ARCHIVO NACIONAL

Informe Auditoría de Sistemas y Tecnologías de Información.

Carta de Gerencia CG-TI 2021.

Informe Final

San José, 31 de agosto de 2022

Señores
Archivo Nacional
Área de Tecnologías de Información

Presente

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2021 al Archivo Nacional y con base en el examen efectuado, observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en los estándares establecidos según los Objetivos de Control para Información y Tecnología Relacionada – COBIT®., los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2021.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o empleados en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con la tecnología de información.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2022.09.14 11:06:17 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado No. 1649
Póliza de Fidelidad Nº 0116 FIG 7
Vence el 30 de setiembre del 2022.

"Exento de timbre de Ley número 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8"

TABLA DE CONTENIDO

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN

I. INTRODUCCIÓN

ORIGEN DEL ESTUDIO

Como parte de la evaluación a los estados financieros del Archivo Nacional, evaluamos los controles generales de la gestión de tecnologías de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés) y en general las mejores prácticas de la industria de tecnología de información.

OBJETIVO DEL ESTUDIO

Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, Procedimientos del auditor en respuesta a los riesgos evaluados, realizamos un diagnóstico a la gestión de las tecnologías de información del Archivo Nacional.

ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

- ✓ Administración del área de tecnologías de información.
- ✓ Seguridad Física.
- ✓ Evaluación de políticas, procedimientos, normas, lineamientos y directrices internas en materia tecnológica.
- ✓ Funcionalidad e integración general de los sistemas.
- ✓ Seguimiento a recomendaciones emitidas en periodos anteriores.

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de julio y agosto del 2022 y corresponde a la auditoría del periodo del 2021.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones al estudio durante la visita de auditoría.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la administración del Archivo Nacional. Solicitamos la documentación que evidenciara las respuestas a las solicitudes y cuestionarios aplicados en formato digital o escrito para respaldo de las aseveraciones manifestadas.

II. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: OPORTUNIDADES DE MEJORA EN EL PROCEDIMIENTO PARA LA GESTIÓN DE RESPALDOS Y RESTAURACIÓN DE INFORMACIÓN. RIESGO BAJO.

CONDICIÓN:

Se determinó que el área de Tecnologías de Información cuenta con procedimientos para la gestión de respaldos y restauraciones de datos, sin embargo, se necesita actualizar dicho documento para establecer aspectos importantes como lo son los pasos lineamientos por seguir para la correcta ejecución de respaldos y restauraciones de datos, así como los debidos responsables de ejecutar estos procesos, monitoreo, medios y reglas de almacenamiento, entre otros aspectos. Cabe mencionar que sí se realizan los respectivos respaldos, no obstante, aún se encuentra en proceso de actualización del procedimiento..

Al no contar con un procedimiento o política de respaldos actualizada, existe el riesgo de no registrar los eventos ocurridos durante un periodo de tiempo determinado, causando una incapacidad de actuar ante problemas operativos, así como, no recuperar las bases de datos críticas debido a incidentes o eventos de desastre no esperados.

CRITERIO:

En el proceso **DSS04 Gestionar la Continuidad**, presente en el estándar de Control Objectives for Information and related Technology 5 (COBIT 5), menciona en la práctica **DSS04.07 Gestionar Acuerdos de Respaldo**: "Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa."
"Mantener la disponibilidad de la información crítica del negocio."

RECOMENDACIONES:

<u>Al Departamento de Tecnologías de Información:</u>

1. Emitir y/o actualizar lineamientos que contemplen la documentación de procedimientos para la gestión de respaldos, los cuales se deben alinear a las necesidades y recursos con los que cuenta el Archivo Nacional. Los lineamientos en cuestión podrían considerar al menos lo siguiente:

    a. Requisitos de retención y protección de respaldos de información.
    b. Generación de registros exactos y completos de las copias de respaldo.
    c. Frecuencia de los respaldos y asignación de responsables.
    d. Asegurar la protección ambiental y física de la información de respaldo.

e. Definir pautas para probar regularmente los medios de respaldo para asegurar que pueden ser confiables para su uso en caso de emergencia, cuando sea necesario.
f. Hay que asegurar que la generación de respaldos esté alineada al procedimiento de continuidad del negocio, para asegurar que cumplen con los requisitos de este.
g. Se debe asegurar que los procedimientos se encuentren revisados y debidamente aprobados.

2. Producto de la atención de la *recomendación 1*, comunicar los lineamientos en cuestión a las partes involucradas

3. Mantener un registro tipo bitácora de las restauraciones y recuperaciones de datos que se realicen producto de las pruebas a los respaldos, la cual contenga entre otros aspectos el nombre del analista, la fecha y estado de la restauración.

4. Revisar y actualizar (esto último cuando sea necesario) la documentación y lineamientos al menos una vez al año, mantener el registro en el control de versiones; esto con el propósito de incluir en los procedimientos los cambios que se realicen en el sistema.

III. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CG 2017	
HALLAZGO 01: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES Y COMUNICACIONES DEL ARCHIVO NACIONAL. RIESGO MEDIO.	
RECOMENDACIÓN	***Al Área de Servicios Generales en coordinación con el Departamento de Tecnologías de la Información:*** 1. Considerar subsanar los siguientes aspectos referentes a las deficiencias evidenciadas en el cuarto de servidores del Archivo Nacional: a. Considerar la instalación de un sistema de aire acondicionado de respaldo, con un sistema de alimentación de energía eléctrica, diferente al del sistema del aire acondicionado principal. Lo anterior, para asegurar que, si un sistema de aire acondicionado falla, el otro sistema puede apoyar con el sistema de refrigeración, antes de que se genere un aumento de calor en los equipos dentro del cuarto de servidores. b. Considerar resguardar los contratos de mantenimiento sobre los sistemas de aires acondicionados del Archivo Nacional, para establecer los respectivos controles de las visitas de mantenimiento. c. Instalar cámaras de seguridad que monitoreen la entrada principal y en el interior del cuarto de servidores. Con el fin de establecer controles de las personas que entran y salen del cuarto, y las acciones que realizan cuando se encuentran dentro del interior de este. d. Considerar etiquetar la totalidad del cableado estructurado, para poseer un mejor control en las redes de datos que se distribuyen por todo el edifico del Archivo Nacional. 2. Con respecto al cuarto de comunicaciones se deben considerar las siguientes acciones: a. Verificar los controles existentes sobre el mantenimiento referente a los extintores, y considerar programar una revisión anual, por parte del proveedor encargado del llenado o recarga de extintores, en todo el edificio del Archivo Nacional. b. Considerar aumentar la seguridad en la puerta del cuarto de comunicaciones, ya que actualmente es propensa a quebrarse o recibir algún tipo de daño, que deje propenso el equipo de cómputo (servidores, racks, etc.) que se encuentran dentro del cuarto de comunicaciones.

	c. Considerar cambiar el llavín de acceso por un sistema de tarjeta electromagnética, sistema de huella digital, o algún otro sistema de control de acceso, que permita tener más seguridad en el cuarto de comunicaciones.
COMENTARIOS DE LA ADMINISTRACIÓN	**Cuarto de servidores del Archivo Nacional:** • En su momento se instaló un aire acondicionado adicional alterno y un monitor de temperatura inteligente independiente del sistema eléctrico, que envía por medio de correo electrónico a los encargados del monitoreo en el DTI y en Servicios Generales, sobre anomalías en la temperatura ambiente del cuarto deservidores para su atención inmediata. • Los contratos de mantenimiento de aires acondicionados están debidamente resguardados en la Unidad de servicios Generales. • Existe una cámara de seguridad en la entrada del Centro de Datos que está en proceso de acomodo para abarcar dentro de su radio de captura la puesta de entrada al Centro de Datos y cuando se tenga el presupuesto necesario, se contratará la instalación de la cámara interna como parte del sistema del CCTV de la Institución. • En su momento se hizo el cambio del Switch Core y con sus funcionalidades es posible identificar de forma rápida y a través del software con que se administra dicho dispositivo y con el cambio, el cableado quedó debidamente etiquetado. **Con respecto al cuarto de comunicaciones:** • Los extintores se mantienen de forma programada y periódica anual con los procesos de vacío y recarga de los componentes activos de extinción de incendio. La última recarga se hizo en agosto del 2021 estando próxima hacerse la nueva recarga en este año. • Este tema se desestimó porque la posibilidad de ocurrencia de un evento como el mencionado es muy remota, dado que le área de acceso es lo suficientemente ancha como para que haya un problema con el descrito. • También se desestima el cambió de llavín en la puerta del cuarto de comunicaciones porque en él se albergan solo switches de red y un equipo PC que controla el sistema de filas, lo que no representa un riesgo alto. Aparte de eso, se cuenta con dos anillos de seguridad, el guardia de la puerta y el acceso al lado adentro del mostrador, en el que se atiende al público, por lo cual la recomendación no amerita inversión.
ESTADO	**EN PROCESO** En el seguimiento del hallazgo se menciona que algunas de las recomendaciones han sido corregidas, se puede mencionar la instalación de un aire acondicionado adicional alterno y un monitor de temperatura inteligente, resguardo de los contratos de mantenimiento, respectivo etiquetado en el cableado, control y revisión de extintores.

	Por otra parte, algunas de las recomendaciones no aplican, en este caso se menciona que el cambio de un llavín de acceso por medio de una tarjeta electromagnética y la seguridad en la puerta del cuarto de servidores no pueden gestionarse debido a que el nivel de riesgo es bajo y las incidencias son muy remotas. Finalmente se menciona que la instalación de cámaras de seguridad se encuentra en proceso, existe una cámara que debe ajustarse para que su radio de alcance sea más amplio, también se procederá a contratar una cámara interna en cuanto se tenga el presupuesto disponible. Dado lo anterior, el hallazgo se mantiene en proceso, ya que aún existen recomendaciones por cumplir.
HALLAZGO 02: AUSENCIA DE LINEAMIENTOS FORMALES PARA LA REVISIÓN DE BITÁCORAS O PISTAS DE AUDITORÍA Y DE LOS ROLES Y PERFILES EN LOS SISTEMAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIÓN	***A las Áreas usuarias en conjunto con el Departamento de Tecnologías de la Información:*** 1. Elaborar un procedimiento para la gestión de roles y perfiles de usuario, de tal manera que se considere la recepción y procesamiento de las boletas de solicitud de cuentas de usuarios de los sistemas y la revisión periódica de los perfiles. Para ello se debe considerar al menos: a. La solicitud formal por parte de las áreas usuarias para otorgar, modificar o revocar permisos a un funcionario en un sistema de información. b. La revisión de los perfiles de usuario cada vez que se requiera. c. La solicitud formal del cambio o modificación de permisos para ajustar los accesos que posee un usuario de acuerdo con sus funciones. d. Comunicación a las áreas usuarias sobre la gestión realizada y el estado en el que queda la cuenta de usuario. 2. Definir un procedimiento formal para la revisión de las bitácoras o pistas de auditoría de los diferentes sistemas de información del Archivo Nacional, considerando aspectos como el responsable de realizar las revisiones, la periodicidad en que se efectuarán y la actualización de las pistas de auditoría. 3. Las jefaturas de las áreas usuarias deben designar al menos una persona encargada de realizar las revisiones de los perfiles de usuario y pistas de auditoría, además, el responsable debe notificar al encargado de la seguridad del sistema los resultados de las revisiones efectuadas, con el propósito de mejorar el control de los accesos de los usuarios e identificar y reportar las posibles inconsistencias o usuarios que no deben acceder a la información.
COMENTARIOS DE LA ADMINISTRACIÓN	• Se crea el procedimiento de administración de roles en sistemas de información que se adjunta.

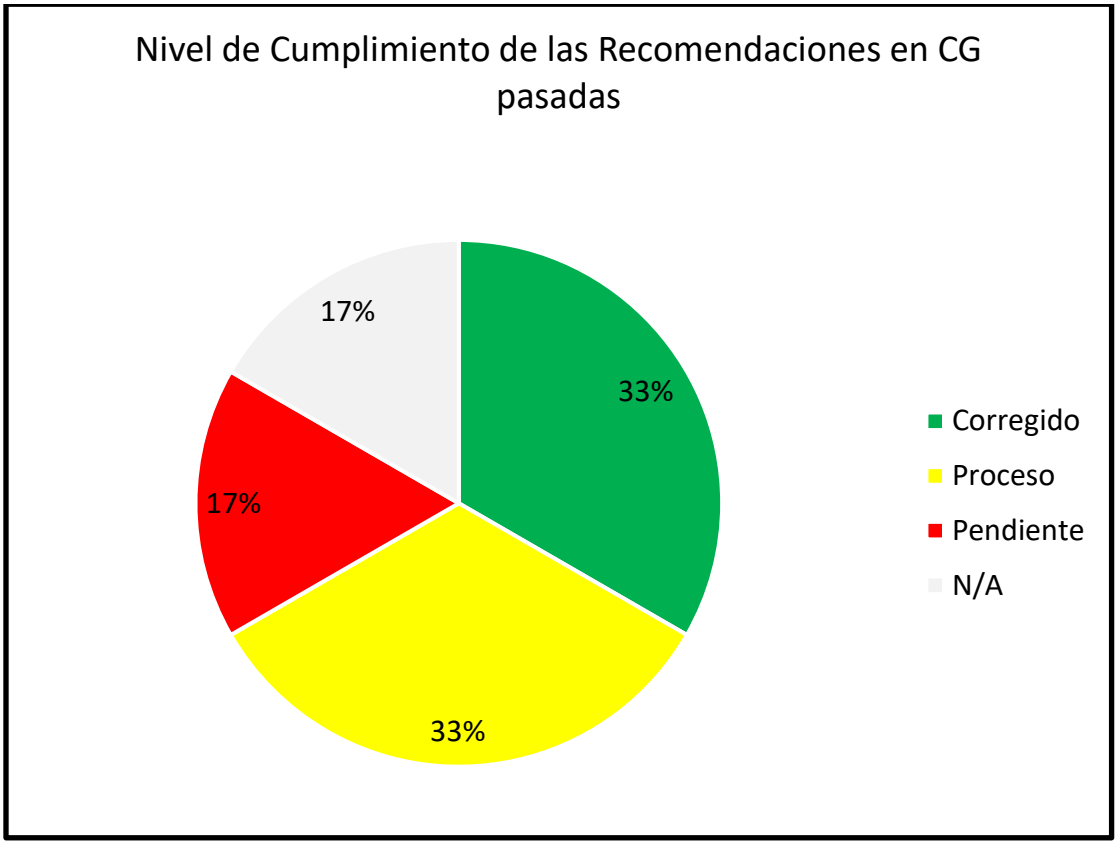
	• No se consideró la creación de un procedimiento para la revisión de pistas de auditoría, porque no es posible normar esta labor dado que los sistemas tienen diferentes formas de brindar la información de pistas de auditoría, además de que no todos los sistemas tienen esa característica programada salvo las revisiones que se puedan hacer a los registros que se ingresen o modifiquen por medio del usuario que ejerce la acción. • Cuando se necesita revisar alguna información relativa a control y pistas de auditoría o revisión de acciones aplicadas por los usuarios, se solicita la ayuda a alguno de los analistas de sistema, ya sea porque trabajaron en él o por el conocimiento que tienen para el acceso a esa información.
ESTADO	**EN PROCESO** En el seguimiento del hallazgo y la evidencia suministrada se identificó el procedimiento para la administración de roles en sistemas de información, el cual fue aprobado en el año 2019. Además, con respecto a las revisiones de pistas de auditoría, control y/o acciones aplicadas por los usuarios, se indicó que estas se realizan cuando es necesario y se solicita la colaboración de alguno de los analistas de sistemas. Sin embargo, es importante que se establezca una periodicidad (al menos dos veces al año) para la revisión de los aspectos mencionados anteriormente, con el propósito de mejorar el control de los accesos de los usuarios y la información a la que acceden, e identificar y reportar posibles inconsistencias.
HALLAZGO 03: DEBILIDADES EN LA SEGURIDAD LÓGICA DEL SISTEMA BOS. RIESGO MEDIO.	
RECOMENDACIÓN	***Al Departamento Administrativo Financiero en conjunto con el Departamento de Tecnologías de la Información:*** Realizar las gestiones necesarias para implementar las medidas de seguridad lógica mínimas en el sistema BOS, con el fin de asegurar que se cumplan con los siguientes aspectos: • Establecer periodos de expiración de las contraseñas a lo sumo cada 60 días naturales de tal modo de que se asegure que las contraseñas se cambien periódicamente. • Implementar un histórico de contraseñas para asegurar que los usuarios no puedan utilizar una misma contraseña reiteradas ocasiones y requieran el cambio constante de la misma. • Implementar mecanismos para exigir cierto nivel de complejidad en la contraseña, entre los aspectos recomendados está el uso de mayúsculas, minúsculas, uso de números, caracteres especiales, etc.
COMENTARIOS DE LA ADMINISTRACIÓN	• En el Ministerio de Cultura se tiene como política para el Bos, cambio de contraseña cada 3 meses. • No se puede implementar un histórico de contraseñas diferente al que tiene el sistema Bos, porque se trata de un software de paquete, de esta manera, el control que se tiene es que no se pueda usar una contraseña anterior.

	• en lo que se refiere a expiración de contraseñas, los sistemas de información permiten implementar esto y se puede hacer. El histórico de contraseñas y la complejidad de contraseña se puede implementar en el Active Directory de Microsoft para contraseñas relacionadas a sistemas, pero para el Sistema Bos 7.0, no es posible cumplir del todo con lo recomendado porque es un software de paquete y la seguridad de claves abarca expiración de claves y advierte la complejidad de la clave que el usuario utilice, pero sin obligar el uso de mayúsculas, minúsculas, uso de números, caracteres especiales, etc. Además, no tiene cuenta con un histórico comparativo de claves. Si la recomendación solicitada al Bos 7.0 se tuviera que aplicar de forma estricta, sería necesario sustituir dicho software de paquete con otro o desarrollar un software a la medida que cumpla con estos requisitos.
ESTADO	**CORREGIDO** En el seguimiento de hallazgos de periodos anteriores se menciona que para la atención de las recomendaciones de seguridad lógica respecto al sistema BOS 7.0, se cuenta con una política del Ministerio de Cultura que indica que se debe hacer un cambio de esta cada tres meses, en cuanto al historial de contraseñas el sistema no permite el uso de una contraseña anterior y finalmente se indica que para cambiar el grado de complejidad en las contraseñas se debería reemplazar el software por uno nuevo que si contemple dichos aspectos en su totalidad. Dado lo anterior, se considera que las recomendaciones se cumplen según los recursos con los que cuenta la organización, ya que sustituir el sistema por uno nuevo no resultaría rentable a nivel operativo para el Archivo Nacional.
HALLAZGO 04: DEPENDENCIA DEL PROVEEDOR TECAPRO PARA EL MANTENIMIENTO DEL SISTEMA BOS. RIESGO MEDIO.	
RECOMENDACIÓN	***Al departamento de Tecnologías de la Información:*** Implementar un plan de contingencia o un proceso de transferencia tecnológica que minimice la dependencia del proveedor TECAPRO.
COMENTARIOS DE LA ADMINISTRACIÓN	En este punto, en lo que se refiere a la dependencia de la empresa TECAPRO para la prestación de servicios relacionados con el sistema Bos 7.0, y que no se cuenta con un proceso de transferencia tecnológica que minimice la dependencia de TECAPRO como proveedor, efectivamente, se mantendría como único proveedor dicha empresa al ser ellos los creadores y propietarios del sistema Bos 7.0 y no habría otra empresa en capacidad de hacer ajustes a dicho software, al ser TECAPRO el propietario exclusivo de su código. Siendo así, la medida contingente que se tiene es la de hacer respaldo diario de todo el sistema y si se dejara de tener mantenimiento para el software por parte de la empresa creadora, se usaría el paquete con la funcionalidad que tiene mientras se adquiere otro con la misma o mejor funcionalidad (pero con la misma dependencia de la empresa creadora, esto es inevitable en el uso de paquetes), o contratar el desarrollo de un software a la medida con la misma

	funcionalidad que se requiera, utilizando herramientas de desarrollo estándares, pero esta opción sería algo inusual porque ya existen en el mercado muchos sistemas de este tipo y no tendría sentido desarrollar software que ya existe. En todo caso, en un proceso de transferencia tecnológica la administración tendría que decidir, si utiliza software de paquete con la dependencia que conlleva hacia la empresa creadora o hacer un desarrollo a la medida.
ESTADO	**NO APLICA** En el seguimiento a los hallazgos se menciona que la recomendación para el sistema ya no aplica, esto debido a que el proveedor es el único que conoce el sistema utilizado y es el propietario exclusivo del código. Además, se menciona que se realizan respaldos diarios como medida de contingencia y en caso de no contar más con el mantenimiento por parte de la empresa creadora, se procedería a contratar un nuevo proveedor.
HALLAZGO 05: INCONSISTENCIAS EN LA BASE DE DATOS DE ACTIVOS FIJOS. RIESGO MEDIO.	
RECOMENDACIÓN	***Al encargado de Activos:*** 1. Analizar y establecer mecanismos de control que validen los campos donde se presentan las inconsistencias. 2. Depurar los registros que presentan inconsistencias.
COMENTARIOS DE LA ADMINISTRACIÓN	En lo relativo a las inconsistencias de bases de datos de activos fijos, no indicamos razones dado que dicha observación la había atendido la señora Nancy Blanco, como encargada de activos fijos en ese momento.
ESTADO	**PENDIENTE** No se suministró evidencia sobre acciones realizadas para subsanar el hallazgo, ni tampoco la base de datos para la evaluación de inconsistencias al periodo auditado.
HALLAZGO 06: MANUALES DE USUARIO DESACTUALIZADOS. RIESGO BAJO.	
RECOMENDACIÓN	***A las Áreas usuarias en conjunto con el Departamento de Tecnologías de la Información:*** 1. Elaborar y/o actualizar los manuales de usuario de forma tal que sirva como guía para uso del sistema, para los nuevos colaboradores del Departamento Administrativo Financiero. 2. Publicar y divulgar los manuales actualizados a las áreas usuarias del sistema. 3. Actualizar los manuales de usuario agregando los cambios que se realicen en las funcionalidades, además mantener un control de versiones sobre las actualizaciones del manual.

COMENTARIOS DE LA ADMINISTRACIÓN	Los manuales de usuario del Sistema Bos se encuentran actualizados y disponibles a los usuarios mediante un Link con el que los pueden acceder. se adjunta muestra
ESTADO	**CORREGIDO** Se verificó que los manuales de usuario del sistema BOS 7.0 se encuentra actualizados, además se suministró el respectivo enlace con el acceso a todos los manuales disponibles. Dado lo anterior el hallazgo queda corregido.

A continuación, se resume el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores de manera gráfica:



La siguiente tabla muestra el cumplimiento de recomendaciones por periodo.

Estado de Recomendaciones	**2017**	**Total**
Corregidas	2	**2**
En Proceso	2	**2**
Pendiente	1	**1**
No Aplica	1	**1**
Total	**6**	**6**

IV. ANEXO I

Análisis de Riesgos T.I.

Departamento de Sistemas de Información
Periodo 2021

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio ☑	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo ☑	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene definido un plan estratégico de TI formalmente aprobado y alineado a los objetivos organizacionales.		✓	Se cumple con la condición.	B
A.2.	Se le da seguimiento al PETI por parte del Comité de TI.		✓	Se cumple con la condición.	B
A.3.	Se define anual un plan anual operativo de TI con los proyectos y actividades que realiza el área de TI y se encuentra alineado a las iniciativas y objetivos del PETI.		✓	Se cumple con la condición, existen un plan de acción para el periodo 2019-2023.	B
A.4.	Se le da seguimiento periódico al cumplimiento del PAO.		✓	Se cumple con la condición.	B

B. GESTIÓN DEL PRESUPUESTO DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se genera un plan anual presupuestario de TI formalmente aprobado.		✓	Se cumple con la condición.	B
B.2.	El presupuesto se encuentra categorizado y priorizado según las actividades críticas del plan anual operativo de TI.		✓	Se cumple con la condición.	B
B.3.	Se mantiene un control de gastos y ejecuciones presupuestarias de TI y se le brinda informes de ejecución a la administración.		✓	Se cumple con la condición.	B
B.4.	Se mantiene alineado el plan presupuestario de TI con el plan anual operativo.		✓	Se cumple con la condición.	B

C. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.		✓	Se cumple con la condición, se cuenta con una matriz de riesgos que sigue la metodología SEVRI.	B
C.2.	La evaluación de riesgos de TI es periódica y se encuentra revisada y aprobada por la administración (de acuerdo con el nivel de tolerancia al riesgo organizacional).		✓	Se cumple con la condición.	B

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

D. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se mantienen controles para el ingreso y salida de equipo tecnológico a la organización.		✓	Se cumple con la condición.	B
D.2.	Se cuenta con un inventario de activos de TI (equipo en uso y desuso, periféricos, equipo de comunicación, dispositivos móviles, etc.), junto con información de su ubicación y responsable.		✓	Se cumple con la condición.	B
D.3.	Se mantiene un inventario actualizado de las licencias de software, así como un catálogo de software permitido en la organización.		✓	Se cumple con la condición.	B
D.4.	Se verifica periódicamente que el software instalado en los equipos corresponda a las licencias adquiridas y al software permitido en la organización.		✓	Se cumple con la condición.	B

III. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

E. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.	✗		El procedimiento se realiza a nivel operativo, además se cuenta con un documento con información de los respaldos, pero no responde a la solicitud de un procedimiento formal, por lo tanto, se emite el **Hallazgo 01** con las respectivas recomendaciones.	B
E.2.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición, se evidenció que las pruebas se realizan.	B
E.3.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).		✓	Se cumple con la condición, la información se almacena en un dispositivo alterno que se guarda en proveeduría.	B
E.4.	Se cuenta con un sitio alterno para el procesamiento de datos en una posición geográfica distinta a la ubicación del cuarto de servidores principal.		✓	Se cumple con la condición.	B

F. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se cuenta con una política de seguridad de la información formalmente aprobado por la administración y divulgado a nivel organizacional.		✓	Se cumple con la condición.	B
F.2.	Se le brinda seguimiento al cumplimiento de la política de seguridad de la información (se aplican medidas correctivas) y se le comunica los resultados a la administración.		✓	Se cumple con la condición.	B
F.3.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).		✓	Se cumple con la condición.	B

F.4.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B
F.5.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).		✓	Se cumple con la condición.	B
F.6.	Se tiene implementado medidas de seguridad para la red institucional (firewall, estudios de vulnerabilidad, segmentación de redes).		✓	Se cumple con la condición.	B

G. GESTIÓN DE LA SEGURIDAD FÍSICA Y AMBIENTAL.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se mantiene una bitácora de acceso para el personal interno y externo que ingresa al cuarto de servidores.		✓	Se cumple con la condición.	B
G.2.	Se tienen instaladas alarmas para la detección de intrusos y/o cámaras de seguridad.	X		La instalación de cámaras de seguridad se encuentra en proceso, existe una cámara que debe ajustarse para que su radio de alcance sea más amplio, también se procederá a contratar una cámara interna en cuanto se tenga el presupuesto disponible.	M
G.3.	El cuarto de servidores se encuentra en un sitio seguro (lugares no propensos a desastres como inundaciones, incendios, etc.).		✓	Se cumple con la condición.	B
G.4.	Los equipos se encuentran ubicados en racks y asegurados en el suelo.		✓	Se cumple con la condición.	B
G.5.	El cableado de datos se encuentra aislado del cableado eléctrico.		✓	Se cumple con la condición.	B
G.6.	El cableado de red se encuentra debidamente rotulado.		✓	Se cumple con la condición.	B
G.7.	El cuarto de servidores cuenta con aires acondicionados exclusivos para esta área (A/C principal y respaldo).		✓	Se cumple con la condición.	B
G.8.	Se les brinda mantenimiento preventivo y correctivo a los aires acondicionados del cuarto de servidores.		✓	Se cumple con la condición.	B
G.9.	Se cuenta con extintores y/o aspersores en el cuarto de servidores.		✓	Se cumple con la condición.	B

IV. SISTEMAS DE INFORMACIÓN.

H. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.1.	Los sistemas de información permiten solo una única sesión simultánea por usuario, de modo que no se pueda abrir una sesión con un mismo usuario en lugares distintos al mismo tiempo.		✓	Se cumple con la condición. El sistema Bos cuenta con restricciones de inicio de sesión únicas.	B
H.2.	Los sistemas de información cuentan con validación de usuarios a través de cuentas y contraseñas (Active Directory, LDAP, otros).		✓	Se cumple con la condición.	B
H.3.	Se han implementado medidas de seguridad lógica en los sistemas de información (vencimiento, histórico, tamaño y complejidad de la contraseña).		✓	• Con relación a las claves se maneja un vencimiento de cada tres meses. • Se maneja un histórico de tres claves. • Se maneja con 8 caracteres como mínimo y se tiene que poner números, letras y algún carácter especial.	B
H.4.	Los sistemas de información cuentan con manuales de usuario y manuales técnicos.		✓	Se cumple con la condición.	B
H.5.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
H.6.	Los sistemas de información se encuentran integrados entre sí, de modo que no se deba enviar información a través de medios externos a los sistemas.		✓	La información no depende de otros sistemas para su trabajo, así mismo el mismo si brinda archivos planos con el fin de enviar la información solicitada por otras instituciones (Tesorería Nacional entre otras).	B
H.7.	Se restringe la entrada de datos de modo que el registro de información sea lo más estándar posible.		✓	Se cumple con la condición. Sigue los estándares presentados por el área contable.	B
H.8.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓	Se indicó que, según la necesidad se coordina con el ministerio de cultura para las capacitaciones.	B

V. ANEXO II

Valoración del nivel de satisfacción sobre la calidad funcional de algunos de los sistemas de información y soporte brindado por el Área de Tecnologías de la Información

OBJETIVO

Medir el nivel de satisfacción que posee el usuario con respecto al (los) sistema (as) que utiliza el Archivo Nacional y al soporte brindado por el Área de Tecnologías de la Información.

RESULTADOS

A continuación, se muestra el resultado de la evaluación realizada con respecto a la calidad funcional de algunos de los sistemas de información implantados en el Archivo Nacional, según la percepción de los usuarios finales.

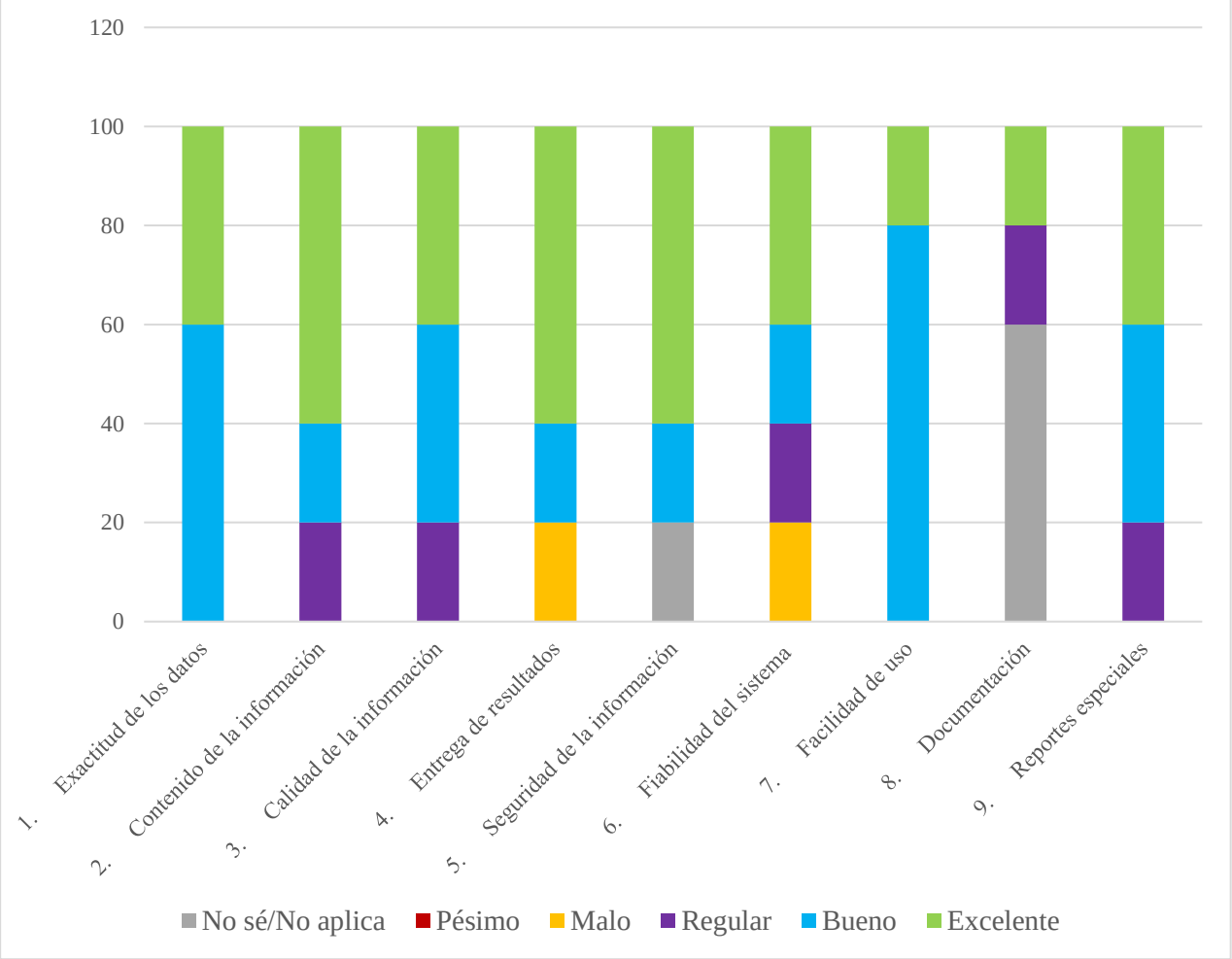
En total, 5 colaboradores brindaron respuesta. Los sistemas de información/módulos que se indicaron en la evaluación pertenecen a las siguientes áreas de trabajo:

- Financiero contable
- Administrativo.
- CAJA 2.
- Oficina Auxiliar de Gestión Institucional de Recursos Humanos.

En los siguientes apartados, se muestran las respuestas registradas según la sección evaluada.

Información sobre el sistema de información

El siguiente gráfico muestra el resumen de respuestas por categoría, esto para atributos relacionados propiamente con los sistemas/módulos utilizados.



Tal y como se observa en el gráfico, las respuestas brindadas en su mayoría se ubican entre las valoraciones de excelente y bueno, los únicos atributos en los cuales se presentaron calificaciones de "malo" son *Entrega de resultados y Fiabilidad del sistema*.

Para cada uno de los atributos, los usuarios tenían un espacio para brindar comentarios adicionales a su calificación (esto de forma opcional), entre las respuestas registradas indicaron que:

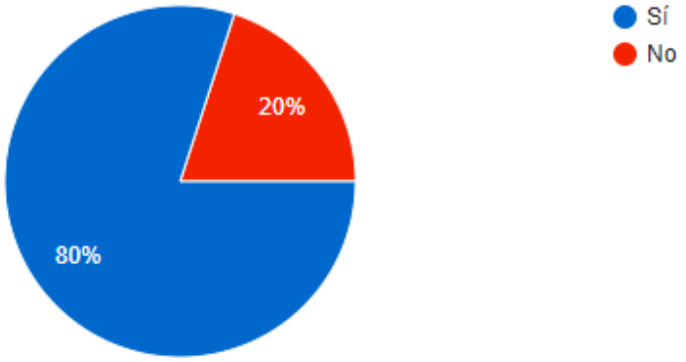
- Se presentan inconsistencias permanentes con el cálculo de las incapacidades y licencias de maternidad.
- La documentación disponible se encuentra desactualizada.
- El sistema no genera gráficos.
- Los reportes están estandarizados y en ocasiones se necesitan reportes adicionales que no se pueden obtener.

En caso de que se desee indagar a profundidad sobre los atributos antes señalados u otros, es recomendable tomar una muestra de usuarios mayor y especifica (un solo sistema/módulo).

Opinión sobre el soporte brindado por el Departamento de Sistemas de Información

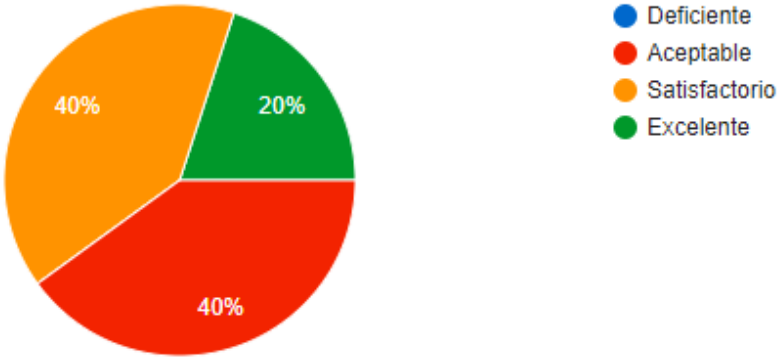
A continuación, se muestran las respuestas graficadas relacionadas con opiniones acerca del soporte brindado por el Departamento de Sistemas de Información.

El departamento brinda los resultados esperados



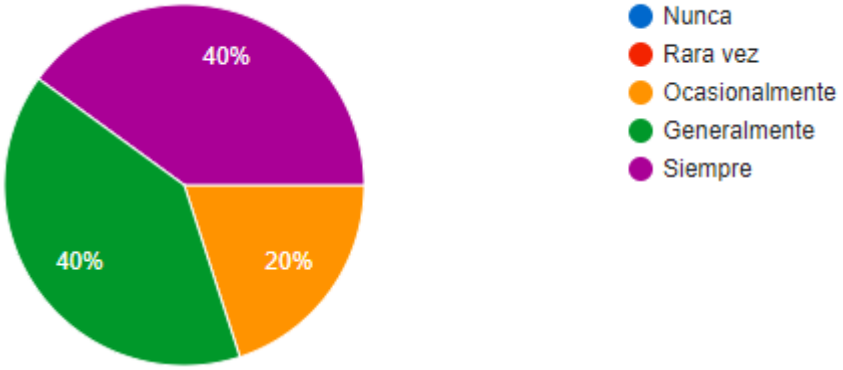
Al respecto amplían indicando que, TI del Archivo no es el encargado de los problemas del Sistema Contable. Este proceso se trasladó al Ministerio de Cultura, por lo que la respuesta puede ser algunas veces lenta, sin embargo, se atienden incidencias y averías con prontitud. Otro usuario indica que el Departamento de TI colabora en la remisión masiva de las coletillas salariales a las personas servidoras cada quincena. Se aclara que el Sistema es privado, cuando presentamos incidentes se resuelven en el menor tiempo posible.

Servicio proporcionado por el departamento



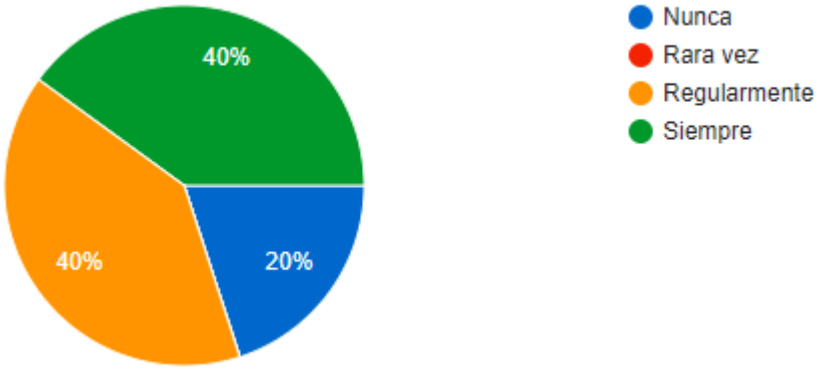
Al respecto amplían indicando que, el personal del departamento tiene iniciativa y dan apoyo cuando se les pide, y eso da seguridad. Además, se menciona que, dependiendo del caso, el personal actúa de forma rápida.

Disponibilidad del departamento



Al respecto amplían indicando que, se deben adaptar a los elementos tecnológicos emergentes y se han realizado gestiones para la atención de nuevos requerimientos de manera satisfactoria. Sin embargo, como se indicó anteriormente en el caso del tema del Sistema Contable, el responsable es el Ministerio de Cultura y Juventud por lo que a veces es lento el proceso.

Puntualidad con la entrega de solicitudes

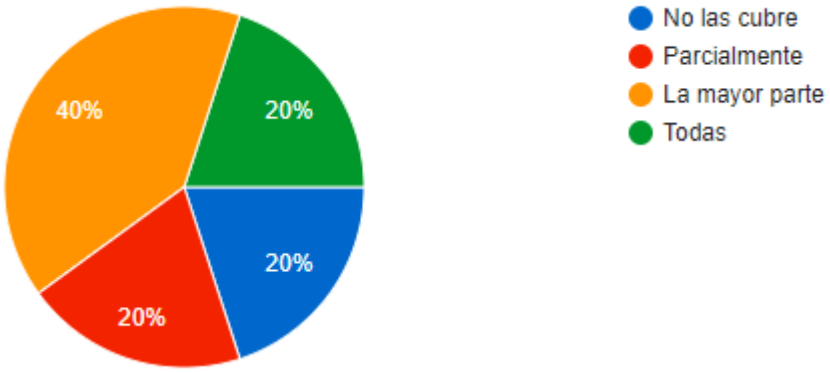


Al respecto amplían recalcando que el trabajo que realizan y el control que implementan, han permitido que hasta el momento se atiendan los problemas e incidentes reportados con rapidez, pero a veces es por la demanda, que todos requerimos al mismo tiempo y no se da abasto.

Opinión sobre otros atributos adicionales

A continuación, se muestran las respuestas graficadas relacionadas con opiniones acerca de atributos adicionales.

Cobertura de necesidades con el sistema proporcionado



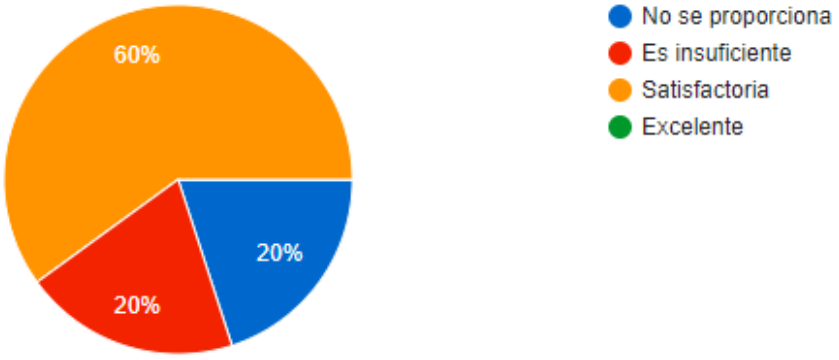
Los usuarios señalan que sistema no lo está proporcionando TI, fue adquirido a una empresa externa y administrado por el Ministerio de Cultura y Juventud. Por lo tanto, hay situaciones que no dependen de ellos. Por otro lado, se menciona que existen inconsistencias que se presentan en las incapacidades, licencias de maternidad y falta el proceso de gestión de viáticos.

Se les consultó sobre nuevas funcionalidades que necesiten y el sistema actualmente utilizado no posee, al respecto indican:

- "PEPS para el inventario".
- "Se cuenta con la facilidad de crear nuestro propio sistema y modificar según las necesidades que se requieran".
- "Que las incapacidades y las licencias de maternidad las calcule de forma correcta y las aplique en los rangos de correspondan".
- "Autogestión de Viáticos".

Como se denota, los comentarios anteriores reflejan varias necesidades de los usuarios a nivel del sistema que utilizan, es prudente analizarlos, pues, la mayoría contiene requerimientos que deberían considerarse (en caso de no haberlo realizado). A la hora de implementar mejoras a los sistemas actuales, o bien, adquirir uno nuevo, es de vital importancia considerar a los usuarios finales en la toma de requerimientos.

Capacitaciones recibidas en materia informática



El gráfico evidencia que más de la mitad de los colaboradores considera que las capacitaciones son satisfactorias (60%). Un 20% determinó que las capacitaciones recibidas son insuficientes y el otro 20% indicó que no se proporcionan capacitaciones. Según los resultados obtenidos, es prudente analizar -en conjunto con el Departamento de Recursos Humanos o equivalente- la necesidad de capacitar a las áreas usuarias con respecto al uso de sistemas, educación en temáticas tales como seguridad de la información, buenas prácticas relacionadas con TI, plataformas tecnológicas utilizadas u otras, las cuales, si bien son relacionadas al campo de TI impactan las labores de las otras áreas de la organización.

Comentarios adicionales

En la encuesta aplicada se proporcionó una sección final para que los usuarios agregaran (de manera opcional) comentarios, críticas u oportunidades de mejora que sirvan de retroalimentación para mejorar la calidad brindada por el Departamento de TI o de los sistemas en general, parte de las respuestas registradas fueron:

- ✓ “El tiempo de respuesta de TI es bueno y las soluciones que brindan ayudan a continuar sin mayor retraso las labores, por no utilizar sistemas de TI no se cuenta con mayor criterio.”
- ✓ “Los sistemas a veces vienen con lo que se le domina pulgas y eso pues atrasa.”
- ✓ “El Sistema BOS a pesar es un sistema hecho a la medida, es un sistema funcional y adaptado casi totalmente a las necesidades de la institución.”

En estos comentarios finales los usuarios recalcan la necesidad de contar con mejores tiempos de respuesta. Dado lo anterior, es recomendable, a nivel de sistemas, considerar las necesidades de los usuarios finales (tal y como se señaló en el apartado de *Cobertura de necesidades con el sistema proporcionado*), y, por otra parte, hacer un estudio de cargas laborales del Departamento de Sistemas de Información.

--Fin del documento--