucional considera que la plataforma de sistemas de información no es suficientemente estable o rápido para hacer sus funciones.
- El 60% del personal Institucional no puede conectarse remotamente a sus sistemas.

*Con respecto a capacitaciones y entrenamientos:*

- El 63% del personal Institucional no conoce todas las funcionalidades disponibles en los sistemas para hacer su trabajo más eficientemente.
- El 53% del personal Institucional considera que las capacitaciones no se dan en condiciones adecuadas.
- El 60% del personal Institucional considera que las capacitaciones no alcanzan el resultado esperado.
- El 73% del personal Institucional considera que la documentación disponible para los sistemas es insuficiente.

*Con respecto a la ejecución de proyectos de TI:*

- El 57% del personal Institucional no se involucra en proyectos de TI.
- El 50% del personal Institucional no conoce el proceso para solicitar un requerimiento de mejora.
- El 73% del personal Institucional considera que sus requerimientos no son atendidos con los proyectos de TI.
- El 77% del personal Institucional no recibe información de seguimiento o logra resolver sus requerimientos exitosamente.
- El 83% del personal Institucional considera que no recibe soluciones de calidad.
- El 87% del personal Institucional no está satisfecho por cómo se gestionan los proyectos de TI.
- El 77% del personal Institucional considera que el personal de TI no es capaz o conocedor para ejecutar proyectos.
- El 97% del personal Institucional considera que los proyectos de TI no terminan oportunamente.

*Con respecto a la Unidad de TI en general:*

- El 83% del personal Institucional considera que el área no tiene un fuerte enfoque de servicio al cliente
- El 93% del personal Institucional considera que el área no tiene una buena dirección estratégica o está alineada con la DGAC.
- El 70% del personal Institucional no conoce en qué está trabajando el área.
- El 73% del personal Institucional no aporta sobre la dirección del área.
- El 83% del personal Institucional no considera que recibe una ventaja táctica por parte del área.
- El 87% del personal Institucional no está satisfecho con el servicio del área.
- El 77% del personal Institucional considera que TI no responde a sus necesidades.

*Con respecto a los servicios administrados de la plataforma tecnológica:*

- El 60% del personal Institucional considera que la plataforma no es eficiente.
- El 57% del personal Institucional considera que la plataforma no es estable.
- El 73% del personal Institucional considera que el equipo de soporte no atiende sus incidentes oportunamente.
- El 77% del personal Institucional considera que el equipo de soporte no resuelve sus incidentes oportunamente.
- El 73% del personal institucional considera que sus requerimientos funcionales no son atendidos con la plataforma tecnológica actual.

- El 100% del personal Institucional considera que los servicios asociados pueden mejorar.

En general, la Institución le da un promedio de 42 sobre 100 a los servicios relacionados con Tecnologías de Información:

- Soporte: 46% de satisfacción
- Herramientas tecnológicas: 58% de satisfacción
- Capacitación: 42% de satisfacción
- Gestión de proyectos: 35% de satisfacción
- TI en general: 25% de satisfacción
- Servicios administrados: 49% de satisfacción

### **III. CONCLUSIONES**

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

1. Pese a contar con lineamientos y referencias relacionadas con las prácticas comúnmente aceptadas para la debida gestión, seguimiento y control de la ejecución de proyectos, la Unidad de TI no cuenta con capacidad para llevar la debida administración del contrato y el control relacionado con los servicios administrados adquiridos **(Comentario 2.1)**.
2. Además, se han identificado brechas en la entrega de servicio por parte de Consorcio que puede impactar tanto la calidad del servicio como el cumplimiento del objeto contractual, en afectación a los intereses de la DGAC relacionados con la plataforma tecnológica **(Comentario 2.1)**.
3. A la fecha de corte de este informe, la Unidad de TI no ha podido gestionar la atención para atender las capacitaciones especializadas pendientes de cara a la transferencia de conocimiento definido a nivel carterlario, lo que puede materializar la pérdida tanto de la oportunidad de desarrollar talento como de la inversión hecha por la Institución **(Comentario 2.2)**
4. De igual forma, la Unidad de TI no ha podido gestionar junto con el contratista la resolución de cara al enlace establecido con el Aeropuerto de Limón, lo que puede implicar que la sede regional no cuente con infraestructura suficiente para soportar los servicios asociados a la DGAC de forma efectiva **(Comentario 2.3)**.
5. Se presentan debilidades en la forma en que los activos fueron recibidos y aceptados, lo que ha materializado que en la plataforma tecnológica Institucional haya equipo que no cumple con las condiciones carterlarias solicitadas en la licitación **(Comentario 2.4)**.
6. De cara al cumplimiento de los servicios administrados, el contratista ha reconocido que tiene debilidades para la revisión del estado de la central telefónica IP que debe gestionar; por otro lado, la Unidad de TI no había identificado, hasta la fecha de corte de este informe, que existía este incumplimiento **(Comentario 2.5)**.
7. La Unidad de TI ha recibido a satisfacción el 100% del servicio administrado, sin considerar que existe evidencia de incumplimiento en el mes de mayo del

2019 en temas de disponibilidad de la plataforma tecnológica, y no se ejecutaron las cláusulas contractuales relacionadas **(Comentarios 2.6 y 2.7)**.

8. Es complejo para la Institución lograr terminar el contrato de una manera eficiente con solo los términos de la licitación; requiere de un esfuerzo importante para definir una estrategia puntual, efectiva y alineada al interés de la DGAC y de la ciudadanía costarricense para realizar una transición exitosa a otro tipo de servicio de centro de datos, ya sea interno o tercerizado **(Comentario 2.8)**.
9. Como parte de este estudio, se ha ampliado el catálogo de riesgos y controles internos que la Unidad de TI gestiona a través del SEVRI y su metodología relacionada en el PETIC, lo que brinda una oportunidad de mejora de cara a la identificación, categorización y criticidad de los riesgos no solo de la plataforma tecnológica, sino de la Unidad de TI en general, así también la identificación de mejoras y oportunidades de control interno para el área **(Comentarios 2.9 y 2.10)**.
10. La Institución en general no se siente satisfecho con la plataforma tecnológica, los servicios de soporte asociados, herramientas y servicios administrados contratados; además, tienen un nivel reprobatorio con respecto a la gestión de proyectos y la gestión de la Unidad de TI, que urge al área a realizar las actividades pertinentes y dedicar los recursos necesarios al personal Institucional para brindar servicios de una manera efectiva, eficiente y con un espíritu de servicio de alto valor agregado **(Comentario 2.11)**.
11. De este estudio se expone la imperiosa necesidad de articular esfuerzos para robustecer la Unidad de Tecnologías de Información, de cara a la capacidad de gestión, atención, soporte, visión estratégica y ejecución de proyectos, entre otros aspectos, que apoye en la transformación estratégica digital de la Administración Superior y esperado por el personal Institucional **(Comentario 2.11)**.

#### **IV. RECOMENDACIONES**

##### **Al Consejo Técnico de Aviación Civil (CETAC)**

1. Aprobar el Informe y ordenar la implementación de las recomendaciones incluidas en el mismo.
2. Valorar, en conjunto con la Unidad de Tecnologías de Información, el impacto económico y material relacionado con los servicios otorgados por el consorcio que no están vinculados con las especificaciones técnicas del cartel, ya sean mejoras o incumplimientos, para definir el debido proceso a seguir para atenderlos (**Conclusiones 2 y 7**).
3. Articular los esfuerzos necesarios para robustecer el área de Tecnologías de Información Institucional para alinear los esfuerzos tácticos tecnológicos con la visión estratégica y necesidades del personal de la DGAC (**Conclusión 10**).

##### **A la Encargada de la Unidad de Tecnologías de Información**

4. Constituir y ordenar el expediente de la ejecución contractual y servicios administrados de la plataforma de TI, en apego a los lineamientos de administración, control de proyectos y gestión documental (**Conclusión 1**).
5. Implementar los lineamientos e instrumentos necesarios para el control de la ejecución del proyecto, para documentar la verificación y validación de los requerimientos (explícitos a nivel cartelario) con la entrega de valor del Consorcio (reflejada en los informes mensuales de desempeño de la plataforma tecnológica) (**Conclusiones 1 y 2**).
6. Continuar con las gestiones relacionadas con la resolución de requerimientos y especificaciones del cartel de licitación, de cara a los servicios tecnológicos brindados por el contratista (**Conclusiones 3 y 4**).
7. Realizar una revisión de los equipos que forman parte en la plataforma tecnológica y de redes, tanto en el centro de datos como en oficinas centrales y sedes regionales, para cuantificar el nivel de servicio con los activos disponibles y valorar el impacto de los equipos instalados (**Conclusión 5**).
8. Realizar una valoración sobre el costo/beneficio de mantener los activos como están ahora en contraste con su remplazo, el impacto Institucional de

las alternativas existentes y la debida gestión a la decisión a tomar **(Conclusión 5)**.

9. Definir formalmente la estrategia para la valoración de la calidad del servicio recibido, el nivel de satisfacción, pendientes y requerimientos de la plataforma tecnológica, e incorporar los lineamientos necesarios para aplicar sanciones o multas cuando aplique **(Conclusiones 6 y 7)**.
10. Establecer, con la máxima prioridad, la estrategia para la eventual finalización de los servicios contratados, y los lineamientos para la adquisición de un nuevo centro de datos, si aplica y es de interés de la Institución, ya sea por un centro de datos propio o tercerizado **(Conclusión 8)**.
11. Incorporar los riesgos y los criterios de control interno a la evaluación del SEVRI para robustecer la gestión y el gobierno de TI en general de forma eficiente y efectiva, y cuantificar su impacto, probabilidad, criticidad y estrategias de incorporación, atención y remediación **(Conclusión 9)**.
12. Generar un plan de acción para mejorar el nivel de satisfacción del personal Institucional de cara al servicio, atención, percepción y soporte de la infraestructura tecnológica, de la mano con las necesidades de la DGAC y su orientación estratégica **(Conclusiones 10 y 11)**.
13. Realizar una estrategia de revisión y actualización del PETIC en todas sus aristas, que comprenda (aunque no se limite a) los siguientes rubros:
  - a. Valoración del PEI vigente y la misión, visión y valores Institucionales para conocer la trayectoria de corto, mediano y largo plazo de la estrategia de la gestión de la Aviación Civil Costarricense.
  - b. Valoración de la estructura funcional de TI, de cara a: perfiles, responsabilidades, ámbito de acción, perfil y categoría de puesto.
  - c. Valoración de los objetivos específicos del área, alineados con los objetivos del PEI y sus métricas, para constituir un plan táctico de atención ordenado y oportuno.
  - d. Alinear las necesidades técnicas, funcionales y estratégicas de las distintas áreas de la DGAC para que se vean reflejadas como requerimientos del portafolio de proyectos Institucional.
  - e. Constituir acuerdos de nivel de servicio (SLAs) Institucionales.
  - f. Inventariar requerimientos de capacitación tanto al área como al personal Institucional.
  - g. Robustecer la metodología de proyectos, de calidad y de gestión de TI.

- h. Robustecer el marco de gobierno de TI, así como los planes de continuidad de los servicios tecnológicos. **(Conclusiones 9, 10 y 11)**

**Al encargado de la Proveduría Institucional**

- 14.** Apoyar a la Unidad de TI para preparar y validar los requerimientos y términos de referencia requeridos en caso de terminación de contrato **(Conclusión 8)**.

