ARCHIVO NACIONAL DE COSTA RICA.

- ***Informe de Auditoría de Sistemas y Tecnologías de Información***
- ***Carta de Gerencia CG-TI 1-2017***
- ***Informe Final.***

San José, 30 de julio del 2018

Señores
Archivo Nacional de Costa Rica
Junta Administrativa
Dirección General
Departamento de Tecnologías de la Información
Departamento Administrativo Financiero

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa de TI del período 2017 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 el manual de "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" emitido por la Contraloría General de la República y 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 1-2017.

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 colaboradores en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con las Tecnologías de Información.

Es importante señalar que la estructura de control interno establecida, incluyendo los procedimientos de control para la actividad sujeta a evaluación, son de entera responsabilidad de la administración del Archivo Nacional.

La auditoría no está diseñada para detectar todas las deficiencias en los procesos y objetivos de control evaluados, ya que no se lleva a cabo de forma continua durante el período de revisión; las evaluaciones realizadas consisten en un estudio sustentado en muestras y pruebas selectivas de la evidencia que respalda el cumplimiento de los procesos y objetivos de control evaluados, los cuales, producto de sus limitaciones inherentes, pueden presentar resultados fallidos debido a errores o debilidades propias del control interno que ocurran y no sean detectadas. Lo anterior deja manifiesto que los eventos subsecuentes a este informe están sujetos al riesgo de que los controles establecidos se tornen inadecuados, producto de cambios en las condiciones de la Institución.

La auditoría realizada fue requerida por la administración del Archivo Nacional, producto de lo anterior, los resultados expresados en el presente informe son de carácter confidencial y deben ser utilizados exclusivamente por las personas autorizadas para tal fin.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad No. 0116 FIG7
Vence el 30 de setiembre del 2018.

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

CONTENIDO

I. INTRODUCCIÓN

i. ORIGEN DEL ESTUDIO

Como parte de la evaluación de los estados financieros del Archivo Nacional, realizamos la evaluación de los controles generales de la gestión de tecnología 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 el manual de "Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información (N-2-2007-CO-DFOE)" emitidas por la Contraloría General de la República, 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.

ii. ALCANCE

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

1. Seguimiento a recomendaciones relacionadas con las TI emitidas en periodos anteriores.
2. Verificación del control interno en materia tecnológica con base en la normativa interna establecida.
3. Oportunidades de mejora identificadas en la evaluación.

El alcance de la auditoría realizada se fundamenta en lo establecido en las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" emitidas por la Contraloría General de la República.

iii. OBJETIVO DEL ESTUDIO

1. Establecer un entendimiento integral de los procesos evaluados del Archivo Nacional, así como de la plataforma tecnológica que soporta sus operaciones y documentación asociada.

2. 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, evaluamos la gestión de las Tecnologías de Información del Archivo Nacional.

iv. PERIODO DE LA AUDITORÍA.

El estudio se realizó durante el mes de julio del presente año y corresponde a la auditoría del periodo 2017.

v. LIMITACIONES DEL ESTUDIO.

No se presentaron limitaciones al estudio de auditoría de TI.

vi. METODOLOGÍA.

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la jefatura del Departamento de Tecnologías de la Información y áreas usuarias, aplicamos cuestionarios de control interno relacionados con la administración del Departamento, seguridad física y lógica de los sistemas de información, continuidad de las operaciones, planificación de las TI, gestión de riesgo tecnológico, proyectos, respaldos, entre otras áreas.

Además, se formularon preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los colaboradores las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

II. HALLAZGOS

HALLAZGO 01: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES Y COMUNICACIONES DEL ARCHIVO NACIONAL. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada al cuarto de servidores y cuarto de comunicaciones del Archivo Nacional, se identificó una serie de debilidades que se detallan a continuación:

1. ***Sobre el Cuarto de servidores:***

   a) ***Con respecto al Aire Acondicionado:***

   Solo se cuenta con un sistema de aire acondicionado en el cuarto de servidores, lo que limita la capacidad de enfriamiento del equipo presente en dicho cuarto. A continuación, se presenta una imagen de lo mencionado anteriormente:

   b) ***Con respecto a las cámaras de seguridad:***

   No se cuenta con un sistema de cámaras de seguridad en la entrada, ni en el interior del cuarto de servidores, lo que limita el monitoreo y el control de cuales personas entran y salen, y lo que realizan dentro del cuarto de servidores. Además, no se posee un sistema de alarmas contra intrusos, ya que únicamente se posee un sistema de alarmas contra incendios. A continuación, se presenta una imagen de la cámara de seguridad más cercana a la entrada principal del cuarto de servidores, sin embargo, se encuentra a un costado de la puerta principal, y no monitorea la entrada:

c) <u>Con respecto al cableado:</u>

Se determinó que se cuenta con una certificación del cableado estructurado, que se encuentra dentro del cuarto de servidores. Sin embargo, la totalidad del cableado no está debidamente etiquetado, lo que dificulta la comprensión sobre el destino de las redes de datos, que se distribuyen en todo el edificio. A continuación, se presenta una imagen que evidencia lo anterior:

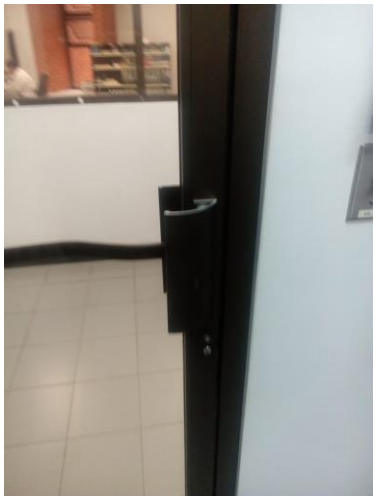
2. <u>*Sobre el Cuarto de Comunicaciones:*</u>

a) <u>Con respecto al extintor:</u>

Se determinó que el extintor que se ubicada en el cuarto de comunicaciones se encuentra vencido, ya que, según su boleta de recarga, no se recarga desde el mes de febrero del año 2014. A continuación, se presenta una imagen correspondiente a la evidencia de lo anteriormente mencionado:

b) <u>Con respecto a la puerta de cristal:</u>

Se determinó que la puerta principal del cuarto de comunicaciones es de vidrio o de cristal, lográndose observar los equipos que se encuentran dentro del cuarto de comunicaciones. Adicionalmente, se determina que el acceso al cuarto de comunicaciones se realiza por medio de un llavín convencional, y el guarda de seguridad, posee la llave, por lo cual, para entrar a efectuar labores dentro de este cuarto, se debe hacer solicitud previa de las llaves al guarda de seguridad del edificio. A continuación, se presentan dos imágenes que evidencia lo mencionado:



Producto de lo expuesto anteriormente y de las deficiencias encontradas en el cuarto de servidores y comunicaciones del Archivo Nacional, se determina que se corre el riesgo de no poseer controles adecuados para la reacción ante eventos imprevistos, como lo pueden ser fallas en el sistema de enfriamiento, detección de intrusos (acceso de terceros) y capacidad de reacción ante un incendio o siniestro que pueda afectar negativamente a los servicios críticos que se brindan a todos los sistemas del Archivo Nacional de Costa Rica.

CRITERIO:

Según el proceso **1.4.3 "Seguridad física y ambiental"** presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, indica lo siguiente: "*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."

RECOMENDACIONES:

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:
Se consideran aceptables y adecuadas las recomendaciones tendientes a subsanar los aspectos referentes a las deficiencias encontradas en el cuarto de servidores, de telecomunicaciones y del cableado estructurado para mejorar su seguridad física y ambiental.

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.

CONDICIÓN:

Durante el proceso de auditoría se determinó que el Archivo Nacional no cuenta con lineamientos formales para el seguimiento por parte de las áreas usuarias a las bitácoras o pistas de auditoria, tampoco se cuenta con lineamientos para la revisión de roles y perfiles en los sistemas de información.

Cabe mencionar que los sistemas de información cuentan con la asignación de roles y perfiles mediante el uso de grupos de usuarios que permite acceder a los diferentes módulos, no obstante, no se efectúan seguimientos ni revisiones de estos perfiles.

Adicionalmente, producto de la revisión del Sistema BOS se identificó que se cuenta con bitácoras de auditoria, no obstante, no se efectúan revisiones periódicas por parte de las áreas usuarias solo en caso de que se requiera.

Al no contar con un procedimiento para la gestión de roles y permisos de usuario, existe el riesgo de que los usuarios no cuenten con los privilegios mínimos necesarios para el acceso a los sistemas, datos y servicios de información o en caso de que no se elimine o bloquee los privilegios por salida o vacaciones de un colaborador, existe la posibilidad de que pueda acceder a la información crítica y/o confidencial y realice acciones no autorizadas en los sistemas de información a los que el usuario estaba autorizado. Por otra parte, al no realizar

revisiones formales periódicas a las pistas de auditoria, por ende, no se podría verificar que la integridad, confidencialidad y calidad de la información sea la adecuada.

CRITERIO:

El proceso **1.4.5 "Control de acceso"** presente en el documento 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, menciona: "*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".*

RECOMENDACIONES:

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 consideran aceptables y adecuadas las recomendaciones tendientes a la creación de un procedimiento de gestión de roles y perfiles de usuario de sistemas de información y del procedimiento para revisión de bitácoras de sistemas, para los encargados de esta labor en cada departamento.

HALLAZGO 03: DEBILIDADES EN LA SEGURIDAD LÓGICA DEL SISTEMA BOS. RIESGO MEDIO.

CONDICIÓN:

Producto del proceso de auditoría efectuado se determinó que el Archivo Nacional cuenta con sistemas de información para la automatización de los procesos contables e inventarios en el Departamento Administrativo Financiero. A continuación, se indican los módulos valorados en esta visita de auditoría:

	Módulos
Sistema BOS	Punto de Ventas
	Control Bancario
	Inventario
	Nómina
	Cuentas por Pagar
	Activos Fijos
	Contabilidad
	Presupuesto

Producto de la revisión de los módulos mencionados anteriormente se identificaron deficiencias en la seguridad lógica, a continuación, se detalla:

Se determinó que el sistema valorado (BOS) cuenta con medios de autenticación mediante el uso de un nombre de usuario y contraseña, los cuales son personalizados para cada colaborador. Sin embargo, se presentaron las siguientes deficiencias en la parametrización y configuración de las contraseñas y cuentas de usuarios:

Aspecto evaluado	Condición identificada
Vencimiento de la contraseña	El módulo de Administración cuenta con la configuración de contraseña. Sin embargo, en el campo de caducidad tiene activa la opción "Nunca" cuando dispone de las opciones de 30 días, 60 días y 90 días.
Histórico de contraseña	El usuario desconoce si cuenta con un histórico para que no se repita la clave. No se pudo evidenciar por parte del Departamento de Tecnologías de la Información la parametrización lógica del sistema, debido a que la implementación del sistema se realizó mediante el proveedor TECAPRO y no se cuenta con dicha información.
Complejidad de la contraseña	El usuario indica que ingresan mayúsculas, minúsculas y números cuando crean la clave. Sin embargo, no se pudo evidenciar por parte del Departamento de Tecnologías de la Información la parametrización lógica, debido a que la implementación del sistema se realizó mediante el proveedor TECAPRO y no se cuenta con dicha información.

Al contar con una configuración inadecuada de parámetros de seguridad lógica de los sistemas de información, podría darse el riesgo de que, si se dieran accesos no autorizados, se vea comprometida la información permitiendo modificar, eliminar, insertar o consultar datos sensibles de la Institución.

CRITERIO:

El proceso **3.2 "Implementación de Software"** presente en el documento 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, menciona: "*La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:*

j. Observar lo que resulte aplicable de la norma 3.1anterior.

k. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implantación de la satisfacción de los requerimientos.

l. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.

m. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.

n. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.

o. *Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.*".

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 este punto, 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.

HALLAZGO 04: DEPENDENCIA DEL PROVEEDOR TECAPRO PARA EL MANTENIMIENTO DEL SISTEMA BOS. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el Archivo Nacional cuenta con un Sistema llamado BOS para la administración de los procesos financieros, el cual fue implementado por el proveedor TECAPRO hace aproximadamente 18 años y actualmente presta los servicios de mantenimiento.

Por otra parte, el jefe del Departamento de Tecnologías de la Información menciona que el servicio recibido ha sido muy satisfactorio y se adapta a las necesidades de la Institución. Con respecto a las modificaciones realizadas al momento, corresponden a cambios en su configuración sin afectar su código, adicionalmente no se han presentado cambios significativos en la estructura y funcionalidad del sistema porque siempre ha funcionado bien según comentarios de la administración, como ejemplo, está la adaptación que se hizo al módulo de planilla para el control de vacaciones de funcionarios.

Sin embargo, no se logró identificar un plan de contingencia en caso de que el proveedor no preste el servicio adecuadamente o que las horas presupuestadas sean consumidas para atención de cambios, ni tampoco se cuenta con un proceso de transferencia tecnológica que minimice la dependencia del proveedor de TECAPRO, para el mantenimiento requerido por el sistema.

Por consiguiente, al tener dependencia total del proveedor contratado para la implementación y mantenimiento de software existe el riesgo de pérdida de disponibilidad de los sistemas en caso de que falte el proveedor o dificultad en la implementación de cambios en el sistema si el proveedor falla.

CRITERIO:

El proceso **3.4 "Contratación de terceros para la implementación y mantenimiento de software e infraestructura"** presente en el documento 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, menciona: *"La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura. Para lo anterior, debe:*

a. *Observar lo que resulte aplicable de las normas 3.1, 3.2 y 3.3* anteriores.
b. Establecer una política relativa a la contratación de productos de software e infraestructura.
c. Contar con la debida justificación para contratar a terceros la implementación y mantenimiento de software e infraestructura tecnológica.
d. Establecer un procedimiento o guía para la definición de los "términos de referencia" que incluyan las especificaciones y requisitos o condiciones requeridos o aplicables, así como para la evaluación de ofertas.
e. Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado; sean instalaciones, hardware o software.

f. Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica."

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.

HALLAZGO 05: INCONSISTENCIAS EN LA BASE DE DATOS DE ACTIVOS FIJOS.RIESGO MEDIO.

CONDICIÓN:

A partir de la revisión de los datos almacenados en la base de datos del sistema de activos fijos del Sistema BOS, con corte al 31 de diciembre del año 2017 se determinaron las siguientes inconsistencias:

- Existen 11 registros sin número de placa en el campo "PLACA ACTIVO".

CODIGO	PLACA ACTIVO	CATEGORIA
5892		ARCH., BIBLIO. Y ARMARIOS
5893		COMPUTADORAS
5894		EQUIPOS DE VENTILACION

CODIGO	PLACA ACTIVO	CATEGORIA
5895		FOTOCOPIADORAS
5896		IMPRESORAS
5897		MESAS Y ESCRITORIOS
5898		MONITORES
5899		OT. EQUIPOS Y MOBILIARIOS
5900		OTROS EQUIPOS DE COMPUTO
5901		SILLAS Y BANCOS
5902		UPS

- Existen 2 números de placa duplicados.

CODIGO	PLACA ACTIVO	CATEGORIA	DESCRIPCION
0484	2474775	MESAS Y ESCRITORIOS	MESA P/ TELEFONO NEGRA CON BLANCO
5975	2474775	MESAS Y ESCRITORIOS	MESA DE FAX
5684	2447597	MESAS Y ESCRITORIOS	Escritorio de Metal 5 Gavetas
5974	2447597	MESAS Y ESCRITORIOS	ESCRITORIO METÁLICO

- El número de placa **2477536** se encuentra duplicado hasta en 136 registros, en la categoría EDIF. DE OFI.-ATE. AL PUB de tipo EDIFICIO con diferente descripción, vida útil, fecha y costo original. Además, es importante mencionar que 107 registros ya cumplieron con la vida útil, mientras que 29 registros no han cumplido con el tiempo estimado de depreciación.

Al existir inconsistencias en los datos almacenada respecto a activos fijos en el sistema BOS, existe el riesgo que se produzca un uso indebido de activos propiedad de la Institución y no ser detectado oportunamente por la administración.

CRITERIO:

El apartado **4.3 Administración de los datos**, presente en el documento "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, menciona: *"La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.*

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.

COMENTARIO DE LA ADMINISTRACIÓN:

Existen 11 registros sin número de placa en el campo "PLACA ACTIVO": Sobre esta situación se informa que estos 11 "activos" corresponden a la revaluación que se realizó a los activos fijos, que por la forma en que realiza la revaluación el sistema contable, no fue posible aplicar la revaluación a cada uno de los activos por separado, por lo que decidió hacerlo de forma grupal según la categoría de los mis mos. De ahí que estas líneas no tengan número de placa, ya que cada línea representa a varios activos fijos. También es importante que se corrija el cuadro del documento, ya que el colocado al no tener mayor información, da la impresión que realmente hay activos sin plaquear, situación que no es correcta.

CODIGO	PLACA ACTIVO	CATEGORIA	DESCRIPCION	VIDA UTIL	FECHA INST	ACT.COSTO ORIGI	DEPRECIACION AC	TOT. VALOR EN L
5892		ARCH., BIBLIO. Y ARMARIOS	REVALUACION ARCH, BIBLIO Y ARMARIO	120	30/11/2014	23,299,854.57	7,184,121.83	16,115,732.74
5893		COMPUTADORAS	REVALUACION COMPUTADORAS	60	30/11/2014	6,990,389.97	4,310,740.48	2,679,649.49
5894		EQUIPOS DE VENTILACION	REVALUACION EQUIPO VENTILACION	120	30/11/2014	143,289.69	44,180.99	99,108.70
5895		FOTOCOPIADORAS	REVALUACION FOTOCOPIADORAS	120	30/11/2014	759,482.31	234,173.71	525,308.60
5896		IMPRESORAS	REVALUACION IMPRESORAS	60	30/11/2014	2,876,514.51	1,773,850.61	1,102,663.90
5897		MESAS Y ESCRITORIOS	REVALUACION MESAS Y ESCRITORIO	120	30/11/2014	5,556,514.12	1,713,258.52	3,843,255.60
5898		MONITORES	REVALUACION MONITORES	60	30/11/2014	1,587,488.49	978,951.24	608,537.25
5899		OT. EQUIPOS Y MOBILIARIOS	REVALUACION OTROS EQUIPOS Y MOBILIARIOS	120	30/11/2014	2,763,819.29	852,177.61	1,911,641.68
5900		OTROS EQUIPOS DE COMPUTO	REVALUACION OTROS EQUIPOS COMPUTO	60	30/11/2014	2,999,184.05	1,849,496.83	1,149,687.22
5901		SILLAS Y BANCOS	REVALUACION DE SILLAS Y BANCOS	120	30/11/2014	2,937,256.91	905,654.21	2,031,602.70
5902		UPS	REVALUACION UPS	60	30/11/2014	808,887.44	498,813.92	310,073.52

Existen 2 números de placa duplicados: Esta duplicidad de placas se da por motivo de la conciliación y proceso de depuración que se ha realizado contra el sistema SIBINET, al encontrar en SIBINET estos dos activos con monto diferente al que se encuentra en la contabilidad. Por lo que se corrige dichos montos en contabilidad, en el Módulo de Activos Fijos del Sistema BOS por medio de la inclusión de la misma placa del activo mencionado solo que por la diferencia de monto, esto se debe realizar de esta forma porque el módulo de Activos Fijos no permite modificar los montos iniciales de los activos.

El número de placa 2477536 se encuentra duplicada hasta en 136 registros: Sobre esta información, se le aclaró a la Señorita Nancy Saborío por medio de un correo en donde ella realiza la consulta, el cual se adjunta. Estos activos corresponden al registro inicial del Edificio, el cual comprende al edificio más algunos activos como lámparas, estanterías, rejas, mejoras que se realizaron, entre otros. Por lo que se podría concluir, es que el encargado de activos fijos que los plaqueó en su momento, consideramos que lo mejor era realizarlo en una sola placa, mientras que el encargado de la contabilidad en el momento de registro en el módulo consideró que lo mejor era hacerlo de forma detallada, aunque tuviera una sola placa. Situación que se ha respetado por la profesional contable, con el fin de no alterar la información existente e inicial que se incluyó.

Sobre las recomendaciones que el informe menciona, es importante aclarar que se indica **"Al encargado de Activos"** asignación que no es correcta, debido a que las situaciones encontradas se desprenden de un reporte que emite el módulo de Activos Fijos del Sistema Bos que es de uso exclusivo del profesional contable, por lo que en este caso me correspondería acatar las recomendaciones del informe.

HALLAZGO 06: MANUALES DE USUARIO DESACTUALIZADOS. RIESGO BAJO.

CONDICIÓN:

Durante el proceso de auditoría se verificó la existencia de los manuales de usuario para el sistema BOS en los módulos de Punto de Venta, Control Bancario, Inventario, Nómina, Cuentas por Pagar, Activos Fijos, Contabilidad y Presupuesto. Sin embargo, estos se encuentran desactualizados y los usuarios desconocen de los documentos para su uso.

Al no contar con los manuales actualizados existe el riesgo de que los usuarios no tengan conocimiento de cómo usar las funcionalidades de los módulos del sistema y asimismo realizar acciones indebidas por mal uso.

CRITERIO:

El proceso **3.2 "Implementación de Software"** presente en el documento 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, menciona: "*La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:*

p. Observar lo que resulte aplicable de la norma 3.1anterior.
q. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implantación de la satisfacción de los requerimientos.
r. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
s. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
t. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
u. *Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.*".

RECOMENDACIONES:

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:
En cuanto al punto de los manuales de usuario del Bos 7.0 desactualizados, efectivamente se requiere su actualización, por lo que se deben solicitar a la empresa las versiones actualizadas y mantenerlas disponibles para las áreas usuarias del sistema y que estos incluyan las actualizaciones que se efectúen a dicho sistema.

III. ANEXOS

ANEXO I: EVALUACIÓN FUNCIONAL DE ALGUNOS SISTEMAS DE INFORMACIÓN IMPLANTADOS EN EL ARCHIVO NACIONAL.

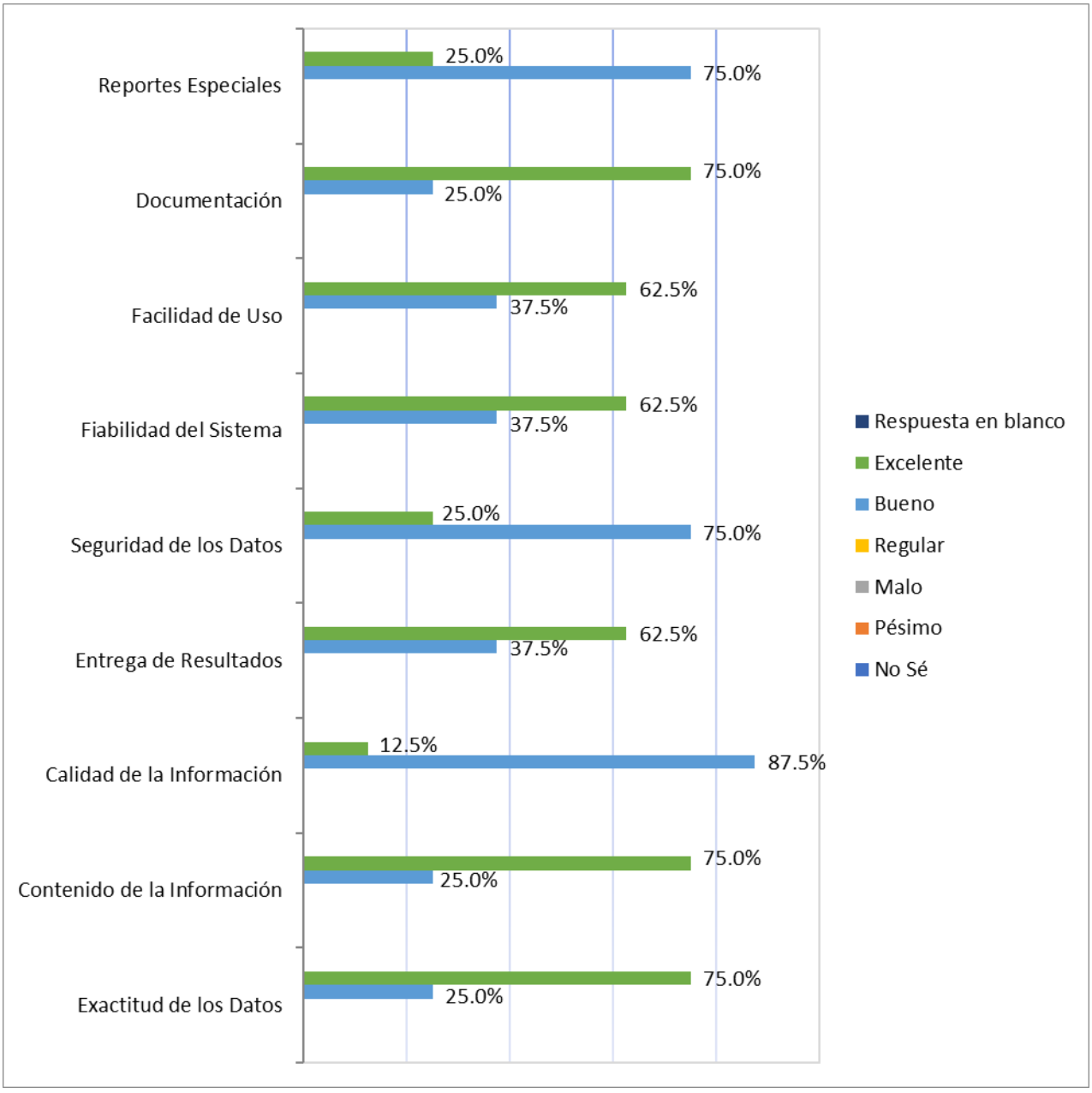
En este apartado se muestra el resultado de la evaluación realizada respecto a la calidad funcional de algunos de los sistemas de información implantados en el Archivo Nacional según la percepción de los usuarios finales.

Los módulos revisados en el proceso de evaluación de la calidad funcional se muestran en la tabla siguiente:

Sistema por Valorar
BOS - Inventarios
BOS - Cuentas por Pagar
BOS - Activos Fijos
BOS - Presupuesto
BOS - Contabilidad
BOS - Punto de Ventas
BOS - Nómina
BOS - Control Bancario

Resultados obtenidos de la evaluación en el Archivo Nacional.

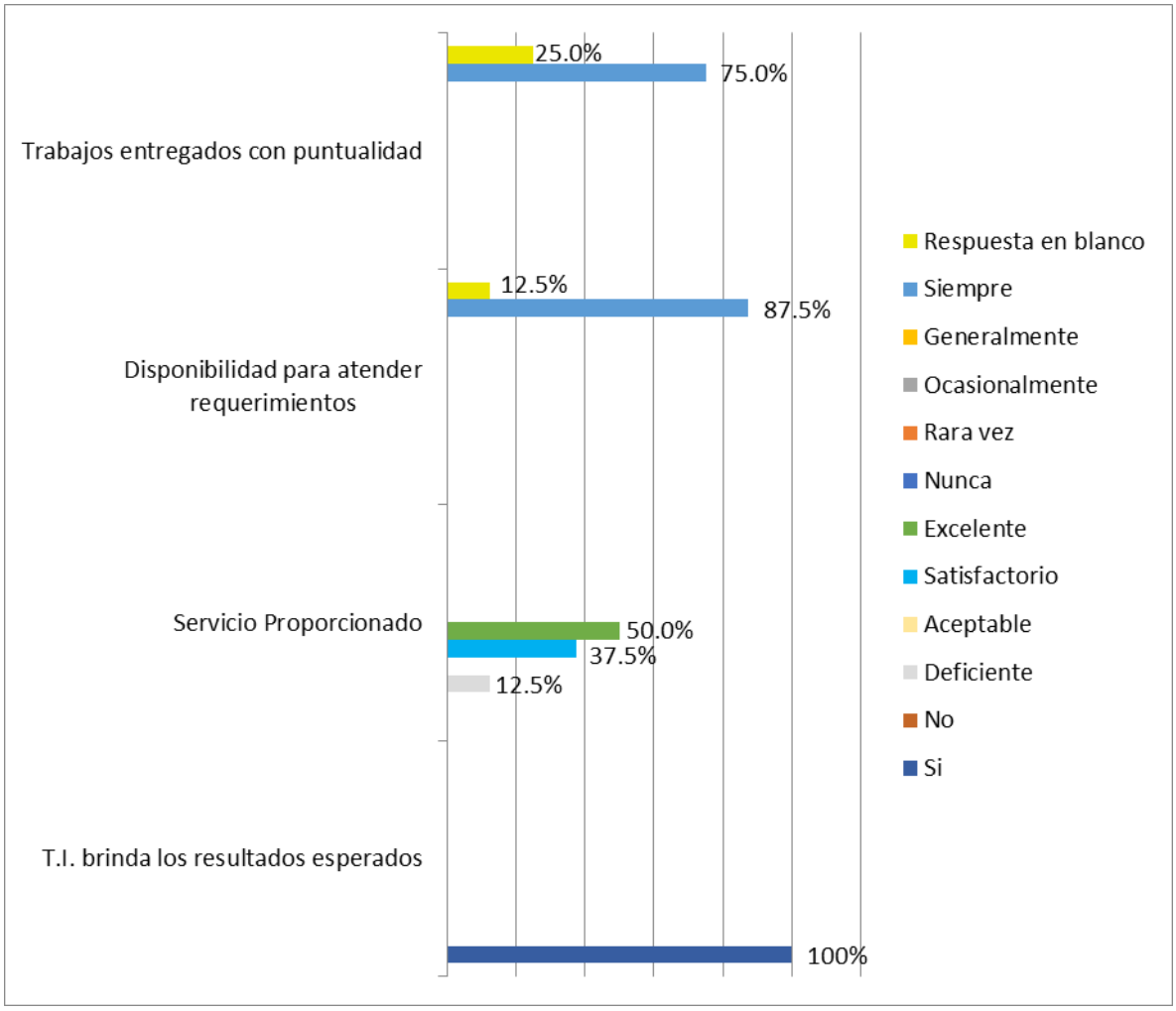
El detalle de la evaluación de la calidad funcional según usuarios de los sistemas evaluados del Archivo Nacional detallados en el cuadro anterior, se muestran en el gráfico siguiente:



Según los resultados obtenidos, los cuales se observan en el gráfico anterior, la percepción de la exactitud de los datos, el contenido de la información y la documentación, son considerados de carácter excelente con un 75% de las opiniones y un 25% aseguran que son buenas, junto con la facilidad de uso, la fiabilidad del sistema y la entrega de resultados, que son considerados por un 62.5% de los usuarios entrevistados, en la categoría excelente, y un 37.5% en la categoría de bueno. Además, la calidad de la información es considerada por un 87.5% de los usuarios como buena, y un 12.5% opina que es excelente. Así como,

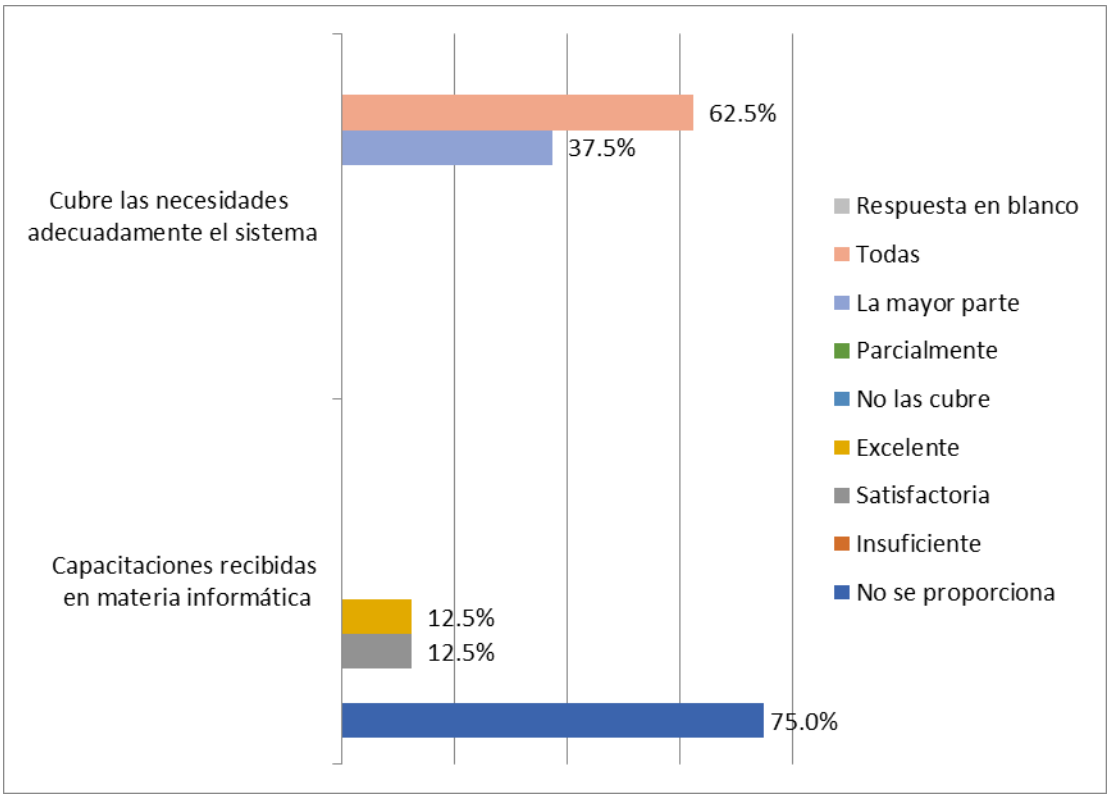
los reportes especiales y la seguridad de los datos, que son considerados por un 75% de los usuarios expertos de carácter bueno, y un 25% dice que son excelentes.

La percepción de los usuarios finales respecto al servicio brindado por parte del Departamento de Tecnologías de la Información se muestra en el gráfico siguiente:



El gráfico anterior, corresponde principalmente a la satisfacción que poseen los usuarios respecto al servicio que brinda TI, en función a los sistemas de información utilizados. En el mismo se ve reflejado que la mayoría de las opiniones de los usuarios reflejan están conformes con el servicio de TI. No obstante, hubo un pequeño porcentaje de la población (12.5%), que considera deficiente el servicio proporcionado por el Departamento de Tecnologías de Información. Además, dentro de las opiniones encontradas sobre la disponibilidad para atender requerimientos y trabajos entregados con puntualidad, se encuentran comentarios haciendo énfasis en que el Departamento de TI no es el encargado directo de atender las necesidades del sistema BOS, sino que es su proveedor, por lo que no consideran importante el papel de TI en estos aspectos.

Percepción de los usuarios finales respecto a si los sistemas de información del Archivo Nacional cubren la mayor parte de las necesidades actuales:



El gráfico anterior corresponde a la comodidad que sienten los usuarios frente al uso del sistema de información evaluado. Se puede evidenciar que el 62.5% de los usuarios indicaron que el sistema cubre todas sus necesidades laborales, así como, el 37.5% de las personas, afirman que los sistemas cubren la mayoría de sus necesidades, lo cual puede evidenciar que aún hay aspectos a los cuales se les puede prestar la debida atención para ofrecer un mejor servicio.

Sin embargo, se identifica que un total del 75% de los usuarios entrevistados, indican estar inconformes con las capacitaciones recibidas, ya que solo un 12.5% indican estar satisfechos y un 12.5% indican que son excelentes. Lo cual puede reflejar una notable falta de capacitación ante el uso de los sistemas.

Comentarios o mejoras por parte de los usuarios referentes a la valoración de los sistemas de información:

- Con respecto a todos los módulos, considerar la inclusión de un módulo de asistencia, que permita una interacción más cercana con el servicio de soporte al usuario.

- Con respecto a los reportes que son programados en todos los módulos, analizar la posibilidad de realizar cambios en su programación, de acuerdo con las necesidades de los usuarios.

RECOMENDACIÓN

Propiciar una reunión entre el Departamento de TI, el proveedor del soporte técnico del Sistema BOS (TeCapro) y los usuarios de las áreas involucradas, con el fin de llevar a cabo las mejoras que correspondan, levantando los requerimientos necesarios para cubrir las necesidades o debilidades que, de una u otra forma, afectan los servicios que brinda el Archivo Nacional. Además, considerar elaborar material para generar capacitaciones sobre los módulos actuales del Sistema BOS, ya que los usuarios sienten que existen debilidades en las capacitaciones sobre el uso de los módulos.

ANEXO II: ANÁLISIS DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Departamento de Tecnologías de la Información
Periodo 2017

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.

A. SEGURIDAD FÍSICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.1	Proceso de autorización de ingreso		✓	Se cuenta con un lineamiento debidamente formalizado.		B
A.2	Personal interno y externo debidamente identificado (gafete)		✓	Personal de TI ingresa por medio de huella táctil, además utilizan su gafete representativo.		B
A.3	Revisión de equipos de ingreso y salida		✓	Se hace por medio de inventario, y se hace por medio del responsable de cada equipo.		B
A.4	Bitácoras de acceso al edificio y centro de cómputo		✓	Sí se cuentan con bitácoras de acceso para funcionarios y para terceros.		B
A.5	Acceso restringido a personal de informática definido		✓	Solo personal de TI puede ingresar.		B
A.6	Una sola vía de acceso		✓	Solo existe una vía de acceso (la puerta principal).		B
A.7	Externos son acompañados por internos		✓	Sí, solo pueden ingresar externos acompañados de un interno.		B
A.8	Puerta de acceso segura		✓	Sí, ya que la única manera de entrar es por medio de la huella táctil.		B
A.9	Acceso con tarjeta electrónica al centro de datos		✓	No se realiza por tarjeta electrónica.	Se realiza por medio de huella digital.	B
A.10	Alarmas de detección de intrusos	✗		No se cuenta con alarmas de detención de intrusos.		M
A.11	Monitoreo de la entrada por cámara de seguridad	✗		No se cuenta con cámaras de seguridad para la entrada del centro de datos.		M
A.12	Ubicación en un sitio seguro (lugares colindantes)		✓	El sitio es un lugar seguro, ya que se encuentra en un primer piso y no tiene lugares colindantes.		B
A.13	Lugar completamente cerrado		✓	El lugar está completamente cerrado.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.14	Paredes de concreto		✓	Todas las paredes son de concreto.		B
A.15	Cielo raso sellado		✓	El cielo raso se encuentra completamente cerrado.		B
A.16	Equipos ubicados en rack		✓	Los equipos del cuarto de servidores se encuentran debidamente ubicados en racks.		B
A.17	Los racks están asegurados		✓	Los racks se encuentran debidamente asegurados.		B
A.18	Cableado de datos independiente del eléctrico		✓	Se poseen dos tubos independientes, donde se separa el cableado de datos y el eléctrico.		B
A.19	Cableado entubado y canaleteado		✓	Sí se cuenta con cableado debidamente entubado y canaleteado.		B
A.20	Cableado debidamente rotulado	✗		El cableado se encuentra parcialmente rotulado, ya que no todos los cables cuentan con su debida etiqueta.		B
A.21	Hay un sitio alterno	✗		No existe un sitio alterno, sin embargo, existe un Depósito de Seguridad donde se almacenan las cintas de respaldo.		M

B. INSTALACIÓN ELÉCTRICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
B.1	Hay pararrayos		✓	Sí se cuenta con pararrayos.		B
B.2	Circuito eléctrico independiente		✓	Sí existe un circuito eléctrico totalmente independiente.		B
B.3	Interruptor de emergencia en la sala de cómputo (palanca)		✓	Existe una palanca de emergencias dentro de la sala de cómputo.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
B.4	Cableado eléctrico debidamente entubado o cubierta contra incendios		✓	Sí existe cableado eléctrico debidamente entubado dentro de todo el edificio.		B
B.5	Conexión de los equipos a UPS		✓	Los equipos se cuentan conectados a la UPS.		B
B.6	UPS ubicada en un sitio seguro		✓	La UPS principal se encuentra dentro del cuarto de servidores.		B
B.7	Pruebas periódicas de la UPS (bitácora)		✓	Sí se realizan pruebas periódicas a la UPS.	Se realizan como parte del contrato con la empresa Sistemas de Energía SERC.	B
B.8	UPS en contrato de mantenimiento preventivo y correctivo		✓	Sí se cuenta con un contrato de mantenimiento preventivo y correctivo (SERC).		B
B.9	Conexión a Planta eléctrica		✓	Sí se está conectado con la planta eléctrica.		B
B.10	Planta eléctrica ubicada en un sitio seguro		✓	La planta eléctrica se encuentra resguardada en un lugar seguro.		B
B.11	Pruebas periódicas de la planta eléctrica		✓	Si se realizan pruebas, durante la ejecución del mantenimiento preventivo a la planta eléctrica.		B
B.12	Planta eléctrica en contrato de mantenimiento preventivo y correctivo		✓	Si se cuenta con un contrato para el mantenimiento de la planta eléctrica.		B
B.13	Luces de emergencia en el centro de cómputo o cercanías	✗		No existen luces de emergencia dentro del centro de cómputo, sin embargo, afuera del centro de cómputo, se cuenta con un sistema de luces de emergencia.		B
B.14	Pruebas periódicas de sistema de iluminación de emergencias		✓	Se realizan pruebas bajo demanda, se reportan las averías y se arreglan inmediatamente.		B

C. INSTALACIÓN AIRE ACONDICIONADO

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
C.1	Equipo de aire acondicionado independiente para el centro de datos		✓	Se comprueba que existe un equipo de aire acondicionado independiente para el centro de datos. Sin embargo, no existe equipo de respaldo.		B
C.2	Equipo de respaldo para el aire acondicionado	✗		No existe un equipo de respaldo para el aire acondicionado.		M
C.3	Contrato de mantenimiento preventivo y correctivo	✗		El departamento de TI afirma que, si existen contratos de mantenimiento preventivo y correctivo, sin embargo, no se suministró evidencia de lo anterior.		M
C.4	Control y monitoreo de humedad y temperatura		✓	Se cuenta con un dispositivo para el control y monitoreo de humedad y temperatura.		B

D. DESASTRES NATURALES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
D.1	Brigada de emergencias		✓	Si existe una brigada de emergencias, en este caso se llama la Comisión Auxiliar de Emergencias.		B
D.2	Capacitación del personal	✗		El departamento de TI afirma que existe una capacitación anual en el uso de extintores, y dos simulacros de emergencias por año, sin embargo, no se suministraron evidencias de lo anterior.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
D.3	Rutas de evacuación y salidas de emergencia		✓	Sí se cuentan con rutas de evacuación y salidas de emergencia.		B
D.4	Señalización		✓	Todo el edificio tiene una buena señalización.		B
D.5	Simulaciones periódicas		✓	Se realizan simulaciones de emergencias dos veces por año.	El área de TI no tiene injerencia en este tema.	B
D.6	Fácil acceso por Unidades de Bomberos		✓	Sí es de fácil acceso para las Unidades de Bomberos.	Cada piso cuenta con tomas de agua para cualquier emergencia.	B
D.7	Sistemas de detección de humo/calor/fuego		✓	Sí se cuenta con un sistema de detección de humo y fuego.		B
D.8	Sistemas automáticos y manuales de alarma		✓	Si se cuenta con sistemas automáticos y manuales para cualquier emergencia dentro del edificio.		B
D.9	Extinguidores cercanos portátiles (revisados al día)	✗		Cada piso del edificio cuenta con al menos un extintor visible.	Se comprueba de que los extintores se encuentran recargados a excepción del que se encuentra en el cuarto de comunicaciones ya que, según su boleta de recarga, no se recarga desde el mes de febrero del año 2014.	B
D.10	Uso de aspersores		✓	No se utilizan aspersores.	Cuentan con alarmas de incendio.	B
D.11	Pisos falsos		✓	No se cuenta con piso falso.	Se cuenta con techo falso.	B
D.12	Desnivel en el piso	✗		No se cuenta con un desnivel en el piso.		B

E. FALLAS HARDWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
E.1	Redundancia de servidores críticos		✓	Se tiene un clúster con 2 nodos, con servidores virtualizados, en caso de la pérdida de un nodo, la carga se balancea en el otro nodo.		B
E.2	Mantenimiento preventivo		✓	Sí se realiza un mantenimiento preventivo de los servidores, por los colaboradores del área de TI.		B
E.3	Mantenimiento correctivo		✓	Sí se realiza un mantenimiento correctivo para subsanar fallas en los servidores, por los colaboradores del área de TI.		B

H. RESPALDOS Y RECUPERACIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
H.1	Política de respaldos		✓	Se cuenta con una política de respaldos de información.		B
H.2	Procedimientos para respaldo y recuperación		✓	Sí se cuentan con procedimientos para el respaldo y recuperación de información.		B
H.3	Almacenamiento de información		✓	Se almacena una copia de información en el cuarto de servidores y otra se envía al sitio alterno.	Se posee un plan de contingencia, que estipula periodicidad de respaldos.	B
H.4	Traslado de respaldos		✓	Sí se realizan traslados de respaldos de forma manual.		B
H.5	Configuración de programas para respaldo		✓	Se realiza una configuración previa, antes de realizar los respaldos.		B

J. INTRUSIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
J.1	Política de acceso lógico		✓	Se tiene un procedimiento documentado para la solicitud de accesos.		B
J.2	Control de acceso a aplicaciones		✓	Las jefaturas realizan la asignación de roles al sistema.		B
J.3	Monitoreo de usuarios y accesos	✗		Se realiza ocasionalmente la revisión, generalmente bajo demanda.	El área de TI solo administra los servicios.	M

L. RIESGOS DE LA GESTIÓN DE TI

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.1	¿Se han implementado antivirus y firewalls?		✓	Sí se ha implementado un Antivirus corporativo y el firewall FORTINET.	Se suministró evidencia del Antivirus Corporativo (ESET).	B
L.2	¿Se han establecido los protocolos para la realización de copias de seguridad?		✓	Sí se cuenta con protocolos para realizar las copias de seguridad de la información.		B
L.3	¿Se tiene definido el perfil para cada cargo de TI y los colaboradores vinculados cumplen con el mismo?		✓	Se cuenta con un documento el cual describe los perfiles de los funcionarios de TI.		B
L.4	¿La creación de usuarios y la asignación de los permisos y/o perfil en los aplicativos es solicitada y aprobada formalmente por cada líder de área?		✓	Las jefaturas son las que solicitan los permisos al Área de Informática.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.5	¿Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de TI y dicho seguimiento es documentado?		✓	Se hacen seguimientos bajo demanda, ya que se tiene un documento donde se encuentran las fechas para brindar, renovar o recibir un servicio contractual.		B
L.6	¿Se ha establecido el plan de continuidad para los procesos de TI?		✓	Sí se cuenta con un plan de continuidad para los procesos de TI.		B

M. SISTEMAS DE INFORMACIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.1	Los accesos son autorizados por un nivel superior.		✓	Los accesos son generados por las jefaturas de las áreas.		B
M.2	Los accesos otorgados son revisados periódicamente.	✗		Las revisiones se realizan bajo demanda o solicitud de alguna jefatura.		M
M.3	La asignación de los accesos parte de la segregación de funciones.		✓	Si se hace una asignación de accesos, a partir de la segregación de funciones.		B
M.4	Cada usuario tiene asignada una clave de composición alfa numérica y de mínimo 8 caracteres	✗		No, ya que el mínimo de caracteres es de 6, y no se requiere una composición alfa numérica.	Se desconoce la configuración de la parametrización lógica del Sistema BOS.	M
M.5	Se pueden rastrear las operaciones realizadas por los usuarios por medio de los logs		✓	Sí se pueden rastrear operaciones por medio de logs.		B
M.6	Se cuenta con una política de copias de seguridad y de restauración.		✓	Se cuenta con un procedimiento para la realización de respaldos de información.		B
M.7	La información sensible se encuentra protegida de modificaciones no autorizadas.		✓	Sí se protege la información sensible en el área de Informática.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.8	Se cumplen con los niveles de seguridad físicos para los servidores.		✓	Sí se cumplen con los niveles de seguridad físicos para los servidores.		B
M.9	Asignación de usuarios y claves personalizada		✓	Los usuarios siguen un estándar, y las claves si pueden ser personalizadas.		B
M.10	Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.		✓	Se solicitan los cambios por medio de una solicitud de los usuarios expertos a la Jefatura inmediata. Después el proveedor o el departamento de TI realizan los cambios, para su aprobación.	Los cambios en el sistema los realiza la empresa TeCapro.	B
M.11	Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.		✓	Las áreas usuarias son las encargadas de solicitar cambios, por lo que se notifica cuando se implementa un cambio.		B
M.12	Las modificaciones en las bases de datos son realizadas por un área independiente a la que utiliza la información.		✓	Si se realiza por una empresa independiente a la que utiliza la información.	La empresa TeCapro, es la única que puede realizar cambios a las bases de datos.	B
M.13	Los cambios en la base de datos permiten tener la trazabilidad de quien los realiza por medio de los logs.	✗		Son realizados por externos al departamento de TI.		M
M.14	Se tiene un número reducido de administradores.		✓	Sí se tiene un número reducido de usuarios administradores.		B
M.15	Se cuenta con un diccionario de datos para la base de datos, identificando las relaciones internas que tiene y los accesos de consulta o modificación.	✗		TI no tiene conocimiento de este aspecto.		M
M.16	Definición y documentación de la Política de Cambios		✓	Se entrega una boleta de solicitud de cambio al departamento de TI, para estudiar si se escala a la empresa proveedora TeCapro.		B
M.17	Segregación de funciones entre el desarrollador, aprobador y responsable de administrar en producción	✗		TI no tiene conocimiento de este aspecto, ya que el servicio es brindado por un tercero.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.18	Aprobación del usuario final de los cambios.		✓	Se cuenta con la aprobación del usuario final perteneciente al departamento de Financiero del Archivo Nacional.		B
M.19	Asignación usuarios y permisos, previo requerimiento y aprobación del Director y/o Responsable del área que utiliza la aplicación.		✓	Las jefaturas de las áreas usuarias son las que asignan los permisos de los sistemas.		B
M.20	Reportes periódicos de los cambios que se consideran críticos en las aplicaciones, para validar su autorización por parte del nivel aprobador de los cambios.		✓	Se generan reportes de cambios realizados, únicamente cuando las jefaturas aprueben los cambios realizados.		B
M.21	Validación periódica de los cambios en permisos y asignación de usuarios por parte del nivel autorizador.	✗		La revisión de los cambios de permisos se realiza bajo demanda.		M
M.22	Bloqueo de usuarios retirados, previa comunicación de Gestión Humana.		✓	Se realiza un bloqueo de usuarios retirados. A partir de su salida de la Institución. Esto lo hace la jefatura a cargo.		B
M.23	Revisión periódica de la compatibilidad de los accesos otorgados de acuerdo con el reporte de funciones de Gestión Humana y el principio de segregación de funciones.	✗		La revisión de permisos se realiza bajo demanda.		M
M.24	Bloqueo de usuarios en vacaciones	✗		No se realiza un bloqueo de usuarios que están en vacaciones.		B
M.25	Identificación de los usuarios que realizan las transacciones, por medio de los Logs.		✓	Sí se puede identificar las acciones de los usuarios por medio de logs.		B
M.26	Plan de contingencia para migrar a otro servidor		✓	Sí se cuenta con un plan de contingencias.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.27	Plan de capacitaciones en seguridad, para los usuarios con accesos más vulnerables.		✓	Se han realizado capacitaciones a los usuarios.		B
M.28	Cifrar las bases de datos más sensibles, junto con controles de monitoreo.	✗		No se cifran las Bases de Datos.		M
M.29	Limitar el acceso a los datos y/o solicitar mayores autenticaciones, de acuerdo al dispositivo y al lugar desde donde se ingresa.		✓	Se puede acceder a la información desde fuera de la Institución, utilizando la herramienta TeamViewer.		B
M.30	Instalar en los dispositivos móviles parches que permitan aislar los datos de la compañía de los personales.		✓	Se instalan aplicaciones a dispositivos móviles, únicamente con permiso y solicitud de la Jefatura, y deben ser aprobados por la Dirección General del Archivo Nacional.	El departamento de TI es el que habilita a los funcionarios autorizados.	B
M.31	Se realizan pruebas periódicas sobre la recuperación de datos.	✗		Se realizan bajo demanda.		M

--Última Línea--