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

INFORME Nº AI-15-2017

AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN

DICIEMBRE, 2017

ÍNDICE

ÍNDICE DE CUADROS Y GRÁFICOS

ABREVIATURAS

Abreviatura	Significado
DGAC	Dirección General de Aviación Civil
CETAC	Consejo Técnico de Aviación Civil
PEI	Plan Estratégico Institucional
PETIC	Plan Estratégico de Tecnologías de información y Comunicación
SEVRI	Sistema Específico de Valoración del Riesgo Institucional
TI	Tecnologías de Información
TIC	Tecnologías de Información y Comunicación
Acuerdo de Nivel de Servicio Operativo (OLA)	OLA Operational Level Agreement. Es un acuerdo entre el proveedor de servicios de TI y otra parte de la misma organización. Este le da soporte al proveedor de servicios de TI para proporcionar servicios de TI a los clientes, y define los productos o servicios que deben prestarse y las responsabilidades de ambas partes.
Acuerdo de nivel de servicio (SLA)	Service Level Agreement (SLA). Acuerdo escrito entre el proveedor del servicio (Tecnología de Información) y el cliente (Usuario) que detalla el nivel de servicio acordado.
Administración de la configuración	Gestión encargada de definir y controlar los elementos de configuración que conforman la infraestructura tecnológica y que permiten la entrega de los servicios de negocio.
Administración del conocimiento	Conjunto de herramientas y bases de datos que se emplean para gestionar el conocimiento y la información.
Administración de incidentes	Proceso responsable de atender eficientemente las

Abreviatura	Significado
	solicitudes de servicio e incidentes reportados por los usuarios de los servicios de TIC.
Atención de solicitudes de servicio	Solicitud que hace un usuario pidiendo información (sobre funcionalidades de un sistema, procedimientos para la obtención de un servicio o disponibilidad de los mismos, etc.), asesoramiento o acceso a un servicio de TI. Por ejemplo, la inicialización de una clave, o provisionar a un nuevo usuario con Servicios de TI estándares.
Base de Datos de Conocimiento (Knowledge Data Base - KDB)	Es un tipo especial de base de datos para la gestión del conocimiento. Provee los medios para la recolección, organización y recuperación computarizada de conocimiento.
Catálogo de servicios	Es un documento estructurado con información correspondiente a aquellos servicios que actualmente se encuentran en operación o disponibles para la implementación (ya sea servicios de cara al cliente y servicios de soporte a los de cara al cliente). El Catálogo de Servicios es la única parte publicada de Portafolio de Servicios, y se utiliza para soportar la venta y entrega de los Servicios de TIC. El Catálogo de servicios incluye puntos de contacto y procesos que se gestionan a través de las solicitudes de servicio
CMDB (Configuration Management Data Base)	Base de Datos de Gestión de la Configuración. Es una base de datos que contiene detalles relevantes de cada EC (ítem/elemento de configuración) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de TI.
Ciclo de vida	Son las diferentes etapas en la vida de un servicio de TI, elemento de configuración, incidente, problema, cambio, solicitud, etc. El ciclo de vida define las categorías por estado y las transiciones de estado permitidas.
COBIT	Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) proporciona orientación y las mejores prácticas para la gestión de procesos de TI. COBIT es publicado por ISACA, en conjunto con el Instituto de Gobierno de TI (IT Governance Institute - ITGI). Para más información,

Abreviatura	Significado
	véase www.isaca.org
Competencias	Son aquellas características personales de los individuos (motivación, valores, rasgos, etc.) que le permiten hacer de forma óptima las funciones de su puesto de trabajo. Las competencias se deberán definir a nivel de rol o de perfil de puesto, según lo estipulado por las políticas de gestión de recursos humanos del Banco Central.
Elementos de Configuración (EC)	Cualquier Componente que necesite ser gestionado con el objeto de proveer un servicio de TIC. La información sobre cada EC se almacena en una base de datos de administración de la configuración (CMDB, por sus siglas en inglés) y es mantenido durante todo su Ciclo de Vida por Gestión de la Configuración. Los EC están bajo el control de los procesos de Administración de Cambios. Típicamente, los EC pueden ser servicios de TIC, hardware, software, edificios, personal, entre otros.
Estacionalidad	Relación de dependencia con respecto a un intervalo específico de tiempo. Ejemplo: demanda de servicios que presenta picos en ciertos periodos del año.
Incidente	Cualquier evento que no forma parte de la operación estándar de un servicio y puede causar, una interrupción o una reducción de calidad del mismo.
ITIL®	Es un conjunto de publicaciones de mejores prácticas para la gestión de servicios de TI. Es propiedad de la Oficina del Gabinete (parte del Gobierno de Su Majestad), ITIL proporciona guías de calidad para la prestación de servicios de TI y los procesos, las funciones y otras competencias necesarios para sustentarlas. El marco de trabajo ITIL se basa en el ciclo de vida de servicio y dicho ciclo consta de cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio), cada una de ellas tiene su propia publicación de apoyo. También hay una serie de publicaciones complementarias de ITIL que proporcionan orientación específica para sectores de la industria, tipos de organización, modelos operativos y arquitecturas de tecnología. Para más

Abreviatura	Significado
	información véase www.itil-officialsite.com.
ISO 20000	Es la norma internacional sobre Gestión de servicios de TI (ITSM), publicada por ISO (Organización Internacional de Normalización). La norma describe un conjunto de procesos de gestión diseñados para ayudarle a brindar servicios de TI más eficaces.
Portafolio de Servicios	Es el conjunto completo de servicios que son gestionados por un proveedor de servicios. El portafolio de servicios se utiliza para gestionar el ciclo de vida completo de todos los servicios, e incluye tres categorías: servicios bajo consideración (propuestos o en desarrollo), catálogo de servicios (en-producción o disponibles para su implementación), y servicios retirados. Véase también portafolio de acuerdos con clientes, gestión del portafolio de servicios
Proceso	Es un conjunto estructurado de actividades diseñadas para lograr un objetivo específico. Un proceso tiene una o más entradas definidas y las transforma en salidas definidas. Puede valerse de cualquier rol, responsabilidad, herramientas y controles de gestión que sean necesarios para entregar de forma confiable los resultados. Un proceso puede definir, si son necesarios, políticas, normas, directrices, actividades e instrucción de trabajo.
Tiempo de Ciclo	Es el tiempo en el que se llevan a cabo las etapas del proceso, desde que se inicia hasta que termina.
Sistema de Gestión de la Seguridad de la Información (SGSI)	Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información
ISO/ IEC 27 000	E s un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
WIFI	Redes Inalámbricas
Cifrado	Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave

Abreviatura	Significado
	necesaria para descifrarlos.
Patrocinador	El rol del patrocinador es fundamental para la ejecución exitosa de proyectos en cualquier área profesional, incluyendo la Tecnología de Información (TI), pues es quien realiza la principal labor de promoción y la procura del apoyo necesario dentro de la organización.
Kick Off	Reunión de arranque o inicio de proyecto
SLAS	Acuerdos para cumplir con las expectativas de sus clientes.
SIFCO	Sistema Integrado Financiero Contable
FAQ	Frequently Asked Questions. Lista de preguntas y respuestas que surgen frecuentemente dentro de un determinado contexto y para un tema en particular.
PMO	Del inglés project management office. Oficina de Gestión de Proyectos.
CITI	Comité Institucional de Tecnologías de Información

RESUMEN EJECUTIVO

El presente estudio responde a una necesidad de la Auditoría Interna del CETAC de realizar una evaluación del estado actual de los procesos de la Unidad de Tecnologías de Información, con el fin de determinar el cumplimiento de los criterios básicos de control que deben observarse en la gestión de las tecnologías de conformidad con las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República, Resolución R-CO-26-2007.

Los procesos incluidos en el alcance de esta auditoría son:

a) Gestión de Proyectos en TI.
b) Gestión de la Seguridad de la Información.
c) Prestación de Servicios y Mantenimiento.
d) Gestión de Riesgos de TI.

Como resultado de la auditoría desde la perspectiva de cumplimiento de los procesos se obtuvo que la Unidad de Tecnologías de Información requiere realizar un esfuerzo adicional para garantizar la implementación de los procedimientos establecidos para cada uno de los procesos.

Según lo refleja el informe y con base los procesos definidos por las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, algunos de éstos se encuentran documentados pero no ejecutados y otros son ejecutados pero no existe documentación formal, es por esto que es necesario documentar, revisar e implementar los procesos y procedimientos. Esto permitirá, además, de una revisión e identificación de puntos de falla o mejora, su optimización dará como resultado la entrega de un mejor servicio por parte de la Unidad de Tecnologías de Información.

El informe contiene 38 recomendaciones concretas, tendientes a que la Administración Activa, corrija las citadas deficiencias y cumpla así con la normativa aplicable en materia de gestión de Tecnologías de Información.

I. INTRODUCCIÓN

1.1.- NATURALEZA DEL ESTUDIO

La tecnología ha transformado la forma de hacer negocios y su presencia en las organizaciones es inminente, su impacto en las diferentes facetas del negocio ha conllevado a exigencias en cuanto a la coordinación de las operaciones y a la información que se procesa, almacena y transmite mediante las tecnologías de la información (TI). Por este motivo, TI se ha convertido en un recurso de gran valor que demanda una óptima gestión y una práctica eficiente de seguridad de la información, que permita establecer las estructuras, procesos, responsabilidades y mecanismos adecuados para proteger la información y la continuidad de las operaciones en apoyo a la estrategia institucional de la Unidad de Tecnologías de Información de la Dirección General de Aviación Civil.

Como respuesta a esta realidad, en junio del año 2007, mediante la Resolución del Despacho de la Contraloría General de República, se aprueban las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información", la cual es una "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."[1]

Consciente de esta realidad, la Auditoría Interna del CETAC decidió llevar a cabo un proyecto para evaluar el estado actual de las Normas Técnicas para la Gestión de las Tecnologías de Información emitidas por la Contraloría General de la Republica, alineado con el marco de referencia de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) y en apoyo a la misión de la Unidad de Tecnologías de Información, de "Ser la Unidad proveedora de servicios integrales que define los mecanismos de gestión y control requeridos en materia de tecnología de información y comunicaciones, para apoyar el cumplimiento de las labores de la Dirección General de Aviación Civil"

[1] Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)

1.2.-JUSTIFICACIÓN

El presente estudio se efectuó 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 2017 de esta Auditoria Interna.

1.3.-OBJETIVOS

1.3.1.- Objetivo general

Evaluar el cumplimiento de los criterios básicos de control que deben observarse en la gestión de las tecnologías de conformidad con las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República, Resolución R-CO-26-2007 del 07/06/2007, publicadas en "La Gaceta" № 119 del 21/06/2007 y verificar el avance en el Plan Estratégico de Tecnologías de Información y Comunicación (PETIC).
|

1.3.2.- Objetivos específicos

1. Revisar y validar el cumplimiento de recomendaciones anteriores. Seleccionar al menos ocho de las recomendaciones –relevantes– emitidas entre los Informes AI- 03-2014 y AI-04-2014, y evaluar las acciones informadas por la Unidad de Tecnologías de Información y emitir opinión sobre el adecuado cumplimiento o no; debidamente justificado

2. Gestión de Proyectos en TI. Verificar que la institución administre sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos, incluye al menos:

    2.1 Verificar la existencia de una adecuada metodología de administración de proyectos informáticos y evaluar el cumplimiento que realiza la Unidad de Tecnologías de Información a la metodología. Se debe considerar los siguientes puntos contenidos en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República de Costa Rica: 1.1 Marco estratégico 1.2 Gestión de la calidad 1.5 Gestión de proyectos 1.6 Decisiones sobre asuntos estratégicos 2.1 Planificación de las tecnologías de información.

2.2 Evaluar el cumplimiento de la planificación y ejecución de los proyectos, de conformidad con el PETIC; seleccionados por muestra. Considerando al menos: verificar que el avance –tiempo– la etapa de ejecución y que el costo de la implementación de la cartera de proyectos esté acorde con la planeación de los mismos, según el PETIC.

2.3 Verificar la existencia de una metodología para la administración de riesgos al menos sobre los proyectos más críticos.

3. Gestión de la seguridad de la información: Verificar que la institución garantiza de manera razonable, la confidencialidad, integridad y disponibilidad de la información, protegiéndola eficientemente contra uso, divulgación o modificación no autorizada, daño o pérdida u otros factores disfuncionales, incluye al menos:

3.1 Comprobar la existencia y aplicación de una adecuada política de seguridad de la información y de los procedimientos correspondientes.

3.2 Evaluar el marco de seguridad de la información y su cumplimiento.

3.3 Evaluar el compromiso del personal –entendimiento y divulgación– con la seguridad de la información.

3.4 Verificar que los recursos de TI están protegidos; en un ambiente seguro y controlado –Seguridad física y ambiental–.

3.5 Evaluar que la información esté protegida de accesos no autorizados y control de acceso.

4. Prestación de servicios y mantenimiento. Verificar que la función de TI garantice, de manera razonable, la entrega de servicios de TI concordantes con los niveles requeridos para la consecución de los objetivos institucionales, incluye evaluar y verificar al menos:

4.1 La definición y administración de acuerdos de servicios.

4.2 La administración y operación de la plataforma de servicios.

4.3 La administración de los datos

4.4 La atención de requerimientos de usuarios de TI.

4.5 El manejo de incidentes

4.6 La administración de servicios prestados por terceros.

5. Gestión de riesgos en TI. Evaluar la existencia de una metodología de gestión del riesgo de las tecnologías de la información (TI) que esté

integrada al sistema específico de valoración del riesgo institucional (SEVRI) y considere el marco normativo que le resulte aplicable para responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, incluye al menos:

5.1 Revisar y comprobar la existencia y aplicación de una metodología de gestión de riesgo informático integrada al SEVRI institucional.
5.2 Evaluar el cumplimiento de la normativa aplicable.
5.3 Verificar la universalidad del uso del SEVRI para la toma de decisiones y planificación de la Función TI.

1.4.- ALCANCE

1. El estudio de auditoría requerido, se enfocará hacia la evaluación verificación, de cada uno de los objetivos específicos.
2. El estudio de auditoría, se debe desarrollar con sujeción a:
   - La Ley General de Control Interno, Ley № 8292 del 31 de julio de 2002
   - Las “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información” (N-2-2007-CO-DFOE) emitidas por la CGR3, publicadas en “La Gaceta” № 119 del 21/06/2007
   - Las “Normas para el ejercicio de la auditoría interna en el Sector Público”, (Resolución R-DC-119-2009 del 16/12/2009), publicado en “La Gaceta” № 28 del 10 de febrero de 2010.
   - Las “Normas Generales de Auditoria para el Sector Público”, R-DC-64-2014, publicadas en “La Gaceta” № 184 del 25/09/2014 que rigen a partir del 01 de enero de 2015.
   - Los Procedimientos del Sistema de Gestión de la Auditoría Interna, certificados bajo la norma ISO 9001:2008.

1.5.- METODOLOGÍA

La Metodología utilizada es la definida por la Auditoría Interna y publicada en el Sistema de Gestión, cuyos procedimientos son certificados por la norma norma ISO 9001:2008.

1.6.- TIPO DE AUDITORÍA

Auditoría de Tecnologías de Información.

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)[2]
d. Normas Generales de Auditoría para el Sector Público (R-DC-064-2014)[3]
e. Las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" (N-2-2007-CO-DFOE) emitidas por la CGR3, publicadas en "La Gaceta" № 119 del 21/06/2007

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,

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

contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

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

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

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

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

> Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente.
>
> El jerarca, los titulares subordinados y los demás funcionarios públicos también incurrirán en responsabilidad administrativa y civil, cuando corresponda, por obstaculizar o retrasar el cumplimiento de las potestades del auditor, el subauditor y los demás funcionarios de la auditoría interna, establecidas en esta Ley.
>
> Cuando se trate de actos u omisiones de órganos colegiados, la responsabilidad será atribuida a todos sus integrantes, salvo que conste, de manera expresa, el voto negativo."

1.8.- CUMPLIMIENTO CON NORMAS GENERALES DE AUDITORÍA

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

1.9.- LIMITACIONES

- Para conocer la percepción de los usuarios de negocio sobre la calidad de los servicios de Tecnología recibidos, se envió una encuesta, sin embargo, la participación no fue representativa por lo que los resultados no serán tomados en cuenta para este informe.

1.10.- GENERALIDADES DEL ESTUDIO

En junio del año 2007, mediante la Resolución del Despacho de la Contraloría General de República, se aprueban las "Normas Técnicas para la

Gestión y el Control de las Tecnologías de Información", la cual es una "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.

Estructura de las Normas Técnicas

La normativa establece los criterios básicos a ser aplicados en la gestión de las tecnologías de la información.

Capítulo I Normas de aplicación general

1.1 Marco Estratégico de TI
1.2 Gestión de la Calidad
1.3 Gestión de riesgos
1.4 Gestión de la seguridad de la información
1.4.1 Implementación de un marco de seguridad de la información
1.4.2 Compromiso del personal con la seguridad de la información
1.4.3 Seguridad física y ambiental
1.4.4 Seguridad en las operaciones y comunicaciones
1.4.5 Control de acceso
1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica
1.4.7 Continuidad de los servicios de TI
1.4.8 Gestión de proyectos
1.4.9 Decisiones sobre asuntos estratégicos de TI
1.4.10 Cumplimiento de obligaciones relacionadas con la gestión de TI

Capítulo II Planificación y organización

2.1 Planificación de las tecnologías de información
2.2 Modelo de arquitectura de información
2.3 Infraestructura tecnológica
2.4 Independencia y recurso humano de la Función de TI
2.5 Administración de recursos financieros

Capítulo III Implementación de tecnologías de información

1.1 Consideraciones generales de la implementación de TI
1.2 Implementación de software

1.3 Implementación de infraestructura tecnológica
1.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura

Capítulo IV Prestación de servicios y mantenimiento

4.1 Definición y administración de acuerdos de servicio
4.2 Administración y operación de la plataforma tecnológica
4.3 Administración de los datos
4.4 Atención de requerimientos de los usuarios de TI
4.5 Manejo de incidentes
4.6 Administración de servicios prestados por terceros

Capítulo V Seguimiento

5.1 Seguimiento de los procesos de TI
5.2 Seguimiento y evaluación del control interno en TI
5.3 Participación de la Auditoría Interna

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 30 de enero del 2018 se remitieron notas con el fin convocar a la conferencia final con el propósito de atender, escuchar y valorar opiniones, discrepancias y aportes que puedan surgir de los resultados finales que obtuvimos durante el estudio. Este ejercicio se llevó a cabo el 12 de febrero del 2018 en la sala de reuniones de la Auditoría Interna, con la presencia, por parte de la Administración de la señora Malou Guzmán Quesada, Encargada de la Unidad de Tecnologías de Información, así como el señor Rolando Richmond Padilla, Sub Director General de Aviación Civil. En esa oportunidad no se presentaron observaciones al documento que propiciaran cambios de fondo al mismo.

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. Seguimiento a Recomendaciones Anteriores

Recomendación # 11 (INFORME AI-03-2014): Establecer y aprobar una política de seguridad que se encuentre alineada con los estándares internacionales.

Se comprobó el desarrollo de la política de seguridad de la información (**DGAC-UTI-PO-004)**, sin embargo está no ha sido implementada.

Recomendación # 20: (INFORME AI-03-2014): Establecer y aprobar un procedimiento para la revisión periódica de los privilegios otorgados en los sistemas.

En el apartado 2.20 del procedimiento “6P03- Gestión de TI” se desarrolló un procedimiento que define los pasos para la revisión periódica de los privilegios otorgados en los sistemas, sin embargo, no se identificaron registros del cumplimento del mismo.

Recomendación # 22: (INFORME AI-03-2014): Establecer y aprobar un procedimiento para el control de calidad en la documentación elaborada por la Unidad.

La recomendación fue acatada y la Unidad de Informática incluyó un procedimiento “Control de calidad en la documentación” en el apartado 2.21 del documento “Procedimiento 6P03 Gestión de TI”.

Recomendación # 2 (INFORME AI-03-2014): Elaborar un plan formal y aprobado donde se indiquen las acciones a seguir en caso de una eventualidad, basado en una normativa de continuidad de negocios.

La recomendación no ha sido implementada, En la cartera de proyectos se tiene identificado un proyecto para definir un proceso de la gestión de la continuidad de los servicios de TIC (C03-004), sin embargo, este debía iniciar en el año 2016 y a la fecha ni si quiera existe el acta constitutiva.

Recomendación # 3 (INFORME AI-03-2014): Elaborar un documento formal donde se indique la criticidad de la información de los sistemas.

La recomendación fue acatada y en el apartado "SISTEMAS EN PRODUCCIÓN" del Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) 2016-2020 se clasificaron los sistemas de información por su criticidad.

Recomendación # 4 (INFORME AI-03-2014): De ser posible, establecer procedimientos automáticos para el respaldo de la información y documentar las pruebas de legibilidad de respaldos.

La recomendación de establecer procedimientos automáticos para el respaldo de la información fue implementada, sin embargo, los respaldos son almacenados en los mismos servidores de producción, por lo que la institución está expuesta a perder sus copias de seguridad.

No se evidencian pruebas de restauración y legibilidad de los respaldos.

Recomendación # 8 (INFORME AI-03-2014): Establecer manual para la revisión de actividades de proveedores.

Se Incorporó el procedimiento en el apartado 2.7 Administración de Contrataciones TI y 2.12 Validación y pruebas de contrataciones TI en el procedimiento 6P03 Gestión de TI. No obstante, se indicó que no existen revisiones periódicas de las actividades de proveedores y ni documentación de las mismas.

2.2.- El Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) no está Alineado a los Objetivos Institucionales

Los objetivos estratégicos definidos en el PETIC están enfocados en gestionar las tecnologías de información, pero no en cómo garantizar el alineamiento de las TI con los retos y definiciones estratégicas de la DGAC.

En ninguna sección del documento del PETIC se hace referencia o se menciona una alineación con el Plan Estratégico Institucional (PEI), razón por la cual no es posible asegurar que las acciones estratégicas de TI que se definieron dentro del PETIC logren apoyar el alcance de los objetivos estratégicos y metas establecidas en el PEI.

Según el apartado 1.1 (marco estratégico,) de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (Resolución R-CO-26-2007 del 07/06/2007), el jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

Por lo que se deduce que los responsables del desarrollo del PETIC no consideraron el PEI, como la guía fundamental para establecer los objetivos estratégicos de las TI.

El no tener una Planificación de Tecnologías de Información alineada a los objetivos institucionales puede causar un espejismo tecnológico, invirtiendo en tecnologías y funcionalidades que no son necesarias o que no suplen las necesidades de los interesados y con ello comprometer la facilidad y crecimiento organizacional.

2.2.- Incumplimiento al Manual Metodológico para Administrar Proyectos de TI

La Unidad de Informática tiene un “Manual Metodológico para Administrar Proyectos de TI”, alineado a la metodología institucional que es la guía aprobada que debe utilizarse en cada una de las iniciativas o proyectos que se presenten ante el CETAC. Sin embargo, el manual no es utilizado de forma estándar para todos los proyectos que proponen y ejecutan

Es importante mencionar que la Unidad de Tecnologías de Información no tiene definido formalmente un responsable o gestor de proyectos, que cuente con las habilidades técnicas necesarias para gestionar proyectos. Además, la Unidad tampoco ha desarrollado una distribución adecuada de roles y funciones que

permita establecer los esfuerzos de capacitación y conocimientos a los encargados.

Si los proyectos no son gestionados utilizando las metodologías de la institución, estos no podrán lograr sus objetivos en términos de calidad, tiempo, presupuesto y requisitos de los interesados.

2.3.-Limitado seguimiento del Plan Estratégico de Tecnologías de Información (PETIC) 2016- 2020

La Coordinadora de la Unidad de Tecnologías de Información, la Alta Dirección de la DGAC y demás áreas administrativas no se han empoderado del PETIC, pues de los veinte (23) proyectos definidos en la cartera de Proyectos, y que nacieron como necesidad de mejorar la gestión y control de las TI, después del diagnóstico realizado en el proyecto de desarrollo del PETIC, se tiene el siguiente avance:

- Cinco (05) finalizados
- Once (11) pendientes: Los once proyectos debieron iniciar en el año 2016, pero a la fecha no existe ni el acta constitutiva.
- Siete (07) proyectos se encuentran en ejecución, cuatro de ellos incluidos en el proyecto de modernización tecnológica.

A pesar del incumplimiento en el cronograma de ejecución de los proyectos, la Unidad de Tecnologías de Información no ha actualizado la planificación de la cartera de proyectos.

La razón principal es que las Tecnologías de Información no son administradas a un nivel organizacional estratégico, es decir, la participación del negocio y la alta administración es limitada. Pues el cronograma de proyectos del PETIC está desactualizado, y las actas constitutivas de los proyectos no están respondiendo a una debida planificación.

Además, la Unidad de Tecnologías de Información ha enfocado sus esfuerzos en el proyecto de modernización denominado “CO1-002- Definir e implementar un proceso de mejora continua de la infraestructura de TIC”, el cual aún se encuentra en el proceso de contratación al momento de esta revisión.

Según la coordinadora de la Unidad de Tecnologías de Información, los proyectos que siguen pendientes dependen del proyecto de modernización, pero no existe un documento formal que respalde esa justificación técnica

Las tecnologías de información son un medio para que el negocio alcance sus objetivos a lo largo de la cadena de valor, si los proyectos de TI no se ejecutan o no se alinean a los objetivos estratégicos, los servicios que brinda podrían no cumplir con las expectativas de sus clientes en tiempo de respuesta y calidad.

2.4. No se Evidencia la Gestión de Riesgos en la Ejecución de los Proyectos de TI

Se identifica una inexistencia de gestión de riesgos tanto en la planificación como en la ejecución de los proyectos administrados por la Unidad de Tecnologías de Información.

Al respecto, es conveniente recordar lo que regula "Normas técnicas para la gestión y el control de las Tecnologías de Información (Resolución R-CO-26-2007 del 07/06/2007) Capítulo I 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.

Además de lo estipulado en una de las actividades de la fase II del "Manual Metodológico para Administrar Proyectos de TI":

> "Identificar los riesgos del proyecto. El director de proyectos en conjunto con los involucrados identificados como equipo de trabajo, identifican los riesgos del proyecto y establecen un plan de respuesta para cada uno de los riesgos identificados, lo cual se documenta en DGAC-UTI-FM-006 Acta Constitutiva del Proyecto. (…)"

La Unidad de informática no cuenta con un proceso para la identificación, valoración y tratamiento adecuado de riesgos tecnológicos, para garantizar resultados apropiados en la gestión de Tecnologías de Información, dado a eso, tampoco tienen la práctica de gestionar riesgos en los proyectos que administran.

El no contar con una gestión de riesgos, ocasiona que no se puedan monitorear y dar respuesta o definir planes de acción para minimizar o evitar su

materialización que puede ocasionar desviaciones en la calidad, tiempo, costo y alcance de los proyectos.

2.5. No se Evidencia Ninguna Metodología Utilizada para la Gestión del Proyecto CO2-007 –Implementación de Herramienta para la Gestión de Proyectos–

Sobre documentación asociada a la gestión del proyecto "CO2-007 Implementación de Herramienta para la Gestión de Proyectos", se identificó únicamente un cronograma y una minuta de la reunión de lanzamiento del proyecto (Kick Off).

En la minuta del kick Off, se había acordado "Ejecutar el proyecto únicamente para la Dirección de Informática, en fase dos se incluirán a las otras Direcciones". Sin embargo, en el transcurso de implementación el acceso a la herramienta se cedió al Área de Planificación, sin embargo, no existe un documento de control de cambios ni donde se justifique tal decisión.

Lo anterior evidencia la falta de un análisis previo de requerimientos y una inadecuada gestión de cambios.

Los criterios que justifican el hallazgo, son.

1. Normas técnicas para la gestión y el control de las Tecnologías de Información -Capítulo I Normas de aplicación general
   1.5 Gestión de proyectos
   La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos

2. Manual Metodológico para administrar proyectos de TI (6M03)

3. Manual de Gestión de Proyectos la DGAC (M02)

Importante recalcar que la Unidad de Tecnologías de Información no se ha alineado a la metodología para la gestión de proyectos definida en la institución, motivo por el cual no podrían lograr sus objetivos en términos de calidad, tiempo, presupuesto y requisitos de los interesados.

2.6. No se Evidencia Ninguna Metodología Utilizada para la Gestión del Proyecto CO2-004 –Implementación de la Mesa de Ayuda de la DGAC–

No se identificó la existencia de documentación relacionada a la gestión del proyecto “CO2-004- Implementación de la Mesa de Ayuda de la DGAC”.

El proyecto se desarrolló a lo interno de la Unidad de Tecnologías de Información, la intención del proyecto era automatizar la solicitud de servicios y atención de incidentes de tecnología. Sin embargo, la implementación de la herramienta (soporte.dgac.go.cr/tickets.php), conocida como “Soporte TI”, se realizó de forma aislada del proyecto “**Definición e implementación de un proceso de administración y operación de los servicios de TIC**”, por lo que actualmente la solución no responde a ningún proceso definido que contemple las mejores prácticas de la industria, respecto a la atención de servicios de TI.

Los criterios que justifican la inconformidad, son.

1. Normas técnicas para la gestión y el control de las Tecnologías de Información -Capítulo I Normas de aplicación general
   1.5 Gestión de proyectos
   La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos

2. Manual Metodológico para administrar proyectos de TI (6M03)

3. Manual de Gestión de Proyectos la DGAC (M02)

La Unidad de Tecnologías de Información no se ha alineado a la metodología para la gestión de proyectos definida en la institución, motivo por el cual podrían no lograr sus objetivos en términos de calidad, tiempo, presupuesto y requisitos de los interesados.

2.7. Inexistencia de un Documento que Respalde el Estudio de Mercado para el Proyecto C02-002 Desarrollo e Implementación de un Sistema de Gestión Documental

En la documentación que pertenece al proyecto "C02-002- Desarrollo e implementación del Sistema de Gestión Documental" no se identifica la existencia de un documento que incluya un estudio de mercado sobre herramientas tecnológicas que puedan apoyar la gestión documental en la DGAC.

Los usuarios de negocio y la Unidad de Tecnologías de Información se limitaron a analizar dos herramientas tecnológicas denominadas "Alfresco" y "Epower"

Se evidencia el incumpliendo de las siguientes metodologías:

1. Manual de Gestión de Proyectos de la DGAC (Metodología PMI-M02)
2. Manual Metodológico para Administrar Proyectos de TI (6M03)

Es fundamental contar con un análisis de la oferta del mercado considerando más opciones que incluso pueden ser más versátiles para adaptarse a la institución.

2.8. Inconsistencias del Acta de Constitución del Proyecto C02-002- "Desarrollo e Implementación del Sistema de Gestión Documental"

El acta de constitución del proyecto "C02-002" fue desarrollada casi al final del proyecto, por una solicitud que realizó la Auditoría Interna en el oficio AI-212-2017(Observaciones sobre el Proceso de Planificación de Proyecto Ti".

Durante el análisis del acta se determinó que la información que incluyeron no se adapta a los requisitos de un documento que constituye un proyecto, por ejemplo:

En el "Alineamiento estratégico", se espera que se explique cómo se alinea el proyecto a los objetivos estratégicos de la institución y por el contrario, lo que se propuso fue:

"Unidad de tecnologías de información"

> Implementar el plan estratégico de tecnologías de información y comunicación DGAC-2016-2020 para contar con un proceso planificado que asegure que el departamento de TI se defina las estrategias requeridas para cumplir con la misión, visión y objetivos estratégicos, así como las normas técnicas de la gestión y control."

El proyecto no busca implementar plan estratégico de tecnologías de información y comunicación, por lo que se debió alinear a un objetivo estratégico de la institución.

Lo que incluyeron en "supuestos del proyecto" hace referencia una restricción, y lo que incluyeron como restricciones obedece más a riesgos del proyecto.

En los criterios de éxito, incluyeron parte del alcance del proyecto y no métricas para el monitoreo del éxito del proyecto.

En razón de lo anterior se considera que el administrador del proyecto (Ólman Durán Arias) no siguió la metodología definida para la dirección de proyectos en la DGAC, y además, existe un desconocimiento sobre los procesos en la gestión de proyectos.

En gestión de proyectos, si el acta de constitución no se crea o se crea de forma incorrecta no se tendrá claridad y transparencia sobre el alcance del proyecto.

Además, si el acta de constitución no existe no se oficializa formalmente la existencia del proyecto.

2.9. Sobre el oficio de Auditoría AI-212-2017

Durante la realización de la presente auditoría se observó que los hallazgos identificados sobre el proyecto C02-002- "Desarrollo e implementación del Sistema de Gestión Documental" aún se mantienen.

Sobre las respuestas emitidas por la Unidad de Tecnologías de Información, en referencia a esos hallazgos, se expone los siguientes comentarios:

Una de las actividades iniciales de los proyectos, es el levantamiento de requerimientos de alto nivel. Esto por cuanto en ese momento, se cuenta con ideas generales de las necesidades, por ejemplo, si el área de negocio financiera requiere de un nuevo sistema un requerimiento de alto nivel es que el sistema permita contabilizar transacciones.

Pasada esta actividad, es que se debe realizar el estudio de mercado para analizar cuál es la mejor solución que podría satisfacer esa necesidad inicial, si durante este estudio se determina que ninguna opción del mercado satisface la necesidad, se podría llegar a pensar entonces que la solución debería desarrollarse internamente. Es en este momento que se definen los requerimientos específicos contestando básicamente preguntas como por ejemplo, "Cómo se realiza la contabilización, porqué se realiza la contabilización, cuándo se realiza la contabilización, quién realiza la contabilización, entre otras preguntas, esto permite tener un mejor detalle de la necesidad, y permite a un externo al negocio (ya sea del área de TI o un proveedor), realizar estimaciones del esfuerzo que llevaría desarrollar ese requerimiento. El fin de esta estimación es poder definir las prioridades de desarrollo de los requerimientos.

Lo anterior se realiza con la finalidad también de que cuando se contraten paquetes de hora de consultoría para desarrollar software se cuente con herramientas de control que permiten monitorear su implementación. Además le permite a la Administración prever el alcance y la limitación de la atención de los requerimientos para así realizar un plan de acción que permita en el futuro poder satisfacer todas las necesidades del negocio, por ejemplo, un plan de acción podría ser que un desarrollador del área de TI esté involucrado 100% durante la ejecución del proyecto y que reciba los conocimientos necesarios que permita atender requerimientos que no fueron incluidos en el paquete inicial.

La respuesta a la recomendación 1 que indica: "Que el restante 20%, de la implementación del METRO BMP, se completará en el 2018 bajo la modalidad de horas por consumo, y conforme los requerimientos que soliciten". Aquí es importante destacar que es sano y recomendable que se cuente con herramientas de control que permita monitorear el cumplimiento de ese 20% en función a lo descrito anteriormente.

Sobre la respuesta a la recomendación 3: Según el informe (ASPECTOS TÉCNICOS ARCHIVÍSTICOS EN RELACIÓN A LA CONTRATACIÓN 2016CD-000175-0006600001) del señor Francisco Soto, Archivista Institucional, se puede evidenciar que el sistema ALFRESCO, no cumple con los requerimientos del

proceso archivístico, sus observaciones están bien fundamentadas con la legislación nacional, entonces no es factible indicar que la recomendación no tiene validez y que se cumple lo sugerido por la Auditoría Interna. (Ver AI-212-2017 en Anexo № 1)

2.10. Inconsistencias del Acta de Constitución del Proyecto CO2-005 Mejorar la Página Web Institucional

Durante el análisis del acta de constitución del proyecto CO2-005 Mejorar la Página Web Institucional, se determinó que la información que se incluyó no se adapta a los requisitos de un documento que constituye un proyecto, por ejemplo:

En el "Alineamiento estratégico", se espera que se explique cómo se alinea el proyecto a los objetivos estratégicos de la institución y por el contrario, lo que se propuso fue:

> *"Unidad de tecnologías de información"*
> *Implementar el plan estratégico de tecnologías de información y comunicación DGAC-2016-2020 para contar con un proceso planificado que asegure que el departamento de TI se defina las estrategias requeridas para cumplir con la misión, visión y objetivos estratégicos, así como las normas técnicas de la gestión y control.*

El proyecto no busca implementar plan estratégico de tecnologías de información y comunicación, por lo que se debió alinear a un objetivo estratégico de la institución.

Lo que incluyeron en "supuestos del proyecto" (Se tiene estimado un presupuesto de 15.000.000.00 para iniciar su desarrollo) hace referencia una restricción de presupuesto, y lo que incluyeron como restricciones obedece más a riesgos del proyecto.

En los criterios de éxito, incluyeron parte del alcance del proyecto y no métricas para el monitoreo del éxito del proyecto.

En la descripción de requerimientos incluyeron el medio como iban a lograr la implementación del proyecto y no las necesidades que se quieren suplir con el proyecto.

Observando la situación se considera que el administrador de proyectos no posee conocimientos en los procesos y términos de gestión de proyectos, además de que no se ha alineado totalmente a la metodología de gestión de proyectos definida por la Unidad de Tecnologías de Información y la institución.

Si el acta de constitución no se crea o se crea de forma incorrecta no se tendrá claridad y transparencia sobre el alcance del proyecto.

2.11. El proyecto CO2-005 Mejorar la Página Web Institucional no se Apegó Totalmente a la Metodología para Gestionar Proyectos de TI

Se analizó la documentación del proyecto y no se identificó lo siguiente:

- Estudio de factibilidad
- Clasificación del índice del riesgo

Con lo anterior se evidencia que la Unidad de Tecnologías de Información no se ha alineado totalmente a la metodología de gestión de proyectos definida (Manual de Gestión de Proyectos de la DGAC (Metodología PMI-M02) y Manual Metodológico para Administrar Proyectos de TI (6M03), lo que podría provocar que los proyectos no puedan lograr sus objetivos en términos de calidad, tiempo, presupuesto y requisitos de los interesados.

2.12. El Proyecto C03- 01 - Reorganización de la Función de TIC de la DGAC: Procesos y Perfil del Recurso Humano no se ha Implementado

Durante el desarrollo del PETIC, la Universidad Nacional organización contratada para la elaboración del mismo, realizó una recomendación sobre una nueva estructura para la Unidad de Tecnologías de Información, asimismo, diseñó los perfiles de puesto requeridos en la Unidad.

Dichas recomendaciones fueron aprobadas por el CETAC, sin embargo, a la fecha no se ha logrado reestructurar la Unidad.

La coordinadora de la Unidad de Tecnologías de Información indicó que ella solicitó a la Unidad de Planificación los formularios requeridos para efectuar la

solicitud de la nueva estructura, sin embargo, se le indico que el proceso quedaba detenido debido a que MIDEPLAN había aprobado una nueva estructura organizativa para la DGAC, y está debía implementarse primero.

La Institución debe considerar que no definir una estructura adecuada de procesos y manuales de puesto para la gestión de Tecnologías de Información impedirá el aprovechamiento de los recursos disponibles para brindar a la DGAC un servicio adecuado basado en las necesidades esta Dirección para desarrollar nuevas iniciativas y asegurar la continuidad de las operaciones institucionales.

2.13. Inexistencia de un Marco de Seguridad de la Información

La Institución no ha establecido un sistema de gestión que les permita establecer, implementar, operar, monitorear y revisar, así como mantener y mejorar la seguridad de la información.

Durante el desarrollo del Plan Estratégico 2016-2020, se definió una política de seguridad de la información y sus procedimientos asociados, sin embargo la implementación se iba a llevar a cabo con el proyecto "**CO3-003 (Definir e implementar un proceso de gestión de la seguridad de la información para la DGAC)",** por lo que actualmente la política no está implementada.

La citada situación se contrapone a las normas técnicas que regulan la gestión y control de las tecnologías de información, en la siguiente clausula:

> "Capítulo I: Normas de aplicación general
>
> 1.4 Gestión de la seguridad de la información
>
> 1.4.1 Implementación de un marco de seguridad de la información:
>
> La organización debe implementar un marco de seguridad de la información, para lo cual debe:
>
> a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de

seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.

b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.

c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.

El Plan Estratégico de Tecnologías de Información 2016-2020 definió el marco estratégico de TIC, que enmarca la misión, la visión y los objetivos estratégicos que determinarían la dirección en materia de Tecnologías de Información y Comunicaciones, así como el cumplimiento de las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República de Costa Rica (CGR), en la Dirección General de Aviación Civil.

En el proceso de definir el Plan Estratégico de TI, se realizó un diagnóstico de la situación actual de la Unidad de Informática y se identificó la necesidad de implementar un sistema de gestión de la seguridad de la información, motivo por el cual se incorporó un proyecto para tales efectos, el cual fue presentado al CETAC y aprobado por el mismo.

El proyecto se planificó para ejecutarlo entre el I semestre del 2016 y el I semestre del 2017, sin embargo, a la fecha no se tiene un plan para la implementación del mismo.

Lo que evidencia que la Coordinadora de la Unidad de Tecnologías de Información y la Alta Administración no se han apoderado del Plan Estratégico para cumplir con los objetivos que en él se plantearon.

Importante recalcar que a partir del 09 de mayo del 2017, en una sesión celebrada por el CETAC se designa a Director Juan Scott Chaves Noguera, como responsable de la coordinación de la ejecución de los proyectos de TIC'S.

La coordinadora de la Unidad de Tecnologías de Información, indica que el proyecto de "CO3-003- Definir e implementar un proceso de gestión de la seguridad de la información para la DGAC" depende del proyecto de

modernización impulsando prioritariamente por el CETAC, pero no existe un documento formal que respalde esa justificación técnica.

Se debe considerar que tener infraestructura tecnológica es solo una parte de gestionar adecuadamente la seguridad de la información y que no debe ser justificante para no establecer la estrategia de la seguridad de la información para la institución.

Por no tener un marco de seguridad definido e implementado la DGAC, está incumpliendo el ordenamiento jurídico y administrativo al no acatar las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por la Contraloría General de la República (CGR).

Además el no contar un marco de gestión de seguridad de la información aumenta el riesgo de afectar la confidencialidad, integridad y disponibilidad de la información y recursos, haciendo inviable la continuidad del negocio.

2.14. Limitada Capacitación y Comunicación sobre la Administración de la Seguridad de la información en los Funcionarios de la Dirección General de Aviación Civil

La ausencia de un sistema (Marco) de gestión de seguridad, la inexistencia de políticas y capacitaciones relacionadas a temas de seguridad de la información, ha imposibilitado generar conciencia y conocimiento en los funcionarios de la institución sobre los riesgos asociados a gestionar la protección de los activos de la institución.

Según indican las Normas técnicas para la Gestión de Tecnologías de Información, en su capítulo 1, sobre las Normas de aplicación general, 1.4 Gestión de la seguridad de la información -1.4.2 Compromiso del personal con la seguridad de la información:

> "El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe:
>
> a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad,

confidencialidad y riesgos asociados con el uso de las TI.

b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades."

Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.

Esa situación es producto de la inexistencia de un marco de gestión de seguridad y el escaso involucramiento de la Dirección General e iniciativas no ejecutadas por parte de la Unidad de Tecnologías de Información para la implementación de un marco de seguridad y por ende capacitaciones al resto de la institución sobre la materia.

Se debe considerar que las personas son el eslabón más débil y mayoritario en la cadena de seguridad, según la encuesta global de PwC sobre ciberseguridad 2016, más del 34% de los incidentes de seguridad son responsabilidad de los empleados.

2.15. Incumplimiento del Proceso "Ingreso de Visitantes"

Vigilancia exterior

La institución cuenta con un guarda de seguridad en la entrada del edificio (Portón), este se encarga de permitir el ingreso al edificio, este consulta al visitante el motivo de su visita, pero no verifica con ningún funcionario de la DGAC si lo que le indica el visitante es cierto, por lo que el ingreso a la institución se da sin mayores obstáculos.

Otro guarda de seguridad se encuentra en la puerta de entrada al edificio, este es responsable de administrar la bitácora de los visitantes y las pertenencias que estos llevan, sin embargo, se logró identificar que lo único que revisan es si el visitante carga una computadora, y esto lo hacen de forma esporádica.

Vigilancia Interior (LOBBY)

Previo a que una persona ingrese al interior de la DGAC, la recepcionista le solicita la identificación y además como requisito debe registrarse en la bitácora de "control de visitas".

Sin embargo, tampoco toma registro de los equipos que se ingresan, ni localiza al funcionario responsable de atender la visita para que este lo dirija dentro de las instalaciones.

Para este hallazgo, se identifican dos criterios básicos:

1. Normas técnicas para la Gestión de Tecnologías de Información (Resolución R-CO-26-2007 del 07/06/2007),emitidas por la Contraloría General de la República,

Dominio I: Normas de aplicación general

1.4 Gestión de la seguridad de la información (…)

1.4.3 Seguridad física y ambiental:

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. Como parte de esa protección debe considerar:

a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.
b. La ubicación física segura de los recursos de TI.
c. El ingreso y salida de equipos de la organización.
d. El debido control de los servicios de mantenimiento.
e. Los controles para el desecho y reutilización de recursos de TI.
f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.
g. El acceso de terceros.
h. Los riesgos asociados con el ambiente

2. La Política de “SEGURIDAD FÍSICA Y AMBIENTAL” de la DGAC, en sus cláusulas:

“

5.1 El personal de Seguridad y Vigilancia, debe revisar el contenido de toda maleta, bolsa, caja u otro que presente sospechas para prevenir la sustracción de componentes de equipos de cómputo o de información en medios magnéticos o físicos.

5.2 Está prohibido introducir a la DGAC elementos potencialmente peligrosos para la seguridad de las personas, los equipos de cómputo y de comunicaciones de la DGAC tales como armas o explosivos.”

El no contar con un marco de gestión de la seguridad de la información genera que se creen políticas de forma aisladas sin que se tenga certeza cierta de que es lo que se requiere resguardar, las políticas deben seguir objetivos que permita determinar el cumplimiento de un proceso específico.

Además se encuentra que hay incumplimiento de la política “**SEGURIDAD FÍSICA Y AMBIENTAL”** que define las acciones que el guarda de seguridad debe seguir al recibir a un visitante y la falta de conocimiento y concientización por parte del personal de seguridad.

Lo descrito anteriormente podría provocar el ingreso de personas no autorizadas a la institución, que pudieran tener otras intenciones como robo, actos vandálicos, entre otros.

2.8. Red Inalámbrica con Protocolos de Encriptación Vulnerable

Las redes inalámbricas (Wi-Fi), no cuentan con los controles necesarios para restringir la visualización de la contraseña de acceso a la misma, lo que facilita a los usuarios con habilidades de “hackeo” obtener fácilmente el acceso a la red. Además, la información no viaja cifrada a través de las redes de telecomunicaciones.

Las Normas Técnicas para la Gestión de Tecnologías de Información indican en el Capítulo I:

Normas de aplicación general

1.4.4 Seguridad en las operaciones y comunicaciones:

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

La inexistencia de un marco de gestión de seguridad y desconocimiento técnico por parte del personal de la Unidad de Tecnologías de Información, propicia situaciones como la anterior que pueden provocar accesos no autorizados a la información y divulgación de la misma

2.9. Prácticas Inadecuadas para los Respaldos de Información –Equipos Desactualizados–

Los respaldos de la información contenida en bases de datos de producción, se ejecutan de forma automática y diaria en un horario definido durante las madrugadas, los archivos generados motivo del proceso de respaldo se almacenan en el mismo servidor donde se encuentran los ambientes de producción.

Debido a esta práctica y a la poca confianza del proceso, los funcionarios de la Unidad de Tecnologías de Información, responsables de darle mantenimiento a los sistemas y bases de datos, copian los archivos de respaldo en sus computadoras locales o en dispositivos de almacenamiento externos.

Importante mencionar que los discos duros de los servidores de producción están al límite de su capacidad de almacenamiento, además los equipos (servidores) están obsoletos, pues su garantía de funcionamiento caducó.

No se evidencian pruebas de restauración de los respaldos generados.

Se debe considerar que las Normas Técnicas para la Gestión de Tecnologías de Información en el Dominio I: Normas de Aplicación General, indican:

"1.4 Gestión de la seguridad de la información.

1.4.4 Seguridad en las operaciones y comunicaciones
La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe:

a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.

c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.

La DGAC no cuenta con equipos (hardware) con la capacidad de almacenamiento y funcionalidad para mantener buenas prácticas en el respaldo de información o bien para asegurar la continuidad de los servicios.

Actualmente se encuentran en proceso de adjudicación los siguientes proyectos:

CO1-002: Definir e implementar un proceso de mejora continua de la infraestructura de TIC

CO1-003: Mejoramiento de la infraestructura de TIC De la DGAC

Al momento en que se desarrollaba este trabajo, los proyectos han sufrido un atraso debido a las apelaciones realizadas por las empresas que participaron en el proceso de licitación.

La evaluación de la adjudicación se encontraba en la Contraloría General de la Republica, y aún no se tenía una fecha estimada para que el proceso de adjudicación sea finalizado, y así poder iniciar los proyectos, esto al momento de la revisión efectuada

Además la ausencia de un marco de seguridad de la información ha limitado la posibilidad de establecer una estrategia para resguardar los datos de la institución.

Debido a la situación descrita La organización está expuesta a la pérdida de uno de sus activos más valioso, la información.

El no contar con la información disponible puede impedir la continuidad de los servicios, afectando a todos los clientes internos y externos de la institución, lo que además provocaría daños reputacionales en DGAC.

Además, se estaría ante el incumpliendo del ordenamiento jurídico – administrativo, al no acatar las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por la Contraloría General de la República (CGR).

2.10. Inexistencia de un Proceso para la Clasificación de la Información

La Institución no cuenta con un proceso para la clasificación de la información y por lo tanto no existe una administración de acuerda de ésta. Es decir, no existe una distinción entre información pública, de uso interno, de uso restringido- confidencial o bien secreta – sensible.

La situación descrita incumple con lo estipulado en Normas Técnicas para la Gestión de Tecnologías de -Capítulo I Normas de Aplicación General, las cuales señalan:

"1.4 Gestión de la seguridad de la información

1.4.5 Control de acceso

> La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe: (…)
>
> b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad."

El incumplimiento refleja la inexistencia de una gobernanza de Tecnologías de Información que considere como prioridad o que defina la necesidad de identificar y clasificar los datos críticos, para cumplir con las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, específicamente el proceso de gestionar la seguridad de la información, más aun, considerando que las tecnologías de información se han convertido en un instrumento esencial en la prestación de los servicios y representan rubros importantes en los presupuestos del Sector Público.

Al no existir una clasificación de datos no se les puede asignar una categoría a estos que impulse los requisitos de control interno destinados a protegerlos contra robo o uso inadecuado.

Por ejemplo:

Si el acceso oportuno y confiable a la información de uso se ve afectado, podría resultar en la pérdida de negocios o reputación de la institución.

Si no se protege la privacidad personal y la información de propiedad se pueden provocar violaciones de la Ley № 8968, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, que podrían resultar en multas o sanciones e impactar individuos o la empresa, si se ven comprometidos

2.11. Uso inapropiado de las impresoras

La DGAC no cuenta una política de seguridad relacionada con el uso de las impresoras.

Las impresoras no poseen funcionalidades que permitan resguardar los documentos que se envían a imprimir, es decir los funcionarios envían documentos para impresión y estos se despliegan inmediatamente.

Las Normas Técnicas para la Gestión de Tecnologías de Información indican en el Dominio I: Normas de aplicación general, lo siguiente:

> "1.4.5 Control de acceso
> La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:
> (…)
>
> b. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación."

En razón de no existir un sistema de gestión de la seguridad y por ende una política para el uso de las impresoras, es muy difícil que los funcionarios generen conciencia sobre el riesgo que existe al exponer información confidencial a accesos no autorizado y divulgación de la misma.

2.12. Control de Acceso Inadecuado en los Sistemas

No se identificó un proceso documentado para la administración de accesos a los sistemas de información, en el cual se establezcan los tipos de usuario y sus capacidades de operación.

Además, no se evidenció la ejecución de revisiones periódicas sobre los usuarios activos e inactivos y la debida concordancia con sus roles, en los diferentes perfiles.

Para este hallazgo, se identifican dos criterios básicos:

1. Normas Técnicas para la Gestión de Tecnologías de Información (Resolución R-CO-26-2007 del 07/06/2007) , emitidas por la Contraloría General de la República

> "Dominio I: Normas de Aplicación General
>
> 1.4.5 Control de acceso
>
> La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:

a) Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.

b) Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.

c) Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.

d) Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

e) Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.

f) Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.

g) Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.

h) Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.

i) Manejar de manera restringida y controlada la información sobre la seguridad de las TI.

2. Procedimiento desarrollado por la Unidad de tecnologías de Información para la Gestión de TI, denominado "6P03 PROCEDIMIENTO GESTIÓN DE TI", específicamente en el punto 2.20, donde se describe un proceso para la Revisión de Privilegios en los Sistemas**.**

La Inexistencia de un Marco de Gestión de la seguridad que contemple todos los elementos necesarios para resguardar la información de accesos no autorizados y el Incumplimiento del apartado 2.20 Revisión de Privilegios en los Sistemas del procedimiento 6P03 Gestión de TI "GESTIÓN DE TI, imposibilita el poder garantizar que el proceso de solicitud, establecimiento, emisión, suspensión, modificación y cierre de las cuentas de usuario, sea totalmente funcional y controlado.

2.13. Acceso a los Ambientes de Desarrollo y Producción y Servidores de la Institución

Los analistas de sistemas de la Unidad de Tecnologías de Información, encargados de darle mantenimiento a los sistemas de información, tienen acceso a los ambientes de desarrollo y producción, incluyendo las bases de datos y aplicaciones. No existen controles cruzados para validar y evaluar los accesos y cambios que realizan.

También es importante mencionar que debido a la antigüedad y tecnología en que fueron desarrollados los sistemas y las bases de datos, estos no cuentan con funcionalidades que procesen y almacenen los datos de forma cifrada.

La situación actúa en contra de Normas Técnicas para la Gestión de Tecnologías de Información, en el siguiente apartado:

"Dominio I: Normas de Aplicación General. (…)

1.4 Gestión de la seguridad de la información

1.4.5 Control de acceso

La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:

a) Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.

b) Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.

c) Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.

d) Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

e) Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.

f) Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y

actualización periódica y atención de usos irregulares.

g) Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.

h) Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.

i) Manejar de manera restringida y controlada la información sobre la seguridad de las TI.

La encargada de la Unidad de Tecnologías de Información considera que debido al limitante recurso humano con el que cuenta, es muy difícil establecer una segregación de funciones y roles, si se desea ser efectivos en la atención de requerimientos e incidentes. Sin embargo, la razón principal es que no han establecido responsabilidades diferenciadas entre los funcionarios de la Unidad, siguiendo las mejores prácticas de la industria.

Por la falta de controles los analistas podrían realizar cambios no autorizados a nivel de la estructura de la base de datos y los datos almacenados, además de revelar información confidencial.

2.14. Inexistencia de una Metodología que Defina los Procesos para la Gestión de Servicios de Tecnología

No se identifica la existencia de una metodología que defina los procesos o prácticas que contribuyen al logro del propósito de los servicios de tecnología.

El Plan Estratégico de Tecnologías de Información 2016-2020 definió el marco estratégico de TIC, que enmarca la misión, la visión y los objetivos estratégicos que determinarían la dirección en materia de Tecnologías de Información y Comunicaciones, así como el cumplimiento de las “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información” emitidas por la Contraloría General de la República de Costa Rica (CGR), en la Dirección General de Aviación Civil.

En el proceso de definir el Plan Estratégico, se realizó un diagnóstico de la situación actual de la Unidad de Tecnologías de Información y se identificó la necesidad de implementar un sistema de gestión de servicios de tecnología, motivo por el cual se recomendó un proyecto para tales efectos, el cual fue presentado al CETAC y aprobado por el mismo.

El proyecto se planificó para ejecutarlo desde el I semestre del 2017 al II semestre del 2018, sin embargo, a la fecha no se ha iniciado ni tampoco se ha reprogramado.

La situación evidencia el incumplimiento con Normas Técnicas para la Gestión y el Control de las Tecnologías de Información- Capítulo IV Prestación de servicios y mantenimiento, el cual a la letra dice:

> "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"

La razón o causa principal del incumplimiento es que las Tecnologías de Información no son administradas a un nivel organizacional estratégico, es decir la participación del negocio y la Alta Administración no se evidencia.

La Coordinadora de la Unidad de Tecnologías de Información y la Alta Dirección no se han apoderado del Plan Estratégico para cumplir con los objetivos que en él se plantearon.

La Unidad de Tecnologías de Información ha enfocado sus esfuerzos en el proyecto de Modernización denominado "CO1-002- Definir e implementar un proceso de mejora continua de la infraestructura de TIC", el cual aún se encuentra en el proceso de contratación.

La coordinadora de la Unidad de Tecnologías de Información, indica que el proyecto de "CO3-004- Definir e implementar un proceso de gestión de la continuidad de los servicios de TIC" depende del proyecto de modernización, pero no existe un documento formal que respalde esa justificación técnica.

Importante resaltar que el no contar infraestructura tecnológica de última generación no limita el poder implementar una metodología para la gestión de servicios de TI.

Además del incumplimiento por parte de la Dirección General de Aviación Civil (DGAC) de las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, específicamente el capítulo IV Prestación de Servicios y Mantenimiento, el no contar con una metodología de gestión de Servicios e incidentes de tecnología impide alinear los servicios de TI proporcionados con las necesidades de la Institución.

2.15. Inexistencia de Acuerdos de Nivel de Servicio (SLAS)

No existen prácticas relacionadas con la definición y negociación de acuerdos de nivel de servicio (SLAS) entre la Unidad de Tecnologías de Información y el negocio.

Las Normas técnicas para la Gestión y el Control de las Tecnologías de Información en su Capítulo IV Prestación de servicios y mantenimiento- 4.1 Definición y administración de acuerdos de servicios, indica:

> "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:
>
> a. Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
>
> b. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
>
> c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
> 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, incluidos los contratos con terceros".

Al no existir un proceso para la gestión de Servicios de Tecnología ni una definición formal y aprobada de un catálogo de servicios, impide desarrollar los acuerdos de nivel de servicio.

El no contar con acuerdos de niveles de servicio (SLAS) e indicadores de desempeño limita la capacidad de realizar un monitoreo sobre la calidad del servicio que se entrega, lo que impide evaluar si el negocio está recibiendo el servicio requerido para la consecución de los objetivos institucionales.

Por ejemplo, no se puede asegurar el cumplimiento de tres pilares fundamentales:

- Entregar el servicio a tiempo (cumplir las agendas establecidas)
- Entregar el servicio con calidad (colmar las expectativas de los clientes, los requisitos acordados)
- Entregar el servicio dentro de los costes esperados (ajustarse al presupuesto)

2.16. Inexistencia de un Catálogo de Servicios

No existe un catálogo de servicios de tecnología formal que establezca el concepto y el alcance de "Servicio de TI", así como sus diferencias y relaciones con servicios de negocio y soluciones tecnológicas.

Según las Normas técnicas para la Gestión y el Control de las Tecnologías de Información, en el Capítulo IV Prestación de servicios, establece:

"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."

Dado a la inexistencia de una metodología para la gestión de servicios de tecnología, no se ha contemplado la definición de un catálogo de servicios, y eso dificulta poder establecer medidas de desempeño para valorar si los servicios brindados están alineados a las necesidades del negocio, además, al no contar con una base de conocimiento documentada de los servicios brindados no permite controlar ni garantizar disminución de costos por cuanto se debe invertir en el análisis e investigación de las incidencias aunque sean recurrentes.

2.17. Plataforma de Solicitud de Servicios no Considera las Necesidades y Servicios que Demanda el Negocio

La Unidad de Informática cuenta con una plataforma de Servicios (soporte.dgac.go.cr/tickets.php), conocida como "Soporte TI", encargada de centralizar la atención inicial, el escalamiento y seguimiento de la solicitud de servicios. Actualmente se documenta la información mínima requerida para la atención de las solicitudes de servicio: el registro inicial (usuario solicitante, tipo de incidente (incidente con sistemas, incidente con hardware, incidentes SIFCO) y descripción.

El sitio carece de herramientas de autoayuda que faciliten el servicio al usuario, tales como preguntas frecuentes (FAQ), además no permite generar reportes que pueden ser utilizados para medir indicadores como el tiempo de atención, cantidad de incidentes o servicios atendidos, solicitudes pendientes, satisfacción de los usuarios, etc., que conlleven a una mejora continua.

No se tienen definiciones claras sobre perfiles de usuario de la mesa de servicio que permitan estandarizar el acceso y autorización para los trámites más comunes, el sistema tampoco permite priorizar las solicitudes.

La implementación de la herramienta no ha sido aceptada por el 100% de los usuarios, pues algunas solicitudes de servicio siguen llegando a la Unidad de Tecnologías de Información por correo electrónico o llamadas telefónicas.

Según las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, en el Capítulo IV Prestación de servicios, establece:

"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."

El software implementado para "solicitud de servicios" fue seleccionado por la Unidad de Tecnologías de Información sin tener una metodología y procesos definidos para la gestión de servicios, y como se describe el no contar con una plataforma tecnológica que responda a las necesidades y servicios que demanda el negocio limita poder responder de una manera oportuna, eficiente y con alta calidad a las peticiones que los usuarios realicen, en relación a los diversos aspectos de la Tecnología de la Información.

Además, impide tener indicadores de gestión que permitan evaluar la calidad del servicio que se brinda o la sobrecarga de trabajo de los funcionarios que atienden las solicitudes.

2.18. Inexistencia de un Proceso para la Gestión de Incidentes

No se cuenta con documentación formal de un proceso de gestión de incidentes debidamente aprobado y formalizado, por lo que hay una debilidad en la gestión integral de incidentes de tecnología. La Unidad de Tecnologías de Información cuenta con funciones naturales de Service Desk y ésta asume las tareas de atención de los mismos.

No se cuenta con un esquema estándar de clasificación y priorización de los incidentes.

No se identificaron acuerdos de nivel de servicio que sean tomados en cuenta para la definición de tiempos de atención internos.

Debido a la inexistencia de un proceso para la gestión de incidentes, se está incumpliendo con lo que dictan las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, las cuales en lo que interesa dicen:

"Capítulo IV Prestación de servicios y mantenimiento

4.5 Manejo de incidentes

La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario."

La inexistencia de una metodología para la gestión de servicios e incidentes en la Unidad de Tecnologías de Información y desconocimiento del personal sobre la diferencia entre un incidente y un servicio, es la causa principal de la situación descrita anteriormente.

El no contar con un proceso de gestión de incidentes, dificulta poder medir si los incidentes o problemas se analizan y resuelven de manera oportuna, además impide tener métricas para identificar si la Unidad de Tecnologías de Información necesita más recursos, para atender eficazmente las necesidades del negocio.

2.19. Inexistencia de un Proceso para la Gestión Integral de Riesgos

La institución cuenta con una metodología para la Gestión Integral de Riesgos alineada al Sistema Específico de Valoración de Riesgo Institucional (SEVRI) emitido por la Contraloría General de la República. Sin embargo, la Unidad de Tecnologías de Información no se ha alineado al cumplimiento de la Directriz Institucional sobre la Gestión Integral de Riesgos, lo que evidencia que no existe una identificación, valoración y tratamiento adecuado de riesgos tecnológicos, para garantizar resultados apropiados en la gestión de Tecnologías de Información.

La citada situación se contrapone a:

1. Normas técnicas para la gestión y el control de las Tecnologías de Información Capítulo I 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".

2. Sistema Específico de Valoración de Riesgo Institucional (SEVRI)- Resolución N° D-3-2005-CO-DFOE

3. Incumpliendo al procedimiento " 6P03 GESTIÓN DE TI " Apartado 2.19: Administración y mitigación del riesgo en TI : El personal del proceso de Soporte Técnico, de la Unidad de Tecnologías de Información, debe definir todos los conceptos involucrados según el análisis de riesgo a realizar, tales como:

   - Realiza un inventario completo de todos los componentes de hardware, software e intangibles propensos a riesgos informáticos.
   - Categoriza los riesgos y realizan una descripción del riesgo.
   - Escoge la metodología más apropiada que le permitirá evaluar el riesgo
   - Establece la metodología de captura que le permitirá evaluar el riesgo.
   - Establece el nivel de probabilidad y le dan un grado de calificación.
   - Establece el nivel de impacto que posee el riesgo y le dan un grado de calificación.
   - Analiza los resultados para clasificar el nivel del riesgo.
   - Establece la estrategia de mitigación del riesgo y asigna responsabilidades de cumplimiento, así como el estado.
   - Realiza revisiones periódicas que permitan actualizar o mejorar los cambios que surjan en el tiempo.

La Unidad de Tecnologías de Información no cuenta con personal capacitado en la gestión integral de riesgos, y ningún funcionario tiene asignado dentro de sus responsabilidades la administración de riesgos.

Dado a esta situación la institución está incumpliendo de la normativa vigente. Además, una organización que no gestiona sus riesgos tecnológicos podría estar expuesta a: Daños en los sistemas informáticos, suplantación de identidades, accesos no autorizados y alteraciones a la información, daños en los equipos informáticos, fallos en la disponibilidad de los servicios, entre otros.

III. CONCLUSIONES

Importante recalcar que el cumplimiento con las Normas Técnicas para el Control y Gestión de Tecnologías de Información, no es solo responsabilidad de la Unidad de Informática, sino más bien es responsabilidad de la Administración General y la Unidad de Informática dentro de sus funciones deberá apoyar la implementación y mantenimiento de las mismas.

Las conclusiones han sido estructuradas según los objetivos específicos del presente estudio:

a. Gestión de Proyectos en TI.

La estrategia de TI de la DGAC no está respondiendo a los requerimientos de la Institución, es decir las acciones estratégicas del PETIC no se han orientado a responder a las metas estratégicas definidas por la institución.

Durante los últimos cuatro años no se ha implementado ningún proyecto que apoye o esté alineado a uno de los objetivos estratégicos de la DGAC.

Para esta observación se consideró el SISTEMA SIRH, utilizado en la Unidad Gestión Institucional de Recursos Humanos, el cual fue donado por el CONAVI, sin embargo, este no era totalmente funcional para los requerimientos de la DGAC, por lo que se ha tenido que invertir en adaptaciones que a la fecha no satisfacen totalmente los requerimientos de la institución, pues el sistema no es totalmente independiente de tecnología, y constantemente presenta errores en la ejecución de diferentes procesos.

La plataforma del sistema es bastante obsoleta, lo que evidencia que se ha invertido en aplicaciones que pronto deberán ser sustituidas, lo anterior provocado por no hacer estudios de costo beneficio.

La gestión de proyectos en la Unidad de informática es muy básica, es decir no se contemplan las guías establecidas por la Unidad y por el área de gestión de Proyectos Institucional (PMO) para dicho fin.

Algunos de los proyectos implementados, como por ejemplo el de la "Implementación de la Mesa de Ayuda de la DGAC" no tiene documentación sobre un estudio de mercado, acta constitutiva, cronograma, gestión de riesgos, entre otros de los requisitos contemplados en el manual metodológico para la gestión de proyectos.

Lo mismo sucede con el proyecto C02-002- Desarrollo e implementación del Sistema de Gestión Documental", no se identificó nada relacionado a: gestión de riesgos, gestión de interesados, plan de calidad.

Se evidencia un incumplimiento al seguimiento del PETIC y la limitada gestión del cambio, pues a la fecha el cronograma de implementación de los proyectos no ha sido actualizado. Es importante considerar que el seguimiento de los proyectos no es solo responsabilidad de la Unidad de Informática, sino también de la PMO, de la CITI y el CETAC.

La Unidad de informática no gestiona riesgos en el desarrollo de los proyectos, debido a que no tienen establecido un proceso para dicho fin, por lo que estos están expuestos a no cumplir sus restricciones asociadas al alcance tiempo, presupuesto y calidad.

b. Gestión de la Seguridad de la Información

En temas de Seguridad de la Información, la Unidad de Tecnologías de Información ha realizado esfuerzos aislados sin considerar un marco de gestión de la seguridad de la información, por ejemplo:

- Tienen un procedimiento denominado “Gestión de la Seguridad (DGAC-UTI-FM-030)”, donde se indican los lineamientos o actividades para gestionar la seguridad de la información, sin embargo, analizando su contenido aún no se ha implementado.
- Mantienen una segmentación de las redes, es decir la red inalámbrica para invitados es diferente a la red que utilizan los empleados. También tienen cifrada la configuración de los Switches (contraseñas).Sin embargo, para evitar filtraciones de información es importante mantener controles en todas las redes de la institución.

Al no existir un sistema o marco para la gestión de la seguridad de la información, los funcionarios de la DGAC no ponen en práctica medidas como administrar la privacidad de la información, además la falta de capacitación y concientización es uno de los principales motivos de fracaso de los proyectos de seguridad de la información en las organizaciones.

La información que se utiliza en el desarrollo de las actividades de la DGAC es un activo valioso que debe ser protegido desde el momento de su creación, durante su uso y hasta el momento de su destrucción, sin importar el formato que se encuentre. Debido a esto, la información debe ser clasificada apropiadamente para reflejar su importancia y confidencialidad para la DGAC.

La organización guarda sus copias de seguridad de información en el mismo lugar, por lo que tiene un alto riesgo de perder la información original y la de respaldo.

Como conclusión general se tiene que la institución está expuesta a la destrucción, divulgación y modificación de la información.

Según la encuesta global de PWC sobre seguridad de la información las regulaciones de privacidad de datos crean nuevos desafíos para las organizaciones, y generan preocupación entre los ejecutivos.

Entre los encuestados, la prioridad más citada en los próximos 12 meses es la formación y concientización en materia de políticas y procedimientos de privacidad.

c. Prestación de Servicios y Mantenimiento

Se evidencia el incumplimiento con el mandato de gestionar servicios de una manera que se tenga claridad completa de los servicios y sus atributos, y analizar su costo y beneficio para el negocio.

El no contar con la identificación de los servicios que realiza TI se torna difícil poder hacer un monitoreo y seguimiento a la atención de necesidades de los usuarios y el cumplimiento de sus expectativas.

Tener la clasificación de servicios, permite incluso tener una base para la toma de decisiones para el mantenimiento de aplicaciones por ejemplo y si se requiere en algún momento buscar su sustitución, por cuanto ya la aplicación no se va adaptando a los cambios que pueda ir desarrollando el negocio, nuevas regulaciones nuevas tendencias, entre otros

d. Gestión de Riesgos de TI

La Unidad de Tecnologías de Información no cumple con el marco de trabajo definido para la evaluación de riesgos, lo que limita garantizar resultados apropiados en la ejecución de sus actividades. Al no con contar con una gestión de riesgos de TI, no se logran identificar todos aquellos eventos (amenazas y vulnerabilidades) con impacto potencial sobre metas o las operaciones de la institución, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos.

La presencia de los riesgos en las actividades ejecutadas por la Unidad de Tecnologías de Información, llevan a que una de las medidas a considerar, sea la implementación y seguimiento de un proceso de gestión de riesgos, que permita identificar, valorar y tratar los riegos con el fin de disminuir el impacto que pueda ocasionar la materialización de los mismos y que con ello no se vea afectado el nivel de servicio aceptable ni el cumplimiento de los objetivos de la institución.

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

2. Dar Seguimiento al Plan Estratégico e implementación de los proyectos definidos en la cartera de proyectos.
   La Administración General de la DGAC y la Unidad de informática deben garantizar la implementación de los proyectos definidos y aprobados en el PETIC, para cumplir con las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, emitidas por la Contraloría General de la República

A la Unidad de Tecnologías de Información y a la PMO

3. **Gestionar la estrategia de TIC como parte integral de la estrategia de la DGAC**
   Alinear las acciones estratégicas en TI con los objetivos y metas de la estrategia institucional.

4. **Evaluar y replantear las iniciativas del portafolio del proyectos**
   Inventariar los proyectos de TIC actuales y previstos en la organización: identificar objetivos de negocio, plazos e inversiones asociadas y evaluar si es necesario detenerlos o seguirlos.

5. **Darle seguimiento al Plan Estratégico de Tecnologías de Información**
   Priorizar la inversión y la ejecución de iniciativas, alinear los proyectos con los objetivos del negocio y actualizar las fechas de ejecución de cada uno de los proyectos, para monitorear el avance de su cumplimiento.

6. **Darle 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)**
   Se recomienda darle seguimiento al Plan Estratégico de Tecnologías de información, mantener y actualizar el programa de proyectos e implementar el proyecto "Definir e implementar un proceso de gestión de la seguridad de la información para la DGAC", el cual debe crear y formalizar un marco de seguridad de la información, considerando las mejores prácticas de la industria plasmadas en modelos tales como COBIT e ISO 27001.

   Este proyecto debe incluir el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

7. **Darle seguimiento al Plan estratégico de Tecnologías de Información- "Proyecto Definición e implementación de un proceso de administración y operación de los servicios de TIC".**
   Se recomienda reprogramar el proyecto "Definición e implementación de un proceso de administración y operación de los servicios de TIC", y ejecutarlo alineado a las mejores prácticas de la industria.

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".**

A la Unidad de Informática

9. **Utilizar la metodología establecida para la ejecución de los proyectos**.
   Es fundamental que todos los proyectos, desde su concepción que es el anteproyecto sean desarrollados aplicando los lineamientos definidos en el "Manual Metodológico para Administrar Proyectos de TI", esto permitirá contar con las herramientas necesarias para hacer el monitoreo correspondiente a la ejecución de proyectos y de esta forma garantizar que se cumpla el alcance, tiempo y costo y requerimientos de los interesados.

10. **Facilitar capacitación y designar a un gestor de proyectos**
    La Unidad de Tecnologías de Información debe contar con personal que tenga conocimiento sobre elementos que faciliten la compresión de la ejecución de los proyectos desde diversos ámbitos como líderes de proyectos, miembros de equipo ejecutor, entre otros.

11. **Utilizar una metodología para la gestión de riesgos en los proyectos**
    El enfoque metodológico se emplea para determinar los riesgos iniciales del proyecto, así como los que puedan surgir durante el desarrollo del mismo, con el fin de darles seguimiento durante la ejecución del proyecto e ir previendo acciones para la no materialización del riesgo, o que en su defecto si esto ocurre, que su impacto no afecte de forma considerable la ejecución del proyecto.

12. **Facilitar capacitación técnicamente a los funcionarios de la Unidad de Tecnologías de Información en seguridad de la Información**
    Si bien es cierto el documento de "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información", establece los criterios básicos de control que deben observarse en la gestión de las tecnologías de información, éstas dejan a criterio y decisión de los jerarcas el cómo implementar cada uno de los procesos y controles.
    Es por esa razón que la institución debe determinar la importancia de contar con personal capacitado para hacerle frente a los objetivos estratégicos planteados y al cumplimiento de las normativas y regulaciones vigentes.
    Se recomienda evaluar los planes de capacitación y seleccionar cursos que después de ser recibidos, les permitan a los funcionarios poner en práctica lo aprendido y así apoyar al cumplimento de los objetivos de la Unidad, en este caso la seguridad de la información.
    En el mercado existen metodologías o estándares como ISO 27001 que al aplicarla completa y correctamente permite el aseguramiento, la confidencialidad e integridad de los datos y de la información.

Eso también le permitirá a la Unidad de Tecnologías de Información ser un equipo de "contraparte" con criterio en la ejecución del proyecto **CO3-003(Definir e implementar un proceso de gestión de la seguridad de la información para la DGAC)**, y así garantizar la operatividad del Sistema de Gestión de Seguridad.

13. **Gestionar la segunda fase del proyecto CO2-007 - Implementación de herramienta para la gestión de proyectos, utilizando la metodología de gestión de proyectos de la Institución.**

    Según indicó la Unidad de Tecnologías de Información, este proyecto tendrá una segunda fase, cuyo alcance será implementar la herramienta en otras direcciones de la DGAC, motivo por el cual se recomienda establecer desde un inicio el alcance del proyecto, identificar a los involucrados, y crear cada uno de los planes que solicita la metodología de gestión de proyectos de la DGAC. Esto permitirá contar con las herramientas necesarias para hacer el monitoreo correspondiente a la ejecución del proyecto y de esta forma garantizar que se cumpla el alcance, tiempo y costo y requerimientos de los interesados.

14. **Realizar estudios de mercado**

    Para futuras iniciativas de proyectos, se recomienda realizar un estudio de mercado para identificar diferentes opciones que los proveedores puedan ofrecer, eso permitirá elegir la opción que mejor se adecue a solventar las necesidades de la DGAC.

    Una vez que el usuario (área de negocio) tenga los requerimientos funcionales, éste en conjunto con la Unidad de Tecnologías de Información deben indagar y evaluar diferentes herramientas tecnológicas, y posteriormente la coordinadora de Informática como experta en el tema tecnológico, debe asesorar al negocio, tomando en consideración reputación, estabilidad y experiencia del proveedor, funcionalidad de la herramienta, requerimientos técnicos y costo beneficio.

    Es importante que consideren como mejor práctica que el área de negocio que solicita los proyectos de implementación de software, sea el responsable de gestionar el proyecto y tendrá un apoyo del área de tecnologías de información para los requerimientos técnicos.

15. **No iniciar proyectos sin el Acta Constitutiva**

    Se recomienda no iniciar un proyecto sin antes tener aprobada el acta de constitución, pues ésta implica el reconocimiento de la existencia de un proyecto, y de la importancia que tiene para la organización, además es la evidencia de que el proyecto ha sido aprobado por el área competente.

16. **Modificar la Política DGAC-UTI-PO-005 –Seguridad Física y Ambiental**
    Se recomienda realizar una modificación dentro del diseño de la política, de tal manera que se incorpore un periodo de revisión de la política.

    Además, se recomienda que el personal de Seguridad y Vigilancia revise todas las pertenencias que los visitantes ingresan a la DGAC y no solo lo que genera sospechas, esto para evitar subjetividad en la revisión de bolsos y/o maletines.

17. **Implementación de Controles**
    Se recomienda la implementación de controles ya sean elementos de cifrado de la contraseña (Configuración del router para invisibilizar la contraseña de la red WIFI), cambios periódicos en la combinación de la clave de acceso, implementación de perfiles mediante el "Active Directory

18. **Buscar y Validar diferentes opciones para almacenar respaldos como medio paliativo para la protección de la información de la DGAC**

    Dado que el proyecto de modernización tecnológica (CO1-002: Definir e implementar un proceso de mejora continua de la infraestructura de TIC) aún no se ha adjudicado y su implementación puede tardar más ocho meses (según cartel de licitación) se recomienda buscar y validar opciones para el resguardo de los respaldos de información.

    Los respaldos deben almacenarse en lugares que consideren las mejores prácticas en seguridad de la información, continuidad y disponibilidad del servicio.

19. **Actualizar garantías de equipos**
    Revisar la viabilidad de poder actualizar las garantías de todos los equipos que componen la plataforma tecnológica y sus respectivos soportes mientras se ejecuta el proyecto de modernización tecnológica.

20. **Pruebas de restauración de los respaldos de información**
    Validar la posibilidad de adecuar un equipo con un ambiente de pruebas y realizar una restauración de los archivos generados en el proceso de respaldo.

Las pruebas de restauración deben ser realizadas utilizando al menos un respaldo que contenga información crítica para el negocio. Los respaldos deben ser seleccionados de manera aleatoria entre la población que contienen información crítica, de forma que la muestra a ser evaluada sea lo suficientemente confiable para garantizar la integridad del respaldo. Las pruebas de restauración deben ser formalmente documentadas en una bitácora, la cual debe incluir al menos la fecha y hora de revisión, identificación de la cinta revisada, responsable de la revisión y el resultado de la revisión del respaldo. Dichas bitácoras deben ser revisadas y aprobadas por el funcionario asignado encargado de los respaldos y adicionalmente, es importante que se involucre a los dueños de la información en estas pruebas, de manera que ellos verifiquen que los datos fueron restaurados correctamente.

Es importante recalcar que este tipo de pruebas deben ser documentadas dentro del marco o estrategia de gestión de las seguridad de información como una política a seguir, donde se definan responsables, recursos, periodos de ejecución, periodos de revisión y/o consecuencias por el incumplimiento de las mismas.

21. Creación de un esquema de clasificación formal de la información

La clasificación de la información es el acto de colocar los datos en categorías para determinar el nivel de seguridad y tratamiento que se le debe dar a la misma de acuerdo al valor que tiene para el negocio.

La Institución debe establecer responsabilidades sobre la administración de los datos, definir métricas básicas de desempeño y establecer los procedimientos de administración de datos con el apoyo del equipo de TI. Se debe considerar el uso de herramientas para asegurar la generación de los respaldos, la recuperación y desecho de los equipos.

Se deben tomar en cuenta, al menos, los siguientes componentes:

1. Identificar el valor de la información
2. Evaluar los riesgos
3. Categorizar la información
4. Gestionar los controles

22. Creación de una política de seguridad para el uso de las impresoras

Las políticas de seguridad informática están orientadas a proporcionar las directrices de utilización de los recursos informáticos. Es necesario crear

una para el uso de las impresoras y así evitar la divulgación no autorizada de información sensible.

23. Crear, definir y aprobar un proceso para el control de acceso a los sistemas

En el proceso se deben establecer los accesos a sistemas, los tipos de usuario y sus capacidades de operación en los distintos sistemas.

Además debe incorporar un periodo para la realización de las revisiones sobre los usuarios activos y la debida concordancia con sus roles o perfiles.

24. Modificar el "Procedimiento Gestión de TI, punto 2.20 Revisión de privilegios

En el proceso se deben establecer los accesos a sistemas, los tipos de usuario y sus capacidades de operación en los distintos sistemas.

Además, debe incorporar un periodo para la realización de las revisiones sobre los usuarios activos y la debida concordancia con sus roles o perfiles.

25. Implementar una adecuada segregación de funciones o controles que minimicen el riesgo de accesos no autorizados

La organización de TI debe estar alineada con la estrategia de TI, establecer roles y responsabilidades. Las funciones y actividades a realizar por parte del personal de TI y los usuarios deben estar claramente definidas al igual que los requerimientos esenciales y de la experiencia del personal de TI, que permitan consolidar un ambiente de control interno estable.

26. Facilitar capacitaciones a los funcionarios de la Unidad de Tecnologías de Información en "Gestión de Servicios"

Si bien es cierto el documento de "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información", establece los criterios básicos de control que deben observarse en la gestión de las tecnologías de información, éstas dejan a criterio y decisión de los jerarcas el cómo implementar cada uno de los procesos y controles.

Es por esa razón que la institución debe determinar la importancia de contar con personal capacitado para hacerle frente a los objetivos estratégicos planteados y al cumplimiento de las normativas y regulaciones vigentes.

Se recomienda evaluar los planes de capacitación y seleccionar cursos que después de ser recibidos, les permitan a los funcionarios poner en práctica lo aprendido y así apoyar al cumplimento de los objetivos de la Unidad, en este caso la prestación de servicios de tecnología.

En el mercado existen metodologías como ITIL e ISO 20000, diseñadas para ayudarle a brindar servicios de TI más eficaces.

Eso también le permitirá a la Unidad de Tecnologías de Información ser un equipo de "contraparte" con criterio en la ejecución del proyecto "Definición e implementación de un proceso de administración y operación de los servicios de TIC", y así garantizar la operatividad del Sistema de Gestión de Servicios.

27. Definir y aprobar un catálogo de servicios de Tecnologías de Información

La Unidad de Tecnologías de Información debe darle seguimiento e implementar el proyecto: "Definición e implementación de un proceso de administración y operación de los servicios de TIC **",** el cual debe contemplar la definición y documentación de un catálogo de los servicios.

La creación de un catálogo de servicios, debe considerar a las unidades de negocio, procesos y servicios, sus relaciones y dependencias con los servicios de TI, con el objetivo de gestionar las tecnologías de información con las mejores prácticas

28. Definir, acordar y documentar acuerdos de nivel del Servicio (SLAs)

Los servicios y los niveles de servicio deben estar claramente definidos, documentados y se deberá establecer un proceso estándar a utilizar. El proceso de desarrollo del acuerdo de los niveles de servicio, debe contar con puntos de control que permitan la revaloración de los niveles de servicio y la satisfacción de los clientes, así como mantener una equidad entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado.

Se deben considerar los recursos con los que dispone la Unidad de Tecnologías de Información y crear indicadores que sean posibles de cumplir.

29. **Adecuar la herramienta considerando las necesidades de toda la organización**
    Una vez que hayan definido un proceso estándar para la gestión de servicios, el catálogo de servicios, acuerdos de nivel de servicio, se recomienda configurar la herramienta con la lista completa de los servicios, prioridad de atención de solicitudes, guías de auto- ayuda, reportes, distinción de usuario por solicitudes autorizadas, niveles de escalamiento, reportes de información. Se recomienda seguir las mejores prácticas plasmadas en modelos como ITIL o ISO 20000.

30. **Desarrollar y documentar un proceso para la gestión de incidentes**
    Este proceso busca brindar atención y solución a los incidentes y problemas que minimicen la calidad del servicio brindado.

    El propósito primordial de la gestión de incidentes es restaurar la operación normal del servicio tan pronto como sea posible y minimizar el impacto adverso en las operaciones del negocio.

31. **Definir un esquema de clasificación y priorización de incidentes**
    Que considere, al menos, los siguientes elementos:
    - Componentes afectados (hardware o software)
    - Servicios de TI afectados
    - SLA relacionados.

32. **Estandarizar la definición de incidentes críticos y los procedimientos especializados, con el fin de poder establecer prioridades de atención según la criticidad de los incidentes**.

33. **Diseñar y/o adoptar e implementar una política con la metodología de gestión integral del riesgo (seguimiento al proyecto CO3-002)**
    Según Cobit, cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los interesados y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

Al definir una política con la metodología, permite identificar actores principales en el proceso de valoración de riesgos, y se pueden establecer los deberes, responsabilidades y consecuencias por el incumplimiento de la política, además se definen los periodos de revisión de la política y el responsable por esta revisión.

34. Facilitar Capacitación al personal de TI en Gestión de Riesgos

Se recomienda que se incluya temas relacionados con la gestión de riesgos como parte de la capacitación que reciben los empleados de la Unidad de Tecnologías de Información, de manera tal que se aumente la concientización en administración de riesgos y de cómo impacta la gestión de riesgos de TI en toda la organización.

35. Asignar responsabilidades para la Gestión Integral de Riesgos en la Unidad de Informática

Las personas que tienen roles de dueños, líderes o expertos de proceso, por lo general tienen la responsabilidad de identificar y gestionar sus riesgos, además de comunicarlos a las personas correspondientes dentro de la institución. Por tal razón es recomendable que se designe un responsable de la gestión de riesgos.

A la PMO

36. Capacitación y más seguimiento por parte de la PMO

Se recomienda a la PMO capacitar a las Unidades Funcionales de la DGAC sobre el debido proceso para completar cada uno de los apartados del acta de constitución de un proyecto, incluso tener guías de ejemplo y así cumplir con uno de sus objetivos, el cual es:

> "Divulgar, capacitar y dar seguimiento y control de la aplicación de la metodología institucional para facilitar la rendición de cuentas"

Además de que una vez que reciban las actas las revisen y de ser necesario sugieran cambios, esto como responsables designados en la DGAC para dichos efectos.

Al Proceso de Recursos Humanos

37. Incluir en el Plan de Capacitación para el Personal de la DGAC temas sobre Seguridad de la Información

Se recomienda que se incluya temas de seguridad como parte de la capacitación que se brinda a los empleados de la DGAC, de manera que se aumente la concientización en administración de seguridad a nivel de toda la organización.

Lo anterior, puede ser apoyado también mediante campañas internas breves que vayan recordando a los funcionarios aspectos relevantes sobre Seguridad de la Información y su importancia para la Dirección General de Aviación Civil.

38. Validar que el personal de seguridad y vigilancia se apegue su programa de trabajo

Se recomienda validar con frecuencia la labor de los oficiales de seguridad con la intención de generar conciencia sobre los efectos negativos que pueden ocurrir en caso de accesos de personas u objetos no autorizados a la Institución

39. Incluir dentro del procedimiento de funciones de la recepcionista , el registro del personal que ingresa a la institución

Agregar al procedimiento "5I03 Instructivo para la recepción, radicación, distribución de documentos " una sección para establecer las funciones del registro de visitantes y además la obligación de que el personal de recepción conozca y se apegue a las políticas de seguridad de la institución

AI-212-2017

21 de agosto del 2017

ADVERTENCIA

Señor
Enio Cubillo Araya
Director General de Aviación civil
Su Oficina

ASUNTO: OBSERVACIONES SOBRE EL PROCESO DE PLANIFICACIÓN DE PROYECTO TI[4]

Estimado señor:

De conformidad con lo que establece la Ley General de Control Interno № 8292, en su artículo № 22 inciso d), que señala como una competencia de las auditorías internas el "(…) advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento. (…)" y en atención a seguimiento realizado por esta Auditoría Interna, sobre la adquisición de un software para la gestión de Ventanilla Única –ALFRESCO– y un software para la gestión de acuerdos –Metro BPM–, se atisban serias deficiencias en la fase de planificación de este proyecto, establecido mediante la Contratación Directa 2016CD-000175-0006600001, estimado su costo inicial en $60.000.00[5] y no sometido al proceso ordinario de Contratación Administrativa.

Al respecto se observó lo siguiente:

1. **No se realizó una descripción clara, completa y oportuna de las especificaciones técnicas de los usuarios; de ambos software que requería la DGAC para la gestión de la ventanilla única y la gestión de acuerdos del CETAC.**

[4] Tecnologías de Información.
[5] Según oficio DGAC-ACB-OF-126-2016 de 22/09/2016; suscrito por la funcionaria Rosemary Aguilar Guzmán, como Encargada de Administración y Control de Bienes.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Tanto la Encargada de la Unidad de Informática; como Unidad Técnica de esta contratación, como el Encargado del Proceso de Recursos Materiales y la funcionaria a cargo de Ventanilla Única, como Unidad Solicitante, indican que por tratarse de software de código libre, sujeto a adaptación según se considere necesario; no era necesario determinar con puntualidad las especificaciones técnicas de los usuarios, de la necesidad a satisfacer, ya que lo que se contrata son horas para la adaptación. Además, de que inicialmente la idea nació únicamente para atender necesidades de Ventanilla Única. Las citadas posiciones se contraponen a normativa que regula el Reglamento a la Ley de Contratación Administrativa y normas técnicas emitidas por la CGR[6], por cuanto:

a. El artículo Nº 8 del Reglamento de Contratación Administrativa, regula puntualmente en lo que interesa, que la decisión inicial será emitida por las Unidades Competentes, una vez que se haya acreditado al menos lo siguiente:

> "(…)
>
> b) **La descripción** del objeto, **las especificaciones técnicas y características** de los bienes, obras o servicios **que se requieran,** (…)". (El destacado no es del original)

b. Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE), emitidas por la CGR, en la Norma 3.1 denominada "Consideraciones generales de la implementación de TI", regulan

> "La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información (…). Para esta implementación y mantenimiento debe:
>
> (…)

[6] Contraloría General de la República

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

> f. **Contar con una definición clara, completa y oportuna de los requerimientos,** (…).”

c. Esta Auditoría Interna, realizó consulta[7], al profesional fiscalizador del área de Informática, con la finalidad de confrontar la citada normativa con la posición de los funcionarios de la DGAC, al respecto se confirmó que:

i. El hecho de que el software sea de tipo código libre, o privado -o no libre-, no exime a la administración activa de diseñar la especificación técnica, lo cual es un ejercicio esencial, para tener claridad de lo que se requiere para satisfacer las necesidades que se pretenden solventar.
ii. El diseño completo de la especificación técnica permite comparar los requerimientos de los usuarios frente a las características del software y valorar si cumple las necesidades.
iii. Solo diseñando con la mayor completitud la especificación técnica, era factible, **estimar el costo de la contratación**.

La ausencia de las especificaciones técnicas de frente a las necesidades de los usuarios, limitó seriamente **la definición del alcance del proyecto**. Se visualizó la gestión documental de ventanilla única y la gestión de acuerdos del CETAC, **aislada de los requerimientos técnicos del Archivo Central**, que se rige por la Ley № 7202 Ley del Sistema Nacional de Archivos, no obstante que; tanto los subprocesos de Ventanilla Única como Archivo Central, son subordinados del Proceso de Recursos Materiales de la Unidad de Servicios de Apoyo.

El cartel planteó el objeto como:

> “Contratar los servicios de implementación y soporte de una solución basada en el software Alfresco y Libre firma, **tanto para la gestión de Ventanilla Única de la DGAC,** como para la firma digital de documentos y el **Gestor de Procesos de**

[7] Verbal, el 28/07/2017, funcionario fiscalizador de TI de CGR.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Negocios METRO BPM, para los acuerdos del CETAC."[8], y la fase de ejecución dio inició el 16/12/2016:

No obstante lo anterior:

i. La Secretaría del CETAC, manifestó[9] a esta Auditoría Interna; que no se le solicitó previamente los requerimientos específicos y que tampoco se le informó lo que ofrecía el citado software, que, a su juicio, no cumple con las necesidades de la Secretaría CETAC.

ii. El Encargado del Archivo Central emitió en junio 2017 amplios informes[10] con la posición técnica de la materia a su cargo, en la que informa que el Archivo Central no fue consultado ni considerado para la definición de las especificaciones técnicas de la citada contratación.

De los informes señalados; se infiere que la gestión electrónica de ventanilla única, firma digital y la gestión de acuerdos, **no podía abordarse** desde una posición aislada de la materia que regula la gestión documental, independientemente del medio en que se produzcan los documentos –físicos o electrónicos–.

Al respecto, el profesional-funcionario[11] de la DGAC en materia de archivística, señaló sobre el software para ventanilla única; 85 aspectos de los cuales, en su criterio técnico, al menos 21 equivalentes a un 25% serían desarrollos nuevos e incluso indicó que algunos; en caso de que no se lograran desarrollar, no serían de recibo para una adecuada gestión documental electrónica.

Sobre 35 aspectos, está pendiente de verificar si se logran satisfacer, y la solución en su opinión técnica cumple un 34% de sus requerimientos. A continuación se resume lo indicado.

[8] El resaltado en negrita no es del original.
[9] En mayo 2017, verbalmente.
[10] Oficio DGAC-AC-OF-016-217 de 06/06/2017 y DGAC-AC-OF-018-2017 de 14/06/2017.
[11] Sr. Francisco Soto Molina.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Cuadro Nº 1
Resumen de Aspectos según Criterio del Archivo Central
Software Alfresco

Cumple	Pendiente de verificar si cumple o no	No cumple
29	**35**	**21**
34%	41%	25%

Un detalle completo puede ser leído en el Anexo Nº 1[12], el cual es remitido por correo electrónico –considerando la extensión del documento–.

Además, indicó[13], entre otros aspectos; que:

"En este punto es necesario desechar cualquier criterio que pretenda hacer ver que la contratación no era para el Archivo Central, sino para la Ventanilla Única y por lo tanto el criterio archivístico innecesario. Puesto que la Ley es la que establece las competencias del Encargado del Archivo Central y es en este departamento donde se aplican las disposiciones finales en relación con la documentación producida por ese ente.".

"(…) Es preciso hacer notar que la gestión documental **no** es tema resorte de esa unidad de ventanilla única, que se limita a recibir y distribuir documentos."[14]

[12] Cuadro comparativo de especificaciones técnicas del Archivo Central frente a la posición de Unidad de Informática y resumen de datos por confrontación.
[13] Oficio DGAC-AC-OF-018-2017, de 14/06/2017.
[14] El destacado en negrita y subrayado es del original.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

2. No se cumplió con normativa interna para la administración de proyectos TI[15]

Se advierte que este proyecto de tecnologías de información (TI), no cumplió con las etapas definidas por la Unidad de Informática en el procedimiento del sistema de gestión institucional 6P03 "Gestión de TI[16]", también definidas en el manual 6M03 "Manual Metodológico para Administrar Proyectos de TI", que regulan en cuanto a la gestión de proyectos TI, las actividades que deben seguir los funcionarios de la Unidad de Informática.

Se observa que se omitió etapas a esenciales, tal como la siguiente, regulada en el citado manual 6M03:

"4.1. Etapa 0. Anteproyecto.
(…)
• **Se determinan las expectativas generales de los interesados,** así como el **efecto y resultados esperados.**".
• **Identificar los actores involucrados** en el proyecto a desarrollar.
• Confeccionar la ficha de anteproyecto.

Someter el anteproyecto a la evaluación del Comité Gerencial de Tecnologías de Información y Comunicación (CGTIC), el cual valorará su viabilidad y prioridad dentro de la organización.".
(La negrita no es del original)

[15] Tecnologías de Información.
[16] Actividad 2.4 "Gestión de Proyectos".

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Asimismo, lo regulado en el Procedimiento 6P03, que indica:

Sr. Enio Cubillo Araya –7– 21 de agosto del 2017

"2.4.2 El o los funcionarios de TI inician formalmente el proyecto.

- **Corroboran** las expectativas generales de los usuarios, gerentes y de cualquier otro interesado, para establecer los resultados esperados y el alcance del proyecto.
- Definen la organización del proyecto y selecciona el equipo de trabajo.
- **Realizan un informe de diagnóstico** que permita establecer **las diferentes opciones** de solución a ser evaluadas.
- **Eligen la alternativa de solución a ser desarrollada.**"[17]

Al respecto la Encargada de la Unidad de Informática, reiteró –por escrito[18] y verbalmente– que los recursos presupuestarios estaban asignados al Proceso de Recursos Materiales de la Unidad de Servicios de Apoyo.

Asimismo, la Unidad de Informática indicó que había cumplido con el citado Procedimiento y Manual, aspectos que fueron analizados por esta Auditoría Interna, determinándose que no se encontró:

- Las entrevistas realizadas a los interesados que servirían para determinar las expectativas.
- El enunciado –integrado– de los interesados con la identificación de los requerimientos institucionales.
- La identificación de todos los actores involucrados tanto a nivel macro como micro del entorno del proyecto.
- La definición del alcance del proyecto.
- La Ficha de Anteproyecto según lo establece el Anexo Nº 7 del citado Manual 6M03, la cual incluye aspectos relevantes como: Enfoque del

[17] El resaltado en negrita en este párrafo y el anterior, no corresponde al original.
[18] Oficio DGAC-UI-OF-0128-2017 de 22/06/2017 en general y pág. 5 párrafo segundo en particular.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

proyecto, relaciones de coordinación, responsables, requerimientos iniciales, nombre del que elabora la ficha.

- La corroboración de la expectativas generales de los usuarios, gerentes y de cualquier otro interesado, para establecer los resultados esperados.

- El informe del diagnóstico que permitiera establecer las diferentes opciones a ser evaluadas.
- No se encontró el informe con el análisis de alternativas.

En el Anexo No 2 se presenta un detalle con los elementos que establece el Procedimiento y/o el Manual 6M03, la forma en que informó Unidad de Informática que lo cumplió y el comentario de Auditoría Interna.

La anterior posición, no es compartida por esta Auditoría Interna, considerando por una parte; que el citado proyecto se encuentra enunciado en el Plan Estratégico de Tecnologías de Información –PETIC– identificado como "Desarrollo e implementación del Sistema de Gestión Documental", "PETIC-DGAC-C02-002-2016" y por otra, en apego a los propios procedimientos de la Unidad de Informática, en lo que interesa, en el citado Manual 6M03 define:

> "Un proyecto en Tecnologías de Información y Comunicaciones (TIC) **es todo aquel que introduzca** en la organización elementos tecnológicos que soporten y hagan más eficiente la ejecución o el desarrollo de un proceso.". (El destacado no pertenece al original)

De igual forma, el citado Procedimiento 6P03 Gestión de TI, por su parte regula:

> "2.4. Gestión de proyectos 2.4.1. El o los funcionarios de TI mediante lo estipulado en el Plan Estratégico de Tecnología de Información, PETIC identifican una serie de necesidades que pueden ser atendidas mediante el desarrollo de proyectos utilizando el 6M03, Manual Metodológico para Administrar Proyectos de TI.".

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

A juicio de esta Auditoria Interna, de frente al Procedimiento y Manual establecidos, la gestión realizada para la planificación de este proyecto no se ajustó a los citados procedimientos.

Sr. Enio Cubillo Araya –9– 21 de agosto del 2017

3. Sobre la planificación para optar –toma de decisión– por los software libres Alfresco y el Metro BPM y la decisión de oferente único

No se encontró en el expediente físico –Ampo– facilitado por la Encargada de Ventanilla Única, el estudio que acreditara que solamente el citado software libre ALFRESCO y el Metro BPM eran las únicas alternativas en el mercado, idóneas para satisfacer la necesidad institucional.

La funcionaria encargada de Ventanilla Única, –hasta el 14/07/2017– indicó que el estudio o indagatoria de mercado fue realizado por la Unidad de Informática y no justificó con base en un estudio técnico de indagatoria de mercado, la aplicación del artículo 131 a) que acreditara que la opción propuesta era la única apropiada y que no existían en el mercado otras alternativas que pudieran considerarse idóneas.

La Encargada de la Unidad de Informática, informó[19] que valoró el software "EPOWER" y aportó como evidencia dos minutas de reunión del 25/01/16 y del 02/02/2016 sin resultado de la valoración realizada e indicó que la indagatoria de mercado, fue realizada por el Proceso de Recursos Materiales, por su parte el Encargado de Recursos Materiales indicó[20] que:

> "No se realizó estudios preliminares de factibilidad relacionados. No se documentó el análisis comparativo de las soluciones de software libre similar en el mercado costarricense.".
>
> "En una reunión sobre espacios, con la participación de la Encargada de Unidad de

[19] Oficio DGAC-UI-OF-0128-2017 del 22/06/2017.
[20] Reunión del 21/07/2017.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Informática y la señora Subdirectora en ese momento, se conversó sobre la necesidad de un software para la gestión de la ventanilla única.

Malou Guzmán Quesada, Encargada de Informática, ya conocía el software ALFRESCO que lo utilizaban en el

Sr. Enio Cubillo Araya –10– 21 de agosto del 2017

MICITT, coordinó con ellos y la empresa vino y realizó una presentación.

Nos decidimos por el software libre ALFRESCO y el METRO BPM ya que de la lectura de información en Internet, más el conocimiento previo del citado software de la Encargada de Informática, vimos muchas facilidades o fortalezas en estos softwares. Por mi parte realicé una indagatoria en Internet, -se facilitan los documentos fotocopiados- en la que se observan las facilidades y opiniones sobre el software Alfresco.”.

Es criterio de esta Auditoría Interna; que haber considerado únicamente dos opciones de software, resulta una indagatoria de mercado muy limitada, además, no se encontró el resultado final de la valoración que acreditara comparativamente las facilidades técnicas y de precio que llevó a decidirse por el software ALFRESCO y el Metro BPM, ambos sobre los que; según la administración activa es oferente único; ya que el soporte únicamente lo brinda en Costa Rica la empresa I.T. Alkaid Consulting Group, S.A.

Al respecto, es conveniente recordar lo que regula el Reglamento a la Ley de Contratación Administrativa, en cuanto a la decisión de no promover un concurso y optar por la decisión de oferente único:

“Artículo 139.-Objetos de naturaleza o circunstancia concurrente incompatibles con el concurso. (…):

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

a) Oferente único: Los bienes o servicios en los que se acredite que **solamente una persona o empresa** está en condiciones de suministrar o brindar, sin que existan en el mercado alternativas que puedan considerarse idóneas para satisfacer la necesidad institucional. **La procedencia de este supuesto ha de determinarse con apego a parámetros objetivos en relación con la necesidad, acreditando que la opción**

propuesta es la única apropiada y no sólo la más conveniente.". (El resaltado no es del original)

Otro aspecto que llama la atención, es que la Encargada de la Unidad de Informática, presentó[21] a solicitud del CETAC una propuesta para el control y seguimiento de acuerdos y correspondencia, mediante oficio DGAC-TI-OF-042-2016 de 15/03/2016, denominado "Informe ACUERD_SOFT", en el que expone la forma en que opera el sistema AcuerdSoft[22] que utiliza actualmente la Secretaría del CETAC; de seguido pasa a las "Conclusiones" para en resumen indicar:

i. Que existe una serie de herramientas en el mercado. Pero no especifica cuáles.
ii. Que la herramienta que se puede adaptar a las necesidades y al quehacer de la institución se conoce como Metro BPM ya permite ser un Software para la Gestión de Procesos de Negocio, en el cual se puede diseñar y ejecutar procesos de negocio baja una única plataforma robusta, personalizable y extendible.
iii. Menciona cinco características, tales como a) Más productividad b) Disminución de Riesgo, c) Reducción de costos, que usualmente opera sobre un entorno completamente libre y de código abierto, reduciendo costos de licenciamiento, entre otros d) Menor resistencia y e) Cambio

[21] Propuesta solicitada por el CETAC mediante artículo 03 de la sesión ordinaria 16-2016 celebrada el 09/03/2016.
[22] Sistema electrónico para control de acuerdos utilizado actualmente por Secretaría CETAC.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

continuo: permite añadir, mejorar y actualizar sus procesos de negocio de forma continua bajo una única plataforma, reduciendo esfuerzos adicionales de compra, mantenimiento o creación de software adicional.

En cuanto a las "Recomendaciones" en resumen indica:

i. "La aplicación que se propone se conoce como METRO-BPM, y puede ser vista a través de la siguiente dirección".
ii. La plataforma se integraría con Alfresco, Active Directory, y además habilitaría no solo el seguimiento de Reuniones, sino que eventualmente

podrá servir a la institución para una amplia diversidad de procesos de negocio.

iii. Los costos son relativamente bajos, **reduciendo a $0 el costo de desarrollo**, que normalmente oscila entre $5.000 y $20.000, dependiendo de la complejidad se tendría que invertir en la implementación y capacitación al personal de planta tanto a nivel técnico como funcional.
iv. **El tiempo de instalación e implementación se percibe en un mes.**
v. **El mantenimiento sería propio de los técnicos de TICS's, no dependeríamos del proveedor.**".[23] (La negrita no es del original)

Con base en el citado informe el CETAC aprobó[24] el 04 de mayo del 2016; la implementación de la citada herramienta para el seguimiento de acuerdos, con un monto de $10.200.00 que no se encontraron enunciados en la propuesta de la Unidad TI.

Al ser consultada la Encargada de la Unidad de Informática, sobre las discrepancias anteriores indicó:

[23] El resaltado en negrita no es del original.
[24] Sesión Ordinaria 30-2016 del 04/05/2016, Oficio CTAC-AC-2016-0593.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

a. En cuanto al monto de $10.200.00, indicó que el mismo 04/05/2016 le presentó al CETAC una cotización de la empresa ALKAID, por $10.200.00.
b. En cuanto a lo informado al CETAC de que "El mantenimiento sería propio de los técnicos de TICS's, no dependeríamos del proveedor" no obstante, se incluyó en la Contratación Directa 2016CD-000175-0006600001, sobre este aspecto se le consultó[25] a la Encargada de Informática, pero no se recibió respuesta al respecto.

Sr. Enio Cubillo Araya –13– 21 de agosto del 2017

En cuanto a que; el tiempo de instalación e implementación se percibe en un mes, se observó que el 01/08/2017[26] se indicó que "Lo del CETAC posiblemente se podrá desarrollar el próximo 2018, para este año se haría el análisis y diseño".

De las recomendaciones de la propuesta anterior, se infiere que en el plazo de un mes y con cero costo por desarrollo la aplicación estaría implementada, asimismo, que el mantenimiento sería realizado por personal de la Unidad de Informática, no obstante, la adaptación de esta aplicación fue incorporada en la Contratación Directa 2016CD-000175-0006600001, que en el cartel, en lo que interesa indica:

> "(…) la aplicación conocida como Metro BPM la cual funge como Gestor de Procesos de Negocio, habilitada para el seguimiento a reuniones y actas del CETAC (…)".

Con lo expuesto, se evidencia que el proceso de planificación y toma de decisión tanto del software Alfresco como del Metro BPM es omiso, confuso y no está debidamente documentado.

4. Comisión de la Gestión de Documentos Electrónicos

[25] Correo electrónico del 31/07/2017.
[26] Minuta de reunión DGAC-UTI-FO-MNT-013 del 01/08/2017.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Se encontró que en febrero 2012 el Encargado[27] del Proceso de Recursos Materiales, solicitó al Director General, la conformación de la Comisión de Gestión de Documentos Electrónicos, esto en cumplimiento de la "Directriz con las regulaciones técnicas sobre la administración de los documentos producidos en medios automáticos", la cual quedó formalmente conformada[28] por la Coordinadora de la Unidad de Servicios de Apoyo, el Encargado de la Unidad de Informática y la Encargada del Archivo Central.

Sin embargo, no se localizó evidencia que la citada Comisión esté funcionando.

Sr. Enio Cubillo Araya –14– 21 de agosto del 2017

El citado órgano funcional, se conformó para cumplir con la necesaria coordinación interdisciplinaria entre los archivistas, administradores e informáticos en el diseño y aplicaciones informáticas que respondan a las necesidades reales de información, según lo regula la citada directriz y se transcribe en el oficio de conformación de la citada Comisión.

5. Ejecución presupuestaria al 31/07/2017

Al 31/07/2017 se tiene una ejecución presupuestaria de ¢4.770.000.00 y un saldo para ejecución en la Orden de Compra No. 876 por ¢150.000.00, para un total de ¢4.920.000.00 y es de conocimiento de esta Auditoría Interna, que se estaban realizando acciones para brindar más contenido presupuestario durante 2017.

Para el 2018 la Administración Activa, estimó[29] 640 horas que son equivalentes a ₡18.032.000.00, para servicios según demanda.

6. Observaciones al Manual 6M03 "Manual Metodológico para administrar proyectos de TI"

[27] Funcionario Olman Duran Arias.
[28] Oficios DGAC-URM-OF-0083-2012 de 16/02/2012; Oficio DGAC-DG-OF-0602-2012 de 19/03/2012.
[29] Oficio DGAC-VU-OF-005-2017 del 15/06/2017; firmado por la Encargada de Ventanilla Única.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Se observó que el Manual institucional 6M03 denominado "Manual Metodológico para administrar proyectos de TI", disponible en el Sistema de Gestión Institucional, es una copia casi idéntica del documento de Contraloría General de la República denominado "Guía Metodológica para administración Proyectos TI", y alude en catorce párrafos a la expresión "CGR" o "Contraloría General de la República".

Al respecto no se encontró documento alguno donde se indique que se siguió un procedimiento de adopción del documento de CGR.

A continuación se transcriben algunos de los párrafos del Manual para administrar proyectos TI en la DGAC; que define obligaciones para la CGR:

"6. Anteproyecto (Etapa 0)

Sr. Enio Cubillo Araya –15– 21 de agosto del 2017

Todo proyecto tecnológico a desarrollar debe estar contemplado en el Plan Táctico de TIC (PTAC), el cual responde a las orientaciones que plantea el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) de la Contraloría General de la República (CGR)."

"5.1 Planteamiento de proyectos
En el proceso de planeación estratégica de la CGR se determinarán dichas necesidades y de un primer análisis de éstas se deberá plantear ante la jefatura de la USTI, una ficha de anteproyecto (…)."

"10.3 Expediente actualizado del proyecto
(…)
Este expediente debe contener todos los entregables de cada fase del proyecto, y debe mantenerse en

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

formato digital de acuerdo al expediente electrónico definido en la CGR."

"c. Definición de infraestructura tecnológica
(…) incluyendo aquella que no esté disponible en la CGR y que se constituye en un riesgo tecnológico."

"Efecto
Para que un proyecto sea viable dentro de la CGR, el mismo debe aportar un valor agregado a la misma."

"Recursos tecnológicos
(…) se requiere contar con un servidor instalado en la red central de la CGR, a partir del mes de octubre, con las siguientes características técnicas.....".

"Anexo 1
Definición de roles

Comité Gerencial de Tecnologías de Información y Comunicaciones (CGTIC):

Por delegación del máximo jerarca (Contralor o Contralora General), es el máximo ente en lo referente a recomendar sobre las directrices y lineamientos a seguir en la planificación y dirección de los procesos de desarrollo tecnológico.

Está conformado por representantes de alto nivel gerencial, por el Jefe de Auditoria Interna como asesor del Comité y por el Jefe la Unidad de Sistema y Tecnologías de Información (USTI). Este Comité reporta al máximo jerarca, quien lo preside.".

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

Así las cosas, preocupa profundamente a esta Auditoría Interna, el manejo desarticulado y omiso en su fase de planificación del citado proyecto, al punto que se prescindió los procedimientos institucionales para la gestión de proyectos de TI; lo que hace inferir que condujo a buscar una solución; sin analizar el contexto de la organización; sus necesidades reales y las implicaciones para la adecuada gestión documental, entendida como la creación, recepción, organización, uso, comunicación, conservación o eliminación documental institucional electrónica, garantizando su integridad, autenticidad, confiabilidad e inalterabilidad.

Asimismo; llevó a la administración a comprometer fondos públicos y optar por la "Implementación y soporte Un sistema de Gestión Documental para la Ventanilla Única de la Dirección General de Aviación Civil basada en el Software Alfresco y Gestor de Procesos de Negocios METRO BPM", sin disponer de una sólida indagatoria de mercado, sin los requerimientos técnicos de los usuarios, sin los requisitos para una adecuada gestión documental electrónica y por ende; sin un costo estimado cercano a la realidad de la citada solución, en la medida en que si no se determinó de previo; de la manera más completa y clara posible los requerimientos, no es factible estimar la dimensión real del proyecto[30] -su alcance- ni su costo, aunque éste sea de código libre.

Dicho lo anterior y; sin que ello signifique una intromisión en las competencias de la Administración Activa, se recomienda al señor Director General,

que es aconsejable instruir de inmediato –sin que esto signifique una lista taxativa–por principios de sana administración pública, lo siguiente:

1. Retrotraer la planificación del citado proyecto para revisar y plantear la planificación del proyecto de frente a la normativa externa e interna aplicable y las mejores prácticas; de tal forma que se asegure que la solución elegida, efectivamente apoya el modelo de gestión documental electrónica del CETAC-DGAC de forma eficiente, eficaz y económica.

[30] Conceptos generales consultados el 28 de julio del 2017 en http://www.evaluandosoftware.com/gestion-requerimientos-proyecto-software-empresarial/

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

2. Realizar la identificación lo más completa posible de las especificaciones técnicas de los usuarios y realizar el costeo de las horas de contratación requeridas para adaptar el software ALFRESCO y Metro BPM a las necesidades de los usuarios, CETAC y Archivo Central y/u otros que se lleguen a identificar.

3. A partir de los análisis anteriores y otros que se realicen; asegurarse que las soluciones por la que se optó –ALFRESCO y Metro BPM–, es factible que cubran las necesidades institucionales de los usuarios y en materia archivística –gestión documental electrónica–, en caso contrario, replantear la solución.

4. Sobre lo anterior; emitir un informe en un plazo razonable que no debería sobrepasar dos meses, en el que la Encargada de la Unidad de Informática, la Encargada de la Unidad de Servicios de Apoyo y el Encargado del Archivo Central, expongan ampliamente los resultados de la revisión realizada, con análisis y evidencia suficiente y que la decisión que se llegue a tomar, se realice conjuntamente con el criterio técnico del profesional en Archivo Central y el o los usuarios más representativos que se lleguen a identificar.

5. Revisar el Manual 6M03 `Manual Metodológico para administrar proyectos de TI` para asegurarse que el mismo sea aplicable a la DGAC y no a CGR.

6. Revisar que la Comisión de Documentos Electrónicos conformada en el 2012 con la participación del Archivo Central y la Unidad TI para dar cumplimiento a normativa relacionada con la Dirección General del Archivo Nacional; la CITI que se menciona en el procedimiento 6P03 de Gestión de TI y el Comité

Gerencial de Tecnologías de Información y Comunicaciones (CGTIC) que se menciona en el Manual 6M03, son o no la misma instancia. Definir ya sea en el 6M03 o en 6P03 la existencia, funciones y responsabilidad de cada una de esas instancias o de la instancia que llegue a unificarse si así se considera conveniente.

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

7. Sobre las dos revisiones anteriores informar de los resultados en un plazo razonable que no debería sobrepasar un mes.

Atentamente,

Original Firmado por:
Lic. Oscar Serrano Madrigal, MBA
AUDITOR GENERAL

C.C.:
Sra. Lorena Murillo Quirós, Encargada Unidad Servicios de Apoyo
Sra. Malou Guzmán Quesada, Encargada Unidad de Informática
Sr. Francisco Soto Molina, Encargado Archivo Central Institucional
Papeles de trabajo
Archivos** ☜COPIA
OSM/iga

Central Tel: 2242-8000 Teléfono directo: 2290-0092 Fax: 2290-0092 S:http://.dgac.go.cr Apdo. Postal 5026-1000 San José Costa Rica

ANEXO Nº 1

Auditoria Interna-CETAC

Anexo No. 1 del Oficio AI-212-2017

Cuadro comparativo de especificaciones técnicas del Archivo Central frente a la posición de Unidad de Informática y resumen de datos por confrontación

Aspecto	Requerimiento según Archivo Central	Archivo Central		Unidad Informática			Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-			
		¿Cumple?		¿Cumple?		Observaciones		Cant.	CUMPLE	Ptes de Verificación	No cumple
		Si	No	Si	No						
Columna	1	2	3	4	5	6	7	8	9	10	11
Generalidades y Requerimiento Técnico.	Entrega del código fuente del sistema.	X		X				1	1		
	El sistema deberá inter-operar con otros sistemas (uso SDK o similar) y abstraer la documentación producida por estos para ser administrada en el gestor documental.		X	X			**Pendiente de verificación**; con este requerimiento se busca asegurar que todos los documentos públicos generados por cualquier sistema en la institución (ejemplo sistema contable) pueda ser abstraída o integrada por el gestor documental.	2		1	
	Instalación de la solución y capacitación a los usuarios.	X		X				3	1		
	El sistema deberá funcionar en modalidad web.	X		X				4	1		
	Las bases de datos que requiera para su funcionamiento se encuentran en SQL.		X	X			**Pendiente de verificación**; no fue visto en la presentación del sistema	5		1	
	El sistema, sus módulos e interface se encuentran en español. Ley 7623.	X		X				6	1		

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?		Unidad Informática ¿Cumple?		Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-			
		Si	No	Si	No			Cant.	CUMPLE	Ptes de Verificación	No cumple
Columna	1	2	3	4	5	6	7	8	9	10	11
	El sistema deberá poder funcionar con múltiples browsers: Internet Explorer, Safari, Mozilla Firefox, Google Chrome, entre otros.	X		X			**Se comprueba su complimiento; después de verificar el sistema;** no fue visto durante la presentación pero se constata luego de usar el sistema.	7	1		
	El sistema deberá contar con la correspondiente documentación de usuario final y de referencia técnica editado/redactado en idioma español.		X	X		Disponible en idioma inglés	**No cumple**; Siendo una dependencia pública, la DGAC tiene que satisfacer el principio de legalidad, en este caso el artículo # 4 de la Ley 7623.	8			1
	El sistema tendrá una interfaz de usuario sencilla en la que se presente la información de todos los módulos que lo conforman.		X	X			**No cumple**; podría verificar si hay cambios en la interface. Sin embargo los términos y usos vistos en los botones de uso; son extraños. (No es amigable ni sencilla)	9			1
	El sistema permite visualizar el documento desde su propia interface.	X		X			**Se comprueba su complimiento, después de verificar el sistema;** no fue visto durante la presentación	10	1		

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?		Unidad Informática ¿Cumple?		Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-			
		Si	No	Si	No			Cant.	CUMPLE	Ptes de Verificación	No cumple
Columna	1	2	3	4	5	6	7	8	9	10	11
							pero se constata luego de usar el sistema.				
	El sistema es capaz de generar documentos desde él mismo.		X	X		Usando integración con Office y GoogleDrive,tambiénte HTML	**No cumple**; el sistema requiere que se creen los documentos en un editor de texto y sea subidos a él, igualmente es importante indicar que las modificaciones a los documentos se generan desde los editores de texto y el sistema versiona los documentos modificados. (Esto es vital, si no cumple el sistema no es de recibo para el AC)	11			1
	El sistema permite la utilización de cualquier software (editor de texto) para la generación de documentos electrónicos, sin estar vinculado a ninguna empresa de software especifica.	X		X			**Se comprueba su complimiento, después de verificar el sistema;** no fue visto durante la presentación pero se constata luego de usar el sistema.	12	1		

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?		Unidad Informática ¿Cumple?		Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna- Cant.	CUMPLE	Ptes de Verificación	No cumple
		Si	No	Si	No						
	El sistema deberá permitir la creación, instalación y modificación de plantillas documentales por tipo documental (cartas, memorandos, correos electrónicos, certificaciones, constancias, informes, entre otros) garantizando un estándar de los documentos elaborados desde el sistema. El modelo deberá basarse en el Sistema de Gestión de Calidad. "Instructivo para la Confección de tipos documentales de uso institucional para las comunicaciones escritas" 5IO2 y sus formularios.		X	X		El sistema soporta la instalación, modificación y creación de plantillas documentales, sin embargo desconocemos los alcances del instructivo 5102, por lo cual no nos referimos a ello.	**No cumple;** Es necesario, para cumplir con esta especificación, que el sistema sea capaz de crear documentos desde sí mismo. Las plantillas requeridas son para tipos documentales y deben ser creadas por editores de texto de manear que se pueda modificar el contenido de cada tipo, desde el propio editor. Aquí no se refiere a formularios electrónicos para bases de datos, sino plantillas insertas de editores de texto.	13			1
	El sistema debe ser capaz de generar cada plantilla (por tipo documental) y garantizar que estos cumplan con los siguientes elementos: Poder seleccionar de una lista predeterminada, el tipo documental a utilizar. El editor de texto debe generar los documentos con base al código ACSII, cumpliendo los criterios de la norma ISO/IEC-8859-1. Generar y almacenar metadatos (ver sección de metadatos) de forma automática. Completar un formulario de metadatos (ver sección de metadatos) de forma manual. Debe ser capaz de descargar documentos (.docx /.odt/.PDF, entre otros). Convertir el documento generado en formato PDF/A, cumpliendo los criterios de la norma ISO/DIS 19005-1. Firmar el documento electrónico digitalmente, según lo establecido por el art. 9 de la Ley Nº 8454 y lo dispuesto en la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente del MICIT.		X	X		El conjunto de caracteres es UTF8, extendido y estándar. No genera PDF/A pero es posible implementarlo mediante un desarrollo adicional que la plataforma permite.	**No cumple;** es relevante indicar que el conjunto de caracteres UTF8 incluye la codificación ACSII. Sin embargo; el sistema no indica cumplir con los requerimientos de este apartados. **Se marca como pendiente de verificación**; porque de los 6 criterios vistos en este punto, el sistema cumple por lo menos con 3 y queda pendiente verificar los siguientes: Poder seleccionar	14		1	

							documentos desde una lista predeterminada, Conversión a PDF/A, Descargar documentos de distintas extensiones y poder usarlos (lectura, escritura/modificación).				
	El sistema genera códigos por unidad administrativa (código de referencia) a partir de la nomenclatura aprobada para la estructura organizacional de la Dirección General de Aviación Civil, en su última versión vigente.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada. (Requiere implementación)	15			1
	El sistema debe ser capaz de generar consecutivos automáticamente para todos los documentos generados por el sistema		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada. (Requiere implementación)	16			1
	El sistema controla las versiones de los documentos producidos.	X		X			**Se comprueba su complimiento, después de verificar el sistema;** no fue visto durante la presentación pero se constata luego de usar el sistema.	17	1		

Gestión documental	El sistema debe conservar las versiones anteriores del documento hasta la versión final, debe registrarse a. El nombre del documento, Fecha, Hora, Valor o versión anterior, Usuario principal, Último usuario que modificó, Peso del archivo.	**X**		X			**Se comprueba su complimiento, después de verificar el sistema**; no fue visto durante la presentación pero se constata luego de usar el sistema.	18	1		
	El sistema emite avisos automáticos a los usuarios sobre tareas pendientes, cuando estos: -Reciban un documento, -Se emita una nueva versión de un documento previamente conocido. -Obligando a los usuarios a ejecutar sus pendientes por medio de alertas de conocimiento / lectura, dentro del ambiente de tareas del sistema.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	19		1	

Aspecto documental	**Requerimiento según Archivo Central**	**Archivo Central**		**Unidad Informática**			**Observaciones Archivo Central**	**Resumen de datos por confrontación - Auditoría Interna-**			
		¿Cumple?		**¿Cumple?**							
		Si	**No**	**Si**	**No**	**Observaciones**		**Cant.**	**CUMPLE**	**Ptes de Verificación**	**No cumple**

	El sistema permite el préstamo de documentos, estableciendo plazos de devolución y alertas al usuario cuando esté vencido.	X		X		Es posible compartir para solo lectura, para edición fuera de línea. Un registro aparte es posible implementarlo. No se le encuentra sentido debido a que el documento no sale del Archivo ni requiere devolución	**Cumple;** No puede operarse un gestor documental solo con los criterios para la recepción y remisión de documentos, dejando de lado las funciones procesos y actividades que compelen la gestión documental y el tratamiento archivístico. Es necesario que un gestor documental pueda satisfacer las funciones archivísticas dadas por ley. A la fecha de la emisión de este informe, el Archivo Central registra 62 préstamos de documentos; con salida; hacia otras dependencias. Es importante hacer notar que son varias las unidades, que deben compartir documentos con otras dependencias, tal es el caso de Recursos Humanos, que también registra los préstamos entre dependencias. Sobre lo manifestado en la observación de	20	1		

							informática; cuando manifiesta "que no se le encuentra sentido" es preciso indicar que los requerimientos dados por este proceso de Archivo Central, son los requerimientos mínimos para el uso de un gestor documental.				
	El sistema permite subir documentos con distintos tipos de archivos y extensiones, docx, odt, PDF/A.		X	X			**Pendiente de verificar.**	21		[1]	
	El sistema posee mecanismos de trazabilidad que permite establecer procesos de trabajo y quienes deben conocer un documento y emitir alertas de conocimiento/lectura para su atención.		X	X		El sistema soporta la implementación de flujos de trabajo, es factible implementar con desarrollo adicional procesos como el que se describe.	**Pendiente de verificar** el cumplimiento según la observación indicada.	22		[1]	

	El sistema permite gestionar expedientes y cuenta con un índice electrónico que vincula cada documento.		X	X			**No cumple**; este sistema no posee índices electrónicos que vinculen los documentos de un expediente; con listas de control, en las cuales se indiquen cada documentos de manera única e inconfundible. (Este incumplimiento es relevante, no es de recibo si no cumple)	23			1

Aspecto	**Requerimiento según Archivo Central**	**Archivo Central**		**Unidad Informática**			**Observaciones Archivo Central**	**Resumen de datos por confrontación - Auditoría Interna-**			
		¿Cumple?		**¿Cumple?**							
		Si	**No**	**Si**	**No**	**Observaciones**		**Cant.**	**CUMPLE**	**Ptes de Verificación**	**No cumple**

	El expediente electrónico, deben ser capaz de incluir todos los documentos que requiera integrarse. Para el caso se recomienda acudir a las normas ISO 14721 e ISO 32000 y tener en cuenta los siguientes: Índice electrónico: Incorporará un índice electrónico de los documentos que contiene el expediente y sus metadatos. Conversión: La conversión de los documentos a los formatos de ficheros admitidos para su conservación permanente. (sección metadatos para conservación) Captura: Captura y aplicación de protocolos de comprobación de integridad y legibilidad de los documentos. Paquetes de información de archivos: Registro de la captura en el sistema de producción de los Paquetes de Información de Archivo. Paquetes de Información de Comunicación: Proceso de producción de los Paquetes de Información de Comunicación o PIC, para su recuperación y consulta. Acceso: Aplicación de los protocolos de administración del sistema relativo al acceso, para garantizar el cumplimiento de la normativa de privacidad y de seguridad de acceso. Evolución tecnológica: Aplicación de las políticas y los procesos periódicos para comprobar que los archivos se puedan leer, así como las políticas de cambio de los archivos a nuevos formatos que puedan aprobarse de acuerdo con la evolución de la tecnología. Soportes: Aplicar las políticas de conservación de los medios o soportes de los documentos, para garantizar la estabilidad y legibilidad de los datos.		X	X		Hay conceptos cuyo alcance no es comprendido con certeza, por lo cual no nos referimos a estos.	**No cumple,** Se indica por parte de informática que existen criterios no comprendidos con certeza. Para el caso se aclara que como base para la elaboración de estos requerimientos, se emplearon conceptos y métodos científicos de la archivística contemporánea, universalmente aceptados y normas ISO, que son bases de estandarización internacionalmente aceptadas. (Este requerimiento es muy importante, no es de recibo si no cumple)	24			1
	El sistema deberá permitir la inclusión simultánea de documentos, generados por distintos usuarios relacionados con un mismo expediente, también escaneos.		X	X			**No cumple.**	25			1
	El sistema utiliza el correo electrónico para realizar notificaciones.	X		X				26	1		
	El sistema establece pistas de auditoría, que registran la actividad de cada usuario.	X		X				27	1		
	El sistema permite establecer “capas” o niveles de uso, para usuarios.	X		X				28	1		
	El sistema permite compartir documentos con otros funcionarios, a los cuales se les puede asignar un permiso específico. a. solo Vista, Vista y Editar, Editar y Compartir.		X	X			**No cumple.**	29			1

Facilidad de compartir documentos.	El sistema debe notificar vía correo electrónico a las personas interesadas; que se le ha compartido un documento		X	x		El sistema envía un correo diario con los documentos eliminados, creados y modificados en los cuales la persona cuenta con acceso	**Pendientede verificar** el cumplimiento según indicada. la observación	30		1	
	El sistema permite archivar los documentos por carpetas y estas a su vez en carpetas o sub carpetas. Siendo que se pueda archivar documentos por año, serie documental, tipo documental, entre otros.	X		X				31	1		
	El sistema permite enviar documentos por correo electrónico y abstraeros desde él, para integrarlos a la ubicación de carpeta respectiva.	X		x				32	1		
Metadatos.	La gestión documental por medio ofimático; debe cumplir con los datos contenidos en el esquema de metadatos del Archivo Central (ver pág.. 33 del documento)	X		X		Es posible implementarlo mediante un análisis, diseño y configuración, de metadatos que la plataforma permite, determinando la forma más conveniente de representarlo en el software	**Se comprueba su complimiento; después de verificar el sistema**; no fue visto durante la presentación pero se constata luego de usar el sistema.	33	1		
	El sistema permite generar metadatos de forma automática.	X		X				34	1		
	El sistema permite seleccionar metadatos de una lista predeterminada.	X		X				35	1		
	El sistema permite la introducción manual de metadatos ingresados por el usuario, según sea requerido.	X		X				36	1		
	El sistema genera un documento XML por cada documento de archivo producido o recibido en el sistema y vincula todos los metadatos del documento con el documento de archivo.		X		X	Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	37		1	
	El sistema permite la inclusión de esquemas de metadatos y la posibilidad de cambiarlo.	X		X				38	1		

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?		Unidad Informática ¿Cumple?		Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-			
		Si	No	Si	No			Cant.	CUMPLE	Ptes de Verificación	No cumple
Conservación.	El sistema cumple con el principio de Neutralidad Tecnológico: a.Pueden ser empleados en escenarios multiplataforma. b.No están sujetos a un determinado producto licenciado. c.Cuentan con una adecuada documentación técnica. d.Permiten la incorporación de múltiples firmas en un documento electrónico. e.Implementan los principios de un mecanismo de firma confiable: f.Garantía de la autenticidad del documento electrónico. g.Garantía de la integridad del documento electrónico. h.Ubicación fehaciente del documento electrónico en el tiempo.	X		X				39	1		
	El sistema permite convertir todos los documentos tramitados por él, en formato PDF/A con base en el estándar de la norma ISO 19005-1.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	40		1	
	El sistema deberá prevenir, retardar o detener el deterioro o eliminación de los documentos digitales, con el objetivo de preservarlos en condiciones de uso, estabilidad tecnológica y reconversión a nuevos soportes.		X		X	Este requerimiento no es competencia del software sino del hardware y la administración de estos recursos.	**No cumple.** Para el cumplimiento de este punto, se requiere verificar que el sistema sea compatible con otro tipo de aplicaciones correlacionales que varían o sufren actualizaciones en el tiempo "up dates" y que lo haga seguir siendo interoperable, sea por el uso de nuevos (por ejemplo, si utiliza software editores de texto como Word y este sufre alteraciones o modificaciones que obligue al sistema a sufrir mejoras para	41			1

							que pueda seguir siendo operable) . Además debe conservar los metadatos que permitan la conservación por analogía y conversión.				
	El sistema cuenta con la función de revalidación automática de los documentos por otros periodos determinados de tiempo.		X	X		La revalidación se encuentra presente en el módulo de RM en el módulo de DM no se encuentra, pero es posible implementarlo mediante un desarrollo adiciona que la plataforma permite	**Pendiente de verificar** según el cumplimiento la observación indicada.	42		1	
	El sistema debe alertar en por lo menos 10 asuntos pendientes a los usuarios responsables de una acción, para anticiparse al vencimiento de los documentos.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** cumplimientosegún el la observación indicada.	43		1	
	El sistema almacena todos los documentos electrónicos que genere o ingresen a la Institución.		X	X			**Pendiente de verificar** el ya cumplimiento que no hay e observación Jnidad de d nformática.	44		1	

	El sistema debe garantizar la preservación de todos los documentos electrónicos producidos por la Dirección General de Aviación Civil, de conformidad a lo establecido en "Las regulaciones técnicas sobre la administración de los documentos producidos por medios automáticos, publicada en La Gaceta Nº 221 de 11 de noviembre de 2004" de la Junta Administrativa del Archivo Nacional y la Norma ISO 14721:2003 Open Archivar Information System (OAIS) -- Reference Model que proponen el marco reglamentario de archivos para la conservación y acceso a la información electrónica a largo plazo.	X		X				45	1		
Aspecto	**Requerimiento según Archivo Central**	**Archivo Central ¿Cumple?**		**Unidad Informática ¿Cumple?**		**Observaciones**	**Observaciones Archivo Central**	**Resumen de datos por confrontación - Auditoría Interna-**			
		Si	**No**	**Si**	**No**			**Cant.**	**CUMPLE**	**Ptes de Verificación**	**No cumple**
	El Sistema permite la encriptación de documentos son base al estándar CAdES-XL. Basado en la especificación ETSI TS 101 733, en su última versión oficial. Para documentos con información codificada en binario. Para su codificación en soluciones a la medida, se propone el perfil CAdES Baseline Profile de la ETSI, el cual puede encontrarse en la especificación ETSI TS 103 173, en su última versión oficial.		X	X		El sistema permite almacenar documentos generados en ese formato	**Pendiente de verificar** según el cumplimiento la observación indicada.	46		1	
	El Sistema permite la encriptación de documentos son base al estándar PadES Long Term (PadES LTV). Basado en la especificación ETSI TS 102 778, en su última versión oficial. Para documentos en formatos PDF y sus formatos extendidos. Para su codificación en soluciones a la medida, se propone el perfil PAdES Baseline Profile de la ETSI, el cual puede encontrarse en la especificación ETSI TS 103 172, en su última versión oficial.	X		X		El sistema permite almacenar documentos generados en ese formato		47	1		
	El Sistema permite la encriptación de documentos son base al estándar XadES-X- L. Basado en la especificación ETSI TS 101 903, en su última versión oficial. Para documentos en formatos XML. Se recomienda para el desarrollo de soluciones informáticas en donde sea necesaria la interoperabilidad con otras instituciones.		X	X		El sistema permite almacenar documentos generados en ese formato	**Pendiente de verificar** según el cumplimiento la observación indicada.	48		1	
	Acuse de recibido de documento con firma digital.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** según el cumplimiento la observación indicada.	49		1	

	El sistema permite la creación de un flujo de trabajo sencillo para la inclusión de firmas que no sean del productor del documento y solicitar la aprobación específica de un documento y firmarlo digitalmente. Este flujo debe contemplar el establecimiento de un orden específico de firmas, de tal forma que la siguiente persona en firmar no pueda hacerlo, hasta que el anterior lo haya firmado.		X	X			aspecto no **No cumple;** este fue posible verificarlo.	50			1
	Cada una de las firmas generadas por el sistema, debe registrarse en el esquema de metadatos asociado al documento.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	51		1	
	El sistema deberá permitir que el documento a ser firmado, se le puedan adjuntar documentos relacionados, para que los firmantes puedan validar la información si es necesario.		X	X			**Pendiente de verificar.**	52		1	
	El sistema deberá contar con una funcionalidad de recordatorio para los documentos y notificar a los funcionarios que deban firmarlos y notificar vía correo electrónico a las personas interesadas, a las que se les haya compartido un documento.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	53		1	
Firma Digital: para la producción de los documentos electrónicos, se	Para la producción de los documentos electrónicos, se utilizarán los formatos de firma digital avanzados vigentes en el país que permitan definir de manera estandarizada los atributos suficientes para garantizar la verificación de validez del documento en el tiempo, que estén auspiciados por alguna entidad autorizada y que sus especificaciones técnicas sean de acceso público.						Esto es un comentario de aclaración que intencionalmente se incluye en el cuadro comparativo de evaluación. **(No evaluable es comentario)**	0			
utilizarán los formatos de firma digital avanzados vigentes en el país que permitan definir de manera estandarizada los atributos	Los documentos electrónicos, legalmente válidos en Costa Rica, son aquellos que cuenten con la encriptación oficial que dispone para ello la Ley N°8454. Así, los formatos oficiales y válidos de firma digital en Costa Rica, serán los que se enmarquen dentro del cumplimiento de los requerimientos de firma electrónica avanzada, dispuesto por la Dirección de Certificadores de Firma Digital. Bajo esa premisa, se dispone que los formatos oficiales de firma electrónica sean aquellos emitidos con base a las normas técnicas del Instituto de Estándares de Telecomunicaciones Europeo (ETSI), en un nivel de especificación que contemple la inclusión de todos los atributos necesarios para garantizar la verificación de su validez en el tiempo de manera irrefutable.						Esto es un comentario de aclaración que intencionalmente se incluye en el cuadro comparativo de evaluación. **(No evaluable es comentario)**	0		0	

suficientes para

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple? Si	Archivo Central ¿Cumple? No	Unidad Informática ¿Cumple? Si	Unidad Informática ¿Cumple? No	Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna- Cant.	CUMPLE	Ptes de Verificación	No cumple
suficientes para garantizar la verificación de validez del documento en el tiempo, que estén auspiciados por alguna entidad autorizada y que sus especificaciones técnicas sean de acceso público.	El sistema deberá ser capaz de soportar y firmar, por lo menos, en los siguientes formatos: a. ODT ODS ODP XLSX DOCX PPTX DOC XLS PPT PDF (PDF/A con base a la ISO 19005-1) XML MP4 MP3 AVI MPEG WMA WAV PNG JPG BMP MIDI FLV		X	X		El sistema soporta el almacenamiento y gestión de todos los formatos mencionados. En cuanto a firmar permite el formato en PDF.	**Pendiente de verificar** el cumplimiento según la observación indicada.	54		1	
	En el ciclo de vida de un documento electrónico firmado digitalmente, se identifican dos conjuntos de responsabilidades relacionados con mecanismos de firma digital: la firma digital y la verificación de validez de la firma digital. Para la emisión de un documento electrónico firmado digitalmente, y para la recepción o verificación de su validez, se establecen una serie de actividades que deben realizarse para garantizar que la firma digital asociada tenga valor en el tiempo. El lugar y la manera en que se codifican estos atributos en el documento electrónico corresponden con lo indicado en las especificaciones de la ETSI mencionadas anteriormente.						Esto es un comentario de aclaración que intencionalmente se incluye en el cuadro comparativo de evaluación. **(No evaluable es comentario)**	0			
	Cuando se firma digitalmente un documento electrónico, el sistema deberá implementan los mecanismos de firma digital, incluyendo los atributos descritos, ver pág. 41 punto 6						Esto es un comentario de aclaración que intencionalmente se incluye en el cuadro comparativo de evaluación. **(No evaluable es comentario)**	0			

	Cuando se verifica la validez de un documento electrónico firmado digitalmente, es imperativo que se realicen las siguientes validaciones de los diferentes atributos que el documento contiene, ver pág. 42, punto 7		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	55		1	
	Los atributos e información relacionada con la emisión de la firma electrónica, deberá almacenarse en un documento XML que se asocie de forma única con el documento producto del acto público; de manera que estos metadatos puedan incluirse en la ficha de descripción correspondiente.		X		X			56			1
	El sistema debe ser capaz de atender el riesgo que al tratar de hacer una firma digital en formato oficial, los servicios de respuesta en línea o los repositorios de información de revocación no estén disponibles. Con el objetivo de que dicha eventualidad no limite la creación de firmas digitales en documentos electrónicos, a los que posteriormente pueden incluirse todos los atributos adicionales que permiten la verificación de la validez de la firma digital del documento electrónico a largo plazo.”		X		X	No es posible, dado que siempre se deben contar con disponibilidad de los servidores de firma digital costarricense para extraer los certificados.	**No cumple**, este requisito se cumple cuando el sistema tiene la capacidad de conservar el documento encriptado, por el creador del mismo, y a pesar de no contar con servicio de internet en el momento de la encriptación, mantenerlo en una carpeta de salida que de forma automática, al restablecerse el servicio de internet, se comunique con el servidor del Banco que emite el certificado y pueda generarse la firma.	57			1
	El sistema es capaz de recibir documentos electrónicos firmados digitalmente a través del correo electrónico institucional.	**X**		X			**Se comprueba su complimiento; después de verificar el sistema;** no fue visto	58	1		

							durante la presentación pero se constata luego de usar el sistema.				

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple? Si	Archivo Central ¿Cumple? No	Unidad Informática ¿Cumple? Si	Unidad Informática ¿Cumple? No	Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna- Cant.	CUMPLE	Ptes de Verificación	No cumple
Acuse de Recibido Digital.	El sistema recibe el correo y verificar que el documento adjunto este firmado correctamente.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite. La validación requerida se efectuaría luego de que el documento sea cargado	**Pendiente de verificar** el cumplimiento según la observación indicada.	59		1	
	El sistema verifica que el certificado de firma no este revocado o vencido, esta validación debe realizarse automáticamente.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite. La validación requerida se efectuaría luego de que el documento sea cargado	**Pendiente de verificar** el cumplimiento según la observación indicada.	60		1	
	El sistema genera un acuse de recibo electrónico automático, de forma tal que alerte a la persona que envió el documento, si el mismo es válido o no.		X	X		Es posible implementarlo mediante un	**Pendiente de verificar** el cumplimiento según la observación indicada.	61		1	

						desarrollo adicional que la plataforma permite					
	El sistema cuenta con la facilidad de envío de correo electrónico desde la misma aplicación, sin necesidad de salir del sistema para utilizar el correo electrónico institucional	X		X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimientosegúnla observación indicada.	62		1	
Eliminación.	El sistema deberá generar listados de aquellos documentos que perdieron su vigencia administrativa y legal, para proceder con su respectiva eliminación de acuerdo a lo establecido en la legislación vigente.	X		X				63	1		
	El sistema permite seleccionar del listado de documentos, aquellos que serán eliminados de forma permanente.		X	X			**Se comprueba su complimiento; después de verificar el sistema;** no fue visto durante la presentación pero se constata luego de usar el sistema.	64	1		
	El sistema genera un acta de eliminación para los documentos seleccionados. La cual será firmada: El encargado del Archivo de Gestión. El superior jerárquico de la Instancia o quién funja como presidente del CISED.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**No cumple:** el cumplimiento según la observación indicada.	65			1
	El sistema garantiza que la instancia competente de autorizar la eliminación de documentos sea el Archivo Central, mediante el acta de eliminación que de fe de la eliminación.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimientosegúnla observación indicada.	66		1	

	El sistema deberá garantizar que los documentos dispuestos para ser eliminados, sean eliminados definitivamente, sin oportunidad que estos se puedan restablecer.	X		X				67	1		
Clasificación.	El sistema debe ser capaz de generar un cuadro de clasificación documental, en el que se presente todos los tipos documentales generados por la institución. El cuadro de clasificación deberá contener los criterios establecidos en el Proceso de Clasificación del Archivo Central de la Dirección General de Aviación Civil.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según observación indicada.	68		1	
	El sistema debe ser capaz de establecer modelos de Clasificación de tipo orgánico, y tipo funcional según los criterios establecidos en el Proceso de Clasificación del Archivo Central de la Municipalidad. Para lo que se requiera, se entiende como clasificación: -Clasificación Orgánica. De acuerdo con la estructura orgánica de la Institución, se deben crear carpetas para la adecuada organización de los documentos. -Clasificación por Funciones. Se crearan carpetas de acuerdo con la Instancia Ejecutora.		X	X			**No cumple.**	69			1
Descripción: La descripción es el proceso archivístico que busca explicar de forma precisa y clara, la función y contenido de los documentos	El sistema debe incluir una plantilla que se constaten todos los elementos de las normas de descripción archivística: Norma Internacional de Descripción Archivística (ISAD-G) Norma Internacional para la Descripción de Funciones (ISDF) Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias (ISAAR-CPF) Norma internacional para describir instituciones que custodian fondos de archivo (ISDIAH) Ver pág. 45, punto 2 (existe una plantilla específica)		X	X		Es posible implementarlo mediante un desarrollo o configuración adicional que la plataforma permite	según la observación **No cumple:** indicada.	70			1
	El sistema deberá contar con la función de revalidación automática de los documentos por otros periodos determinados de tiempo.		X	X			**No cumple.**	71			1
	El sistema permite establecer criterios y parámetros para realizar transferencia de documentos de los archivos de gestión al central.	X		X				72	1		

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?		Unidad Informática ¿Cumple?		Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-			
		Si	No	Si	No			Cant.	CUMPLE	Ptes de Verificación	No cumple
Transferencia.	El sistema deberá permitir la creación de una plantilla de transferencia de documentos, para la remisión de documentos que contenga las siguientes informaciones. Numero de orden Tipo o Serie documental Nº de Expediente Nº de Caja Contenido Fechas extremes Cantidad Caducidad Administrativa – Legal Valor legal/cultural. Puede eliminarse en el mes y año.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	73		1	
	El sistema permite que la plantilla de transferencia documental, sean firmadas por los encargados de cada departamento remitente y por la unidad administrativa receptora.		X	X		Es posible implementarlo mediante un	**Pendiente de verificar** el cumplimiento según la observación indicada.	74		1	

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?		Unidad Informática ¿Cumple?		Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-			
		Si	No	Si	No			Cant.	CUMPLE	Ptes de Verificación	No cumple
						desarrollo adicional que la plataforma permite					
Búsqueda en el sistema.	El sistema permite la búsqueda booleana de documentos.		X	X			**Pendiente de verificar** cumplimiento según la indicada. el observación	75		1	
	El sistema permite el uso de distintos descriptores para realizar búsquedas de documentos: palabras clave (código de referencia, número de finca, nombre del productor, etc.), atributos del documento, asunto, estado del documento, autor, etc.	X		X				76	1		
	El sistema deberá contar con un mecanismo de control de acceso a los documentos por diferentes niveles. a. publico, departamental, funcional, por usuario, entre otros.		X	X			**No cumple.**	77			1
	El sistema deberá contar una interface de búsqueda única, permitiendo consultas a múltiples repositorios de modo transparente para el usuario (según su nivel de acceso a los documentos).		X	X			**No cumple.**	78			1
	La interface del sistema es amigable, permite realizar la búsqueda a distintos repositorios u fondos, sin que requiera ubicarse en cada repositorio o fondos.		X	X			**No cumple.**	79			1
Expediente en Soporte Electrónico	Los expedientes producidos por el sistema deben garantizar la inclusión de elementos de seguridad para garantizar la integridad, seguridad y confiabilidad de las piezas documentales que se anexen al expediente.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** cumplimiento según la indicada. el observación	80		1	
	El sistema debe ser capaz de crear una Tabla de Plazos de Conservación, por cada unidad administrativa.		X	X		Es posible implementarlo	**Pendiente de verificar** cumplimiento según la indicada. el observación	81		1	

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple? Si	Archivo Central ¿Cumple? No	Unidad Informática ¿Cumple? Si	Unidad Informática ¿Cumple? No	Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna- Cant.	CUMPLE	Ptes de Verificación	No cumple
						mediante un desarrollo adicional que la plataforma permite					
	La información de las Tablas de Plazos debe estar dispuesta en una plantilla de 10 columnas y la cantidad de filas requeridas para anotar los tipos documentales producidos por cada unidad administrativa.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** según el cumplimiento indicada. la observación	82		1	
	Las tablas de plazos deben poseer la siguiente información. a. N de orden Serie o tipo documental ¿O/ Copia? ¿Cuáles otras oficinas tienen esta serie? Señale a la par si es O o Ce. Contenido Soporte Vigencia para documentos en cada soporteOficina Arch. Ctrl. Cantidad en metros/ peso en BITS del documento Fechas extremas Observaciones		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**de verificar** según el la observación **Pendiente** cumplimiento indicada.	83		1	
	Las tablas de plazos de eliminación de documentos deben ser aprobadas por el Comité Institucional de Selección y Eliminación, por lo que se requiere que se versionen las tablas de plazos de eliminación de cada departamento.		X	X		Es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** según el cumplimiento indicada. la observación	84		1	
La valoración documental											

Aspecto	Requerimiento según Archivo Central	Archivo Central ¿Cumple?	Unidad Informática ¿Cumple?	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna-

Aspecto		Requerimiento según Archivo Central	Archivo Central ¿Cumple? Si	Archivo Central ¿Cumple? No	Unidad Informática ¿Cumple? Si	Unidad Informática ¿Cumple? No	Unidad Informática Observaciones	Observaciones Archivo Central	Resumen de datos por confrontación - Auditoría Interna- Cant.	CUMPLE	Ptes de Verificación	No cumple
			Si	No	Si	No	Observaciones		Cant.	CUMPLE	Ptes de Verificación	No cumple
		Una vez aprobada la tablas de plazos de eliminación de documentos para cada Instancia se requiere que el sistema debe ser capaz de: Advertir cuando y cuales documentos se pueden eliminar, de acuerdo a la vigencia administrativa y legal de dicho instrumento. Alertar a cada Instancia el plazo de vencimiento de la tabla de plazos de eliminación de documentos, según lo dispuesto por la normativa vigente.		X	X		El punto a si se encuentra implementado en la aplicación, el punto b, es posible implementarlo mediante un desarrollo adicional que la plataforma permite	**Pendiente de verificar** el cumplimiento según la observación indicada.	85		1	
		Totales	**29**	**56**	**81**	**4**				**29**	**35**	**21**
										34%	41%	25%

Nota 1: Las columna 1 a 3 elaboradas por el Encargado de Archivo Central. De 4 a 6 por Unidad de Informática, 7 y 8 por Archivo Central, y 9 a 11 por

Nota 2: Auditoría Interna ajustó desmarcó los 4 casos no evaluables según lo indicó el Encargado del Archivo Central.

No Evaluables = 4 = Comentario 89-4= 85

Nota 1: La columna 1 "Requerimiento según Archivo Central" fue elaborada por el Encargado del Archivo Central.

Nota 2: Las filas marcadas como pendiente de verificar, no implican que se encuentren en cumplimiento. Si no que; en razón de las dos presentaciones a las que asistió el encargado del Archivo Central, en relación con la operatividad del software ALFRESCO, no le fue posible constatar su cumplimiento con cada requisito. Por lo que tiene que verificarse en relación con lo indicado por Informática. La columna 6 muestra la posición de la Unidad de Informática en relación con el requerimiento del Archivo Central expuesto en la columna 1.

Nota 3: La indicación de "No evaluables", se crea para determinar algunas filas que fueron vistas como requisitos según el Encargado del Archivo Central, pero que hacen mención a explicaciones y aclaraciones dadas para hacer comprensible cada punto de los requerimientos técnicos.

Nota 4: Columna 1 a 3: Elaboradas por el Encargado de Archivo Central. Columnas de 4 a 6: Elaboradas por la Unidad de Informática. Columna 7: Elaborada por el Archivo Central.

ANEXO № 2

Análisis de Auditoría Interna, sobre la respuesta brindada por Unidad de Informática correo-e del 10/08/2017**,** sobre el cumplimiento del Procedimiento 6P03 Gestión TI y el 6M03 Manual Metodológico para Administrar Proyectos de TI.

La estructura de este anexo es la siguiente: a) Se transcribe lo que indica el procedimiento o manual. b) se indica la respuesta a cómo lo cumple según lo indicó la Unidad de Informática c) en un recuadro se presenta el análisis de auditoría Interna.

a) Lo que indica el procedimiento 6P03 Gestión de TI

1.1. *Gestión de proyectos*

1.1.1. El o los funcionarios de TI mediante lo estipulado en el Plan Estratégico de Tecnología de Información, PETIC identifican una serie de necesidades que pueden ser atendidas mediante el desarrollo de proyectos utilizando el ***6M03, Manual Metodológico para Administrar Proyectos de TI****.*

- *Determinan las expectativas generales de los interesados, por medio de una entrevista realizada a los interesados.*

b) Cómo se realizó según UI:

Se inicia el proceso verificando las necesidades del área usuaria, mediante recolección de insumos que se identificaron con varias reuniones con ayuda de diferentes empresas para entrevistarlos, e identificar así sus requerimientos técnicos y de usuario necesarios. Ver anexo de minutas.

Reunión con empresa GSI (ePower)
Se desarrolló reunión con minuta DGAC-UTI-FO-MNT-01-2016 con fecha 25/01/2016, en donde se identificaron los requerimientos institucionales de la ventanilla única. Además de eso, se revisó el proceso actual de la ventanilla única, la logística que se requiere cuando se llegue a implementar algún sistema para la ventanilla única y lo que ofrecía el sistema propuesto por ellos. Los insumos fueron entregados por los usuarios expertos Rosemary Aguilar, Olman Durán y Yesenia Castillo.

Reunión con empresa Alkaid (Alfresco)
Se desarrolló una segunda reunión con minuta DGAC-UTI-FO-MNT-03-2016 con fecha 31/01/2016, en donde se identificaron los requerimientos de los usuarios expertos. Asimismo se explicó a la empresa la necesidad y los usuarios finales validaron la información del proceso actual de la ventanilla única, adicional a esto la empresa Alkaid presentó el funcionamiento del sistema Alfresco y se conversó sobre la parametrización a la medida que

se podía realizar al mismo para determinar si podía cubrir todas las necesidades de los usuarios solicitantes, entre estos el flujo de ventanilla única.

c) Comentario de AI:

No se encontró las entrevistas realizadas a los interesados que servirían para determinar las expectativas.

No se encontró el enunciado –integrado– de los interesados con la identificación de los requerimientos institucionales.

Se observa que las minutas obedecen a una presentación/demostración de lo que ofrecen los proveedores comerciales Alkaid y GSI.

a) Lo que indica el procedimiento 6P03 Gestión de TI:

- Identifican los actores involucrados en el proyecto a desarrollar (macro y micro entorno del proyecto así como el alcance del mismo).

b) Cómo se realizó según UI:

Reunión con empresa GSI (ePower)
Se desarrolló reunión con minuta DGAC-UTI-FO-MNT-01-2016 con fecha 25/01/2016, en donde se identificaron los requerimientos institucionales de la ventanilla única. Además de eso, se revisó el proceso actual de la ventanilla única, la logística que se requiere cuando se llegue a implementar algún sistema para la ventanilla única y lo que ofrecía el sistema propuesto por ellos. Los insumos fueron entregados por los usuarios expertos Rosemary Aguilar, Olman Durán y Yesenia Castillo.

Reunión con empresa Alkaid (Alfresco)
Se desarrolló una segunda reunión con minuta DGAC-UTI-FO-MNT-03-2016 con fecha 31/01/2016, en donde se identificaron los requerimientos de los usuarios expertos. Asimismo se explicó a la empresa la necesidad y los usuarios finales validaron la información del proceso actual de la ventanilla única, adicional a esto la empresa Alkaid presentó el funcionamiento del sistema Alfresco y se conversó sobre la parametrización a la medida que se podía realizar al mismo para determinar si podía cubrir todas las necesidades de los usuarios solicitantes, entre estos el flujo de ventanilla única.

c) Comentario de AI:

En las minutas no se observa la identificación de todos los actores involucrados. Las minutas citadas, son las únicas y son iniciales en las que participa la encargada del Archivo Central en

ese momento.

El procedimiento regula que a nivel macro y micro entorno del proyecto, se deben identificar los actores, y el alcance.

Precisamente es causa de la debilidad en la etapa de planificación de este proyecto la ausencia de una identificación adecuada de esos actores y del alcance del proyecto.

a) Lo que indica el procedimiento 6P03 Gestión de TI:

- Confeccionan la ficha de anteproyecto según lo establecido en el **6F92, Ficha de Proyecto TI**

b) Cómo se realizó según UI:

El 18 de mayo se recibe por parte del CTAC la aprobación del PETIC. La ficha de anteproyecto ya se había confeccionado a través del documento del PETIC llamado Cartera de Proyectos 2016 - 2020, el proyecto tiene asignado el código C02-02.

c) Comentario de AI:

El Manual 6M03 incluye el Anexo 7 con el diseño de la Ficha de anteproyecto que no es coincidente con la utilizada en el PETIC.

Incluye puntos adicionales, relevantes como: Enfoque del proyecto, alcance, Relaciones de Coordinación, Responsable, Requerimientos iniciales. Nombre del que elabora la ficha.

a) Lo que indica el procedimiento 6P03 Gestión de TI:

- Someten el anteproyecto a la evaluación de la CITI, donde se valorará su viabilidad y prioridad dentro de la organización.

b) Cómo se realizó según UI:

Se presenta el proyecto ante el CTAC el día 16 de Junio del 2017 (sic), a la CITI el 21 de Junio del 2017 (sic) donde el señor Olman Durán indica que está en busca del presupuesto y se solicitó la inclusión del proyecto a la PMO el día 28 de Setiembre del 2016. Para el 31 de octubre en la reunión #3 se informa que el sistema de ventanilla única y acuerdos se estaba tramitando el proceso de adjudicación la señora Rosemary Aguilar, el 22 de setiembre remite la decisión inicial a la Proveeduría por medio del oficio con número DGAC-ACB-OF-125-2016. El CTAC por medio del oficio CTAC-AC-2016-0322 solicita a la Dirección General instruir a la Unidad de Informática para que presente en 8 días una propuesta para que se incluya en la Modernización de TI un sistema para los acuerdos y correspondencia del Consejo Técnico de Aviación Civil, en la siguiente sesión se presentó el proyecto.

c) Comentario de AI:

Sobre el documento presentado por Unidad de Informática al CETAC, se analiza en el oficio de Auditoría Interna: al respecto se hace la observación sobre el documento denominado "Informe Acuerd_Soft" en lo que interesa, recomienda el METRO BPM, indica que: reduciendo a cero el costo de desarrollo, el tiempo de instalación en un mes y el mantenimiento sería propio de los técnicos de TIC' S, no dependería del proveedor.

a) Lo que indica el procedimiento 6P03 Gestión de TI

1.1.2. El o los funcionarios de TI inician formalmente el proyecto.

- Corroboran las expectativas generales de los usuarios, gerentes y de cualquier otro interesado, para establecer los resultados esperados y el alcance del proyecto.

b) Cómo se realizó según UI:

Mediante minuta DGAC-UTI-FO-MNT-12-2016 con fecha 22/02/2016, se da a conocer el proceso actual de la ventanilla única, se realiza una demostración a detalle del funcionamiento del sistema Alfresco, se realizó una demo y se aclararon tanto dudas como consultas por parte de la empresa Alkaid.

c) Comentario AI:

El procedimiento de TI es acertado al regular, la necesidad de corroborar las expectativas con: usuarios, gerentes y cualquier otro interesado.

La minuta que se señala como evidencia es insuficiente, nuevamente por la omisión al identificar a los usuarios, en la citada reunión no aparece registrado el representante del Archivo Central, instancia/unidad técnicas rectora en cuanto a la administración de documentos. Se observa únicamente a representantes de URM/TI y el potencial contratista Alkaid.

a) Lo que indica el procedimiento 6P03 Gestión de TI

- Definen la organización del proyecto y selecciona el equipo de trabajo.

b) Cómo se realizó según UI:

La organización del proyecto se realizó por medio de un cronograma de trabajo el cual se realizó en conjunto con la usuaria final experta señora Rosemary Aguilar, la cual fue designada como Administradora Funcional del Proyecto. En el caso de TI se seleccionó al señor Greivin Fallas.

c) Comentario de AI:

1) El 6M03 en el Anexo 1, orienta sobre los roles de los diferentes actores. Entre ellos la Comisión de TI, que en la DGAC se denomina "Comisión de Gestión de Documentos Electrónicos" que como se comenta en el oficio borrador está conformada desde el 2012, e incluye al encargado (a) de Archivo Central.

No se identificó ni solicitó el criterio técnico del Archivo Central, área competente en materia de gestión documental, definido por la Ley del Sistema Nacional de Archivos –Ley 7202 del 27/11/1990) –

a) Lo que indica el procedimiento 6P04:

- Realizan un informe de diagnóstico que permita establecer las diferentes opciones de solución a ser evaluadas.

b) Cómo se realizó según UI:

El usuario final evaluó las funcionalidades que ofrecía cada uno de los siguientes sistemas:

- **Empresa Alkaid con el sistema Alfresco**

Se desarrolló una reunión con minuta DGAC-UTI-FO-MNT-03-2016 con fecha 31/01/2016, en donde se identificaron los requerimientos de los usuarios expertos. Asimismo se explicó a la empresa la necesidad y los usuarios finales validaron la información del proceso actual de la ventanilla única, adicional a esto la empresa Alkaid presentó el funcionamiento del sistema Alfresco y se conversó sobre la parametrización a la medida que se podía realizar al mismo para determinar si podía cubrir todas las necesidades de los usuarios solicitantes, entre estos el flujo de ventanilla única.

- **Empresa GSI con el sistema ePower**

Se desarrolló reunión con minuta DGAC-UTI-FO-MNT-01-2016 con fecha 25/01/2016, en donde se identificaron los requerimientos institucionales de la ventanilla única. Además de eso, se revisó el proceso actual de la ventanilla única, la logística que se requiere cuando se llegue a implementar algún sistema para la ventanilla única y lo que ofrecía el sistema propuesto por ellos. Los insumos fueron entregados por los usuarios expertos Rosemary Aguilar, Olman Durán y Yesenia Castillo.

c) Comentario de AI:

No se encontró el informe que contenga el diagnóstico; que haya permitido establecer las diferentes opciones a ser evaluadas.

No aporta evidencia de la entrega de los insumos por parte de los denominados: usuarios expertos.

a) Lo que indica el procedimiento 6P04:

- ❖ Eligen la alternativa de solución a ser desarrollada.

b) Cómo se realizó según UI:

El usuario solicitante eligió a la empresa Alkaid debido a que el sistema propuesto por ellos cumplía las expectativas y era mucho más barato que el sistema propuesto por la empresa GSI. La señora Rosemary Aguilar remitió el oficio de la decisión inicial a la Proveeduría, donde indica proceder con la contratación del sistema.

c) Comentario de AI:

No se encontró el análisis de alternativas. Evaluar sólo dos opciones es muy limitado. No se encontró documento con el análisis sobre el cumplimiento de expectativas.

No se encontró evidencia de que la elección de la alternativa, fuera compartida/aceptación al menos por ejemplo con secretaria CETAC y con el Archivo Central.

La expresión *El usuario solicitante* y la mención únicamente de la funcionaria Rosemary Aguilar; denota que no hubo una identificación clara y completa de los *actores involucrados en el proyecto a desarrollar (macro y micro entorno del proyecto así como el alcance del mismo*), como procedimiento 6P04 regula.

Si bien la funcionaria Rosemary Aguilar, se constituía como actor por ser parte de la unidad solicitante, se dejó de lado la posición técnicas del archivista central y de los interesados/usuarios que debieron identificarse previamente.

Conforme a lo indicado en el manual metodológico para administrar proyectos de TI se tiene:

1.2. Etapa 0. Anteproyecto.

La organización identifica una serie de necesidades que pueden ser atendidas mediante el desarrollo de un proyecto.

- ❖ Se determinan las expectativas generales de los interesados, así como el efecto y resultados esperados.

b) Cómo se realizó según UI:

Se inicia el proceso verificando las necesidades del área usuaria, mediante recolección de insumos que se identificaron con varias reuniones con ayuda de diferentes empresas para entrevistarlos, e identificar así sus requerimientos técnicos y de usuario necesarios. Ver anexo de minutas.

- ❖ **Empresa Alkaid con el sistema Alfresco**

Se desarrolló una reunión con minuta DGAC-UTI-FO-MNT-03-2016 con fecha 31/01/2016, en donde se identificaron los requerimientos de los usuarios expertos. Asimismo se explicó a la empresa la necesidad y los usuarios finales validaron la información del proceso actual de la ventanilla única, adicional a esto la empresa Alkaid presentó el funcionamiento del sistema Alfresco y se conversó sobre la parametrización a la medida que se podía realizar al mismo para determinar si podía cubrir todas las necesidades de los usuarios solicitantes, entre estos el flujo de ventanilla única.

- ❖ **Empresa GSI con el sistema ePower**

Se desarrolló reunión con minuta DGAC-UTI-FO-MNT-01-2016 con fecha 25/01/2016, en donde se identificaron los requerimientos institucionales de la ventanilla única. Además de eso, se revisó el proceso actual de la ventanilla única, la logística que se requiere cuando se llegue a implementar algún sistema para la ventanilla única y lo que ofrecía el sistema propuesto por ellos. Los insumos fueron entregados por los usuarios expertos Rosemary Aguilar, Olman Durán y Yesenia Castillo.

c) Comentario de AI:

No se encontró documentado el resultado del ejercicio ineludible de determinar las expectativas generales de los interesados.

Con la citada minuta no se adjunta, los requerimientos de los usuarios.

- ❖ Identificar los actores involucrados en el proyecto a desarrollar.

b) Cómo se realizó según UI:

Reunión con empresa GSI (ePower)

Se desarrolló reunión con minuta DGAC-UTI-FO-MNT-01-2016 con fecha 25/01/2016, en donde se identificaron los requerimientos institucionales de

la ventanilla única. Además de eso, se revisó el proceso actual de la ventanilla única, la logística que se requiere cuando se llegue a implementar algún sistema para la ventanilla única y lo que ofrecía el sistema propuesto por ellos. Los insumos fueron entregados por los usuarios expertos Rosemary Aguilar, Olman Durán y Yesenia Castillo.

Reunión con empresa Alkaid (Alfresco)
Se desarrolló una segunda reunión con minuta DGAC-UTI-FO-MNT-03-2016 con fecha 31/01/2016, en donde se identificaron los requerimientos de los usuarios expertos. Asimismo se explicó a la empresa la necesidad y los usuarios finales validaron la información del proceso actual de la ventanilla única, adicional a esto la empresa Alkaid presentó el funcionamiento del sistema Alfresco y se conversó sobre la parametrización a la medida que se podía realizar al mismo para determinar si podía cubrir todas las necesidades de los usuarios solicitantes, entre estos el flujo de ventanilla única.

c) Comentario de AI:

En las minutas no se observa la identificación de todos los actores involucrados. Las minutas citadas, son las únicas y son iniciales en las que participa la encargada del Archivo Central en ese momento.

El procedimiento regula que a nivel macro y micro entorno del proyecto, se deben identificar los actores, y el alcance.

Precisamente es causa de la debilidad en la etapa de planificación de este proyecto la ausencia de una identificación adecuada de esos actores y del alcance del proyecto.

- Confeccionar la ficha de anteproyecto.

b) Cómo se realizó según UI:

El 18 de mayo se recibe por parte del CTAC la aprobación del PETIC. La ficha de anteproyecto ya se había confeccionado a través del documento del PETIC llamado Cartera de Proyectos 2016 - 2020, el proyecto tiene asignado el código C02-02.

c) Comentario de AI:

La ficha a que hace referencia la Unidad de Informática, lo que comprueba es que el proyecto está incorporado en el PETIC; requisito esencial para iniciar un proyecto TI.

El Manual establece el Anexo 7 "*Ficha de Anteproyecto*" la cual no fue completada.

La ficha del anteproyecto tal como la establece el Anexo 7 del 6M03; incorpora requisitos puntuales relevantes del anteproyecto específico; tales como: resultado esperado, alcance, relaciones de coordinación, responsables, requerimientos iniciales, fecha de inicio, fecha de finalización.

- Someter el anteproyecto a la evaluación del Comité Gerencial de Tecnologías de Información y Comunicación (CGTIC), el cual valorará su viabilidad y prioridad dentro de la organización.

b) Cómo se realizó según UI:

Se presenta el proyecto ante el CTAC el día 16 de Junio del 2017 (sic), a la CITI el 21 de Junio del 2017 (sic) donde el señor Olman Durán indica que está en busca del presupuesto y se solicitó la inclusión del proyecto a la PMO el día 28 de Setiembre del 2016. Para el 31 de octubre en la reunión #3 se informa que el sistema de ventanilla única y acuerdos se estaba tramitando el proceso de adjudicación la señora Rosemary Aguilar, el 22 de setiembre remite la decisión inicial a la Proveeduría por medio del oficio con número DGAC-ACB-OF-125-2016. El CTAC por medio del oficio CTAC-AC-2016-0322 solicita a la Dirección General instruir a la Unidad de Informática para que presente en 8 días una propuesta para que se incluya en la Modernización de TI un sistema para los acuerdos y correspondencia del Consejo Técnico de Aviación Civil, en la siguiente sesión se presentó el proyecto.

Comentario de AI:

Esta Auditoría Interna, encontró que la Comisión para la Gestión de Documentos Electrónicos creada en el 2012, está conformada por el Encargado del Archivo Central, y en la CITI creada en el 2008 no incorpora al responsable del Archivo Central.

4.2. Etapa 1. Iniciación.

- Corroborar las expectativas generales de los usuarios, gerentes y de cualquier otro interesado, para establecer los resultados esperados y el alcance del proyecto.

b) Cómo se realizó según UI:

Mediante minuta DGAC-UTI-FO-MNT-12-2016 con fecha 22/02/2016, se da a conocer el proceso actual de la ventanilla única, se realiza una demostración a detalle del funcionamiento del sistema Alfresco, se realizó

una demo y se aclararon tanto dudas como consultas por medio de la empresa Alkaid.

c) Comentario AI:

El procedimiento de TI es acertado al regular, la necesidad de corroborar las expectativas con: usuarios, gerentes y cualquier otro interesado.

La minuta que se señala como evidencia es insuficiente, nuevamente por la omisión al identificar a los usuarios, en la citada reunión no aparece registrado el representante del Archivo Central, instancia/unidad técnicas rectora en cuanto a la administración de documentos. Se observa únicamente a representantes de URM/TI y el potencial contratista Alkaid.

- Definir la organización del proyecto y seleccionar el equipo de trabajo.

b) Cómo se realizó según UI:

La organización del proyecto se realizó por medio de un cronograma de trabajo el cual se realizó en conjunto con la usuaria final experta señora Rosemary Aguilar, la cual fue designada como Administradora Funcional del Proyecto. En el caso de TI se seleccionó al señor Greivin Fallas.

Comentario de AI:

Cronograma aportado por el funcionario Greivin Fallas en correo del 28/07/2017.

Nota: El cronograma no se logró abrir, ya que viene en Microsoft Project y la computadora solicitó una actualización de la versión; la cual fue reportada a Unidad de Informática por medio del servicio de soporte ticket y está pendiente de resolverse.

Nota de Auditoría Interna: A partir de este punto; no se continúa con los comentarios, por cuanto en general ya fueron abordados en los aspectos anteriores.

- Realizar un informe de diagnóstico que permita establecer las diferentes opciones de solución a ser evaluadas.

  El usuario final evaluó las funcionalidades que ofrecía cada uno de los siguientes sistemas:

  - **Empresa Alkaid con el sistema Alfresco**

  Se desarrolló una reunión con minuta DGAC-UTI-FO-MNT-03-2016 con fecha 31/01/2016, en donde se identificaron los requerimientos de los usuarios expertos. Asimismo se explicó a la empresa la necesidad y los

usuarios finales validaron la información del proceso actual de la ventanilla única, adicional a esto la empresa Alkaid presentó el funcionamiento del sistema Alfresco y se conversó sobre la parametrización a la medida que se podía realizar al mismo para determinar si podía cubrir todas las necesidades de los usuarios solicitantes, entre estos el flujo de ventanilla única.

- **Empresa GSI con el sistema ePower**

Se desarrolló reunión con minuta DGAC-UTI-FO-MNT-01-2016 con fecha 25/01/2016, en donde se identificaron los requerimientos institucionales de la ventanilla única. Además de eso, se revisó el proceso actual de la ventanilla única, la logística que se requiere cuando se llegue a implementar algún sistema para la ventanilla única y lo que ofrecía el sistema propuesto por ellos. Los insumos fueron entregados por los usuarios expertos Rosemary Aguilar, Olman Durán y Yesenia Castillo.

- Elegir la alternativa de solución a ser desarrollada.

El usuario solicitante eligió a la empresa Alkaid debido a que el sistema propuesto por ellos cumplía las expectativas y era mucho más barato que el sistema propuesto por la empresa GSI. La señora Rosemary Aguilar remitió el oficio de la decisión inicial a la Proveeduría, donde indica proceder con la contratación del sistema.

4.3. Etapa 2. Planeación.

- Revisar los objetivos y alcances del proyecto en función de un adecuado balance entre resultado, tiempo y recursos.

Mediante la minuta DGAC-UTI-FO-MNT-004 con fecha 07/02/2017, se aprobó el plan de proyecto que incluye el propósito, el alcance, los riesgos, el equipo de trabajo y el cronograma.

- Listar las tareas y actividades que se deben ejecutar para lograr los alcances definidos del proyecto.

Mediante la minuta DGAC-UTI-FO-MNT-004 con fecha 07/02/2017, se aprobó el plan de proyecto que incluye el propósito, el alcance, los riesgos, el equipo de trabajo y el cronograma.

- Secuenciar u ordenar las actividades en función de las dependencias técnicas entre ellas y de los recursos disponibles.

Mediante la minuta DGAC-UTI-FO-MNT-004 con fecha 07/02/2017, se aprobó el plan de proyecto que incluye el propósito, el alcance, los riesgos, el equipo de trabajo y el cronograma.

- ❖ Elaborar el calendario de requerimientos de recursos en el tiempo, para lograr los alcances deseados.

Mediante la minuta DGAC-UTI-FO-MNT-004 con fecha 07/02/2017, se aprobó el plan de proyecto que incluye el propósito, el alcance, los riesgos, el equipo de trabajo y el cronograma.

- ❖ Obtener la aprobación para el plan de trabajo.

Mediante la minuta DGAC-UTI-FO-MNT-004 con fecha 07/02/2017, se aprobó el plan de proyecto que incluye el propósito, el alcance, los riesgos, el equipo de trabajo y el cronograma.

- ❖ Mantener los planes de trabajo balanceados durante todo el desarrollo del proyecto, en función de las variaciones que se produzcan en los alcances, tiempos y recursos.

El plan de trabajo y el cronograma se modifican cada vez que hay una variación en el proyecto por alguna razón. Tanto las revisiones como las modificaciones, en caso de ser necesario, se realizan mensualmente. Adicional a esto se mantiene un repositorio de informes y cronograma de avance del proyecto actualizado mes a mes.

2. ¿El citado proyecto de software (TI) fue tramitado según requisitos de la PMO? Por favor sírvase indicar: ¿si, no? ¿Por qué?

Sí se tramitó por medio de la PMO, debido a que es la oficina que rige la forma de desarrollar un proyecto en la DGAC, se incluyó en la cartera de proyectos de la PMO el día 28 de Setiembre del 2016. El 30 de Setiembre 2016 en la sesión 33 de la PMO, TI da a conocer el proyecto que promovió la Unidad de Recursos Humanos en conjunto con la Subdirección General, siendo avalado ese mismo día por la Coordinadora de la PMO.