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

INFORME Nº AI-12-2020

EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA DE LA DGAC

DICIEMBRE- 2020

ÍNDICE

ÍNDICE DE CUADROS Y GRÁFICOS

ABREVIATURAS

Abreviatura	Significado
CGR	Contraloría General de la República
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)
VPN	Virtual Private Network (siglas en inglés)
MOPT	Ministerio de Obras Públicas y Transporte
PETIC	Plan Estratégico de Tecnologías de Información y Comunicación
SLAs	Acuerdos de Nivel de Servicio (siglas en inglés)

RESUMEN EJECUTIVO

¿Cuál fue el objetivo del estudio?

Evaluar el estado actual de la plataforma tecnológica de la DGAC para valorar: el nivel de cumplimientos normativo que las normas de la Contraloría General de la República (CGR) exige de cara a la gestión y control de TI, la capacidad de brindar continuidad de servicios de TI, posibles brechas y oportunidades de mejora con base en prácticas comúnmente aceptadas en temas de gestión de TI, efectividad en los controles ante riesgos tecnológicos, y posibles brechas de cumplimiento normativo y mejores prácticas que impacten el uso eficiente, efectivo y económico de los recursos de TI; en apego con la condición de emergencia que impacta el país y la Institución por la pandemia COVID-19.

¿Por qué se justificó el estudio?

A raíz de la condición de emergencia sanitaria que se vive en el país y el mundo, la DGAC se vio en la necesidad de realizar sus labores sustantivas y de apoyo por medio de trabajo remoto, definido por la Gerencia y las áreas de la Institución como “trabajo en casa por emergencia”.

Por esta situación, se realizaron inversiones en materia de seguridad tecnológica y se robustecieron protocolos para facilitar el trabajo del personal Institucional desde fuera de las instalaciones físicas de la DGAC y sus sedes regionales, con un mínimo de personal operativo laborando en sitio, y con horario rotativo.

Debido a lo anterior, la Auditoría Interna decidió llevar a cabo un estudio especial con el propósito de verificar que los servicios de la DGAC se están ejecutando en apego a las prácticas esperadas en materia de continuidad, seguridad de la información, controles operativos y tecnológicos, en especial a la condición “tele trabajable”; todo en apego a la normativa que le rige.

¿Cuáles fueron los principales hallazgos?

- Falta de involucramiento de la Función de TI en la proyección tecnológica de la DGAC
- Falta de Instrumentos para la validación de entrega de servicios de TI y Acuerdos de Nivel de Servicio (SLA)
- Formalización del marco de gestión de teletrabajo
- Debilidades en la Ejecución del Marco de Gestión de TI

- Divergencia en la percepción de participación de la Auditoría Interna de la DGAC de cara a la Función de TI
- Falta de un Diagnóstico de Capacidades de TI y necesidades de la DGAC
- Debilidades en la Evaluación de riesgos y Control Interno para la Función de TI
- Falta de una visión formal de la DGAC en materia tecnológica
- Alta Dependencia con el proveedor del SIFCO

¿Qué esperamos de la Administración?

La aceptación e implementación de las recomendaciones tienen como propósito establecer la visión estratégica de la Institución en materia tecnológica, robusteciendo y formalizando una Función de TI a la altura de la DGAC en su marco de gobierno, entrega de servicio, operación, fiscalización y aporte de valor.

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 que la plataforma tecnológica de la DGAC permita mantener la continuidad del servicio, seguridad de la información, controles operativos y tecnológicos; entorno a requerimientos normativos, a la condición tele trabajable, al ámbito de acción de la DGAC y a la administración eficiente, efectiva y económica de recursos institucionales.

1.2.-JUSTIFICACIÓN

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

A raíz de la condición de emergencia sanitaria que se vive en el país y el mundo, la DGAC se vio en la necesidad de realizar sus labores sustantivas y de apoyo por medio de trabajo remoto, definido por la Gerencia y las áreas de la Institución como “trabajo en casa por emergencia”.

Por esta situación, se realizaron inversiones en materia de seguridad tecnológica y se robustecieron protocolos para facilitar el trabajo del personal Institucional desde fuera de las instalaciones físicas de la DGAC y sus sedes regionales, con un mínimo de personal operativo laborando en sitio, y con horario rotativo.

Debido a lo anterior, la Auditoría Interna decidió llevar a cabo un estudio especial con el propósito de verificar que los servicios de la DGAC se están ejecutando en apego a las prácticas esperadas en materia de continuidad, seguridad de la información, controles operativos y tecnológicos, en especial a la condición “tele trabajable”; todo en apego a la normativa que le rige.

1.3.-OBJETIVOS

1.3.1.- <u>Objetivo general</u>

Evaluar el estado actual de la plataforma tecnológica de la DGAC para valorar: el nivel de cumplimientos normativo que las normas de la Contraloría

General de la República (CGR) exige de cara a la gestión y control de TI, la capacidad de brindar continuidad de servicios de TI, posibles brechas y oportunidades de mejora con base en prácticas comúnmente aceptadas en temas de gestión de TI, efectividad en los controles ante riesgos tecnológicos, y posibles brechas de cumplimiento normativo y mejores prácticas que impacten el uso eficiente, efectivo y económico de los recursos de TI; en apego con la condición de emergencia que impacta el país y la Institución por la pandemia COVID-19.

1.3.2.- Objetivos específicos.

1. Comprobar que las acciones emprendidas por la Administración en el ámbito de tecnologías de información se realicen en apego a la normativa aplicable y la establecida por la Contraloría General de la República.

2. Comprobar que la plataforma tecnológica de la Dirección General de Aviación Civil se organice y administre en procura de mantener la continuidad de los servicios, con los mayores estándares en seguridad de la información y en alineamiento a los requerimientos tecnológicos, producto de la emergencia provocada por la Pandemia de la COVID-19; específicamente en condiciones de teletrabajo.

3. Advertir y recomendar en torno a las mejores prácticas, que, en materia de tecnología de información, corresponde se realice la gestión operativa de la Dirección General de Aviación Civil, donde se requiere alta experiencia profesional para satisfacer los requerimientos propios de su ámbito de acción.

4. Identificar, evaluar y evidenciar la efectividad de las medidas de control tomadas por la administración para mitigar los impactos por riesgos operativos y económicos, que afecten la gestión de la Dirección General de Aviación Civil en el corto y mediano plazo; todo a partir de las recomendaciones resultado de los estudios realizado por la Auditoría Interna.

5. Identificar posibles brechas en el cumplimiento de la normativa y sanas prácticas, establecidas en materia de tecnologías de información y que estén afectando el funcionamiento de la Dirección General de Aviación Civil y por ende la administración eficiente, efectiva y económica de los recursos utilizados.

6. Otros aspectos a criterio de la Auditoría Interna.

1.4.- ALCANCE

El estudio de auditoría requerido se enfocará en las acciones emprendidas por la Administración en el ámbito de tecnologías de información respecto a la adquisición y uso de la plataforma tecnológica de la DGAC, comprobar que ésta permita mantener la continuidad del servicio, seguridad de la información, controles operativos y tecnológicos; entorno a requerimientos normativos, condición tele trabajable, ámbito de acción de la DGAC y administración eficiente, efectiva y económica de recursos institucionales. Todo lo anterior, que se realicen en apego a lo establecido por la Contraloría General de la República y necesidades de la DGAC. Además de evaluar la participación y cumplimiento de la Unidad de Tecnologías de Información, así como otras coordinaciones con instancias institucionales; en el citado proceso.

El estudio rige desde el 24 de agosto del 2020, con fecha de corte hasta el 30 de octubre del 2020. Se consultó documentación generada durante el 2020 a la fecha de corte para la ejecución de los procedimientos del estudio, facilitada por la Unidad de Tecnologías de Información, la Gerencia General y la Auditoría Interna de la DGAC.

1.5.- METODOLOGÍA

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

1.6.- TIPO DE AUDITORÍA

Auditoría especial.

1.7.- NORMATIVA ADMINISTRATIVA, LEGAL Y TÉCNICA

a. Ley General de Control Interno, Nº 8292.
b. Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE)
c. Normas para el Ejercicio de la Auditoria Interna en el Sector Público, (R-DC-119-2009)[1]
d. Normas Generales de Auditoría para el Sector Público (R-DC-064-2014)[2]

[1] La Gaceta Nº 28, del 10 de febrero del 2010
[2] La Gaceta Nº 184 del 25 de setiembre del 2014, vigente a partir del 01 de enero del 2015

e. 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.
f. Control de Objetivos para Tecnologías de Información y Relacionadas (COBIT ver.5).
g. Marco de referencia para la implementación, gestión y control sistema de control interno COSO.
h. 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, Nº 8292, específicamente en los siguientes artículos:

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

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

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

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

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

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

El jerarca, los titulares subordinados y los demás funcionarios públicos también incurrirán en responsabilidad administrativa y civil, cuando corresponda, por

obstaculizar o retrasar el cumplimiento de las potestades del auditor, el subauditor y los demás funcionarios de la auditoría interna, establecidas en esta Ley.

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

1.8.- CUMPLIMIENTO CON NORMAS GENERALES DE AUDITORÍA

El estudio se ejecutó de conformidad con las "Normas Generales de Auditoría para el Sector Público" (R-DC-64-2014) y las "Normas para el Ejercicio de la Auditoría Interna en sector Público" (R-DC-119-2009).

1.9.- LIMITACIONES

a. A raíz de la emergencia nacional por el COVID-19, no se realizaron actividades presenciales. Los procedimientos de este estudio se realizaron de forma virtual por medio de reuniones de trabajo, cuestionarios digitales y el intercambio de documentos.

1.10.- GENERALIDADES DEL ESTUDIO

Con respecto a la condición de emergencia sanitaria nacional por el COVID:

a. Por la materialización de la pandemia COVID-19 que afectó al país, las instituciones públicas y privadas ejecutaron lineamientos para facilitar el trabajo remoto a personal administrativo y presencialmente no esenciales para reducir la cantidad de personas trabajando colectivamente en espacios cerrados.
b. Conforme la situación de salud escaló, las directrices de salud y de trabajo remoto se extendieron a prácticamente todo el personal que pueda realizar sus labores fuera de las instalaciones físicas de cada institución, inclusive ampliando los plazos hasta quedar sin fecha definida para el regreso a trabajo presencial.
c. Durante el tercer trimestre del año en curso, se analizaron posibilidades para realizar un retorno escalonado en instituciones públicas para personal responsable de la atención presencial de personas interesadas y usuarios de servicios específicos. Por otro lado, las instituciones también están planteando sus requerimientos y necesidades para

mantener el trabajo remoto como parte de su naturaleza funcional y operativa.

Con respecto a la condición de entrega de servicios de la DGAC a través de "trabajo en casa por emergencia":

a. La condición de trabajo remoto se dio como una orden de acatamiento obligatorio, extendida a todo el personal institucional para realizar sus labores sustantivas y de apoyo desde fuera de las instalaciones físicas de la DGAC.
b. Sin embargo, esta condición fue repentina y sin preparación previa con respecto a la capacidad técnica y operativa de la infraestructura tecnológica y de los servicios asociados.
c. El centro de procesamiento y almacenamiento de datos es operada y administrada por un proveedor externo (actualmente CODISA) al 100%, la infraestructura tecnológica estaba asegurada para ser accedida desde el exterior de las instalaciones físicas.
d. Por otro lado, no era de conocimiento de la Unidad de Tecnologías de Información o de la Gerencia General si la plataforma funcionase de forma óptima y segura con el personal trabajando remotamente. Se realizaron inversiones "de emergencia" para solventar las necesidades de seguridad por medio de una contratación de equipos físicos de filtrado y control de acceso, robustecimiento de las capacidades de seguridad del "firewall" del centro de datos y conexiones por medio de redes privadas virtuales (o *VPN* por sus siglas en inglés).
e. También, a raíz del cierre de los servicios aeroportuarios para pasajeros y servicios de turismo, los ingresos de la Institución fueron impactados severamente, lo que además restringe la capacidad presupuestaria y visión de inversión tecnológica, además de acatar las restricciones que las leyes vinculantes a la restricción del gasto y optimización del aparato estatal e instituciones descentralizadas, que ahora son de carácter obligatorio.

Con respecto a la Función de Tecnologías de Información:

a. Desde la emisión del informe AI-14-2019, "Evaluación del centro de datos principal y Servicios asociados implementado en la Dirección General de Aviación Civil" de noviembre del 2019, la Gerencia General se ha involucrado más con la Función de Tecnologías de Información. Al momento de cierre de este informe, la Gerencial General estaba involucrada con la Unidad de TI del MOPT para validar tanto la definición

de PETIC para la DGAC como su estructura organizacional para la Función de TI.

b. De cara a la Función de TI, se identifican los siguientes elementos críticos para la Institución:
    a. Se espera que la DGAC forme parte de la estructura funcional del MOPT, incluyendo la Unidad de Tecnologías de Información, lo que significa la homologación e integración de la Unidad entre instituciones.
    b. El PETIC de la DGAC cumple su ciclo a finales del 2020; la Unidad de TI había planificado el desarrollo del nuevo plan actualizado durante el año en curso, pero el presupuesto no fue aprobado para ejecutar tal proyecto, además de no haber certidumbre de si se puede ejecutar durante el 2021.
        i. Como directriz, la Unidad de TI de la DGAC está trabajando en terminar los proyectos definidos en el PETIC 2016 – 2020, esperando instrucciones de la Administración Superior sobre los siguientes pasos para el 2021 y años subsecuentes, sin un PETIC vigente.
    c. Durante la segunda mitad del año en curso, la Unidad de TI ejecutó un proyecto de actualización y robustecimiento del marco de gobierno y gestión de TI por medio de una contratación de servicios especializados. Al momento de cierre de este estudio, el marco de gobierno (incluyendo políticas y lineamientos) estaba por concluir, quedando pendiente todo el trabajo de presentación y oficialización.
    d. Queda pendiente la propuesta de una contratación del Centro de Procesamiento y Almacenamiento de Datos para la Institución que sea administrado por un tercero, que sirva para reemplazar el contrato vigente con CODISA.
    e. También se requiere contemplar la necesidad técnica y funcional para integrar las iniciativas de sistemas de información que el Ministerio de Hacienda y Presupuesto Nacional están desarrollando, puntualmente el sistema Integra2 para planillas y el SIGAF para ejecución presupuestaria. Al momento de cierre de este estudio, no se cuenta con un pronunciamiento formal de las instituciones responsables sobre el alcance técnico y funcional o requerimientos de integración e información que estos sistemas necesitan por parte de la DGAC.

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 20 de enero del año en curso se remitió nota 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 en forma virtual el 28 de enero, con la participación, por parte de la Administración de:

Sr. Gonzalo Gerardo Coto Fernández, Director CETAC
Sr. Álvaro Vargas Segura, Director General de Aviación Civil
Sra. Cindy Coto Calvo, Directora Despacho de la DGAC
Sra. Malou Guzmán Quesada, Jefe Tecnología de Información

Durante ese ejercicio se formularon algunas observaciones al contenido del informe, de las cuales, cuando se consideró necesario, se llevaron a cabo las adecuaciones requeridas.

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 FALTA DE INVOLUCRAMIENTO DE LA FUNCIÓN DE TI EN LA PROYECCIÓN TECNOLÓGICA DE LA DGAC

La Gerencia General de la DGAC está trabajando en conjunto con la Unidad de Tecnologías de Información del MOPT (a manera de colaboración interinstitucional) para diagnosticar los lineamientos del PETIC y la estructura organizacional de la Función de TI institucional; sin embargo, esta colaboración entre el MOPT y la Gerencia General deja por fuera la participación de la Función de Tecnologías de Información Institucional, donde el personal de TI institucional no está colaborando activa y proactivamente en la definición de su marco estratégico y su estructura organizacional, ni está realimentando sobre la realidad técnica y funcional de la infraestructura tecnológica y las necesidades internas que la Función ha identificado para mejorar su nivel servicio y participación estratégica.

Esta condición se materializa por la falta de una Unidad de Tecnologías de Información funcional y estratégicamente eficiente, además que no se cuentan con insumos para certificar el nivel de atención y entrega de servicios de TI, o si cumple con las necesidades de las diferentes áreas de la Institución.

Esta condición puede materializar una Función deficiente de TI desde la perspectiva de su gobierno y estructura organizacional, al ser justificada con criterios generales de una unidad externa a la DGAC y que puede dejar excluido particularidades que pueden impactar la entrega óptima de servicios de TI por condiciones no gestionadas.

También puede materializar la fuga de talento humano al crear un ambiente laboral de incertidumbre y desconfianza, además de generar resistencia ante una transformación de la Función de TI vista como impuesta por externos.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, en el Capítulo II: *Planificación y organización*, definen:

> *"2.1 Independencia y recurso humano de la Función de TI*
>
> *El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.*
>
> *Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones."*

2.2.- FALTA DE INSTRUMENTOS PARA LA VALIDACIÓN DE ENTREGA DE SERVICIOS DE TI Y ACUERDOS DE NIVEL DE SERVICIO (SLA)

Al momento de desarrollar este informe, como parte de la ejecución del proyecto "Documentación de lineamientos asociados a procesos de TIC en cumplimiento con normativa" (CO3-008) y el proyecto "Definición e implementación de un proceso de gestión de servicios de TIC" (CO3-006), ambos en estado "finalizado", se constituyeron los lineamientos para la gestión y control de servicios de la Función de TI a la Institución.

Sin embargo, al momento de cierre de este estudio, la Unidad de TI no cuenta con un instrumento formal para la evaluación de la entrega de servicios de TI, con sus indicadores de gestión o tiempos definidos y priorizados con base en SLAs formales, más allá de la continuidad de servicio de la infraestructura tecnológica a cargo de CODISA como servicios administrados.

Esto evidencia una debilidad con respecto al monitoreo y control de seguimiento de la ejecución de las actividades vinculantes con la entrega de Servicios de TI, así como la falta de insumos para evaluar la eficiencia y el cumplimiento de la entrega de resultados de una manera objetiva y formal. Al momento de cierre de este informe, solo se pudo evaluar el nivel de satisfacción, por percepción, del personal usuario de la Institución por medio de un cuestionario digital. El resultado de esta evaluación se encuentra en los anexos 1 y 2 de este informe.

La falta de instrumentos formales para la gestión de la entrega de servicios basado en acuerdos formales dificulta la evaluación objetiva de la Función de Tecnologías de Información y la generación de valor por medio de valores cuantitativo. Además, no se pueden sentar responsabilidades por el incumplimiento de atención de solicitudes de servicio o por un uso ineficiente de recursos asignados a TI.

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

a. En el Capítulo II: Planificación y organización:

"2.1 Administración de recursos financieros

La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable."

b. En el Capítulo IV: Prestación de servicios y mantenimiento:

"4.1 Definición y administración de acuerdos de servicio

La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.

El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

[…]
d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.

f. Revisar periódicamente los acuerdos de servicio…"

2.3.- FORMALIZACIÓN DEL MARCO DE GESTIÓN DE TELETRABAJO

El día 23 de octubre, en reunión de trabajo con la Gerencia General, se indicó que la Institución, a raíz de la emergencia sanitaria nacional, estableció lineamientos para cumplir con la directriz de trabajo remoto. A esta condición especial de labores lo nombran "trabajo en casa por emergencia".

Los lineamientos son gestionados por medio de una "Comisión de teletrabajo" que gestiona la estrategia, además de realizar evaluaciones mensuales de desempeño a través de instrumentos formales para evaluar el logro.

Por otro lado, desde la perspectiva tecnológica, no se han desarrollado los lineamientos formales sobre el uso de la infraestructura tecnológica, seguridad de la información, responsabilidades y limitaciones para el personal usuario en trabajo remoto sobre el uso de los servicios de TI, o indicadores sobre el desempeño de la plataforma, continuidad y soporte.

Además, desde la perspectiva de la Función de TI, existe un proyecto de "Definir e implementar un proceso de gestión de la seguridad de la información para la DGAC" (CO3-003) en estado "Finalizado", pero la Gerencia General no cuenta con lineamientos específicos para teletrabajo de cara a seguridad de la Infraestructura Tecnológica.

La falta de lineamientos formales para garantizar la seguridad y continuidad de los servicios tecnológicos en teletrabajo dificulta la evaluación objetiva de la Infraestructura Tecnológica en términos de operación y seguridad, además de la evaluación de la plataforma tecnológica con indicadores cuantitativos, según las condiciones de comunicación y equipos de trabajo del personal.

Además, la falta de lineamientos de seguridad en teletrabajo limita la capacidad sentar responsabilidades por el mal uso de los recursos tecnológicos o la materialización de eventos de riesgo.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, en el Capítulo I: *Normas de aplicación general*, define:

"1.4 Gestión de la seguridad de la información

La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- *La implementación de un marco de seguridad de la información.*
- *El compromiso del personal con la seguridad de la información.*

[…]

- *La seguridad en las operaciones y comunicaciones.*
- *El control de acceso."*

2.4.-DEBILIDADES EN LA EJECUCIÓN DEL MARCO DE GESTIÓN DE TI

Como se mencionó en el comentario 2.2, la Unidad de TI estaba ejecutando un proyecto para alinear sus procesos de TIC con los lineamientos de la normativa aplicable para la Función. A la fecha de cierre de este estudio, el proyecto se encontraba en su etapa final para la entrega de los documentos que regirían la normativa de la Unidad.

Como parte de este estudio, se realizó una evaluación de cumplimiento de los criterios plasmados en las Normas técnicas para la gestión y el control de las Tecnologías de Información, en conjunto con la encargada de la Unidad de Tecnologías de Información y el personal de la Función de TI de la DGAC.

Con base en esta evaluación, y los insumos enviados por la Función de TI, se identificaron los siguientes incumplimientos de las normas de la CGR:

Tabla 4: Requerimientos de las Normas Técnicas no cumplidos

	Criterio	Respuesta
Capítulo I Normas de aplicación general		
1.1 Marco estratégico de TI	Se evalúa el nivel de dominio de las acciones y responsabilidades que los usuarios pueden hacer relacionado con TI	No
	Se evalúa el nivel de satisfacción de los usuarios relacionado con el servicio que recibe del área de TI	No
	Se cuenta con una unidad de gobierno de TI multidisciplinario	No
1.3 Gestión de riesgos	Se cuentan con procedimientos para cuantificar riesgos materializados, incidentes y su impacto	No
	Se cuentan con procedimientos para atender riesgos no identificados	No
1.4 Gestión de la seguridad de la información	Seguridad de Información:	
1.4.1 Implementación de un marco de seguridad de la información	Se cuenta con procedimientos para atender y priorizar incidentes de seguridad	No
	Se cuenta con una unidad de seguridad de información con responsabilidades y roles definidos	No
1.4.2 Compromiso del personal con la seguridad de la información	El personal es evaluado con respecto a su nivel de conocimiento en temas de seguridad de información	No
	Hay sanciones definidas por incidente de seguridad materializado por el personal de TI	No
1.4.3 Seguridad física y ambiental	Se tienen controles ambientales en centros de procesamiento de TI	No
	Se tienen identificados y controlados riesgos ambientales	No
	Se cuentan con bitácoras de trabajo de personal en activos de TI	No
1.4.5 Control de acceso	Se cuentan con perfiles definidos para usuarios técnicos, administrativos y funcionales	No
	Se documentan intentos de accesos no permitidos o materialización de riesgos de acceso	No
1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica	Se cuentan con lineamientos de desarrollo de sistemas y estandarización de equipos tecnológicos	No
	Se cuentan con controles para resguardar códigos fuentes y versiones de software	No
1.4.7 Continuidad de los servicios de TI	La continuidad de TI está alineada con la continuidad de Negocio	No
	Se cuentan con procesos de levantamiento de centros de procesamiento contingentes	No
1.6 Decisiones sobre asuntos estratégicos de TI	Se evalúa la brecha de las capacidades de TI y las necesidades de negocio	No

	Criterio	Respuesta
	Se identifican y documentan tendencias y oportunidades relacionadas con TI	No
1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI	Se cuentan con planes de acción para remediar incumplimientos	No
Capítulo II Planificación y organización		
2.4 Independencia y recurso humano de la Función de TI	La unidad de TI es autosuficiente en su operaciones y funciones de las áreas usuarias	No
	Cuenta con personal suficiente e idóneo	No
Capítulo III Implementación de tecnologías de información		
3.2 Implementación de software ***3.3 Implementación de infraestructura tecnológica***	Se implementan estándares de desarrollo, aprovechamiento de código, estructuras de datos, interconexión, entre otros	No
Capítulo IV Prestación de servicios y mantenimiento		
4.2 Administración y operación de la plataforma tecnológica	Se cuenta con la documentación suficiente para administrar y operar la plataforma tecnológica	No
	Se planifica la capacidad de la plataforma	No
4.3 Administración de los datos	Se cuenta con políticas de gestión, control, custodia, traslado, y destrucción de activos de datos	No
	Se cuenta con un inventario de activos de información y datos	No
	Los activos de datos tienen vigencia	No
	Se evalúa el control de los datos, procesamientos, seguridad y disponibilidad	No
	Se cuentan con políticas y procedimientos de calidad de datos	No
4.4 Atención de requerimientos de los usuarios de TI	Se realiza una planificación de mejora continua con base en los requerimientos de los usuarios de TI	No
4.5 Manejo de incidentes	Se evalúa el nivel de atención de incidentes	No
	El personal Institucional está capacitado para atender incidentes según el debido proceso	No
	Se cuenta con procedimientos de mejora continua	No
4.6 Administración de servicios prestados por terceros	Los contratos con terceros están alineados con las políticas de la Institución relacionados con Talento Humano	No
Capítulo V Seguimiento		
5.1 Seguimiento de los procesos de TI	Se evalúa el nivel de desempeño y efectividad de los procesos de TI	No
	Los procesos están alineado a la Arquitectura Empresarial	No

	Criterio	Respuesta
5.2 Seguimiento y evaluación del control interno en TI	La mitigación de riesgos está dentro del nivel de aceptación Institucional	No
5.3 Participación de la Auditoría Interna	Se cuenta con participación y apoyo del área de Auditoría Interna	No

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

Además, la Unidad de TI no tiene un plan de acción para atender estos incumplimientos.

Esta condición se materializa a causa de una estructura organizacional insuficiente y sin la debida distribución de cargas de trabajo para cumplir con estas funciones normativas; además, la Función de TI en la institución es una unidad reactiva y considera que es requerida para mitigar incidentes materializados que gestionar los servicios de TI propios de la Institución.

Este incumplimiento no solo puede generar procesos administrativos o legales de entidades fiscalizadoras contra la Institución, también impacta negativamente en la eficiencia, gestión y control de los servicios y procesos que la Función de TI debe brindar como servicios, además de dificultar las labores de seguimiento y evaluación.

La resolución de las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, establece:

> *Artículo 1— […] "Normas técnicas para la gestión y el control de las tecnologías de información", normativa que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado.*
>
> *[…]*
>
> *Artículo 3 – Establecer que las "Normas técnicas para la gestión y el control de las tecnologías de información" son de acatamiento obligatorio para la*

Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización…"

En el anexo 3 de este documento se presenta el detalle de la evaluación de las normas técnicas de la CGR realizada por la Función de TI.

2.5.- HALLAZGO 5 APRECIACIÓN DE LA PARTICIPACIÓN DE LA AUDITORÍA INTERNA DE LA DGAC DE CARA A LA FUNCIÓN DE TI

Como se identificó en el hallazgo anterior, la Unidad de TI considera como incumplido el inciso 5.3 *Participación de la Auditoría Interna* de las normas técnicas de la CGR, al considerar que la Auditoría Interna de la DGAC participa de forma reactiva y en función de su plan de trabajo vigente.

Sin embargo, la Auditoría Interna establece su posición de apoyo a la Función de TI con estudios especiales y contrataciones de servicios especializados para evaluar y emitir recomendaciones relacionadas con el gobierno, gestión y ejecución de servicios de TI y de la infraestructura tecnológica Institucional.

Esta apreciación se da por una falta de alineación entre las expectativas de la Función de TI relacionadas con los resultados de los estudios de Auditoría, y el alcance regulatorio y operativo que estos estudios puede aportar a la Función. A la fecha de corte de este estudio, la unidad de TI no entregó un documento donde especifica explícitamente el plan de trabajo con las recomendaciones de los estudios de Auditoria y su atención y resolución.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, en el Capítulo V: *Seguimiento*, define:

"5.3 Participación de la Auditoría Interna

La actividad de la Auditoría Interna respecto de la gestión de las TI debe orientarse a coadyuvar, de conformidad con sus competencias, a que el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en esa materia."

Como parte de las actividades iniciales y el alcance de este estudio, se revisaron las recomendaciones vigentes de los estudios más recientes que la

Auditoría Interna ha realizado de cara a la Función de TI. En el anexo 6 de este documento se presenta un inventario de recomendaciones vigentes a atener.

2.6.-FALTA DE UN DIAGNÓSTICO DE CAPACIDADES DE TI Y NECESIDADES DE LA DGAC

Como se estableció en el Informe de Auditoría DGAC-AI-14-2019 Informe Evaluación del centro de datos principal y Servicios asociados de noviembre del 2019, la Institución realizó una inversión importante en adquirir un Centro de Datos externo, cuya gestión y control se da por la contratación de servicios administrados con un tercero.

Sin embargo, la constitución de este Centro de Datos se definió con base en las características de procesamiento y almacenamiento igual al existente en la Institución y administrado internamente.

Ahora, esta plataforma tecnológica procesa la arquitectura de sistemas existente, sin un plan de modernización de los sistemas de información o lineamientos para incrementar las capacidades del Centro de Datos.

Esta condición se materializa por la falta de una participación proactiva entre las áreas sustantivas y de soporte de la Institución y la Función de TI, que permita atender necesidades de la Institución y planificar las inversiones factibles con base en las capacidades de la Función de TI.

No contar con una planificación de atención de necesidades institucionales ni un debido diagnóstico de las capacidades de la Función de TI, materializa la condición de administrar y operar una arquitectura de sistemas obsoleta, con servicios de soporte y mantenimiento muy limitados, y con una complejidad cada vez mayor para atender necesidades sustantivas para las áreas usuarias.

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

a. En el Capítulo I: Normas de aplicación general:

"1.6 Decisiones sobre asuntos estratégicos de TI

El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a

establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización."

b. En el Capítulo III: Implementación de tecnologías de información:

"3.1 Consideraciones generales de la implementación de TI

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:

[…]

a. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
b. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.
c. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

[…]

i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios."

c. En el Capítulo IV Prestación de servicios y mantenimiento:

"4.1 Definición y administración de acuerdos de servicio

La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades…"

"4.2 Administración y operación de la plataforma tecnológica

La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.
b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas."

"4.4 Atención de requerimientos de los usuarios de TI

La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia."

2.7.- DEBILIDADES EN LA EVALUACIÓN DE RIESGOS Y CONTROL INTERNO PARA LA FUNCIÓN DE TI

A la fecha de corte del estudio, La Unidad de Tecnologías de Información de la DGAC no había adaptado, como parte de sus procesos de gestión, el instrumento

actualizado de gestión de riesgos institucional, con un inventario de riesgos actualizado y asociado a la gestión de TI Institucional.

Los riesgos identificados como parte de la elaboración de este estudio no se encuentran documentados como parte del alcance de revisión y control del ASCII, 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.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, define:

a. En el Capítulo II: Normas de aplicación general:

"1.3 Gestión de riesgos

La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."

b. En el Capítulo V: Seguimiento:

"5.2 Seguimiento y evaluación del control interno en TI

El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas."

En el anexo 4 de este documento se presenta el detalle de la evaluación de Riesgos y Control Interno realizada por la Función de TI.

2.8.- FALTA DE UNA VISIÓN FORMAL DE LA DGAC EN MATERIA TECNOLÓGICA

El día 23 de octubre, en reunión de trabajo con la Gerencia General, se indicó que la Institución no ha redactado una línea base de visión para la Institución en materia tecnológica.

Esta situación se materializa a raíz de los esfuerzos prioritarios para atender debilidades identificadas en la Función de TI, por ejemplo, estructura organizacional, planteamiento de proyectos, planificación de inversiones para el 2021, clima organizacional en la Unidad de TI y su entorno, entre otros asuntos.

Sin embargo, el no contar con una visión de inversión y desarrollo tecnológico puede materializar el riesgo de no contar con recursos justificados para presupuesto de TI, inversiones que no generan valor a la Institución, e incumplimientos normativos. Esta situación se incrementa más al confirmar que para el 2021 la DGAC no contará con un PETIC vigente.

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

c. En el Capítulo II: Planificación y organización:

"2.1 Planificación de las tecnologías de información

La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes."

"2.3 Infraestructura tecnológica

La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI."

d. En el Capítulo III: Implementación de tecnologías de información:

"3.1 Consideraciones generales de la implementación de TI

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:

[…]

b. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias."

e. En el Capítulo IV: Prestación de servicios y mantenimiento:

"4.4 Atención de requerimientos de los usuarios de TI

La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia."

En el anexo 5 de este documento se listan oportunidades de desarrollo institucional basado en tendencias de ámbito tecnológico, para consideración de la Administración.

2.9.- ALTA DEPENDENCIA CON EL PROVEEDOR DEL SIFCO

La Unidad de TI había gestionado un proyecto a ejecutar en el 2021 para atender la necesidad de abarcar cambios grandes al SIFCO para cumplir con las NICSP, sin embargo, según el inventario de iniciativas:

"[…] el proyecto no fue presupuestado debido a que no se expuso con tiempo a la Unidad de TIC´s para agregarle presupuesto para el 2021"

Por otro lado, en reunión de trabajo con la Gerencia General, se habló de una cotización con la empresa dueña de SIFCO para atender los requerimientos más importantes identificados por el área Financiera, además de admitir la necesidad de ampliar la vida útil del sistema y modernizar sus funciones.

Esta condición se materializa porque la Unidad de TI no cuenta, al momento de cierre de este estudio, con una metodología formal para la adquisición de servicios tercerizados para mantenimiento evolutivo, además que sus prácticas de gestión de proyectos han dejado con desconfianza a la Administración Superior.

Complementario a la situación materializada, los requerimientos fueron presentados a la empresa dueña del SIFCO para definir los montos de inversión y talento humano requerido.

Esa situación puede provocar que se amplíe la relación con un proveedor de un sistema que ya cumplió su vida útil, por tanto, la complejidad de implementar nuevas funcionalidades y procesos quedará definido con u "proveedor único", que no debe competir y por tanto no hay base comparativa para valorar si es la solución más rentable para la Institución.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, emitidas por la CGR, definen: En el Capítulo III: Implementación de tecnologías de información:

"3.1 Consideraciones generales de la implementación de TI

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:

[…]

i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios."

III. CONCLUSIONES

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

1. La Gerencia General de la DGAC está realizando diligencias para evaluar la Estructura Organizacional y alcance de gobierno de la Función de TI, sin embargo, lo está realizando con personal externo y sin participación de la Unidad de TI, corriendo el riesgo de generar incertidumbre y resistencia en la Unidad y su personal **(Comentario 2.1).**

2. No se cuentan con lineamientos para realizar evaluaciones sobre la entrega de servicios, su eficiencia y el cumplimiento de expectativas de los usuarios en tiempo y forma, ni tampoco están establecidos los SLAs que permita fiscalizar objetivamente la entrega de servicios tecnológicos **(Comentario 2.2).**

3. La Institución no cuenta con un marco de gestión formal para la ejecución de actividades en teletrabajo para el personal, lo que dificulta valorar en materia tecnológica la efectividad de la plataforma en trabajo remoto, así como la definición de responsabilidades y ámbito de acción con el personal de la DGAC. **(Comentario 2.3).**

4. Si bien la Unidad de TI está realizando esfuerzos para alinear su marco de gobierno con los requerimientos normativos que la rigen, hay brechas de cumplimiento que pueden afectar negativamente la calidad y eficiencia en la gestión de la Función, además de incurrir en sanciones administrativas y legales **(Comentario 2.4).**

5. Existe una divergencia con respecto a la participación y colaboración de la Auditoría Interna de la DGAC y la percepción de apoyo que recibe la Unidad de TI, esto por el contraste entre las expectativas de la Función de TI y el alcance que a nivel normativo puede dar la Auditoría Interna, de cara a las recomendaciones emitidas y la necesidad de planes de acción **(Comentario 2.5).**

6. La institución no ha constituido un inventario de necesidades de las diferentes áreas sustantivas y de soporte, por lo que hay incertidumbre sobre la atención de requerimientos y planificación de iniciativas de TI, además de no contar con una evaluación formal de las capacidades de TI que apoye en realizar un estudio de factibilidad y una gestión correcta de recursos para atender necesidades **(Comentario 2.6).**

7. Con base en los ejercicios de valoración de riesgos y control interno, se desprende que la Unidad de TI tiene debilidades en la constitución del catálogo de riesgos y su respectiva valoración, alienada con la metodología Institucional, además de no contar con insumos suficientes para certificar el nivel de efectividad e inversión de activos de control interno **(Comentario 2.7).**

8. La Institución no cuenta con una visión integral en materia de tecnologías de información, lo que puede traducirse en la ejecución presupuestaria de TI en proyectos que no responden al planteamiento estratégico de la DGAC, no generan valor o atienden necesidades de las áreas usuarias; además de no contar con insumos suficientes para justificar iniciativas o proyectos **(Comentario 2.8).**

9. La plataforma tecnológica tiene un rezago importante en temas de vida útil, flexibilidad para mantenimiento evolutivo y dependencia con proveedores de sistemas propietarios, por ejemplo, el SIFCO. La falta de una valoración comparativa del SIFCO con soluciones “estado del arte” dificulta la evaluación de la factibilidad técnica y económica de la iniciativa, además de quitar independencia de la DGAC al proveedor **(Comentario 2.9).**

IV. RECOMENDACIONES

Al Consejo Técnico de Aviación Civil

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

A la Dirección General de Aviación Civil

1. Desarrollar con las diferentes áreas el desarrollo de la Arquitectura Empresarial para definir formalmente la visión integral, el estado actual, las oportunidades y necesidades institucionales, y el plan de acción en materia tecnológica **(Conclusiones 2, 6, 8, 9).**

2. 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 **(Conclusiones 1 a 9).**

3. Articular los esfuerzos para diseñar, contratar y ejecutar el desarrollo de la Arquitectura Empresarial para definir formalmente la visión integral, el estado actual, las oportunidades y necesidades institucionales y el plan de acción en materia tecnológica **(Conclusiones 2, 6, 8, 9)**.

4. Articular esfuerzos para desarrollar un levantamiento de necesidades, requerimientos y oportunidades en materia tecnológica con todas las áreas sustantivas, estratégicas y de soporte de la Institución **(Conclusión 8).**

5. Apoyar a la Unidad de Tecnologías de Información para robustecer el marco de gobierno, operación y supervisión de la Función y de la entrega efectiva de servicios en materia tecnológica **(Conclusiones 1 a 4, 7).**

6. Apoyar a la Unidad de TI en la implementación de los procesos de la Función en la Institución, incluyendo el desarrollo de una metodología de evaluación y control de entrega de servicios y Acuerdos de Nivel de Servicio. (o SLAs por sus siglas en inglés). Esto se podría llevar a cabo, si se estima prudente, con la participación de la Unidad de Planificación **(Conclusiones 2 a 4)**.

A la responsable de la Unidad de Tecnologías de Información

7. Involucrarse en el planteamiento y desarrollo de la Estructura Organizacional para la Función de TI, entregando evidencia de la capacidad operativa y administrativa de la Unidad, capacidades de la infraestructura tecnológica y cargas de trabajo **(Conclusión 1)**.

8. Desarrollar la metodología de evaluación y control de la entrega de servicios de TI **(Conclusión 2)**.

9. Desarrollar, en conjunto con personal clave de las diferentes áreas de la Institución, los SLAs para la entrega de servicios de TI e indicadores de desempeño de la Función **(Conclusión 2)**.

10. Desarrollar, en conjunto con la Dirección General y la Comisión responsable de la gestión de trabajo remoto, los lineamientos técnicos y operativos para la gestión de operaciones en teletrabajo **(Conclusión 3)**.

11. Articular esfuerzos para oficializar el marco de gobierno de TI desarrollado, y constituir los lineamientos y procedimientos para el cumplimiento de las Normas Técnicas de la CGR, en especial atención los criterios que no se cumplen **(Conclusión 4)**.

12. Desarrollar el plan de acción para atender las recomendaciones emitidas por la Auditoría Interna de la DGAC, con su estrategia de comunicación de avance y resultados, fechas de cumplimiento esperadas y responsables vinculantes **(Conclusión 5).**

13. Desarrollar, en conjunto con personal clave de las diferentes áreas de la Institución, un levantamiento de necesidades, requerimientos y oportunidades en materia tecnológica **(Conclusión 6).**

14. Formalizar y estandarizar los procesos y lineamientos de gestión de riesgos y control interno, y actualizar el inventario de los mismos, para evaluar todos aquellos que se han identificado en ejercicios de valoración anteriores **(Conclusión 7)**.

15. Apoyar, con insumos de evaluación de capacidades, desempeño, servicios y operación de la unidad y la infraestructura tecnológica, además de su experiencia y criterio, a la DGAC y la CETAC en el desarrollo de la visión integral en materia tecnológica **(Conclusión 8)**.

16. Valorar, en conjunto con la Unidad Administrativa Financiera responsable del SIFCO, el desarrollo de un estudio de mercado para implementar un sistema integral administrativo financiero que apoye en la gestión institucional, en el cumplimiento de requerimientos normativos, y en la integración con las iniciativas que instituciones externas están desarrollando **(Conclusión 9)**.

17. Con base en el precedente del SIFCO, y con base en el levantamiento de requerimientos y necesidades de la Institución, realizar un levantamiento de capacidades técnicas y funcionales de la infraestructura tecnológica y todos sus componentes **(Conclusión 9)**.

18. Adicionalmente, desarrollar un estudio de mercado para establecer el portafolio de inversiones en materia de actualización tecnológica, tanto en su arquitectura de sistemas como en su infraestructura tecnológica **(Conclusión 9)**.

19. Con base en el levantamiento de requerimientos institucionales, y el desarrollo de la línea base de la Arquitectura Empresarial, desarrollar el Plan Estratégico de Tecnologías de Información que regirá la operación y estrategia de la Función de TI **(Conclusiones 1 al 9).**

ANEXO 1: EVALUACIÓN DEL NIVEL DE SERVICIO DE TI

A continuación, se presenta el resultado de la evaluación del nivel de servicio de TI por percepción del personal de la Institución, por medio de la ejecución de 30 encuestas digitales.

Tabla 5: Resultados de la percepción del nivel de servicio de TI

Teletrabajo y Soporte técnico	*Favor contestar los siguientes incisos según los siguientes criterios de percepción (seleccione un criterio por inciso con una "x"):*	***Totalmente de acuerdo***	***De acuerdo***	***Indiferente***	***En desacuerdo***	***Totalmente en desacuerdo***	***No desea responder***
	1. Conozco el proceso a seguir cuando necesito asistencia de TI en sitio (oficina).	36.67%	30.00%	20.00%	6.67%	0.00%	6.67%
	2. Conozco el proceso a seguir cuando necesito asistencia de TI en teletrabajo.	20.00%	13.33%	16.67%	33.33%	0.00%	16.67%
	3. Los canales existentes para solicitar atención por parte de TI son adecuados.	20.00%	36.67%	3.33%	20.00%	13.33%	6.67%
	4. La capacidad de TI para atender mis solicitudes en sitio (oficina) es efectiva.	10.00%	36.67%	3.33%	26.67%	13.33%	10.00%
	5. La capacidad de TI para atender mis solicitudes en teletrabajo es efectiva.	10.00%	16.67%	16.67%	16.67%	10.00%	30.00%
	6. El personal de TI busca entender el incidente que estoy describiendo.	16.67%	56.67%	3.33%	13.33%	3.33%	6.67%
	7. El personal de TI se comunica conmigo sin utilizar lenguaje técnico, son pacientes, corteses y profesionales.	30.00%	40.00%	13.33%	3.33%	3.33%	10.00%

	8. Cuando tengo varias solicitudes de atención, puedo indicar en qué prioridad requiero que sean atendidas.	26.67%	26.67%	16.67%	3.33%	10.00%	16.67%
	9. Puedo dar seguimiento a mi solicitud de soporte con el área de TI y lo resuelve a satisfacción.	10.00%	23.33%	16.67%	30.00%	10.00%	10.00%
	10. En general, mis solicitudes son atendidas en un tiempo oportuno.	13.33%	30.00%	20.00%	20.00%	10.00%	6.67%
	11. En general, mis solicitudes son resueltas en un tiempo oportuno.	13.33%	26.67%	23.33%	20.00%	10.00%	6.67%
	12. El Depto. de TI es proactivo y oportuno para reducir la cantidad y severidad de incidentes.	6.67%	10.00%	26.67%	20.00%	20.00%	16.67%
Herramientas tecnológicas	*Favor contestar los siguientes incisos según los siguientes criterios de percepción (seleccione un criterio por inciso con una "x"):*	***Totalmente de acuerdo***	***De acuerdo***	***Indiferente***	***En desacuerdo***	***Totalmente en desacuerdo***	***No desea responder***
	1. Los sistemas y las herramientas que tengo disponibles son adecuadas para realizar mi trabajo.	16.67%	53.33%	3.33%	23.33%	3.33%	0.00%
	2. Conozco todo el software y las herramientas tecnológicas disponibles a nivel institucional para apoyar en el cumplimiento de mis funciones.	40.00%	26.67%	6.67%	20.00%	0.00%	6.67%
	3. Los sistemas y herramientas que utilizo son estables y suficientemente rápidos cuando estoy en sitio (oficina).	20.00%	56.67%	3.33%	10.00%	3.33%	6.67%

	4. Los sistemas y herramientas que utilizo son estables y suficientemente rápidos cuando estoy en teletrabajo.	23.33%	46.67%	3.33%	0.00%	3.33%	23.33%
	5. Puedo extraer la información de negocio que necesito de otros sistemas para cumplir con mis funciones, sin intervención de otros usuarios u otras áreas.	30.00%	30.00%	13.33%	16.67%	0.00%	10.00%
	6. Los datos y la información que consulto son veraces.	30.00%	50.00%	3.33%	6.67%	0.00%	10.00%
	7. Mis requerimientos funcionales son atendidos con los sistemas actuales.	20.00%	50.00%	10.00%	6.67%	3.33%	10.00%
Entrenamiento/ Capacitación	*Favor contestar los siguientes incisos según los siguientes criterios de percepción (seleccione un criterio por inciso con una "x"):*	***Totalmente de acuerdo***	***De acuerdo***	***Indiferente***	***En desacuerdo***	***Totalmente en desacuerdo***	***No desea responder***
	1. Me siento cómodo usando el software y las herramientas que tengo disponibles.	26.67%	50.00%	3.33%	13.33%	0.00%	6.67%
	2. Conozco todas las características y funciones en las herramientas y sistemas que tengo.	23.33%	33.33%	3.33%	33.33%	0.00%	6.67%
	3. La capacitación que recibo por parte de TI se da en condiciones adecuadas.	16.67%	23.33%	20.00%	26.67%	3.33%	10.00%
	4. La capacitación que recibo por parte de TI sobre la plataforma tecnológica alcanza el resultado esperado.	20.00%	20.00%	13.33%	33.33%	3.33%	10.00%
	5. La documentación (manuales de usuario, manuales técnicos, documentación de soporte, otros) que tengo para utilizar los sistemas es suficiente.	13.33%	23.33%	13.33%	30.00%	6.67%	13.33%

	6. Conozco las políticas de TI que debo cumplir con respecto al uso de los servicios, equipos y plataforma tecnológica (seguridad, uso de herramientas, permisos, uso de correo electrónico, entre otros).	20.00%	43.33%	10.00%	20.00%	0.00%	6.67%
	7. Se atienden las capacitaciones y entrenamientos oportunamente.	10.00%	36.67%	13.33%	23.33%	6.67%	10.00%
Proyectos de TI	*Favor contestar los siguientes incisos según los siguientes criterios de percepción (seleccione un criterio por inciso con una "x"):*	***Totalmente de acuerdo***	***De acuerdo***	***Indiferente***	***En desacuerdo***	***Totalmente en desacuerdo***	***No desea responder***
	1. Conozco en lo que está trabajando TI en este momento.	6.67%	10.00%	13.33%	30.00%	33.33%	6.67%
	2. Estoy consciente del impacto que los proyectos tienen / tendrán en mis funciones.	16.67%	16.67%	16.67%	13.33%	30.00%	6.67%
	3. Estoy consciente del impacto que los proyectos tienen / tendrán en la Institución y grupos de interés relacionados.	16.67%	20.00%	16.67%	6.67%	30.00%	10.00%
	4. Conozco el procedimiento para presentar requerimientos para mejoras en aplicativos existentes.	13.33%	20.00%	13.33%	30.00%	20.00%	3.33%
	5. Considero fácil y efectiva la forma de presentar requerimientos y sus prioridades para constituir una iniciativa de TI.	10.00%	26.67%	10.00%	23.33%	16.67%	13.33%
	6. Me relaciono activamente en el trabajado de algún proyecto específico relacionado con TI.	6.67%	20.00%	16.67%	16.67%	23.33%	16.67%
	7. Puedo realizar el debido seguimiento al momento de ejecutar un proyecto.	6.67%	13.33%	20.00%	20.00%	20.00%	20.00%

	8. Al ejecutar un proyecto, el personal de TI se comunica conmigo sin utilizar lenguaje técnico, y son corteses y profesionales.	16.67%	26.67%	16.67%	13.33%	6.67%	20.00%
	9. Se atienden mis objetivos y requerimientos de forma efectiva.	10.00%	23.33%	16.67%	16.67%	16.67%	16.67%
	10. Recibo soluciones de calidad que cumplen con los objetivos de negocio.	6.67%	33.33%	16.67%	6.67%	23.33%	13.33%
	11. En general, estoy satisfecho con la manera en que se gestionan los proyectos.	6.67%	16.67%	20.00%	20.00%	16.67%	20.00%
	12. Los proyectos se terminan de manera oportuna.	3.33%	3.33%	16.67%	26.67%	26.67%	23.33%
TI en general	*Favor contestar los siguientes incisos según los siguientes criterios de percepción (seleccione un criterio por inciso con una "x"):*	***Totalmente de acuerdo***	***De acuerdo***	***Indiferente***	***En desacuerdo***	***Totalmente en desacuerdo***	***No desea responder***
	1. TI tiene un fuerte enfoque en servicio al usuario Institucional.	3.33%	23.33%	20.00%	26.67%	16.67%	10.00%
	2. TI tiene una buena dirección estratégica, alineada con las prioridades y requerimientos de la Institución.	0.00%	10.00%	13.33%	26.67%	16.67%	33.33%
	3. TI comunica sus planes de trabajo y las actividades que realizará durante el año.	0.00%	20.00%	6.67%	30.00%	20.00%	23.33%
	4. TI difunde su marco normativo y operativo.	6.67%	16.67%	0.00%	40.00%	16.67%	20.00%
	5. Soy notificado con anticipación sobre el inicio de proyectos con los cambios tecnológicos que me impactan.	6.67%	26.67%	3.33%	30.00%	20.00%	13.33%

	6. Puedo aportar sobre el plan de acción de TI cuando es necesario.	3.33%	20.00%	16.67%	16.67%	16.67%	26.67%
	7. TI provee una ventaja táctica (tangible) para mi área.	3.33%	23.33%	13.33%	23.33%	23.33%	13.33%
	8. El personal del área de TI es capaz y conocedor.	10.00%	33.33%	16.67%	13.33%	3.33%	23.33%
	9. En general, estoy satisfecho con el servicio que recibo de TI.	3.33%	33.33%	13.33%	23.33%	10.00%	16.67%
	10. En general, TI responde a mis necesidades.	3.33%	30.00%	26.67%	23.33%	6.67%	10.00%

Fuente: elaboración propia.

ANEXO 2: EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA INSTITUCIONAL

A continuación, se presenta el resultado de la evaluación del nivel de la plataforma tecnológica por percepción del personal de la Institución, por medio de la ejecución de 64 encuestas digitales.

Tabla 6: Resultados de la percepción de la plataforma tecnológica

Efectividad de la Plataforma Tecnológica	Cuando se registra como usuario en la plataforma tecnológica (seleccione solo un inciso con una "x"):	45%	La conexión es inmediata y no se desconecta mientras me encuentro trabajando
		42%	La conexión es inmediata, pero se desconecta de forma aislada y debo ingresar a la plataforma de nuevo
		11%	Puede tardar en conectarse a la plataforma, se desconecta de forma aislada y debo ingresar a la plataforma de nuevo
		2%	Requiere de varios intentos para conectarse a la plataforma, se desconecta continuamente y debe ingresar a la plataforma de nuevo
		0%	Requiere de varios intentos para conectarse a la plataforma, se desconecta continuamente y puede materializarse el caso de no poder ingresar
	Cuando utiliza la plataforma (seleccione solo un inciso con una "x"):	17%	Considera que es más estable y responde más rápido cuando está en teletrabajo que en la oficina
		10%	Considera que es más estable y responde igual de rápido cuando está en teletrabajo que en la oficina
		42%	No hay diferencia de estabilidad ni desempeño entre teletrabajo y en la oficina
		13%	Considera que es más estable y responde igual de rápido cuando está en la oficina que en teletrabajo

		18%	Considera que es más estable y responde más rápido cuando está en la oficina que en teletrabajo
	Mientras trabaja en la plataforma (seleccione solo un inciso con una "x"):	35%	Puede realizar sus labores sin interrupción alguna
		37%	Puede realizar sus labores pero pueden materializarse eventos aislados que generan molestias o reducen el tiempo de respuesta de la plataforma
		25%	Puede realizar sus labores pero pueden materializarse eventos aislados que interrumpen su trabajo temporalmente
		2%	Puede realizar sus labores pero pueden materializarse eventos constantes que interrumpen su trabajo por un tiempo determinado
		2%	Puede realizar sus labores pero pueden materializarse eventos constantes que interrumpen su trabajo por un tiempo indefinido
Efectividad de los sistemas de información	*Observaciones*		
	Cuando realiza sus funciones sustantivas en la Institución (seleccione solo un inciso con una "x"):	27%	Realiza todas sus funciones desde un sistema centralizado y solo extrae información por medio de reportes no modificables para fines informativos
		10%	Realiza todas sus funciones desde un sistema descentralizado y debe extraer información por medio de reportes no modificables como insumos para otras áreas
		24%	Realiza parte de sus funciones desde un sistema descentralizado y debe extraer información por medio de reportes modificables y realizar ajustes mínimos
		24%	Realiza parte de sus funciones desde un sistema descentralizado y debe extraer información por medio de reportes modificables y realizar ajustes importantes
		16%	Realiza parte de sus funciones desde un sistema descentralizado y debe extraer datos duros y modificarlos con otra aplicación (por ejemplo, Excel)

	Cuando trabaja con los sistemas de información (seleccione solo un inciso con una "x"):	37%	Opera de forma estable y rápida, si se despliegan errores, son mensajes claros relacionados con un mal uso del sistema o errores humanos
		35%	Opera de forma rápida, pero si se despliegan errores, son mensajes con códigos de referencia o vinculantes con la plataforma tecnológica (ejemplo, bases de datos)
		21%	Opera de forma estable, pero puede cerrarse la aplicación por un error de sistema o materializarse casos aislados que pueden hacer que se pierda información
		5%	Opera lentamente, puede cerrarse la aplicación por un error de sistema/plataforma o materializarse casos constantes que pueden hacer que se pierda información
		2%	Opera de forma inestable, puede cerrarse la aplicación sin causa aparente y se pierde información constantemente
	Cuando ingresa a los sistemas de información (seleccione solo un inciso con una "x"):	44%	Ingresa con su usuario para ingresar a la plataforma tecnológica (por medio de Directorio Activo, igual a cuando enciende su computadora)
		40%	Siempre requiere autenticación por medio de usuario y contraseña y la aplicación se inhabilita por no utilizarlo en cierto tiempo, requiriendo autenticación de nuevo
		13%	Siempre requiere autenticación por medio de usuario y contraseña, pero la aplicación no se inhabilita
		0%	Requiere autenticación por medio de un usuario y contraseña genéricos, que además puede compartir con otros usuarios
		3%	No requiere autenticarse
	Cuando utiliza los sistemas de información (seleccione solo un inciso con una "x"):	94%	Tiene un perfil de usuario formalmente definido en el sistema, con funcionalidades debidamente identificadas y opciones limitadas
		5%	Trabaja con funcionalidades debidamente identificadas y opciones limitadas, pero no tiene definido formalmente un perfil de usuario

		0%	Tiene un perfil de usuario formalmente definido, pero puede utilizar opciones de sistema o ingresar a ciertos módulos que no necesita
		0%	Puede utilizar opciones de sistema o ingresar a ciertos módulos que no necesita, además de no tener un perfil de usuario formalmente definido
		2%	Puede utilizar el sistema con total libertad, eso incluye agregar, modificar y borrar datos; puede utilizar cualquier opción de sistema y no cuenta con un perfil
Gestión de requerimientos	*Observaciones*		
	Con respecto a la atención de necesidades de su área (seleccione solo un inciso con una "x"):	41%	Las necesidades del área han sido resueltas por el área de TI y no se tienen requerimientos pendientes de implementar en los sistemas o plataforma
		21%	Las necesidades del área han sido atendidas por el área de TI y actualmente hay proyectos en curso para atender todos los requerimientos
		10%	Las necesidades más críticas del área han sido atendidas por el área de TI y actualmente hay proyectos en curso para atenderlas; los requerimientos pendientes de atender son parte de un plan de acción debidamente presentado y aceptado
		10%	Las necesidades más críticas del área han sido atendidas por el área de TI y actualmente hay planes de acción para atenderlas, pero los requerimientos pendientes de atender no tienen resolución planificada
		19%	El área tiene necesidades de cara a la plataforma tecnológica, pero no hay un plan de acción para atenderlas o se atienden de forma aleatoria
	Con respecto al mantenimiento evolutivo de los sistemas (seleccione solo un inciso con una "x"):	43%	Cuando hay requerimientos identificados, se trasladan al área de TI para ser resueltos por medio de un contrato de mantenimiento vigente con el proveedor
		11%	Cuando hay requerimientos identificados, se trasladan al área de TI para ser resueltos, en conjunto con personal experto ajeno al proveedor

		3%	Cuando hay requerimientos identificados, se trasladan al área de TI para ser resueltos solo con personal interno; el área participa para su resolución
		8%	Cuando hay requerimientos identificados, se trasladan al área de TI para ser resueltos solo con personal interno; el área de TI lo resuelve de forma unilateral
		35%	Cuando hay requerimientos identificados, se trasladan al área de TI para ser atendidos, pero no hay certidumbre de cuándo serán resueltos
	Con respecto a la aceptación de los sistemas (seleccione solo un inciso con una "x"):	8%	Los sistemas cumplen con las necesidades del área y no requieren de mantenimiento evolutivo
		62%	Los sistemas cumplen con las necesidades del área, pero existen oportunidades que pueden aprovecharse para la mejora continua del área
		19%	Los sistemas tienen brechas funcionales; el área de TI puede implementar soluciones eficientes para alargar la vida útil de los mismos
		5%	Los sistemas tienen brechas funcionales; el área de TI puede implementar soluciones eficaces temporalmente, pero debe ser reemplazado
		6%	Los sistemas han cumplido su vida útil, y el área de TI no puede implementar soluciones que sean técnica, funcional y/o económicamente factibles

Fuente: elaboración propia.

ANEXO 3: EVALUACIÓN DE CUMPLIMIENTO DE LAS NORMAS TÉCNICAS DE LA CGR PARA LA FUNCIÓN DE TI

A continuación, se presenta el resultado de la evaluación del nivel de cumplimiento de las Normas Técnicas de la CGR para la gestión y gobierno de TI aplicable a la Institución.

- *Criterios evaluados: 176* – Cantidad de criterios definidos en las Normas Técnicas que fueron evaluados en conjunto con la Función de TI.
- *Criterios cumplidos en su totalidad: 90* – Criterios que han sido formalmente implementados y cuentan con un instrumento (proceso, política o lineamiento) formalmente definido para gestionarlos.
- *Criterios cumplidos parcialmente: 20* – Criterios que cuentan con una práctica comúnmente aceptada por la Función de TI pero que no están debidamente formalizadas.
- *Criterios no cumplidos: 66* – Criterios que no cuentan con evidencias de implementación, ejecución y control por parte de la Función de TI.

Criterios totales	100%		Criterios que cumple parcialmente	11.36%
Criterios que cumple totalmente	51.14%		Criterios que no cumple	37.50%

A continuación, se presenta el detalle de las respuestas de la Función de TI con respecto al cumplimiento de cada criterio evaluado de las Normas Técnicas de la CGR.

	Criterio	Respuesta	Observaciones
Capítulo I Normas de aplicación general			
1.1 Marco estratégico de TI	Se tiene un marco estratégico de TI documentado y formalizado	Si	Vigencia 2016 - 2020
	Se tienen las políticas y procedimientos de TI documentados y formalizados	No	Pendiente de aprobación por parte del CETAC; finales de octubre cierra proyecto Normas CGR
	Se comunica a la Institución el marco estratégico de TI	Si	Página Web
	Se evalúa el nivel de dominio de las acciones y responsabilidades que los usuarios pueden hacer relacionado con TI	No	
	Se evalúa el nivel de satisfacción de los usuarios relacionado con el servicio que recibe del área de TI	No	Solo auditorías; validar
	Se cuenta con una unidad de gobierno de TI multidisciplinario	No	Solo la CITI y la PMO
	Se cuentan con políticas y planes de capacitación para el personal de TI	Parcial	No se cuenta con una política formal; se tienen planes con base en los proyectos ejecutados y concluidos; falta de acceso a las herramientas de TI; tienen limitación a nivel administrativo sobre la cantidad de capacitaciones que pueden recibir
1.2 Gestión de la calidad	Se cuenta con políticas y procedimientos de gestión de calidad de productos y servicios	Si	
	Se cuentan con un catálogo de productos y servicios de TI, con sus respectivos dueños/responsables de los mismos	Si	
	Se cuenta con lineamientos para garantizar la calidad	Si	
	Se cuentan con indicadores de desempeño relacionado con la entrega de productos y servicios de TI	Parcial	Servicios tercerizados

	Criterio	Respuesta	Observaciones
	Se evalúa la brecha de atención entre productos y servicios de TI y las necesidades de los usuarios y la Institución	Parcial	Las iniciativas se revisan con los usuarios finales; hay pendientes de ejecutar
1.3 Gestión de riesgos	Se cuenta con políticas y procedimientos de gestión de riesgos de TI	Si	SEVRI
	Se cuenta con lineamientos para la identificación y valoración de riesgos de TI	Parcial	Si se cuentan con lineamientos para valorarlos
	Todos los riesgos identificados tienen controles evaluados	Parcial	Hay valoración de riesgos y controles; falta validar vinculación entre ellos
	Se cuentan con procedimientos para cuantificar riesgos materializados, incidentes y su impacto	No	Cuentan con un inventario de riesgos materializados, no se han cuantificado; la persona responsable se retiró
	Se cuentan con procedimientos para atender riesgos no identificados	No	
1.4 Gestión de la seguridad de la información	Seguridad de Información:		
1.4.1 Implementación de un marco de seguridad de la información	Se cuenta con un marco formal de seguridad de información	No	Tiene apartados generales para desarrollo de prácticas de seguridad; el plan final requiere su aprobación
	El marco de seguridad de información está actualizado y vigente	No	Depende de la aprobación de las políticas y su implementación
	Se cuenta con procedimientos para medir el nivel de desempeño de los procesos de seguridad de información	No	ídem
	Se cuenta con procedimientos para atender y priorizar incidentes de seguridad	No	

	Criterio	Respuesta	Observaciones
	Se cuenta con una unidad de seguridad de información con responsabilidades y roles definidos	No	
1.4.2 Compromiso del personal con la seguridad de la información	El personal Institucional conoce las normas de seguridad de información	No	falta formalizarlo
	El personal Institucional está capacitado en temas de seguridad de información	Parcial	Se han dado charlas pero no han sido suficientes
	El personal es evaluado con respecto a su nivel de conocimiento en temas de seguridad de información	No	
	Hay sanciones definidas por incidente de seguridad materializado por el personal de TI	No	
	Se cuentan con acuerdos de confidencialidad	parcial	Para entrega de usuarios para correo electrónico y acceso a la plataforma (AD)
1.4.3 Seguridad física y ambiental	Se tienen controles de acceso físicos a centros de procesamiento de TI	Si	
	Se tienen controles de acceso físicos a áreas de trabajo	Si	
	Se tienen lugares seguros designados para custodia y control de activos de TI	Si	
	Se tiene control de entrada y salida de activos de TI	Si	Formulario y bitácora
	Se tienen controles ambientales en centros de procesamiento de TI	No	Cuarto para procesamiento mínimo
	Se tienen procesos formales de desecho de activos y destrucción segura de información	Parcial	Destrucción segura no
	Se tienen identificados y controlados riesgos ambientales	No	
	Se cuentan con bitácoras de trabajo de personal en lugares de procesamiento de TI	Si	

	Criterio	Respuesta	Observaciones
	Se cuentan con bitácoras de trabajo de personal en activos de TI	No	
1.4.4 Seguridad en las operaciones y comunicaciones	Se cuentan con mecanismos de seguridad en activos de comunicación y operación	Si	CODISA
	Se realizan actividades de monitoreo de uso y acceso a redes de comunicación y operaciones	Si	ídem
	Se cuentan con procedimientos de atención de incidentes de comunicación	Si	ídem
	Se cuentan con procedimientos de actualización de controles de seguridad en la plataforma de comunicaciones	Si	ídem
1.4.5 Control de acceso	Se cuentan con lineamientos de gestión control de acceso	Si	
	Se cuenta con procedimientos y lineamientos de definición de perfiles con sus respectivos permisos de acceso a recursos tecnológicos y funciones relacionadas	Parcial	Para ciertas aplicaciones y servicios
	Se cuentan con perfiles definidos para usuarios técnicos, administrativos y funcionales	No	
	Se cuenta con un inventario actualizado de usuarios con permisos de acceso	Si	Pendiente entrega de inventario de perfiles por sistema y AD
	Se tienen designados responsables para el otorgamiento/revocación de permisos	No	Se tienen identificados pero no está formalizado
	Se documenta el otorgamiento y revocación de permisos	Si	
	Se cuentan con mecanismos de autenticación robustos	Si	
	Se documentan intentos de accesos no permitidos o materialización de riesgos de acceso	No	
	Se cuentan con bitácoras de uso y pistas de auditoría	Parcial	SIFCO si

	Criterio	Respuesta	Observaciones
	Se cuenta con controles para acceso a documentación física, repositorios y almacenes de respaldos	Si	Repositorios particulares son administrados por los usuarios / áreas, documentos físicos lo administra Archivo; se administra por oficio la entrega de documentos de TI físicos; también la entrega de activos digitales
1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica	Se cuentan con lineamientos de desarrollo de sistemas y estandarización de equipos tecnológicos	No	
	Se cuentan con contratos de mantenimiento vigentes para toda la plataforma tecnológica	Parcial	Hay sistemas que no cuentan con mantenimientos
	Se controlan los contratos de mantenimiento de terceros, alcances definidos y riesgos por terminación del servicio	Parcial	Controles por terminación no se tienen
	Se cuentan con ambientes separados de desarrollo, pruebas y producción	Parcial	No está estandarizado
	Se cuentan con cronogramas de trabajo de mantenimiento preventivo	Parcial	ídem
	Se cuentan con bitácoras de trabajos de mantenimiento y resultados obtenidos	Si	
	Se cuentan con controles para resguardar códigos fuentes y versiones de software	No	
1.4.7 Continuidad de los servicios de TI	Se cuenta con una política de continuidad de TI	No	En desarrollo, requiere su aprobación e implementación
	La continuidad de TI está alineada con la continuidad de Negocio	No	No hay plan de continuidad de negocio
	Se cuentan con procesos de recuperación de desastres	No	En proceso
	Se cuentan con procesos de levantamiento de centros de procesamiento contingentes	No	

	Criterio	Respuesta	Observaciones
	Se cuenta con respaldos de la plataforma tecnológica, incluyendo datos	Si	
	Se realizan pruebas para certificar los procesos contingentes de TI y su desempeño	No	Requiere implementación
	Se tiene un equipo encargado de la continuidad de servicios de TI y recuperación de operaciones normales	No	Ídem
1.5 Gestión de proyectos	Se cuenta con un marco de gestión de proyectos	Si	Sujetos al PETI
	Se cuenta con un portafolio de proyectos formal	Si	Ídem
	Se ejecuta el portafolio de proyectos	Si	
	Los proyectos se ejecutan controlando la triple constante (tiempo, costo, alcance)	Si	
	Se controlan los contratos relacionados	Si	Excluyendo software donados
	Se gestionan las relaciones con grupos de interés	Si	
	Se gestiona la calidad de los entregables	Si	
	Se gestiona el equipo ejecutor	Si	De cara a la administración de proyectos y entrega de servicios
	Se gestionan los riesgos	Si	A través del SEVRI
1.6 Decisiones sobre asuntos estratégicos de TI	Se cuenta con un comité de TI	Si	
	El área participa en la toma de decisiones	Si	
	Se cuantifican beneficios /costos de oportunidad de inversiones en TI	Si	
	Se evalúa la brecha de las capacidades de TI y las necesidades de negocio	No	Proyectos de negocio son más impositivos por las áreas
	Se identifican y documentan tendencias y oportunidades relacionadas con TI	No	Vinculante con proveedores de servicios de TI

	Criterio	Respuesta	Observaciones
	Se identifican proyectos e inversiones alineados con la visión de la Institución	Si	
1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI	Se tiene un inventario de marcos normativos y jurídicos a los que TI está sujeto	Si	Entregar inventario
	Se evalúa el nivel de cumplimiento de obligaciones relacionadas con la gestión de TI	Si	IGI
	Se cuentan con planes de acción para remediar incumplimientos	No	
Capítulo II Planificación y organización			
2.1 Planificación de las tecnologías de información	El marco de gestión está alineado con los objetivos Institucionales	Si	
	Cuenta con misión, visión y objetivos específicos	Si	
	Se cuenta con la documentación suficiente que respalde la planificación de TI	Si	Para cada proyecto se cuenta con estudio de mercado; se cuenta con la documentación base para el desarrollo del PETIC vigente
2.2 Modelo de arquitectura de información	Se cuenta con un modelo de arquitectura de información y diccionario de datos	No	Modelado de datos pendiente de desarrollar
	Se evalúa la brecha de la arquitectura existente y las necesidades de la Institución	No	Pendiente proyecto anterior
	Se cuenta con un inventario de activos de tecnología	Si	

	Criterio	Respuesta	Observaciones
2.3 Infraestructura tecnológica	Se cuenta con respaldo y mantenimiento de todos los activos	Si	Plataforma: Codisa; No hay respaldos colectivos de PC; Computadoras de arrendamiento: PC Central
	Se evalúa el nivel de capacidad y disponibilidad de la plataforma	Si	Codisa
2.4 Independencia y recurso humano de la Función de TI	La unidad de TI es autosuficiente en su operaciones y funciones de las áreas usuarias	No	
	Cuenta con una estructura operativa clara y definida	Si	No hay funcionarios suficientes
	Se define una estructura bajo la premisa de segregación de funciones	Si	
	Cuenta con personal suficiente e idóneo	No	
2.5 Administración de recursos financieros	Cuenta con presupuesto suficiente	Si	
	Ejecuta su presupuesto	Si	
	Realiza rendición de cuentas	Si	Ante Contraloría y Admin. Superior
Capítulo III Implementación de tecnologías de información			
3.1 Consideraciones generales de la implementación de TI	Se cuentan con políticas para atender el gobierno, gestión y operación de TI	Parcial	Pendiente de formalizar
	Se cuentan con lineamientos para la definición de términos de referencia para la adquisición de productos y servicios de TI	No	Ídem
	Se cuenta con el respaldo para la ejecución de proyectos	Parcial	Resistencia
	Los grupos de interés participan en la implementación de TI	Parcial	No hay participación activa

	Criterio	Respuesta	Observaciones
	Se cuentan con líderes de proyecto, técnicos y funcionales	Si	
	Se realizan estudios técnicos, económicos y de factibilidad	Si	
	Se vela por la independencia de la Institución con proveedores en temas de TI	Parcial	Caso Codisa
	Se identifica la documentación necesaria	Si	
	Se cuentan con políticas y lineamientos de documentación de lecciones aprendidas y transferencia de conocimiento	Si	PMO
	Se cuenta con un modelo de gestión del cambio	Si	
3.2 Implementación de software 3.3 Implementación de infraestructura tecnológica	Se gestionan requerimientos técnicos y funcionales	Si	
	Se implementan estándares de desarrollo, aprovechamiento de código, estructuras de datos, interconexión, entre otros	No	
	Se cuentan con estándares de configuración	Si	Mínimos requeridos según la plataforma
	Se cuentan con estándares de seguridad de información (confidencialidad, integridad y disponibilidad)	Si	Ídem
	Se cuentan con políticas y procedimientos de pruebas	Si	
	Se cuentan con criterios de aceptación definidos	Si	
	Se cuentan con procesos de certificación de implementación de software en ambiente de producción y cierre de actividades	No	Se tiene la práctica; falta estandarizar y formalizar

	Criterio	Respuesta	Observaciones
	Se gestionan los cambios en la Institución y la plataforma de TI	Si	
	Se realizan controles de versiones	Si	
3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura	Se cuenta con lineamientos de adquisición de servicios de terceros	No	Falta formalizar
	Se cuenta con una gestión de servicios de terceros	No	Se tiene la práctica; falta formalizar
	Se evalúa el nivel de satisfacción del servicio de terceros	No	ídem
	Se cuenta con un proceso de transferencia tecnológica al finalizar los servicios	Si	
	Se cuentan con planes contingentes en caso de interrupción o terminación de servicios de terceros	No	Falta formalizar
Capítulo IV Prestación de servicios y mantenimiento			
4.1 Definición y administración de acuerdos de servicio	Se tienen procedimientos de confección de SLAs	No	Falta formalizar
	Se tiene un inventario de SLAs por servicios, productos y usuarios, con sus respectivos indicadores de desempeño	Si	ídem
	Se definen los responsables de los SLAs	Si	
	Se evalúa el desempeño de los SLAs	No	Falta implementarlos
	Los SLAs desarrollados están formalizados	No	Ídem
	Se ejecutan procesos de revisión y actualización de SLAs	No	Ídem

	Criterio	Respuesta	Observaciones
4.2 Administración y operación de la plataforma tecnológica	Se cuenta con la documentación suficiente para administrar y operar la plataforma tecnológica	No	La Administración está a cargo del servicio tercerizado
	Se evalúa la brecha tecnológica en temas de operación, obsolescencia y capacidad	No	Se tiene los lineamientos para una nueva contratación, requiere revisión y aprobación
	Se planifica la capacidad de la plataforma	No	
	Se gestionan los cambios y el impacto por actualización de la plataforma	Parcial	Se gestiona el cambio; no se cuantifica el impacto por actualización
	Se cuenta con documentación que respalde la operación de la plataforma	Si	informes mensuales, minutas, correos
	Se administran los ambientes de la plataforma de forma permanente	Si	Codisa
	La plataforma cuenta con soporte y mantenimiento	Si	Ídem
	Se cuenta con procesos de respaldo y recuperación de la plataforma	Si	Ídem
4.3 Administración de los datos	Se cuenta con políticas de gestión, control, custodia, traslado, y destrucción de activos de datos	No	
	Se cuenta con un inventario de activos de información y datos	No	
	Los activos de datos tienen vigencia	No	
	Los activos de información tienen responsable asignado	Si	
	Se evalúa el control de los datos, procesamientos, seguridad y disponibilidad	No	Se gestiona control de datos y respaldos
	Se cuentan con políticas y procedimientos de calidad de datos	No	

	Criterio	Respuesta	Observaciones
4.4 Atención de requerimientos de los usuarios de TI	Se cuenta con un inventario de requerimientos de usuarios de TI	Si	
	Se evalúa la brecha entre requerimientos de los usuarios y las capacidades de TI	Si	falta capacidad de atención
	Se realiza una planificación de mejora continua con base en los requerimientos de los usuarios de TI	No	Más bien son "apagafuegos"
	Se atienden los requerimientos de forma eficaz, eficiente y oportuna	No	Ídem
	Se tiene un plan de capacitación en temas de TI para usuarios funcionales	Parcial	Se tiene la práctica; se define en función del alcance de un proyecto
4.5 Manejo de incidentes	Se cuenta con lineamientos de atención de incidentes	Si	Mesa de ayuda
	Se tienen identificados y priorizados los incidentes de TI	Si	
	La atención de incidentes cuenta con SLAs	Si	
	Se cuenta con una mesa de ayuda	Si	
	Se evalúa el nivel de atención de incidentes	No	Falta de capacidad de atención
	El personal Institucional está capacitado para atender incidentes según el debido proceso	No	No tienen esa funcionalidad
	Se cuenta con una base de conocimiento para atención de incidentes	Si	
	Se cuenta con procedimientos de mejora continua	No	
4.6 Administración de servicios prestados por terceros	Se cuentan con políticas de adquisición de servicios de terceros formal	No	Falta formalizar
	Se tiene definido los roles y responsabilidades a adquirir por medio de terceros	Si	

	Criterio	Respuesta	Observaciones
	Se tienen contratos formales y vigentes con terceros	Si	
	Los contratos con terceros están alineados con las políticas de la Institución relacionados con Talento Humano	No	
	Se evalúa el nivel de desempeño y cumplimiento de servicios de terceros	Si	
	Existen procesos de transferencia de funciones y conocimiento por terminación de servicios	Si	
Capítulo V Seguimiento			
5.1 Seguimiento de los procesos de TI	Se tienen documentados los procesos de TI	Si	faltan formalizar
	Se evalúa el nivel de desempeño y efectividad de los procesos de TI	No	
	Se tienen definidos los indicadores de desempeño de TI a nivel Institucional	Si	
	Se tienen procesos continuos de mejora continua y evolutiva	Si	faltan formalizar
	Los procesos están alineado a la Arquitectura Empresarial	No	
5.2 Seguimiento y evaluación del control interno en TI	Se cuenta con políticas y procedimientos de control interno de TI	Si	
	Se cuenta con un inventario de controles, debidamente valorados	Si	
	La gestión de riesgos y controles está alineada a la metodología de riesgos de la Institución	Si	

	Criterio	Respuesta	Observaciones
	La mitigación de riesgos está dentro del nivel de aceptación Institucional	No	Revisar SEVRI
	Se evalúa el nivel de desempeño y efectividad de los controles de TI	Si	
	Se evalúa el nivel de brecha de alcance de los controles de TI	Si	
	Se cuentan con políticas y lineamientos de acciones de remediación de incumplimientos o debilidades	Si	
	Se cuentan con un inventario de excepciones a la implementación de controles, debidamente justificados	Si	
5.3 Participación de la Auditoría Interna	Se cuenta con participación y apoyo del área de Auditoría Interna	No	Participación reactiva; falta capacidad para atender recomendaciones
	Se desarrollan evaluaciones periódicas	Si	
	Se cuentan con planes de acción para mitigación de hallazgos y atención de recomendaciones	No	

Fuente: Elaboración propia, con base en los criterios establecidos en las Normas técnicas para la gestión y el control de las Tecnologías de Información (N2-2007-CO-DFOE) de la CGR.

ANEXO 4: EVALUACIÓN DE RIESGOS Y CONTROL INTERNO DE TI

A continuación, se presenta el detalle de la evaluación de riesgos que impactan la debida gestión, control y ejecución de actividades y servicios vinculantes con la Función de TI. Estos riesgos fueron evaluados de forma individual por miembros de la Unidad de TI de la DGAC.

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
1	No acceso a infraestructura del centro de datos debido a fallas en enlaces de comunicación	Proceso	9	20	16	4	6	Dependemos 100% de la empresa CODISA en donde informática no tiene acceso a la administración de los servidores. Por culpa de un contrato impuesto y mal realizado
2	No acceso a infraestructura del centro de datos por fallas en el equipo perimetral de seguridad	Proceso	6	4	12	4	16	La seguridad depende 100% de la empresa CODISA.
3	No acceso a infraestructura del centro de datos por fallas en servidores	Proceso	6	15	12	2	10	Constantemente se dan fallas de los servidores y hay que estar poniendo tickets a CODISA.
4	Falla en los equipos de la plataforma de VoIP	Proceso	6	4	9	2	15	
5	Fallas en la plataforma de virtualización y ambientes	Proceso	6	5	15	4	20	Si se dan fallas en el VMWARE solo CODISA puede accesar a la plataforma TI de la DGAC no tiene acceso.
6	Incompatibilidad tecnológica con la plataforma Institucional	Proceso	4	3	9	3	10	Si existe compatibilidad con la plataforma.

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
7	Infraestructura tecnológica insuficiente	Proceso	6	6	20	2	5	Muchos casos se ha dado que se han tenido que cerrar servidores con poco uso debido a que la capacidad de CODISA estaba muy limitada.
8	Fallas en la Plataforma Tecnológica que soporta los activos de apoyo Institucional (fuera del centro de datos)	Proceso	6	3	9	2	15	
9	Pérdida de servicios en la infraestructura de sistemas por modificaciones/actualizaciones a la plataforma tecnológica	Proceso	9	4	12	3	10	
10	Falla de los equipos para usuarios finales	Proceso	6	6	4	6	16	muchas veces se han dado casos lo importante es que resguardando la información se puede sustituir por otro equipo.
11	Interrupciones en el uso de la plataforma	Proceso	8	2	9	2	15	
12	Información incompleta o errónea para realizar las labores Institucionales	Información para la toma de decisiones	9	9	12	2	10	
13	Atraso en el procesamiento de la información en los sistemas	Proceso	12	2	9	4	15	

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
14	Accesos no autorizados por falta de seguridad lógica en el perímetro externo	Proceso	6	2	16	4	10	
15	No contar con la información precisa, oportuna y correcta	Información para la toma de decisiones	6	4	12	6	5	
16	Fallas en la continuidad y seguridad del servicio	Proceso	6	4	6	3	9	
17	Fallas en la plataforma de seguridad física	Proceso	6	4	9	3	15	
18	Fallas en la plataforma de seguridad lógica	Proceso	6	4	8	4	15	
19	Pérdida de información irrecuperable	Información para la toma de decisiones	6	4	20	4	10	
20	Gestión insuficiente de respaldos	Proceso	6	6	8	3	15	
21	Debilidades para la autenticación de programas / instalación de equipo ilegal	Proceso	4	8	8	4	10	
22	Debilidades en el monitoreo de la plataforma tecnológica	Información para la toma de decisiones	12	9	12	15	3	el monitoreo de la plataforma es 100% actividad de CODISA ya que TI no puede monitorear ni administrar.

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
23	Defectos o incidentes reportados del sistema desatendidos	Proceso	6	8	6	3	4	
24	Capacitaciones insuficientes	Proceso	6	3	2	6	20	
25	Ausencia de seguimiento oportuno del cumplimiento contractual	Gestión de proyectos	6	4	3	9	12	
26	Debilidades en la adquisición de insumos para la evaluación de la ejecución del servicio asociado	Información para la toma de decisiones	9	4	2	9	6	
27	Incumplimiento de los lineamientos establecidos a nivel contractual	Entorno	6	4	3	4	16	
28	Capacidad de gestión del servicio insuficiente	Proceso	9	9	9	4	16	
29	Entrega tardía de servicios y/o productos	Proceso	4	4	6	3	5	
30	Fallas en el diseño y requisitos de la plataforma tecnológica	Proceso	6	4	6	2	9	
31	Capacidad para la atención de usuarios insuficiente	Proceso	12	4	16	9	25	la parte de soporte posee una gran deficiencia debido a que solo un funcionario cumple esta área.
32	Capacidad de la contraparte técnica insuficiente	Proceso	9	4	12	6	9	Riesgo establecido hace muchos años y nunca se le ha pasado por encima como lo es el personal idóneo para cubrir las

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
								casi 500 plazas con las que cuenta la DGAC.
33	Falta de experiencia del equipo responsable del servicio	Proceso	6	1	2	3	5	El personal si cuenta con la experiencia para dar el servicio.
34	Carencia de información adecuada para el proceso de Mantenimiento	Proceso	6	4	6	4	5	
35	Desatención de recomendaciones de mejora	Proceso	6	1	3	4	5	
36	Inadecuado mantenimiento preventivo	Proceso	9	1	12	4	10	por el personal tan escaso en esta área el mantenimiento no es el más adecuado
37	Debilidades con la ejecución de tareas críticas de TIC soportadas por terceros	Proceso	9	1	9	9	20	se ha tenido debilidad con el soporte que brinda CODISA ya que solo ellos pueden realizar ejecuciones de tareas, se depende al 100% de ellos
38	Adquisición o desarrollo de tecnología sin la participación de TI	Proceso	12	1	3	9	15	Se ha dado casos de comprar sin el consentimiento de TI en equipos de oficina como los son impresoras o copiadoras.
39	Cambios en el alcance del servicio / prioridades Institucionales	Entorno	4	1	3	2	9	
40	Cambios en el Marco Jurídico externo vigente	Entorno	6	2	2	2	9	

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
41	Cambios en el Marco Normativo interno vigente	Entorno	9	1	2	2	9	
42	Pérdida de competitividad	Entorno	4	1	6	2	12	
43	Insatisfacción de los usuarios por el servicio brindado	Entorno	9	4	12	9	10	es muy importante el servicio que se le brinda al usuario interno como externo es por eso que desde hace años se ha establecido el escaso personal de TI y nunca se le ha dado la relevancia necesaria.
44	Obsolescencia tecnológica	Proceso	6	1	2	3	5	
45	Incumplimiento de las expectativas del proyecto	Entorno	6	2	3	6	10	
46	Recursos presupuestarios insuficientes	Proceso	6	4	8	8	8	
47	Brechas de cumplimiento normativo/jurídico	Entorno	6	4	2	2	2	
48	Incumplimiento de Acuerdos de Nivel de Servicio (SLAs)	Proceso	4	4	2	4	1	
49	Renuncia del contratista	Proceso	8	1	2	4	1	
50	Cancelación del contrato	Entorno	4	1	3	4	1	
51	Personal Institucional insuficiente para atender los servicios de TI	Proceso	16	9	20	9	20	punto establecido en valoraciones de riesgos años atrás.
52	Nivel de especialización insuficiente para atender los servicios de TI	Proceso	12	2	3	12	10	

№	Riesgo	Categoría	Criticidad R1	Criticidad R2	Criticidad R3	Criticidad R4	Criticidad R5	Observaciones
53	Disponibilidad insuficiente del personal para atender las necesidades Institucionales	Proceso	16	9	20	12	8	
54	Recursos materiales (equipo, infraestructura, herramientas, transporte, entre otros) insuficientes para atender las necesidades Institucionales	Proceso	9	3	8	8	15	
55	Fuga del personal	Proceso	20	1	16	6	25	Siempre se ha dado fuga de personal ante el escaso apoyo institucional y ante la negativa de mejora de plazas por la experiencia brindada a la institución
56	Falta de respaldo Institucional a la función de TI	Entorno	16	9	16	12	10	Se ha tenido un respaldo muy pobre a través de los años inclusive otras unidades le han ido quitando plazas a la unidad, riesgo que fue detectado hace muchos años como lo es el personal y se le ha pasado por encima siempre

Fuente: elaboración propia, con base en los criterios comúnmente aceptados de gestión de riesgo establecidos en la DGAC.

A continuación, se presenta el detalle de la evaluación de Control Interno de la Función de TI en la DGAC. Estos controles fueron evaluados de forma individual por miembros de la Unidad de TI de la Institución.

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
	Entorno de Control					
1	¿Se cuenta con un Plan Estratégico de TI alineado con el de la organización?	5	3	3	4	3
2	¿Se cuenta con un inventario de aplicaciones e interfases debidamente actualizado?	4	4	4	3	4
3	¿Se dispone de un procedimiento 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?	1	3	3	1	5
4	¿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.?	5	3	3	0	4
5	¿Se cuenta con un plan global de seguridad de T.I., que incluya en conjunto con inversiones apropiadas en servicios, personal, software y hardware?	5	3	4	0	4
6	¿Se cuenta con políticas de instalación de software seguro?	1	4	3	3	4
7	¿La estructura organizacional del área de T.I. es suficientemente robusta para atender las necesidades del negocio?	4	1	2	0	1
8	¿La documentación referente a los procesos de controles generales de TI (control de cambios y accesos) sobre los sistemas de información de la organización, se encuentran actualizados?	5	2	4	3	4
9	¿Se cuenta con manuales, normas, políticas y/o procedimientos para el proceso de Gestión de T.I.?	5	2	3	3	3

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
10	¿El personal del área de T.I., cuenta con la experiencia y habilidades necesarias para realizar su trabajo?	4	5	5	4	5
	Evaluación de Riesgos					
11	¿Se identifican los riesgos que pueden impedir el logro de los objetivos del proceso de Gestión de T.I.?	5	3	4	2	3
12	¿Se realiza un análisis de los riesgos del proceso, en función de la probabilidad de que los mismos se materialice y el impacto que se pudiera dar en dicho escenario?	5	2	4	2	5
13	¿La organización cuenta con un Plan de Continuidad de Negocio que incluya el plan de contingencia ante no disponibilidad de servicios de T.I.?	4	2	5		4
14	¿En la evaluación de riesgos del proceso se considera la probabilidad de fraude de T.I. para la consecución de los objetivos de negocio?	1	3	2	2	3
15	¿Una vez identificados y evaluados los riesgos, se define un plan de tratamiento que permita tener un menor riesgo residual?	1	2	3	2	4
	Actividades de Control					
	Seguridad de los Sistemas de Información					
16	¿Se dispone de un área o un funcionario de alto nivel encargado de la seguridad de T.I.?	2	1	2	2	3
17	¿Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) se identifican de manera única?	5	4	3	5	4
18	¿Los derechos de acceso del usuario a sistemas y datos están alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo?	4	4	4	3	3

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
19	¿Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad?	2	4	2	1	3
20	¿Se garantiza que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, son tomados en cuenta por la gerencia de cuentas de usuario?	3	5	4	2	4
21	¿Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios?	3	4	3	4	4
22	¿Se ha definido una matriz de segregación de funciones que permita evaluar e identificar conflictos en los perfiles y roles asignados a los usuarios y permisos sobre las transacciones o los datos que les son asignados?	2	4	2	3	3
23	¿La implementación de la seguridad de la información es probada y monitoreada de manera permanente?	3	2	2	2	2
24	¿La seguridad en TI es reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado?	2	3	2	2	4
25	¿La función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales y las mismas son atendidas en debida forma?	2	4	2	2	1
26	¿El proceso de asignación de permisos en los sistemas de información de la organización son asignados de acuerdo con perfiles predeterminados según matriz?	4	4	3	3	2
27	¿La política de acceso lógico para el ingreso a los sistemas de información y la configuración cumplen los estándares de buenas prácticas?	5	2	3	4	4

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
28	¿La compañía cuenta con una política de revisión y actualización de permisos en los sistemas de información y se esta se ejecuta en debida forma?	1	3	2	2	4
29	¿La compañía cuenta con políticas y actas en las cuales se indiquen los funcionarios que cuentan con la custodia de los usuarios con privilegios de administrador de los sistemas de información?	5	3	4	2	3
30	¿Los usuarios asignados a funcionarios retirados de la compañía son deshabilitados de los sistemas de información?	5	3	5	4	4
31	¿Se disponen de mecanismos para reportar incidentes? ¿Los mismos son atendidos en debida forma?	4	3	3	3	3
32	¿Se cuentan con medidas de prevención, detección y corrección (Parches de seguridad, control de virus actualizado, etc.), para proteger los sistemas de información contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.)?	4	3	4	4	
33	¿Se cuenta con técnicas y procedimientos de administración asociados (firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos, etc.) para autorizar acceso y controlar los flujos de información desde y hacia las redes?	5	4	4	4	4
34	¿Los accesos al centro de cómputo solo se permiten a personal autorizado?	5	4	5	5	5
35	¿Se aplica una política y se mantienen documentos que especifiquen los sistemas de información a los cuales se les toma copias de respaldo, la periodicidad y la custodia de la información?	5	3	2	4	3
36	¿Se cuenta con procesos de almacenamiento seguro de los" backups" de información de la organización?	5	3	3	4	4
37	¿Se cuenta con un Plan de Continuidad de Negocio que incluya planes de contingencia para la Gestión de T.I.?	4	2	4	2	4

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
38	¿Los planes de contingencia son probados de manera periódica para asegurar la continuidad del negocio y en particular el proceso de Gestión de T.I.?	3	2	2	2	5
39	¿Se garantiza que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen?	4	3	4	4	4
	Administración de Cambios					
40	¿Se está dando estricto cumplimiento a la política de administración y control de cambios?	4	3	4	2	5
41	¿Se garantiza que todas las solicitudes de cambio a programas se evalúan de manera estructurada en cuanto al impacto en el sistema operativo y funcional?	4	3	3	2	4
42	¿Las solicitudes de cambio a programas son categorizados y priorizados?	5	3	4	2	3
43	¿La migración de los cambios a programas a producción es debidamente autorizado por el nivel que corresponda según política?	3	4	3	2	4
44	¿Se da estricto cumplimiento a una política de cambio de emergencia?	3	3	3	2	4
45	¿Siempre se deja evidencia debidamente autorizada de los cambios realizados a programas?	5	3	4	3	3
46	¿Se realiza seguimiento y se mantienen actualizados a los solicitantes de los cambios con relación al estatus de los mismos?	5	3	2	3	3
47	¿La compañía cuenta con una política clara de desarrollo seguro y esta es aplicada al realizar las implementaciones en producción?	N/A	3	3	3	3
48	¿Siempre que se implementan cambios a los programas, se actualizan los procedimientos y documentación de usuarios correspondientes?	3	3	3	3	5

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
	Desarrollo de Sistemas					
49	¿El diseño detallado del software incluye entre otros los siguientes aspectos: definir y documentar los requerimientos de entrada de datos, definir interfaces, la interfaz de usuario, el diseño para la recopilación de datos fuente, la especificación de programa, definir y documentar los requerimientos de archivo, requerimientos de procesamiento, definir los requerimientos de salida, control y auditabilidad, seguridad y disponibilidad, y pruebas?	N/A	3	2	3	5
50	¿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?	2	3	3	3	4
51	¿Desde el punto visa de la seguridad y disponibilidad de aplicaciones, se consideran entre otro los siguientes asuntos en el desarrollo de sistemas: los derechos de acceso y administración de privilegios, ¿protección de información sensible en todas las etapas, autenticación e integridad de las transacciones y recuperación automática?	5	3	3	3	4
52	¿En la configuración e implantación de software adquirido se tienen en cuenta los siguientes aspectos: validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, la integración y los planes de prueba del sistema?	5	3	4	3	4
53	¿Con relación a la actualización de sistemas existentes se realizan análisis de impacto, justificación costo/beneficio y administración de requerimientos?	5	3	3	3	4

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
54	¿Respecto del desarrollo de software aplicativo se aprueban las especificaciones de diseño funcionales y técnicos; se asegura que el software aplicativo es compatible con la producción y está listo para su migración?, ¿Además, se garantiza que se identifica y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros?	N/A	N/A	3	3	3
55	¿Se define y se aplica un plan de aseguramiento de la claridad del software para obtener los resultados esperados en respuesta a los requerimientos, que incluyen criterio de calidad y los procesos de validación y verificación, inspección, revisión de algoritmos y código fuente y pruebas?	N/A	2		3	4
56	¿Se garantiza que, durante el diseño, desarrollo e implantación de software, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios?	N/A	3		3	4
57	¿Se desarrolla una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software que incluya la liberación planeada y controlada, la planeación de recursos, reparación de defectos de programa y corrección de fallas, pequeñas mejoras, mantenimiento de documentación, cambios de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de actualización, condiciones contractuales tales como aspectos de soporte y actualizaciones, revisión periódica de acuerdo a las necesidades del negocio, riegos y requerimientos de seguridad?	N/A	3		3	3
	Información y Comunicación					

№	PREGUNTA EVALUACIÓN CONTROL INTERNO	Respuesta R1	Respuesta R2	Respuesta R3	Respuesta R4	Respuesta R5
58	¿Las políticas sobre el uso de T.I.: código de ética, prácticas de seguridad, confidencialidad, estándares de integridad y responsabilidades de seguridad fueron comunicadas e interiorizadas por el personal de la organización?		2	4	3	4
59	¿Se divulgó y se está aplicando una política de clasificación de información de la compañía en: Pública, privada y confidencial, para asegurar el adecuado control y manejo de la información?		2	3	3	4
60	¿Se dispone de canales de comunicación para que los grupos de interés denuncien situaciones de fraude asociados al proceso de Gestión de T.I.?		2	4	2	5
	Supervisión y monitoreo					
61	¿Se hace seguimiento periódico al cumplimiento del Plan Estratégico de T.I.?	4	3	2	2	5
62	¿Se dispone de indicadores de desempeño para el proceso de Gestión de T.I.?	1	3	2	3	4
63	¿Se definen y cumplen los planes de acción de los dueños del proceso de Gestión de T.I. en respuesta a los hallazgos de las auditorias ya sean estas internas o externas?	4	3	3	3	3
	Suma	200	185	191	167	230
	Puntos	54	62	60	62	62
	Valoración del Control Interno	**3.7**	**3.0**	**3.2**	**2.7**	**3.7**

Fuente: Auditool.

Nota: El “R” se refiere a la identificación del colaborador de la Función de TI de la DGAC para fines de tabulación de la herramienta.

ANEXO 5: TENDENCIAS VINCULANTES CON TECNOLOGÍAS DE INFORMACIÓN

A continuación, se presentan para consideración de la Administración las principales oportunidades de desarrollo institucional, basadas en Tecnologías de Información.

- **Portal de Servicios a través de Internet:** Un Portal de Servicios puede ser definido como una extensión virtual de los diferentes servicios que la Institución provee en sus instalaciones utilizando como canal de entrega la red mundial de Internet. De esta manera, y bajo un principio de "negocio electrónico", se puede mantener contacto con todas las áreas funcionales que componen a la Institución, tanto las de las oficinas centrales como con las Instituciones relacionadas, clientes y proveedores de información y sobre todo con los usuarios finales de los servicios provistos por la Institución utilizando una "Intranet" o "Internet" como medio global.
- **Inteligencia de Negocios:** La cultura Informática de la Institución y la pronta introducción de Sistemas de Información como soporte a los sistemas sustantivos y de apoyo, han permitido lograr mayor conciencia sobre la necesidad de administrar con información, por lo que es fundamental contar con una plataforma robusta de Inteligencia de Negocios que permita una gestión operativa más robusta y un soporte estratégico a la toma de decisiones.
- **Flujos automatizados de procesos de negocio:** La realización de actividades coordinadas, en las que participan dos o más áreas de la Institución, demandan importantes recursos organizacionales tanto a nivel de personal, materiales y equipos de oficina como de logística. La automatización de los procesos que normalmente se realizan pasando formularios en papel, insumos impresos o por medio de canales descentralizados, puede representar a una organización un ahorro significativo en los gastos con inversiones relativamente bajas por cada puesto de trabajo.
- **Auditoría:** Oportunidad de mantener una plataforma centralizada y automatizada de las diferentes actividades relacionadas con un Sistema Integrado de Gestión y Control de Auditoría.
- **Planificación:** oportunidad el acompañamiento en la adquisición e implementación de herramientas que contribuyan a apoyar la unidad de Planificación, de manera que se facilite la concepción, seguimiento y evaluación de planes operativos y mejora continua.
- **Arquitectura Empresarial:** El objetivo principal de la Arquitectura Empresarial es diseñar, formalizar y gestionar un ambiente estructurado, alineando los procesos de negocio y sus relaciones, información, y arquitectura tecnológica con la visión de

negocio, aprovechamiento de oportunidades y ejecución de soluciones, gestión del cambio y planes de migración, bajo un marco de gobernabilidad de implementación, desarrollo y estandarización.

- **Aplicaciones móviles:** Incentivar el uso de aplicaciones móviles que centralicen la interacción de los usuarios internos y externos con los diferentes productos y servicios que la Institución ofrece, facilitando requerimientos como solicitudes de servicios, consultas y trazabilidad de estados de procesos, otorgamiento de productos, aclaraciones, intercambio de datos, pagos, actualización de información, entre otros.
- **Asistentes virtuales:** La implementación, entrenamiento y habilitación de asistentes virtuales que faciliten una interacción eficiente a las consultas más relevantes de los usuarios internos y externos, disminuyendo los tiempos de atención y requerimientos de disponibilidad del personal de la Institución, constituyendo además una base de conocimiento que facilite la estandarización de procedimientos, resoluciones y respuestas.
- **Inteligencia cognitiva:** La Inteligencia Cognitiva permite a los sistemas que la utilizan desarrollar capacidades lógicas y de soporte a las diferentes funciones tanto sustantivas como estratégicas y de apoyo, la cual se fortalece conforme la infraestructura tecnológica y los procesos vinculados maduren y se vuelvan más efectivos.

ANEXO 6: RECOMENDACIONES DE LA AUDITORÍA INTERNA A LA FUNCIÓN DE TI

A continuación, se listan las recomendaciones vigentes, emitidas por la Auditoría Interna de la DGAC, y consideradas dentro de la planificación de este estudio especial, que la Función de TI debe valorar y atender en función de su operación, estrategia y gestión.

- ✓ **Informe N. AI-13-2017:** "Evaluación de la operatividad, funcionalidad y seguridad del Sistema Integrado Financiero Contable SIFCO.

Recomendación	Dirigido a	Criterio
5. Definir un procedimiento para la revisión periódica de las bitácoras definidas en el sistema.	UTI	Cerrar - Se atiende con el cumplimiento de la recomendación 15 de este informe.
12. Asumir la resolución de la brecha operativa del SIFCO.	UTI	Cerrar – Se atiende con el cumplimiento de las recomendaciones 17 y 18.
13. Realizar la contratación para la resolución de la brecha operativa del SIFCO, con una participación activa de la UTI en términos de análisis de requerimientos, programación de las soluciones a las brechas.	UTI	Cerrar - Se atiende con el cumplimiento de las recomendaciones 17 y 18.
14. Asumir la resolución de las deficiencias en materia de NICSP debido a su carácter de obligatoriedad a la mayor brevedad posible.	UTI	Cerrar - Se atiende con el cumplimiento de las recomendaciones 17 y 18.

- ✓ **Informe № AI-15-2017:** "Auditoría Tecnologías de la Información".

Recomendación	Dirigido a	Criterio
2. Dar Seguimiento al Plan Estratégico e implementación de los proyectos definidos en la cartera de proyectos.	Dirección General	Cerrar – El PETIC actual termina su vigencia en diciembre del 2020. Se debe desarrollar un nuevo plan, considerado los requerimientos operativos, administrativos y estratégicos de la Institución. Esta recomendación se atiende con la recomendación 20.

Recomendación	Dirigido a	Criterio
5. Dar seguimiento al Plan Estratégico de Tecnologías de Información	UTI y PMO	Cerrar – El PETIC actual termina su vigencia en diciembre del 2020. Se debe desarrollar un nuevo plan, considerado los requerimientos operativos, administrativos y estratégicos de la Institución. Esta recomendación se atiende con la recomendación 20.
6. Dar seguimiento al Plan Estratégico 2016- 2020 e Implementar el Proyecto - CO3-003(Definir e implementar un proceso de gestión de la seguridad de la información para la DGAC).	UTI y PMO	Cerrar – El PETIC actual termina su vigencia en diciembre del 2020. Se debe desarrollar un nuevo plan, considerado los requerimientos operativos, administrativos y estratégicos de la Institución. Esta recomendación se atiende con las recomendaciones 11, 15,16, 20.
7. Dar seguimiento al Plan estratégico de Tecnologías de Información- “Proyecto Definición e implementación de un proceso de administración y operación de los servicios de TIC”.	UTI y PMO	Cerrar – El PETIC actual termina su vigencia en diciembre del 2020. Se debe desarrollar un nuevo plan, considerado los requerimientos operativos, administrativos y estratégicos de la Institución. Esta recomendación se atiende con las recomendaciones 9, 10, 20.
8. Reevaluar si es factible la implementación del proyecto “C03- 01 -Reorganización de la función de TIC de la DGAC: procesos y perfil del recurso humano”.	UTI y PMO	Cerrar – El PETIC actual termina su vigencia en diciembre del 2020. Se debe desarrollar un nuevo plan, considerado los requerimientos operativos, administrativos y estratégicos de la Institución. Esta recomendación se atiende con las recomendaciones 8, 20.
12. Facilitar capacitación técnicamente a los funcionarios de la Unidad de Tecnologías de Información en seguridad de la Información.	UTI	Cerrar – Esta recomendación se atiende con la recomendación 8.
15. No iniciar proyectos sin el Acta Constitutiva	UTI	Cerrar – Esta recomendación se atiende con la recomendación 12.
16. Modificar la Política DGAC-UTI-PO-005 –Seguridad Física y Ambiental	UTI	Cerrar – La naturaleza institucional, en especial por las condiciones de trabajo producto de la emergencia sanitaria nacional (COVID), ha cambiado, por lo que se requiere considerar una nueva política de seguridad física y ambiental. Esta recomendación se atiende con la recomendación 15.
17. Implementación de Controles	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 9, 10, 11, 15.
18. Buscar y Validar diferentes opciones para almacenar respaldos como medio paliativo para la protección de la información de la DGAC	UTI	Cerrar – Con base en las prácticas implementadas para la contratación de servicios especializados para el procesamiento, continuidad y seguridad de la información en sitio remoto, la

Recomendación	Dirigido a	Criterio
		Institución requiere de lineamientos para salvaguardar la integridad de la información, pero no de almacenamiento. Esta recomendación se atiende con la recomendación 15.
20. Pruebas de restauración de los respaldos de información	UTI	Vigente – La UTI no cuenta con procedimientos formales para realizar pruebas de restauración (excepto las que son parte de los procesos gestionados por el proveedor del centro de datos externo), y no hay evidencia de ejecución de pruebas recientes.
21. Creación de un esquema de clasificación formal de la información	UTI	Vigente – La UTI no cuenta con una política de clasificación formal de la información. Esta recomendación se complementa con la recomendación 12.
22. Creación de una política de seguridad para el uso de las impresoras	UTI	Cerrar – Esta recomendación se atiende con la recomendación 15.
23. Crear, definir y aprobar un proceso para el control de acceso a los sistemas	UTI	Cerrar – Esta recomendación se atiende con la recomendación 15.
24. Modificar el "Procedimiento Gestión de TI, punto 2.20 Revisión de privilegios	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 9, 10, 11, 15.
25. Implementar una adecuada segregación de funciones o controles que minimicen el riesgo de accesos no autorizados	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 9, 10, 11, 15.
26. Facilitar capacitaciones a los funcionarios de la Unidad de Tecnologías de Información en "Gestión de Servicios"	UTI	Cerrar – Esta recomendación se atiende con la recomendación 9.
27. Definir y aprobar un catálogo de servicios de Tecnologías de Información	UTI	Cerrar – La UTI ya cuenta con un catálogo de servicios. Esta recomendación se complementa con las recomendaciones 9, 10.
28. Definir, acordar y documentar acuerdos de nivel del Servicio	UTI	Cerrar – Esta recomendación se atiende con la recomendación 10.
29. Adecuar la herramienta considerando las necesidades de toda la organización	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 14, 16.
33. Diseñar y/o adoptar e implementar una política con la metodología de gestión integral del riesgo (seguimiento al proyecto CO3-002)	UTI	Cerrar – Esta recomendación se atiende con la recomendación 15.

Recomendación	Dirigido a	Criterio
34. Facilitar Capacitación al personal de TI en Gestión de Riesgos.	UTI	Cerrar – Esta recomendación se atiende con la recomendación 15.
35. Asignar responsabilidades para la Gestión Integral de Riesgos en la Unidad de Informática	UTI	Cerrar – Esta recomendación se atiende con la recomendación 15.

- ✓ **Informe № AI-01-2019:** "Evaluación de la Licitación Pública 2017LN-000001-00066000001.

Recomendación	Dirigido a	Criterio
2. Se recomienda realizar una reevaluación del mapa de ruta de la organización con respecto a las herramientas tecnológicas con que se cuenta en la actualidad y con las que debe contar para poder dar soporte a la gestión de la DGAC. Debe existir una relación directa entre los servicios que brinda la DGAC y las tecnologías que deben apoyar dichos servicios, es decir cuál es la visión de la DGAC, cuáles herramientas son requeridas para desarrollar esta gestión operativa y cómo el departamento de Tecnologías de Información estará apoyando dicha visión.	Dirección General	Cerrar – Esta recomendación se atiende con las recomendaciones 4, 5, 14, 16, 19, 20.
3. Establecer un mapa de procesos detallados de la gestión de la DGAC y cuáles herramientas (software, aplicaciones a la medida, hardware, servicios administrados, entre otros) deben soportar dicho mapa de procesos.	Dirección General	Cerrar – Esta recomendación se atiende con las recomendaciones 4, 8, 18.
4. Diseñar un plan de atención al mapa de procesos detallados y el perfilamiento de los proyectos necesarios para completarlo.	Dirección General	Cerrar – Esta recomendación se atiende con las recomendaciones 4, 5, 14, 16, 19, 20.

Recomendación	Dirigido a	Criterio
7. Cumplir en lo sucesivo con la normativa técnica existente interna y externa para la administración de proyectos de TI.	UTI	Cerrar – Esta recomendación se atiende con la recomendación 12.
8. Actualizar el expediente del proyecto 2017LN-000001-0006600001 con un documento de análisis de costo beneficio que contenga el detalle ampliado para el proyecto.	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones emitidas en el Informe N°AI-14-2019: "Evaluación del Centro de Datos Principal y Servicios Asociados implementado en la DGAC"
10. Actualizar el expediente del proyecto 2017LN-000001-0006600001 con: d. Un documento de plan de gestión de la calidad del proyecto. e. Un documento lista de chequeo que demuestre la trazabilidad del proceso de gestión de calidad. f. Los informes de estado de proyecto de acuerdo con el Manual de Gestión de Proyecto.	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones emitidas en el Informe N°AI-14-2019: "Evaluación del Centro de Datos Principal y Servicios Asociados implementado en la DGAC"
14. Redactar y formalizar institucionalmente una metodología para realizar un estudio de mercado para la DGAC que permita contar con información detallada y suficiente para la toma de decisiones apoyada en la normativa aplicable.	Proveeduría Institucional	Cerrar – La práctica interna en la Institución existe, y tiene lineamientos básicos basado en La Ley de Contratación Administrativa. Esta recomendación se complementa con la recomendación 19.
15. Redactar y formalizar institucionalmente una metodología para la elaboración de análisis costo beneficio que permita reducir el riesgo financiero de los proyectos.	Proveeduría Institucional	Cerrar – La práctica interna en la Institución existe, y tiene lineamientos básicos basado en La Ley de Contratación Administrativa. Esta recomendación se complementa con la recomendación 19.
16. Elaborar, oficializar, divulgar e implementar un mecanismo de control, que le permita en general velar y asegurar que las Unidades Solicitantes, cumplan con los Lineamientos en Contratación Administrativa que emite anualmente y en general con la LCA y su reglamento.	Proveeduría Institucional	Vigente – Validar la oficialización y divulgación de los mecanismos de control y su alineación con la LCA.

- ✓ **Informe N°AI-14-2019:** "Evaluación del Centro de Datos Principal y Servicios Asociados implementado en la DGAC".

Recomendación	Dirigido a	Criterio
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.	Dirección General	Vigente – No hay evidencia de este estudio.
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.	Dirección General	Cerrar – Esta recomendación se atiende con las recomendaciones 8, 9, 10, 11, 14, 16, 19, 20.
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).	UTI	Vigente – Se requiere recopilar la evidencia de los expedientes de los proyectos vigentes y terminados el PETIC vigente.
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.	UTI	Vigente – La contratación de servicios especializados para el centro de datos se mantiene en ejecución.
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.	UTI	Vigente – La contratación de servicios especializados para el centro de datos se mantiene en ejecución.
8. Realizar una valoración sobre el costo/beneficio de mantener los activos como están ahora en contraste con	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 8, 16.

Recomendación	Dirigido a	Criterio
su remplazo, el impacto Institucional de las alternativas existentes y la debida gestión a la decisión a tomar.		
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.	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 9, 10, 11, 14.
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.	UTI	Vigente – La contratación de servicios especializados para el centro de datos se mantiene en ejecución.
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.	UTI	Cerrar – Esta recomendación se atiende con la recomendación 15.
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.	UTI	Cerrar – Esta recomendación se atiende con las recomendaciones 9, 10, 11, 14.
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.	UTI	Cerrar – Esta recomendación se atiende con la recomendación 20.

Recomendación	Dirigido a	Criterio
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.		
14. Apoyar a la Unidad de TI para preparar y validar los requerimientos y términos de referencia requeridos en caso de terminación de contrato.	Proveeduría Institucional	Vigente – La contratación de servicios especializados para el centro de datos se mantiene en ejecución.

Con respecto al Informe № AI-16-2019: “Informe Adicional Evaluación del Centro de Datos Principal y Servicios Asociados implementado en la DGAC”, al ser una propuesta de lineamientos de Plan de Acción, su revisión queda embebido en la ejecución del estudio realizado y en las recomendaciones a emitir.