MUSEO NACIONAL DE COSTA RICA (MNCR)

- ***Informe de Auditoría de Sistemas y Tecnología de Información***
- ***Carta de Gerencia TI 2017***
- ***Informe final***

San José, 2 de noviembre de 2018

Señores
Unidad de Informática
Gerencia General
Junta Directiva
Museo Nacional de Costa Rica (MNCR)

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del período 2017 al Museo Nacional de Costa Rica 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, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 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 funcionarios o 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 Museo Nacional de Costa Rica (MNCR)

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 en el Museo Nacional de Costa Rica (MNCR).

La auditoría realizada fue requerida por la administración del Museo Nacional de Costa Rica, 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. Ricardo Montenegro Guillén
Contador Público Autorizado N° 5607
Póliza de Fidelidad No. 0116 FIG7
Vence el 30 de setiembre del 2019.

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

Contenido

ORIGEN DEL ESTUDIO 5
ALCANCE 5
OBJETIVO DEL ESTUDIO 6
PERIODO DE LA AUDITORÍA 6
LIMITACIONES DEL ESTUDIO 6
METODOLOGÍA 6
I. HALLAZGOS Y RECOMENDACIONES 7
HALLAZGO 01: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE LA CALIDAD DE LOS PRODUCTOS Y SERVICIOS DE TI. RIESGO MEDIO. 7
HALLAZGO 02: AUSENCIA DE UN PROCEDIMIENTO FORMAL PARA LA DIVULGACIÓN DE LA NORMATIVA INTERNA RELACIONADA CON T.I. RIESGO BAJO 8
HALLAZGO 03: OPORTUNIDAD DE MEJORA EN EL PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS. RIESGO BAJO. 9
HALLAZGO 04: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE RIESGOS DE T.I. RIESGO MEDIO. 11
HALLAZGO 05: CUMPLIMIENTO PARCIAL DEL DECRETO EJECUTIVO 37549-JP. RIESGO BAJO. 12
HALLAZGO 06: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO. 14
HALLAZGO 07: DEBILIDADES EN LA ADMINISTRACIÓN DE ACCESOS DE LOS USUARIOS EN LOS SISTEMAS DE INFORMACIÓN. RIESGO MEDIO. 16
HALLAZGO 08: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LAS BASES DE ACTIVOS SIBINET Y BOS. RIESGO MEDIO. 19
HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE PROBLEMAS. RIESGO BAJO. 21
HALLAZGO 10: DEFICIENCIAS EN EL SISTEMA DE INFORMACIÓN BOS. RIESGO MEDIO. 22
II. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES 26
III. ANEXOS 41
ANEXO A 41
Evaluación funcional del sistema de información BOS implementado en el MNCR 41
ANEXO B 51
Análisis de Riesgos TI 51

ORIGEN DEL ESTUDIO

Como parte de la evaluación de los estados financieros del Museo Nacional de Costa Rica, realizamos una 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 y en general las mejores prácticas de la industria de tecnología de información.

ALCANCE

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

1. Verificación del control interno en materia tecnológica con base en la normativa interna establecida.

    a. Comité de TI.
    b. Planificación estratégica de TI.
    c. Gestión de inventario de hardware y software.
    d. Gestión de seguridad de la información: administración de usuarios, accesos y vulnerabilidades, seguridades física y lógica.
    e. Respaldos y recuperación de información.
    f. Gestión de cambios.
    g. Gestión de incidentes y problemas.
    h. Contingencias y continuidad de TI.
    i. Evaluación de control interno.
    j. Plan de implementación de Normas Técnicas para la Gestión y Control de las Tecnologías de Información.
    k. Sistemas de información.
    l. Gestión de riesgos de TI.
    m. Divulgación de normativa de TI.
    n. Gestión de la calidad de los productos y servicios de TI.

2. 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)" emitido por la Contraloría General de la República y en general las buenas prácticas de la industria como los estándares establecidos en los Objetivos de Control para Información y Tecnología Relacionada – CobiT®.

OBJETIVO DEL ESTUDIO

1. Establecer un entendimiento integral del Museo Nacional de Costa Rica (MNCR), 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 Museo Nacional de Costa Rica.

PERIODO DE LA AUDITORÍA

El estudio se realizó durante el mes de octubre del año 2018 y corresponde a la auditoría del periodo del 2017.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones al alcance durante el periodo de estudio de la auditoría de Tecnologías de Información.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la Unidad de Informática del Museo Nacional de Costa Rica (MNCR) y de las distintas áreas involucradas en el proceso de auditoría.

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

I. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE LA CALIDAD DE LOS PRODUCTOS Y SERVICIOS DE TI. RIESGO MEDIO.

CONDICIÓN:

Por medio del oficio UI-2018-O-0084, se indica que la Unidad de Informática no ha desarrollado una metodología para la gestión de la calidad de los productos y servicios de TI tal y como lo solicitan las normas técnicas de la Contralia General República. La Unidad de Informática hace mención del PETI indicando que se consideró un apartado para la gestión de calidad de los proyectos, sin embargo, este apartado no sustituye ni se refiere a una metodología para la gestión de calidad de los productos y servicios de TI.

Al no definir métricas e indicadores para la medición y control de la calidad en la gestión de TI, se dificulta el aseguramiento de la mejora continua en los productos y servicios brindados por TI. Además, existe el riesgo de que los servicios de TI no sean suficientes para satisfacer las necesidades de las áreas usuarias o no entregar productos de TI los cuales cumplan con criterios de aceptación de los usuarios, lo que podría provocar fallas, trabajo adicional y afectar la mejora de los productos y servicios de TI.

CRITERIO:

El apartado **1.2 "Gestión de la calidad"** 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: *"La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo."*

RECOMENDACIONES:

A la Unidad de Informática:

1. Gestionar la definición, aprobación y divulgación de una metodología o procedimiento para gestionar la calidad, con el fin de detallar como se llevará a cabo todo el proceso de mejora continua de los servicios y productos que ofrece la Unidad de Informática. El proceso de gestión de calidad de TI se puede enfocar en los siguientes puntos:

    a. Se debe definir un proceso de planeación el cual de contemplar las siguientes actividades:
        i. Definir los servicios y productos de TI que se van a medir.
        ii. Definir las métricas e indicadores que van a dar apoyo al proceso de medición.

iii. Elaborar encuestas de satisfacción a los usuarios del Museo Nacional para medir la percepción en la calidad de los servicios.
iv. Definir un cronograma y programa de trabajo que indique los pasos a seguir para realizar las mediciones.

b. Ejecutar el programa de trabajo y documentar los resultados y mejoras obtenidos.
c. Verificar y dar seguimiento al proceso de ejecución y resultados de las mediciones, para ello se debe considerar lo siguiente:
   i. Verificar e identificar desviaciones entre los resultados obtenidos contra las métricas e indicadores definidos inicialmente.
   ii. Verificar las encuestas de satisfacción de los usuarios y determinar cuáles son los puntos que más requieren atención, según la percepción de estos.
d. Desarrollar una estrategia de mejora contemplando lo siguiente:

   i. Definir y ejecutar planes de acción correctivo para las debilidades identificadas.
   ii. Documentar los resultados obtenidos y presentarlos ante la comisión de informática para su respectivo conocimiento.

2. Presentar el procedimiento o metodología ante la comisión de Informática para su respectiva aprobación.

HALLAZGO 02: AUSENCIA DE UN PROCEDIMIENTO FORMAL PARA LA DIVULGACIÓN DE LA NORMATIVA INTERNA RELACIONADA CON T.I. RIESGO BAJO

CONDICIÓN:

Por medio del oficio UI-2018-O-0084, se indicó que la Unidad de Informática no ha desarrollado un plan o procedimiento para la divulgación de la normativa interna relacionada con TI.

Al no existir un procedimiento formal para la divulgación de la normativa de T.I, se expone a los siguientes riesgos:

- Políticas, estándares y procedimientos del Museo no entendidas o no aceptadas.
- Falta de comunicación de las aspiraciones de informática y la administración.
- Cultura de control no alineada con las aspiraciones de la administración.
- Vulnerabilidades del negocio al no seguir las políticas y procedimientos.

CRITERIO:

El apartado **1.1 "Marco estratégico de TI"** 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: *"El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido."*

RECOMENDACIONES:

A la Unidad de Informática:

1. Realizar e implementar un procedimiento formal para la divulgación de las normas, lineamientos, metodologías, políticas, procedimientos, entre otros relacionadas con la unidad de informática.

2. Asegurarse que los documentos anteriores estén disponibles para el personal del Museo Nacional, de tal manera que no se pueda justificar su desconocimiento.

3. Presentar el procedimiento o mecanismo ante la comisión de Informática para su respectiva aprobación.

HALLAZGO 03: OPORTUNIDAD DE MEJORA EN EL PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS. RIESGO BAJO.

CONDICIÓN:

Se determinó que la Unidad de Informática del Museo Nacional de Costa Rica cuenta con un procedimiento para la gestión de cambios en los sistemas de información llamado "DIRG-UI-010 Manual procedimiento control de cambios". Respecto a los cambios en hardware, se pone en práctica lo establecido en el documento "DIRG-UI-001 Manual procedimiento asignación de hardware y software", según lo indicado por la Jefatura de dicha Unidad.

Sin embargo, ambos procedimientos presentan oportunidades de mejora en su estructura, según lo indicado en las buenas prácticas como COBIT, donde se deben de incluir aspectos como la categorización, priorización, impacto en procesos de negocio y usuarios, y seguimiento e informes del estado de los cambios.

Al no contar con un procedimiento para la gestión de cambios de TI basado en las mejores prácticas, existe el riesgo de que los cambios no se atiendan de la mejor manera, se dé una incorrecta priorización o no se tenga conocimiento del impacto en los usuarios y procesos de negocio que los cambios puedan generar en caso de que no se lleven a cabo o no se gestionen adecuadamente.

CRITERIO:

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

a. *Observar lo que resulte aplicable de la norma 3.1anterior.*
b. *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 postimplantación de la satisfacción de los requerimientos.*
c. *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.*
d. *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.*
e. *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.*
f. *Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento."*

RECOMENDACIONES:

A la Unidad de Informática:

1. Valorar la modificación del documento "DIRG-UI-010 Manual procedimiento control de cambios", de modo que en este se describa el proceso para realizar cualquier cambio relacionado con elementos de TI (no solo sobre los sistemas de información tal como se encuentra actualmente).

2. Incluir en la descripción del procedimiento de cambios los pasos para asignar los siguientes aspectos:

    a. Tipo de cambio (estándar, normal o emergencia).
    b. Clasificación (por ejemplo, infraestructura y sistemas de información).
    c. Impacto.
    d. Prioridad.
    e. Plazo de implementación.
    f. Estado del cambio (rechazado, aprobado, pero aún no iniciado, aprobado y en proceso, cerrado).

3. Aprobar formalmente la modificación del procedimiento.

4. Elaborar un registro de los cambios en el cual se incluyan los aspectos mencionados anteriormente, así como:

    a. Identificación del cambio.
    b. Fecha de la solicitud.
    c. Fecha de la aprobación o rechazo de la solicitud.
    d. Descripción del cambio.
    e. Razón del cambio.
    f. Efecto de no implementar el cambio.
    g. Contacto y detalles del solicitante del cambio.
    h. Responsable de la implementación del cambio.
    i. Detalles de la implementación del cambio.
    j. Fecha de la implementación.
    k. Detalles del cierre del cambio.

5. Realizar un análisis de la herramienta "GLPi", de tal manera que permita ingresar los aspectos antes mencionados. En caso contrario, valorar alguna alternativa en el mercado que cumpla con las necesidades para la debida gestión en la atención de las solicitudes de cambios.

HALLAZGO 04: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE RIESGOS DE T.I. RIESGO MEDIO.

CONDICIÓN:

Por medio del oficio UI-2018-O-0084, la Unidad de Informática indicó: "No se ha desarrollado un plan para la administración de los riesgos de tecnologías de información. Sin embargo, en el Plan Estratégico de Tecnologías de Información se consideró un apartado para la gestión de los riesgos de los proyectos", no obstante, este apartado no sustituye ni se refiere a una metodología para gestionar los riegos de TI a nivel institucional.

Al no contar con una metodología formalmente establecida para la gestión de riesgos de TI, así como, no realizar valoraciones periódicas de los riesgos, existe la posibilidad de incurrir en eventos que impacten negativamente los servicios que se brindan actualmente, ya sea una interrupción parcial o total de algún proceso crítico del museo, vulnerabilidades en la seguridad, incumplimientos de contratos, pérdida de calidad de los servicios, entre otros.

CRITERIO:

El apartado **1.3 "Gestión de riesgos"** 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: *"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión*

continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."

RECOMENDACIONES:

A la Unidad de Informática en coordinación con la comisión de Informática:

1. Realizar e implementar una metodología formal para la gestión de riesgos de TI, considerando como mínimo los siguientes aspectos:

    a. Identificación de los potenciales riesgos, a partir de los sistemas críticos identificados.
    b. Determinar cuáles procesos, podrían verse impactados por la materialización del riesgo bajo estudio.
    c. Definición de roles y responsabilidades de las áreas involucradas.
    d. Identificación del riesgo.
    e. Análisis de riesgo (análisis cualitativo y cuantitativo, así como un mapa de riesgo).
    f. Evaluación de riesgo (descripción del impacto del riesgo en términos comprensibles al negocio).
    g. Administración del riesgo, estableciendo estrategias de tratamiento del riesgo (evitar, mitigar, transferir o aceptar) y los controles requeridos.
    h. Aceptación del riesgo por parte de las áreas involucradas.
    i. Plan o procedimiento de comunicación a nivel de la organización.
    j. Revisión y monitoreo.

2. Presentar la metodología de gestión de riesgos de TI ante la Comisión de Informática para su respectiva aprobación, y una vez aprobada comunicarla a todas las unidades involucradas.

3. Realizar un análisis de riesgos periódicamente y actualizar los riesgos según los resultados obtenidos, al menos una vez al año.

HALLAZGO 05: CUMPLIMIENTO PARCIAL DEL DECRETO EJECUTIVO 37549-JP. RIESGO BAJO.

CONDICIÓN:

Producto del Informe Anual e Inventario realizado por uno de los ingenieros de la Unidad de Informática, se confirmó que se realizó una evaluación para verificar los inventarios de equipos, software y licenciamiento, y así cumplir con el Decreto Ejecutivo 37549-JP (Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central), no obstante, el Artículo 3 establece que se debe realizar una auditoría interna o externa para este informe, por lo que la persona

encargada de realizar dicho estudio no cumplió con el requisito de independencia que debe de tener toda auditoría.

CRITERIO:

El **artículo 3** presente en el Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central emitido bajo el Decreto Ejecutivo 37549-JP indica: *"Cada Ministerio e Institución adscrita al Gobierno Central, deberá realizar anualmente una auditoría interna o externa según las propias posibilidades presupuestarias y organizacionales para determinar el cumplimiento de las disposiciones tendientes a la protección de los derechos de autor, relativos a los programas de cómputo; mediante la auditoria se deberá verificar los equipos existentes y los programas que tengan las computadoras, así como el número de copias autorizadas de cada programa, comprobando la fecha de instalación, versión de cada uno y ajustado a los términos de licenciamiento."*

RECOMENDACIONES:

A la Unidad de Auditoría Interna:

1. Realizar una auditoría interna para determinar el cumplimiento de las disposiciones tendientes a la protección de los derechos de autor, relativos a los programas de cómputo.

2. Abarcar en la auditoría la verificación de los siguientes aspectos:

    a. Equipos existentes.
    b. Programas instalados en cada computadora.
    c. Copias autorizadas por cada programa.
    d. Fecha de instalación.
    e. Versión de cada programa.
    f. Términos del licenciamiento.

3. Producto de la auditoría realizada, presentar un informe anual dentro del primer semestre de cada año ante el Registro de Derechos de Autor y Derechos Conexos.

A la Unidad de Informática:

4. Para cada equipo llevar un expediente u hoja de vida donde se indique el funcionario responsable que autoriza la instalación, fecha de instalación y la persona responsable de hacer la instalación.

HALLAZGO 06: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO.

CONDICIÓN:

Producto de la revisión del cuarto de servidores de la Unidad de Informática del Museo Nacional de Costa Rica (MNCR), se determinó que existen debilidades de seguridad física, las cuales se enlistan a continuación:

1. Uso de un llavín tipo convencional.
2. Se utiliza una puerta de vidrio que colinda con el exterior.
3. Hay una pared de Gypsum.
4. No se cuenta con un aire acondicionado de respaldo.
5. No hay detectores de humo.
6. No se cuenta con medidores de temperatura ni de humedad para el cuarto de servidores.
7. No se cuenta con una bitácora de accesos.
8. El aire acondicionado se encontraba goteando al momento de la revisión. Se colocó una bolsa plástica para desviar el líquido y que no afecte los equipos electrónicos.
9. No se cuenta con bitácoras del mantenimiento de las UPS.
10. Existe un tanque de agua dentro de las instalaciones del cuarto de servidores, el mismo posee tuberías expuestas, el tanque queda aproximadamente a tres metros de los servidores principales.

Además, se verificó que no se cuenta con un sitio exclusivo para el cuarto de servidores, si no que se ubica dentro de la misma área en la que se encuentran las oficinas de informática, por lo cual se comparte el espacio físico, aire acondicionado y la entrada.

Al no cumplir con medidas de seguridad física en los cuartos de servidores se expone a los siguientes riesgos:

1. Amenazas no identificadas a la seguridad física.
2. Acceso no autorizado por terceros en caso de que se fuerce la entrada a través de la ventana o la puerta de vidrio.
3. No se lleva un control adecuado del personal externo que visite el cuarto de servidores.
4. Inadecuada seguridad de los equipos del cuarto de servidores.
5. Riesgo de exposición del equipo ante terceros.
6. No se lleva un adecuado control de los factores ambientales del cuarto de servidores.

7. En la misma área del aire acondicionado se encuentra un tomacorriente, quedando expuesto al goteo, lo cual puede causar un incendio en cualquier momento.
8. En las mismas instalaciones de informática se cuenta con un tanque de agua, el cual puede tener filtraciones de agua, y si se presentará en horario no laboral, no hay mecanismos para detectar tal situación, quedando expuestos todos los equipos computacionales.

CRITERIO:

El apartado **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 menciona: *"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:

A la Unidad de Informática:

1. Valorar reforzar la entrada al área de TI, utilizando una puerta de un material que no sea fácil de vulnerar y con un tipo de llavín apropiado para garantizar la seguridad del sitio, de ser factible agregar mecanismos automáticos como alarmas en caso de ser forzada la puerta.

2. Gestionar la reparación o cambio del aire principal para eliminar el goteo de este, además valorar la adquisición de un aire acondicionado de respaldo, en caso de que se presente una falla en el aire acondicionado principal.

3. Instalar detectores de humo en el cuarto de servidores, con el fin de contar con alarmas para detectar posibles incendios en el sitio.

4. Instalar medidores de temperatura, humedad y agua, de modo que se pueda llevar un mejor control del ambiente y que este no dañe los equipos.

5. Implementar una bitácora de control de ingreso al cuarto de servidores en donde se registren las visitas de externos y se documente como mínimo lo siguiente:

    a. Nombre del visitante.
    b. Fecha de la visita.
    c. Motivo de la visita.
    d. Hora de ingreso y hora de salida.
    e. Firma del visitante.

6. Mantener un registro del mantenimiento que se realiza a las UPS.

7. Realizar un estudio de riesgos respecto a la ubicación del tanque de agua y las demás deficiencias detectas, analizar las vulnerabilidades, amenazas, riesgos e impactos que el Museo está asumiendo al presentarse las situaciones actuales.

A la Comisión de Informática:

8. Analizar las vulnerabilidades señaladas, priorizarlas y gestionar su corrección de acuerdo con los recursos y posibilidades que posee el Museo.

HALLAZGO 07: DEBILIDADES EN LA ADMINISTRACIÓN DE ACCESOS DE LOS USUARIOS EN LOS SISTEMAS DE INFORMACIÓN. RIESGO MEDIO.

CONDICIÓN:

a) Sobre el procedimiento de registro de usuarios en red

Se determinó que el procedimiento de registro de usuarios en red (DIRG-UI-006) indica que en caso de que se requiera crear, deshabilitar o modificar los permisos que posee un usuario en un sistema de información, se deberá de tramitar la solicitud a la Unidad de Informática. Sin embargo, no se indica que se deban realizar revisiones periódicas de todas las cuentas y sus privilegios relacionados, tal como lo mencionan las Normas Técnicas para para la gestión y el control de las Tecnologías de Información y las buenas prácticas como COBIT.

De acuerdo con lo indicado por el jefe de la Unidad de Informática, no se realizan monitoreos de los sistemas de información, dado que es responsabilidad del área usuaria indicar cuándo se debe crear o deshabilitar un usuario o modificar los permisos que este posea sobre un módulo o programa determinado.

Además, se identificó que la introducción, el objetivo general y los objetivos específicos hacen referencia al proceso de compra de equipo informático y de software en el Museo Nacional de Costa Rica, por lo que, no son alusivos a este procedimiento.

b) Sobre la existencia de cuentas de exfuncionarios activas

Al verificar los usuarios que se encuentran activos en el correo electrónico institucional, se identificó la existencia de seis cuentas activas de exfuncionarios, las cuales se muestran a continuación:

Año	Funcionario	Correo	Fecha de salida
2017	Danny Fallas Obando	dfallas@museocostarica.go.cr	24 de febrero
	Guisella Chaves Guevara	gchavez@museocostarica.go.cr	30 de junio
2018	Gilberth Mesén Segura	gmesen@museocostarica.go.cr	01 de enero
	Pablo Murillo Segura	pmurillo@museocostarica.go.cr	01 de abril
	Grace Castro Solano	gcastro@museocostarica.go.cr	08 de abril
	Benjamín Sánchez Leandro	bsanchez@museocostarica.go.cr	18 de mayo

Al haber cuentas de correo activas pertenecientes a exfuncionarios de la institución, se corre el riesgo de que el correo sea utilizado incorrectamente o terceras personas posean acceso a información confidencial y esta sea mal utilizada, por medio de cuentas de usuario que estén disponibles debido a la ausencia de controles de seguridad, tales como el monitoreo periódico de dichas cuentas y sus permisos asociados.

CRITERIO:

Según el punto **1.4.5 "Control de acceso"** del proceso **1.4 "Gestión de la seguridad de la información"**, presente en las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), establece que la organización: *"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.".*

Así mismo, el "DIRG-UI-006_Manual Procedimiento Registro Usuarios Red" establece que, cuando se deba crear o deshabilitar una cuenta de usuario o modificar los permisos que este posee, se deberá de tramitar la solicitud a la Unidad de Informática, para que esta realice lo solicitado de acuerdo con las necesidades expuestas por el usuario.

RECOMENDACIONES:

A Recursos Humanos:

1. Notificar oportunamente la Unidad de Informática, el cambio en las condiciones laborales de una persona con el fin de que se proceda con la debida actualización o eliminación de su cuenta de usuario asociada en la plataforma tecnológica.

A las áreas usuarias en conjunto con la Unidad de Informática:

2. Definir la periodicidad con la cual se debe de realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben de generar.

A la Unidad de Informática:

3. Deshabilitar las cuentas de usuario de funcionarios que cesan sus labores para la institución según lo informe Recursos Humanos.

4. Incluir en el procedimiento DIRG-UI-006_Manual Procedimiento Registro Usuarios Red la periodicidad con la cual se debe de realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben de generar, según lo acordado con las áreas usuarias.

5. Modificar la introducción, el objetivo general y los objetivos específicos del procedimiento contenido en DIRG-UI-006_Manual Procedimiento Registro Usuarios Red, de modo que sean alusivos a este.

6. Realizar las gestiones para que el procedimiento sea aprobado formalmente con los nuevos cambios.

HALLAZGO 08: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LAS BASES DE ACTIVOS SIBINET Y BOS. RIESGO MEDIO.

CONDICIÓN:

A partir del análisis realizado a las bases de activos del sistema BOS y SIBINET con corte al 31/12/2017, se encontraron inconsistencias en la información almacenada. Cabe mencionar que tanto el sistema BOS como el SIBINET deberían poseer la misma información, para el análisis se hizo la separación entre activos y otros bienes históricos y culturales diversos.

Tabla 1 Información suministrada

Resumen información				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
SIBINET Activos	6 009	10 566 254 360,57	1 323 533 793,92	9 242 720 566,65
BOS Activos	4 680	10 319 189 974,72	1 547 001 146,28	8 772 188 828,44
SIBINET Otros Bienes	12	54 429 011 808,00	-	54 429 011 808,00
BOS Otros Bienes	11	54 421 011 808,00	-	54 421 011 808,00
Diferencia Activos	1 329	247 064 386	-223 467 352	470 531 738
Diferencia Otros Bienes	1	8 000 000	-	8 000 000

De la información suministrada la cual se observa en la tabla 1 se determinó que hay una diferencia de 1.329 activos entre los reportes brindados de cada uno de los sistemas, además hay 1.340 activos que únicamente están registrados en el SIBINET y 11 activos que solo se encuentran en el BOS como se muestra en la tabla 3, lo cual provoca diferencias en el valor de compra, depreciación acumulada y valor en libros. En el caso de otros bienes históricos y culturales diversos, se verificó que existen un registro en la base de SIBINET que no está en el BOS, produciendo una diferencia en el valor de compra y valor de libros de ¢8.000.000.

Tabla 2 Información registrada en ambas bases

Resumen registros en ambas bases				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
SIBINET Activos	4 669	10 317 920 152,72	1 262 322 879,26	9 055 597 273,46
BOS Activos	4 669	10 317 920 152,72	1 546 189 592,63	8 771 730 560,09
SIBINET Otros Bienes	11	54 421 011 808,00	-	54 421 011 808,00
BOS Otros Bienes	11	54 421 011 808,00	-	54 421 011 808,00
Diferencia Activos	-	-	- 283 866 713,37	283 866 713,37
Diferencia Otros Bienes	-	-	-	-

Para los 4.669 activos registrados en ambas bases como se observa en la tabla 2, se encontró una diferencia en la depreciación acumulada de ¢283.866.713, ya que el valor en libros de SIBINET es mayor al valor en libros del BOS. En el caso de los 11 registros de otros bienes históricos y culturales no se observaron diferencias, excepto el registro que solamente se encuentra en SIBINET, el cual fue abarcado en la tabla 1.

En la siguiente tabla se detalla el monto en colones de los 11 registros que únicamente se encuentran en el BOS y los 1341 registros que se ubican en SIBINET.

Tabla 3 Información en únicamente un sistema

Resumen registros solo en el BOS				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
BOS Activos	11	1 269 822,00	811 553,65	458 268,35
BOS Otros Bienes	-	-	-	-

Resumen registros solo en SIBINET				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
SIBINET Activos	1 340	248 334 207,85	61 210 914,66	187 122 793,19
SIBINET Otros Bienes	1	8 000 000,00	-	8 000 000,00

Al presentarse las inconsistencias mostradas anteriormente, se pierde los principios de integridad y confiabilidad de la información, dado que, dependiendo de la base utilizada, los resultados serán diferentes, además puede provocar inconsistencias en otros procesos del Museo que a futuro generen consecuencias mayores.

CRITERIO:

El apartado **4.3 "Administración de los datos"** 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: *"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".*

RECOMENDACIONES:

Al Departamento Administrativo y Financiero en conjunto con la Unidad de Informática:

1. Realizar una depuración en conjunto con los responsables de la administración de los activos en ambos sistemas, para corregir las inconsistencias detectadas.

2. Analizar y establecer mecanismos de control que validen los campos donde se presentan las inconsistencias.

HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE PROBLEMAS. RIESGO BAJO.

CONDICIÓN:

Se determinó que el Museo Nacional de Costa Rica no cuenta con un procedimiento para la gestión de problemas de TI, en el cual se contemplen aspectos como identificación de incidentes recurrentes, proceso para detectar la causa raíz de los problemas y planes de acción que permitan mejorar o corregir la situación.

Al no tener un procedimiento para la gestión de problemas, se dificultaría minimizar el impacto de los problemas en el negocio que son causados por errores dentro de la infraestructura de TI.

CRITERIO:

Según el proceso **4.5 "Manejo de incidentes"** presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitida por la Contraloría General de la República menciona lo siguiente: *"La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario".*

RECOMENDACIONES:

A la Unidad de Informática:

1. Elaborar un procedimiento para la gestión de problemas de TI, el cual considere al menos los siguientes aspectos.

    a. Identificar problemas mediante incidentes repetitivos o conocidos.
    b. Registro del problema, incluyendo detalles como:

        i. Servicio afectado.
        ii. Priorización y categorización del problema.
        iii. Descripción del problema.
        iv. Detalles de todos los diagnósticos o intentos de recuperación tomados.

    c. Determinar la causa raíz del problema.
    d. Definir un plan de acción para la resolución de problemas.
    e. Definir el proceso de cierre del problema.

2. Mantener un registro de errores conocidos con el fin de que se tenga conocimiento de la causa raíz y la solución de problemas que han ocurrido, de modo que si surgen problemas adicionales esto represente una fuente de información para identificar y restaurar el servicio de una manera más rápida.

3. Se recomienda tomar en cuenta las buenas prácticas de ITIL V3 2011, para realizar el procedimiento de gestión de problemas, ubicado en la Fase de Operación, en el proceso de Gestión de Problemas.

4. Realizar las gestiones para aprobar formalmente el procedimiento.

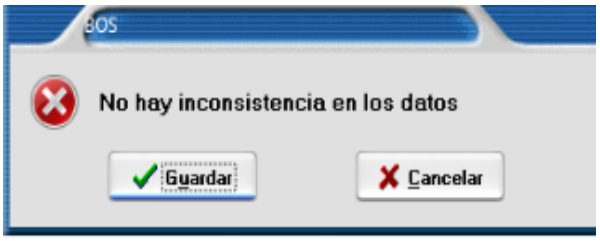
HALLAZGO 10: DEFICIENCIAS EN EL SISTEMA DE INFORMACIÓN BOS. RIESGO MEDIO.

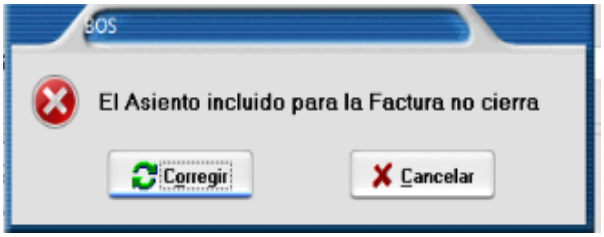
CONDICIÓN:

Se determinó que el sistema de información BOS del Museo Nacional de Costa Rica posee deficiencias a nivel de seguridad lógica, las cuales se identificaron durante la revisión del sistema junto a los usuarios expertos. Dichas deficiencias son las siguientes:

1. No se realiza un proceso de revisión periódico de las pistas de auditoría por parte de las áreas usuarias.
2. Existen usuarios que no les vence la contraseña.
3. No se cuenta con un histórico de claves.
4. El sistema no exige un tamaño de la contraseña mínimo.

En la revisión del módulo de cuentas por pagar se detectó la siguiente irregularidad, el usuario procede a registrar la CxP, al validar el asiento el sistema indica que no hay inconsistencia en los datos, se sigue con el registro y al finalizar, el sistema no permite registrar la CxP, se validó en la revisión que después de cinco intentos de realizar el mismo procedimiento se guardó satisfactoriamente.





Además, en la revisión del módulo de contabilidad se determinó que el estado de flujo de efectivo no se genera correctamente, dado que los montos contenidos en dicho estado no reflejan la realidad del MNCR, por lo que, se debe de generar en Excel.

Al existir las deficiencias antes mencionadas, los sistemas se vuelven susceptibles al error humano, lo cual puede que no se tomen las medidas de seguridad necesarias y comprometan la información de la institución. Si se diera el caso de que las contraseñas sean vulneradas o expuestas a terceros y estas no se cambian periódicamente, existe el riesgo de que terceros mantengan el acceso no autorizado en el sistema. Además, al realizarse el estado de flujo de efectivo en Excel, esto representa un trabajo innecesario que idealmente debería ser ejecutado por el sistema, pudiendo así el personal, dedicarse a otras tareas.

CRITERIO:

El apartado **1.4.5 "Control de acceso"** del proceso **1.4 "Gestión de la seguridad de la información"** 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 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.".

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

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

b. 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.

c. 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.

d. 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.

e. 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.

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

RECOMENDACIONES:

A la Unidad de Informática en conjunto con las Áreas Usuarias:

1. Subsanar las deficiencias identificadas y enlistadas anteriormente, con el fin de evitar posibles vulnerabilidades en la seguridad lógica del sistema.

2. Verificar y determinar la causa del por qué las CxP y el estado de flujo de efectivo no se están realizando satisfactoriamente, en caso de ser necesario, contactar al proveedor para corregir la causa.

II. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CARTA DE GERENCIA 2016	
HALLAZGO 01: NO SE CUENTA CON UN COMITÉ CON LA PARTICIPACIÓN DE LAS ÁREAS USUARIAS PARA LA DEFINICIÓN DE LA ESTRATEGIA DE LA UNIDAD DE INFORMÁTICA. RIESGO MEDIO.	
RECOMENDACIÓN	***A la administración en coordinación con la Unidad de Informática:*** 1. Definir un reglamento para la conformación de un comité de tecnologías de información en el MNCR, el cual especifique lo siguiente: a. Objetivos del comité. b. Responsabilidades del comité. c. Miembros que deben conformar el comité, sus roles y responsabilidades. Es importante definir un sustituto para cada miembro para que el comité no deje de funcionar en caso de que alguno de ellos se ausente. d. Lineamientos específicos de gestión del comité, por ejemplo: i. Establecer la periodicidad en la que debe sesionar. Se recomienda que el comité sesione al menos una vez al mes. ii. Establecer un mecanismo de control para documentar los acuerdos tomados, por ejemplo, actas o minutas de cada sesión realizada del comité. iii. Establecer un mecanismo de seguimiento y control de la ejecución y cumplimiento de los acuerdos tomados. 2. Cumplir con los lineamientos establecidos en el reglamento del comité de tecnologías de información.
COMENTARIOS DE LA ADMINISTRACIÓN	Se creo la comisión de informática con el objetivo de cumplir lo estipulado por la Contraloría General de la República.
ESTADO	**CORREGIDO** Por medio del oficio DG-044-2018 se evidencia la creación de una comisión de informática para el Museo Nacional de Costa Rica. Adicional se corroboró reuniones periódicas de este comité.

HALLAZGO 02: AUSENCIA DE UN INVENTARIO GENERAL DE LICENCIAS CENTRALIZADO Y ACTUALIZADO. RIESGO BAJO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Elaborar un inventario general de licencias en el que se indique al menos lo siguiente: 1. El nombre del producto 2. El proveedor 3. La cantidad de licencias activas 4. La cantidad de licencias inactivas 5. La cantidad total 6. Tipo de licencia (volumen o individual) 7. Descripción 8. Responsable de gestionar la licencia 9. Fecha de vencimiento 10. Referencia del contrato 2. Revisar constantemente que el total de licencias registradas en el inventario general coincida con el total de licencias del inventario específico por equipo.
COMENTARIOS DE LA ADMINISTRACIÓN	Se realizó un inventario de licencias, el cual se encuentra centralizado y resguardado por Informática. Se está en proceso de registro de todo el licenciamiento en el sistema GLPI, para mayor control y facilidad de actualización.
ESTADO	**EN PROCESO** Se entregó el Licenciamiento Software 2018, el cual contiene las licencias instaladas y disponibles del Museo Nacional, no obstante, no se ha terminado de implementar, por tal motivo aún se presentan inconsistencias entre el inventario general y el especifico.

HALLAZGO 03: DEBILIDADES EN LA GESTIÓN DE LAS POLÍTICAS DE LA UNIDAD DE INFORMÁTICA. RIESGO BAJO.	
RECOMENDACIÓN	***A la Unidad de Informática en conjunto con las áreas usuarias:*** 1. Llevar un control documentado del seguimiento y cumplimiento de las políticas de TI, como proceso de gestión de la calidad. Además, se deben realizar evaluaciones para determinar si los funcionarios son conscientes de sus responsabilidades y si estos las cumplen. 2. Girar instrucciones a los funcionarios mediante un comunicado oficial del cumplimiento de las políticas de TI y de seguridad de la información. 3. Realizar capacitaciones formales sobre la implementación y cumplimiento de las medidas de seguridad de la información y demás políticas de TI descritas en el Reglamento de Tecnologías de Información. ***4.*** Establecer un lineamiento sobre la revisión por parte de las jefaturas de los accesos de los usuarios a los sistemas y comunicar a la Unidad de Informática los cambios que sean necesarios. Además, se debe establecer una periodicidad de al menos un año entre cada revisión.
COMENTARIOS DE LA ADMINISTRACIÓN	Este es un proceso constante, para ir consolidando a Informática como un pilar estratégico para la consecución de los objetivos Institucionales y Departamentales. Ya se han logrado mejorar muchas de las debilidades encontradas, y cada día se van depurando los procesos operativos.
ESTADO	**PENDIENTE** Aún no se cuenta con un mecanismo para verificar el cumplimiento de la política de seguridad de la información ni con un lineamiento para la revisión de los accesos de los usuarios en los sistemas de información.

HALLAZGO 04: DEFICIENCIAS EN LA PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN EN FUNCIÓN DE LOS OBJETIVOS ORGANIZACIONALES. RIESGO BAJO.	
RECOMENDACIÓN	***A la administración:*** 1. Documentar formalmente los objetivos organizaciones, con el fin de brindar el insumo que requiere la Unidad Informática para generar su plan estratégico. ***A la Unidad de Informática en conjunto con las áreas usuarias:*** 2. Desarrollar un plan estratégico de tecnologías de información, el cual describa los proyectos concretamente que se trabajarán en el periodo de vigencia definido. Dicho PETI debe contener al menos lo siguiente: a. Objetivos de la institución en materia de tecnologías de información. b. Costos relacionados a los proyectos en específico. c. Riesgos relacionados al plan estratégico y su cumplimiento. Incluir un análisis de riesgo completo según la metodología para la gestión de riesgos. d. Definir las actividades que se realizarán según los objetivos que quiera alcanzar el negocio. e. Definir un conjunto de métricas e indicadores que ayuden a llevar un control del seguimiento del PETI. f. Identificar requerimientos legales y/o regulatorios 3. Alinear el plan estratégico de TI con los objetivos del negocio, y mantener un control continuo de su ejecución, a través del cumplimiento de metas y evaluación de métricas o indicadores. 4. Alinear el plan anual operativo de tecnologías de información, detallando los proyectos y las actividades que conlleva su desarrollo, considerando lo siguiente: a. Detalle de los proyectos que se planean realizar durante el periodo, según lo definido en el PETI.

	b. Identificar los recursos de TI (personal, equipo, procedimientos, etc.) que requieren los proyectos definidos. c. Desarrollar el plan presupuestario alineado al plan anual operativo. d. Monitorear logros y utilización de recursos de TI y presupuesto. e. Identificar los servicios que administran de forma activa, incluyendo los servicios nuevos producto del desarrollo de los proyectos y los servicios a lo que se les da mantenimiento. 5. Elaborar informes de seguimiento al menos cada tres meses, con el fin de dar seguimiento periódico al avance de los proyectos y corregir posibles desviaciones. 6. Documentar formalmente los planes descritos anteriormente y presentarlos ante la alta dirección para que sean evaluados y aprobados formalmente.
COMENTARIOS DE LA ADMINISTRACIÓN	Se desarrolló el PETI, sin embargo, aún se carece de un Plan Estratégico Institucional que consolide los objetivos y planes de cada Departamento.
ESTADO	**EN PROCESO** De acuerdo con las deficiencias expuestas en este hallazgo se presenta lo siguiente para este periodo: • Aún no se cuenta con un Plan Estratégico Institucional vigente. El último que se desarrolló fue para el periodo 2008-2012, el cual fue actualizado en el 2009, por lo que, esta condición se mantiene igual a la expuesta en el hallazgo. • Se desarrolló un PETI para el periodo 2018-2021, sin embargo, este aún no ha sido aprobado. Esta condición está en proceso, puesto que solo faltaría su aprobación. • El PAO 2017 no se encuentra alineado al PETI debido a que este último fue elaborado para el periodo 2018-2021. Esta condición se mantiene igual a la expuesta en el hallazgo. • El seguimiento al PAO se da a través de informes que se le presentan a la administración de forma anual, por lo que, no se da un seguimiento periódico al avance de los proyectos. Esta condición se mantiene igual a la expuesta en el hallazgo. Basado en lo anterior, el hallazgo está en proceso debido a que, de las recomendaciones propuestas, solo se cumplió con la elaboración del PETI, las demás están pendientes de realizarse.

HALLAZGO 05: INEXISTENCIA DE ESTUDIOS DE VULNERABILIDAD DE LA RED DEL MUSEO NACIONAL DE COSTA RICA. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Realizar un estudio de vulnerabilidad de la red para identificar las posibles brechas de seguridad que puedan comprometer la integridad, disponibilidad y confiabilidad de la información y los servicios de TI. El estudio debe considerar entre otras cosas: a. La configuración y parametrización de los dispositivos de comunicación. b. Pruebas de penetración. c. Transferencia de información sensible cifrada a través de la red. d. Monitoreo de software malicioso. e. Uso y configuración de firewalls, segmentación de redes y detección de intrusos. f. Análisis de puertos. g. Uso de conexiones seguras con puntos externos a la institución.
COMENTARIOS DE LA ADMINISTRACIÓN	Se implementó una nueva red de datos, la cual permite el monitoreo constante de cada punto de red.
ESTADO	**PENDIENTE** A pesar de que se instaló una nueva red de datos, no se han elaborado estudios de vulnerabilidad de la red, por lo cual, este hallazgo se encuentra pendiente.
HALLAZGO 06: CUENTAS HABILITADAS DE EXFUNCIONARIOS EN EL ACTIVE DIRECTORY, CORREO ELECTRÓNICO Y BASE DE DATOS. RIESGO MEDIO.	
RECOMENDACIÓN	***A Recursos Humanos en conjunto con la Unidad de Informática:*** 1. Establecer un procedimiento en el cual se informe formalmente a la Unidad de Informática de las salidas de personal para la inactivación inmediata de las cuentas de usuario asociadas a dicho funcionario. ***A la Unidad de Informática:*** 2. Deshabilitar las cuentas de usuario de funcionarios que cesan sus labores para la institución según lo informe el Departamento de Recursos Humanos.
COMENTARIOS DE LA ADMINISTRACIÓN	Se deshabilitaron las cuentas y se mantiene un monitoreo constante.
ESTADO	**CORREGIDO**

	Las cuentas identificadas como activas y que pertenecían a exfuncionarios del MNCR, no estaban en los registros de usuarios activos suministrados para este periodo, por lo cual este hallazgo se encuentra corregido.
HALLAZGO 07: AUSENCIA DE PROCEDIMIENTOS PARA LA ADMINISTRACIÓN, MIGRACIÓN, MANTENIMIENTO Y CONFIGURACIÓN DE LA SEGURIDAD DE LAS BASES DE DATOS. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Elaborar y documentar los procedimientos realizados por la Unidad de Informática para la gestión de bases de datos. Para ello, se debe considerar: a. Instalación: Se debe definir el responsable de llevar a cabo dicho procedimiento e indicar los pasos y parámetros de configuración que requiere el motor de bases de datos. Si la instalación se realiza sobre uno o más servidores virtuales, incluir el procedimiento de su instalación incluyendo los parámetros de la configuración respectiva (recursos del servidor, configuración de red, dominio del servidor, etc.). b. Administración: Se debe indicar los responsables de administrar y monitorear las bases de datos. Además, se debe definir indicadores de rendimiento y uso de recursos de las bases de datos. c. Migración: Elaborar un procedimiento el cual incluya el detalle de los pasos para gestionar y traspasar los datos (incluyendo procesos de conversión de datos si es necesario). En el procedimiento se debe establecer los responsables y las ventanas de tiempo requeridas para llevar a cabo la migración. d. Mantenimiento: Elaborar un procedimiento o manual que indique los pasos para dar mantenimiento a las bases de datos, incluyendo el o los responsables, el detalle de la estructura de la base de datos, la ventana de tiempo sobre la cual se trabajará (en un ambiente de desarrollo/pruebas) y la ventana de tiempo sobre la que se pasarán los cambios (en el ambiente de producción). También se debe monitorear los recursos consumidos por la base de datos y generar reportes periódicos, con el fin de controlar los momentos en los que el servidor requiera aumentar la capacidad. e. Seguridad: Definir el procedimiento para configurar y parametrizar la seguridad de las bases de datos considerando la disponibilidad, confiabilidad e integridad de los datos.

COMENTARIOS DE LA ADMINISTRACIÓN	Se creo el procedimiento.
ESTADO	**PENDIENTE** De acuerdo con lo indicado por el jefe de la Unidad de Informática, actualmente no se cuenta con un procedimiento para la gestión de las bases de datos del Museo Nacional, el cual incluya la descripción de aspectos como la instalación, monitoreo, configuraciones de seguridad y mantenimiento de estas. Dada esta situación, el estado del hallazgo es pendiente.
HALLAZGO 08: DEFICIENCIAS EN LA GESTIÓN DE RESPALDOS DE INFORMACIÓN. RIESGO BAJO.	
RECOMENDACIÓN	***A la Unidad de Informática*** 1. Desarrollar un procedimiento detallado para la elaboración de respaldos y recuperaciones de información lo siguiente: a. Detalle de las tareas que son requeridas para desarrollar un respaldo de información. b. Tipos de respaldos a realizar (completos, incrementales, diferenciales). c. Nomenclaturas de los archivos de respaldo. d. Rutas de almacenamiento. e. Acceso a los respaldos. f. Procedimiento detallado para la ejecución de recuperaciones de respaldos de información. g. Periodicidad de los respaldos. h. Periodicidad de las pruebas a los respaldos. 2. Generar bitácoras de los respaldos realizados para llevar un control de las copias que se ha realizado de la información. 3. Generar bitácoras de las pruebas realizadas a los respaldos de información para llevar un control de estas.
COMENTARIOS DE LA ADMINISTRACIÓN	Se creo el procedimiento.
ESTADO	**PENDIENTE** En los procedimientos “DIRG_UI-007_Manual Procedimiento Respaldo Base de Datos” y el “DIRG_UI-009_Manual Procedimiento Respaldo de Información”, no se indica un detalle de las tareas requeridas para realizar los respaldos, el tipo de respaldo a realizar, nomenclatura de los archivos de respaldo, periodicidad, procedimiento para llevar a cabo la restauración de los respaldos de información, etc. Además, tampoco se

	generaron las bitácoras que evidencien tanto los respaldos como las pruebas realizadas a dichos respaldos en el periodo 2017. Dado lo anterior, este hallazgo se encuentra pendiente.
HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS. RIESGO BAJO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Elaborar, aprobar y divulgar procedimientos para la gestión de cambios en la Unidad de Informática. Para ello, se debe considerar: a. La descripción del procedimiento de cambios que tome en cuenta: i. Impacto del cambio (según categoría y priorización). ii. Proceso de cambios de emergencia. iii. Estado del cambio. iv. Revisión post-implantación. v. Riesgos asociados al cambio. vi. Plan de implementación (incluyendo un cronograma). b. Un control de cambios que incluya la fecha, la versión, responsable y los involucrados. c. Costos relacionados a la implementación del cambio. d. Alcance del cambio. e. Métricas o indicadores para medir la calidad del cambio. 2. Comunicar los resultados del cambio a todos los usuarios que se ven directamente impactados y brindar la capacitación requerida.
COMENTARIOS DE LA ADMINISTRACIÓN	Se creo el procedimiento.
ESTADO	**CORREGIDO** Se comprobó la existencia del procedimiento “DIRG-UI-010 Manual procedimiento control de cambios” que contiene la descripción de los pasos a seguir para realizar cambios en los sistemas de información, el cual fue aprobado por la Junta Administrativa del Museo Nacional y entró a regir el 29 de agosto del 2018.

	Además, la Unidad Informática, indicó que para los cambios en hardware se pone en práctica el procedimiento "DIRG-UI-001 Manual procedimiento asignación de hardware y software", el cual entró a regir en junio del 2017 Dado lo anterior, este hallazgo se encuentra corregido puesto que se creó un procedimiento para la gestión de cambios en sistemas de información y otro para cambios en hardware.
HALLAZGO 10: FALTA DE PRUEBAS AL PLAN DE CONTINUIDAD Y AUSENCIA DE CAPACITACIONES AL PERSONAL RESPECTO A LA IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Elaborar un plan de pruebas que abarque todas las actividades de continuidad definidos en el plan. 2. Ejecutar las pruebas en intervalos de tiempo que no generen interrupciones en la operación normal del MNCR y según lo establecido en el plan de pruebas. Es recomendable ejecutar las pruebas de forma gradual, es decir, no generar pruebas de todos los protocolos a la vez, sino planificar las pruebas a lo largo del periodo. 3. Elaborar un informe con los resultados de la prueba utilizando un formato estándar. El informe debe contener al menos: a. El equipo de trabajo que participó en la ejecución de la prueba (nombre y rol que desempeñó). b. El tipo de prueba que se realizó. c. Fecha y hora en que se realizó la prueba. d. Servicios de TI o protocolos del plan de pruebas que fueron parte de la prueba. e. Equipo utilizado para ejecutar la prueba (PC's, switch, servidores, etc.). f. Descripción del proceso de la prueba. g. Análisis cuantitativo de resultados obtenidos contra los resultados esperados, de acuerdo con las métricas definidas en el plan (tiempos de recuperación, pérdida de información, etc.). h. Conclusiones de la prueba. i. Lecciones aprendidas de la prueba. ***A Recursos Humanos en conjunto con la Unidad de Informática:***

	4. Desarrollar un plan de capacitación que considere a todos los miembros involucrados e interesados en el plan de continuidad. 5. Elaborar un informe con los resultados de la capacitación, incluyendo el personal que participó y los temas tratados en la capacitación (protocolos vistos, medidas, objetivos, etc.).
COMENTARIOS DE LA ADMINISTRACIÓN	Aún se está en desarrollo de la actualización del Plan de Continuidad. Se tiene planificado finalizarlo para el primer trimestre del 2019.
ESTADO	**PENDIENTE** Por medio del oficio UI-2018-O-0084, la Unidad de Informática indica que se está en proceso de actualización del plan de continuidad, y estaría listo para el primer trimestre del 2019. Actualmente no se realizan pruebas ni capacitaciones asociadas al plan de continuidad.
HALLAZGO 11: NO EXISTE UNA METODOLOGÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Gerencia General:*** 1. Establecer una metodología que permita verificar que se cumpla con las políticas, procedimientos y lineamientos referentes a tecnologías de información. Esta metodología debe considerar las evaluaciones de control sobre los procesos establecidos con los terceros que brinden servicios de TI. 2. Establecer procesos o procedimientos para asegurar que las actividades de control se cumplan y las excepciones son prontamente reportadas, seguidas y analizadas. Asegurar que las acciones correctivas sean escogidas e implementadas apropiadamente. 3. Mantener el sistema de control interno de T.I., considerando cambios continuos en el ambiente de control organizacional, relevante a los procesos de negocio y riesgos de TI. Si las brechas existen, evaluar y recomendar cambios. 4. Evaluar periódicamente el desempeño del marco de trabajo de control interno de T.I.

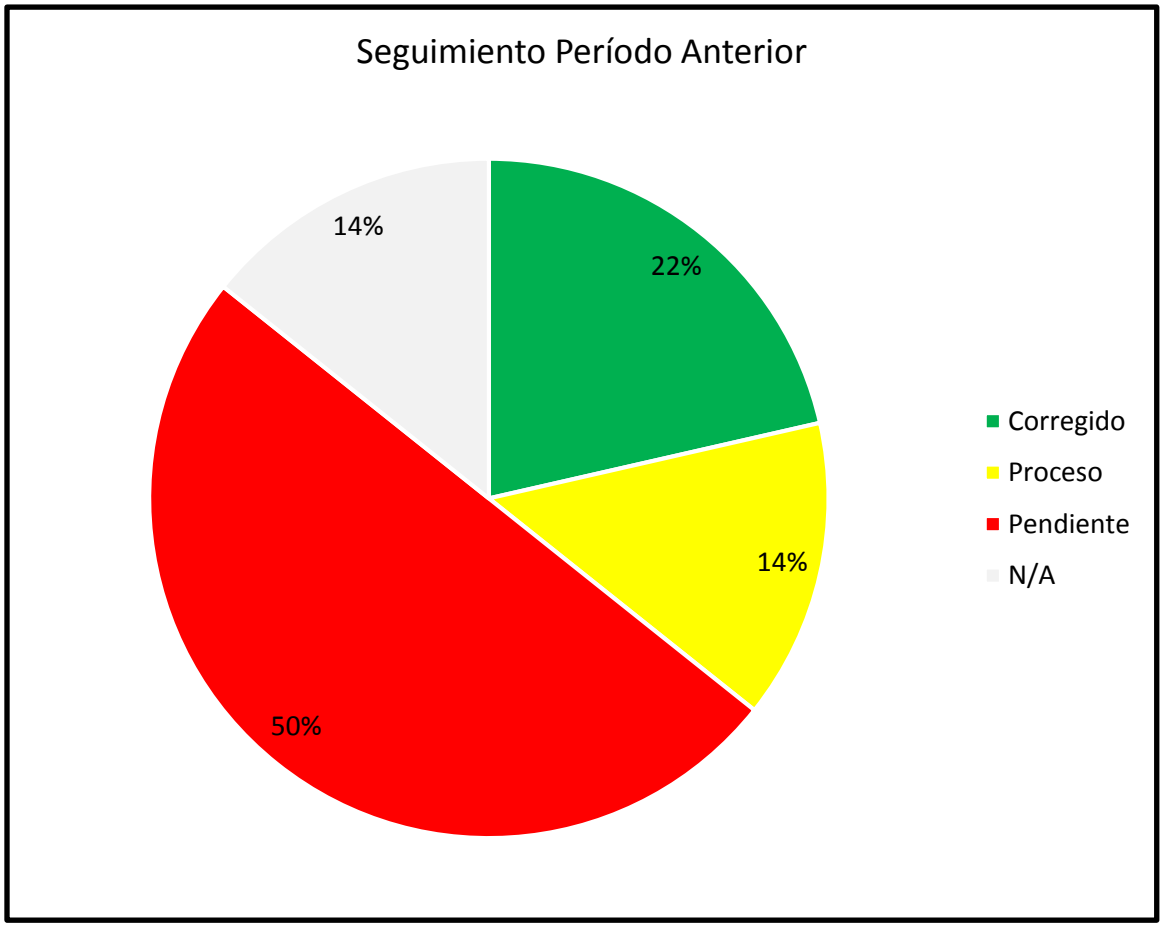
	5. Establecer un proceso para generar excepciones de control en caso de ser requeridos. Cada excepción de control realizada debe estar acompañada de las acciones correctivas respectivas.
COMENTARIOS DE LA ADMINISTRACIÓN	Se está a la espera de la metodología de evaluación del control interno Institucional, para alinear la metodología de TI.
ESTADO	**PENDIENTE** De acuerdo con lo indicado por la Unidad de Informática, la evaluación de control interno se realiza por medio de los planes de trabajo anuales, así como con los proyectos desarrollados durante el periodo respectivo. Dado esto, aún no se ha desarrollado una metodología para la evaluación del control interno de TI y por lo tanto este hallazgo se encuentra pendiente.
HALLAZGO 12: AUSENCIA DE UN PLAN PARA LA IMPLEMENTACIÓN DE LAS NORMAS TÉCNICAS EMITIDAS POR LA CONTRALORÍA PARA LA GESTIÓN DE LAS TI. RIESGO ALTO.	
RECOMENDACIÓN	***A la Unidad de Informática en conjunto con las áreas usuarias:*** 1. Generar un plan de implementación para las Normas Técnicas de la CGR para la gestión de TI, el cual debe contener como mínimo lo siguiente: a. Proceso por implementar, incluyendo el detalle de las actividades. b. Responsable. c. Fecha de inicio. d. Fecha de finalización. e. Presupuesto. 2. Dar seguimiento al avance de la implementación del plan, con el fin de verificar si se cumple con las fechas establecidas o si el mismo requiere ajustes. 3. Presentar el plan ante la administración o Junta Directiva para su respectiva aprobación.
COMENTARIOS DE LA ADMINISTRACIÓN	No se ha iniciado con el plan, ya que primero se debía consolidar la unidad y definir los procesos y procedimientos.
ESTADO	**PENDIENTE** Por medio del oficio UI-2018-O-0084, se indica que la Unidad de Informática todavía no ha desarrollado un plan para la implementación de las normas técnicas de la contraloría para la gestión de las TI.
HALLAZGO 13: DEFICIENCIAS EN EL SISTEMA DE INFORMACIÓN BOS. RIESGO MEDIO.	

RECOMENDACIÓN	***A la Unidad de Informática:*** 3. Subsanar las deficiencias identificadas y enlistadas anteriormente, con el fin de evitar posibles vulnerabilidades en la seguridad del sistema. 4. Vincular el campo "Factura" con el campo "Tipo" de modo que sea consistente el tipo seleccionado con el código de CxP asignado. 5. Reunirse con las áreas usuarias para determinar que campos deben ser obligatorios en los formularios de información, de modo que dichos campos no se puedan dejar en blanco cuando se requiere generar un registro en el sistema. 4. Realizar pruebas exhaustivas para identificar posibles deficiencias en la funcionalidad y la seguridad lógica en el sistema de información.
COMENTARIOS DE LA ADMINISTRACIÓN	Se contrató el mantenimiento y ajustes a las inconsistencias encontradas.
ESTADO	**NO APLICA** Se corrigieron las deficiencias en los módulos, se evidenció la existencia de los manuales del BOS y el cumplimiento de solo poseer una sesión activa, sin embargo, quedan pendientes aspectos de seguridad lógica, por lo cual se procede a realizar un nuevo hallazgo con los aspectos pendientes y las irregularidades detectadas en el momento de la revisión.
HALLAZGO 14: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO.	
RECOMENDACIÓN	***Al Unidad de Informática*** 1. Valorar reforzar la entrada al área de TI, utilizando una puerta de un material que no sea fácil de vulnerar y con un tipo de llavín apropiado para garantizar la seguridad del sitio (llavín de tres puntos, cerraduras magnéticas, etc.).

	2. Valorar la instalación de cámaras de seguridad o alarmas para la detección de intrusos, de tal modo que se pueda alertar la entrada de personas no autorizadas. 3. Valorar la adquisición de un aire acondicionado de respaldo, en caso de que se presente una falla en el aire acondicionado principal. 4. Instalar detectores de humo en el cuarto de servidores, con el fin de contar con alarmas para detectar posibles incendios en el sitio. 5. Instalar medidores de temperatura y humedad, de modo que se pueda llevar un mejor control del ambiente y que este no dañe los equipos. 6. Implementar una bitácora de control de ingreso al cuarto de servidores en donde se registren las visitas de externos y se documente como mínimo lo siguiente: a. Nombre del visitante. b. Fecha de la visita. c. Motivo de la visita. d. Hora de ingreso y hora de salida. e. Firma del visitante. 7. Recargar el extintor de forma oportuna de modo que este se encuentre disponible ante alguna emergencia.
COMENTARIOS DE LA ADMINISTRACIÓN	Se realizaron las siguientes mejoras: 1. Se reforzó la entrada a informática. 2. Se instaló una cámara de seguridad para la entrada. 3. Se está en proceso de adquirir un aire acondicionado de respaldo, en caso de falla en el aire acondicionado principal. 4. Se está en proceso de instalar detectores de humo.
ESTADO	**NO APLICA** Se procede a redactar un nuevo hallazgo con las condiciones actuales, no obstante, efectivamente se realizaron las mejoras indicadas en el comentario de la administración.

Se resume a continuación el cumplimiento de las recomendaciones emitidas en el informe de auditoría anterior:

ESTADO	TOTAL
CORREGIDOS	**3**
EN PROCESO	**2**
PENDIENTES	**7**
N/A	**2**
TOTAL	**14**



III. ANEXOS

ANEXO A

Evaluación funcional del sistema de información BOS implementado en el MNCR

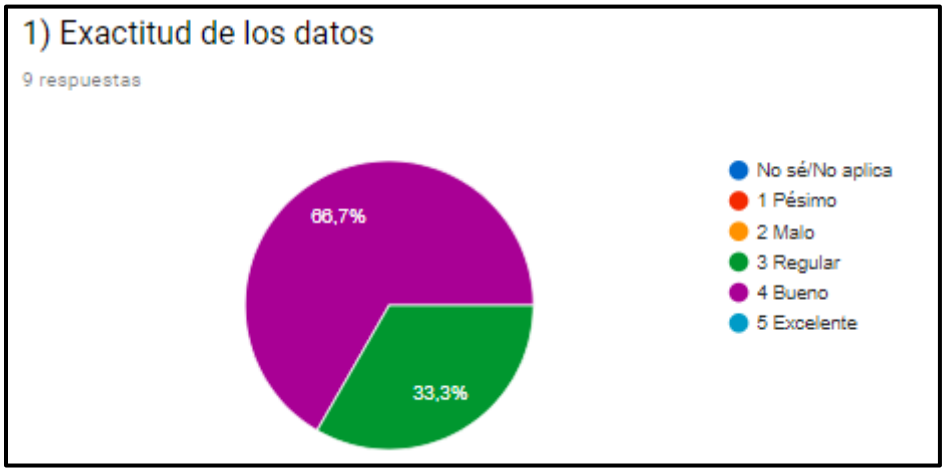
En este apartado se muestra el resultado de la evaluación realizada respecto a la calidad funcional de algunos de los módulos del sistema de información **BOS** según la percepción de nueve usuarios finales de este sistema y sobre el soporte que brinda la Unidad de Informática a los usuarios.

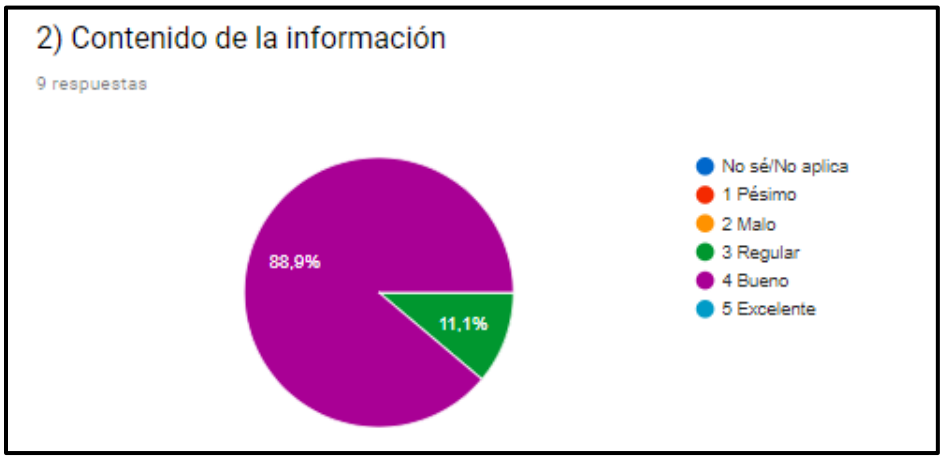
Los módulos del sistema considerados en dicha evaluación se muestran en la siguiente tabla:

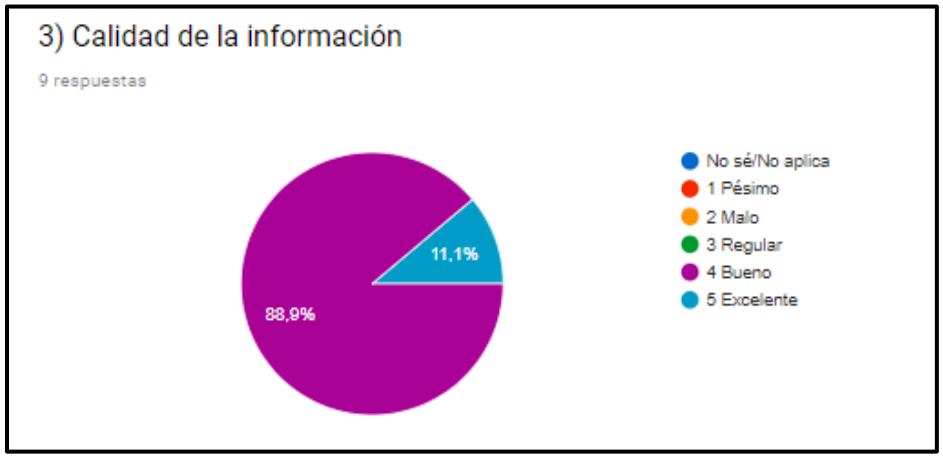
Módulos
Contabilidad
Presupuesto
Bancos
Punto de ventas
Compras
Activos
Inventario
Cuentas por pagar
Nóminas

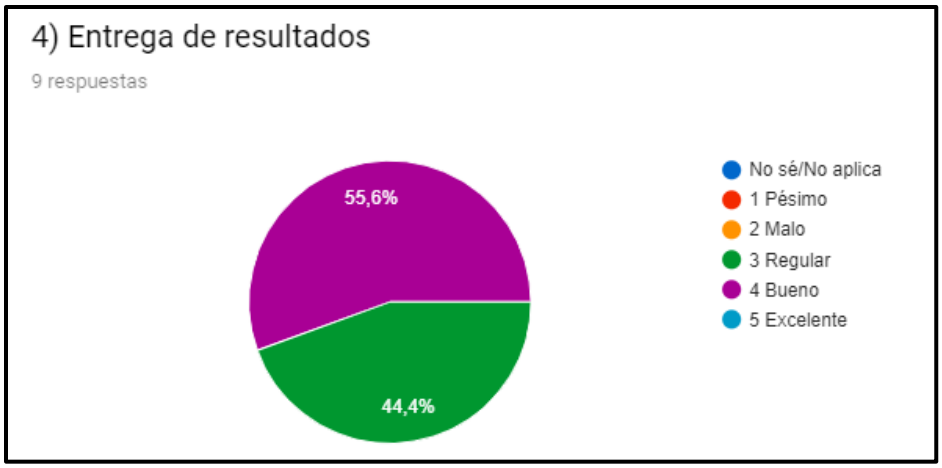
Resultados obtenidos de la evaluación

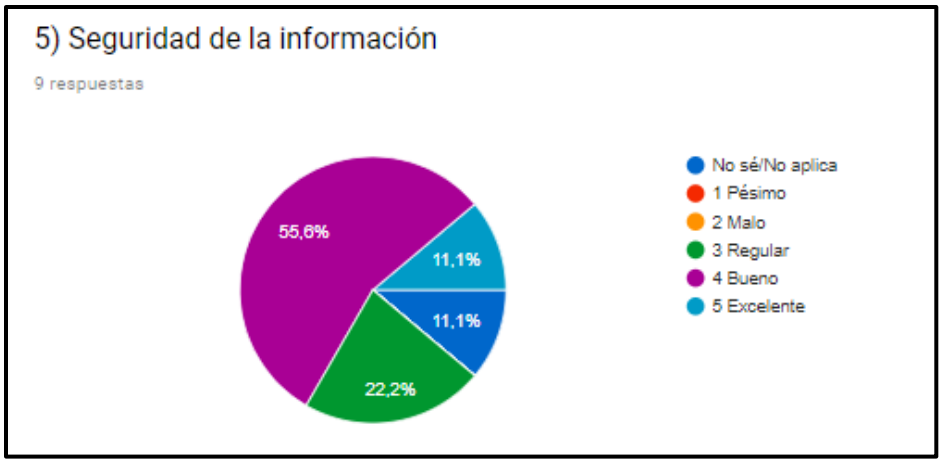
En los siguientes gráficos se muestra un resumen de los resultados obtenidos al aplicar algunas de las preguntas contenidas en el cuestionario:

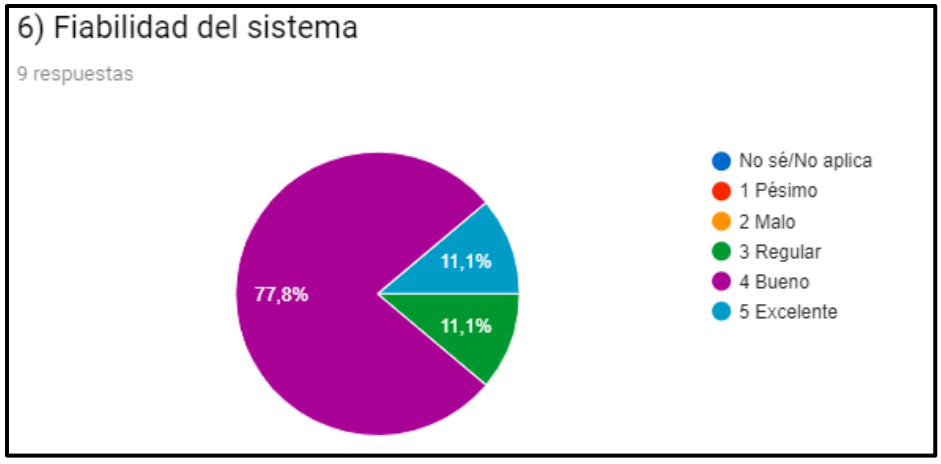


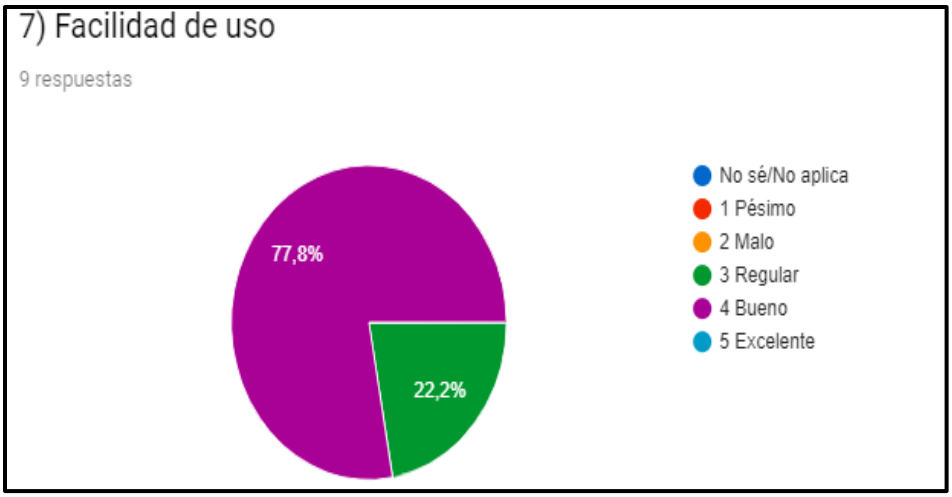


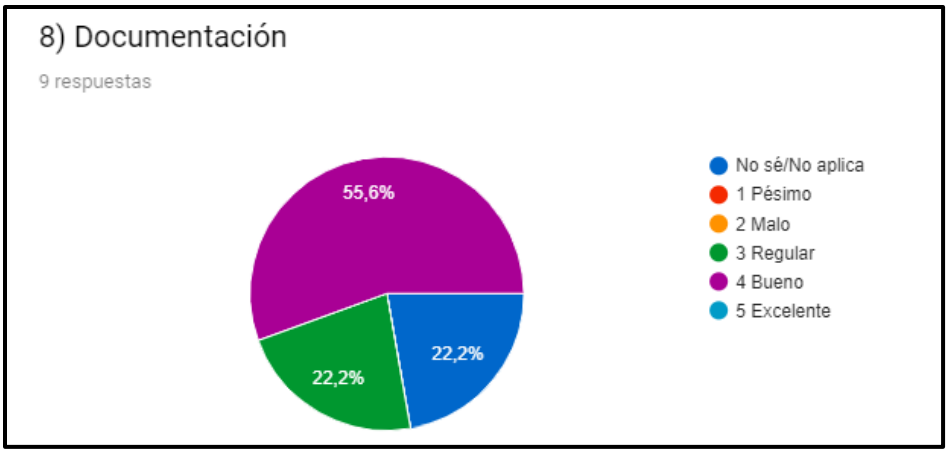


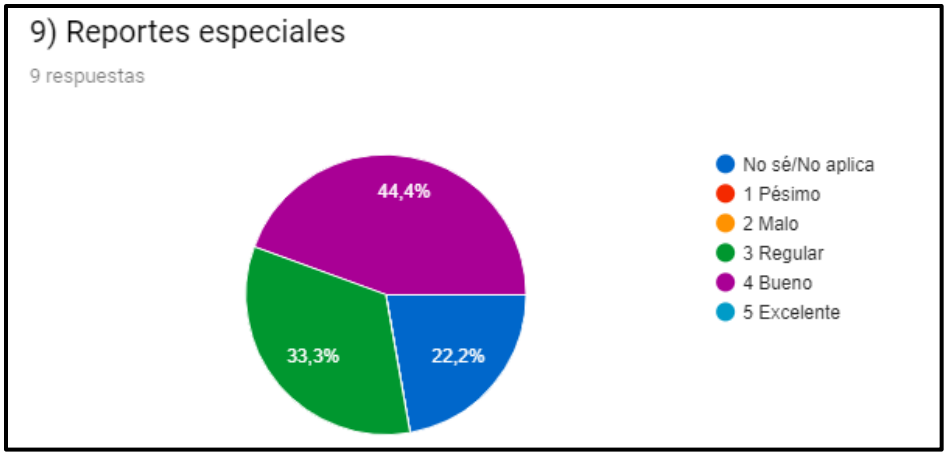

4) Entrega de resultados
9 respuestas
55,6%
44,4%
No sé/No aplica
1 Pésimo
2 Malo
3 Regular
4 Bueno
5 Excelente


5) Seguridad de la información
9 respuestas
55,6%
11,1%
11,1%
22,2%
No sé/No aplica
1 Pésimo
2 Malo
3 Regular
4 Bueno
5 Excelente


6) Fiabilidad del sistema
9 respuestas
77,8%
11,1%
11,1%
No sé/No aplica
1 Pésimo
2 Malo
3 Regular
4 Bueno
5 Excelente


7) Facilidad de uso
9 respuestas
77,8%
22,2%
No sé/No aplica
1 Pésimo
2 Malo
3 Regular
4 Bueno
5 Excelente


8) Documentación
9 respuestas
55,6%
22,2%
22,2%
No sé/No aplica
1 Pésimo
2 Malo
3 Regular
4 Bueno
5 Excelente


9) Reportes especiales
9 respuestas
44,4%
33,3%
22,2%
No sé/No aplica
1 Pésimo
2 Malo
3 Regular
4 Bueno
5 Excelente

Las opciones de respuesta para evaluar cada criterio mostrado en los gráficos anteriores fueron las siguientes:

1. Excelente.
2. Bueno.
3. Regular.
4. Malo.
5. Pésimo.
6. No sé / No aplica.

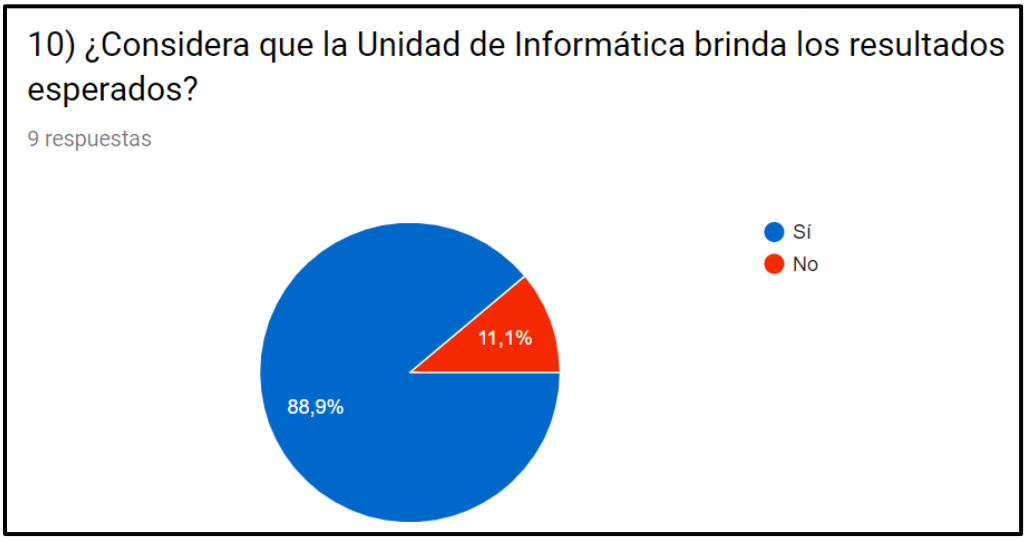
Dado esto, los resultados obtenidos para cada criterio evaluado se mencionan a continuación:

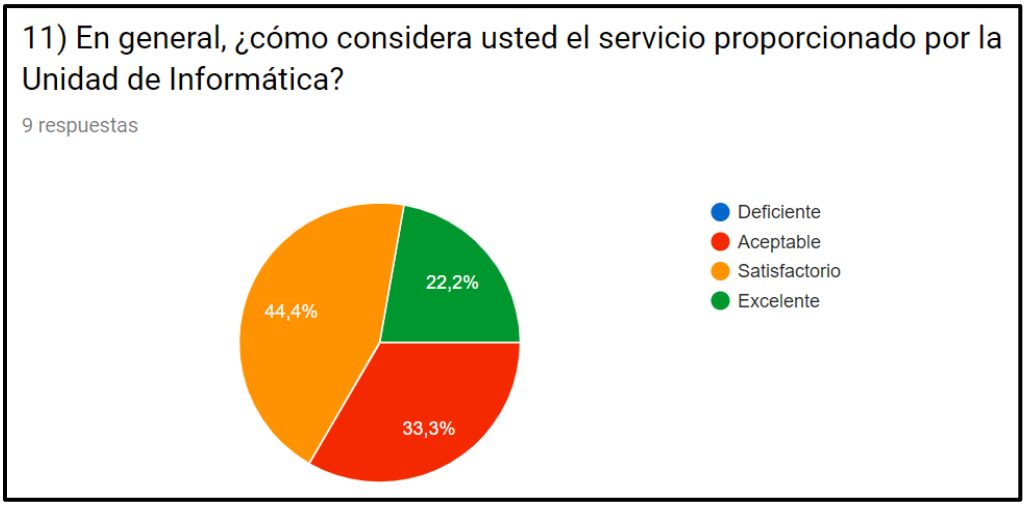
1. **Exactitud de los datos:** En este criterio se evalúa qué tan exactos e íntegros son los datos suministrados por el sistema. El 66.7% de los usuarios indicó que la exactitud de los datos es buena y el 33.3% indicó que esta es regular.
2. **Contenido de la información:** Se evalúa qué tan completa y adecuada es la información suministrada por el sistema para la toma de decisiones. El 89.9% de los usuarios indicó que el contenido es bueno y el 11.11% que es regular.
3. **Calidad de la información:** En este criterio se evalúa si el formato de los reportes suministrados por el sistema es adecuado. El 89.9% de los usuarios indicó que la calidad de la información es buena y el 11.1 % indicó que esta es excelente.
4. **Entrega de resultados:** Se evalúa la velocidad del sistema para ejecutar las operaciones y el tiempo en que la información es suministrada por este. El 55.6% de los usuarios indicó que la entrega es buena y un 44.4% indicó que esta es regular.
5. **Seguridad de los datos:** El 55.6% de los usuarios indicó que el nivel de seguridad que posee el sistema para proteger los datos es bueno, un 22,2% indicó que es regular, un 11,1% desconocen de este aspecto y el 11,1% restante indicó que es excelente.
6. **Fiabilidad del sistema:** Se evalúa si el sistema está disponible cuando se requiere y si este opera confiablemente. El 77.8% de los usuarios indicó que la fiabilidad es buena, un 11.1% que es excelente y otro 11,1% indicó que es regular.
7. **Facilidad de uso:** El 77.8% de los usuarios indicó que la facilidad en el uso del sistema es buena y un 22.2% indicó que es regular.
8. **Documentación:** Se evalúa la claridad, disponibilidad y actualización de la documentación relacionada con las funcionalidades del sistema. El 55.6% de los usuarios indicó que esta es buena, un 22,2% indicó que es regular y un 22.2% que desconocen de esta documentación.
9. **Reportes especiales:** Este criterio evalúa la simplicidad con que se pueden generar gráficos, reportes, operaciones, consultas, etc. El 44.4% de los usuarios indicó que los reportes son buenos, un 33.3% indicó que son regulares y el otro 22.2% indicó que desconocen de reportes especiales que el sistema puede generar.

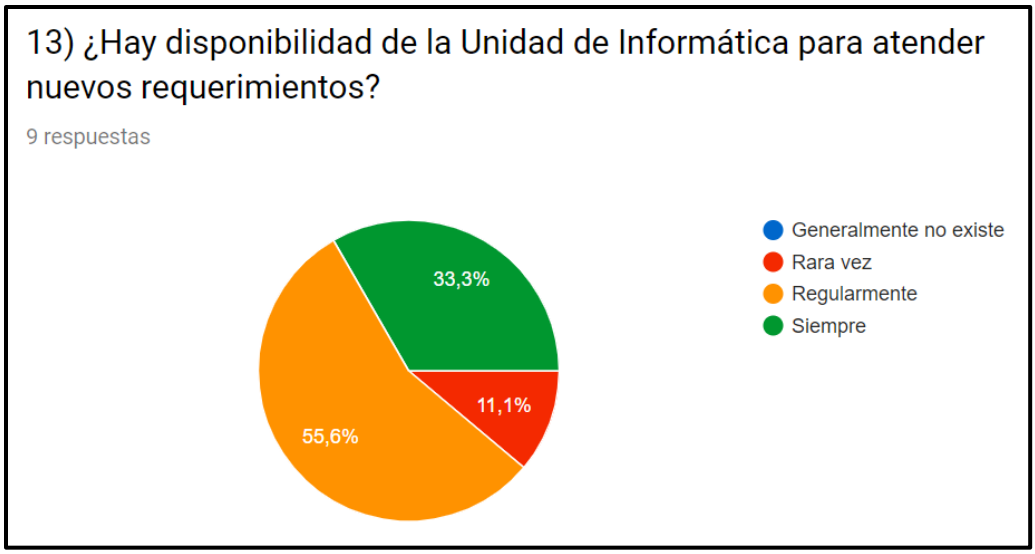
Basado en los resultados anteriores, se puede observar que la mayoría de las respuestas fueron “bueno” y “regular”, reflejando que el sistema satisface adecuadamente la mayoría de los

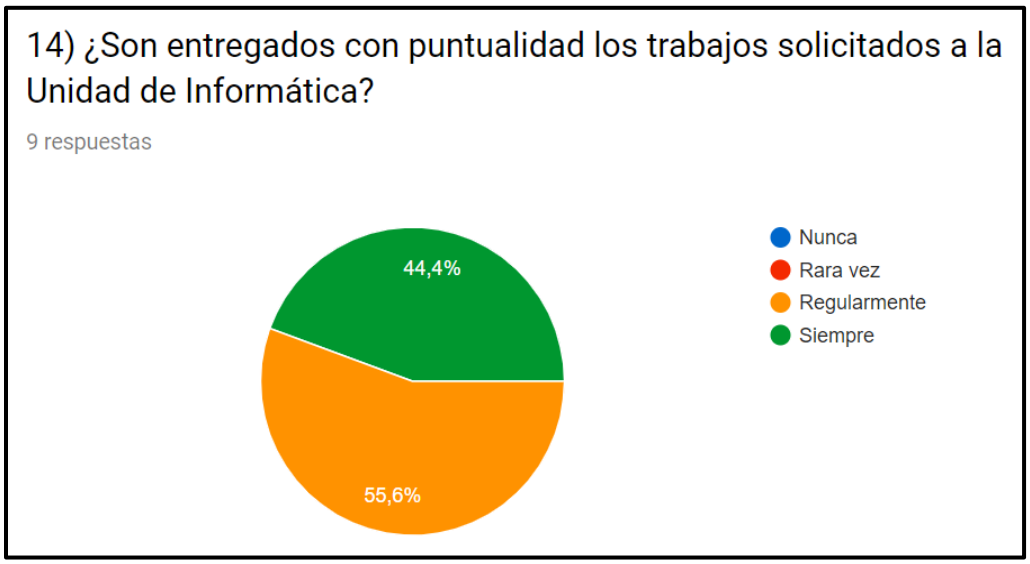
criterios evaluados. En el caso del criterio "seguridad de la información", las respuestas fueron muy divididas ya que el 55.6% indicó que esta es buena, el 22.2% que es regular, el 11,1% que es excelente y el 11.1% desconocen de qué tan seguro es el sistema. Desde la perspectiva de los usuarios, esto refleja que el BOS quizá carece de controles adecuados que permitan tener una respuesta consensuada en la cual se indique que el sistema es lo suficientemente seguro. Durante la revisión a dicho sistema, se pudo identificar que la contraseña utilizada para ingresar a este no posee una fecha de vencimiento. Además, se identificó que no existe un proceso para la revisión periódica de los usuarios y sus permisos en los sistemas, representando así, una debilidad en cuanto a seguridad de la información.

Por otra parte, la percepción de los usuarios finales respecto al servicio brindado por la Unidad de Informática se muestra en los siguientes gráficos:









Basado en los gráficos anteriores, los resultados obtenidos para cada criterio mostrados en estos se mencionan seguidamente:

1. **Resultados esperados:** Para evaluar este criterio, las posibles opciones de respuesta fueron “Sí” o “No”, donde el 89.9% indicó que la Unidad de Informática sí brinda los resultados esperados y el 11.1% indicó que no.

2. **Servicio proporcionado:** Las opciones de respuesta para evaluar este criterio fueron “Deficiente”, “Aceptable”, “Satisfactorio” o “Excelente”. El 44.4% de los usuarios indicó que el servicio brindado por la Unidad de Informática es satisfactorio, el 33.3% que es aceptable y el 22.2% indicó que es excelente.

3. **Disponibilidad para atender requerimientos:** Para este criterio las opciones de respuesta fueron "Generalmente no existe", "Hay ocasionalmente", "Regularmente" o "Siempre". El 55.6% de los usuarios indicó que la Unidad de Informática regularmente está disponible para atender nuevos requerimientos de los sistemas de información, el 33.3% indicó que siempre está disponible y el 11,1% indicó que rara vez.

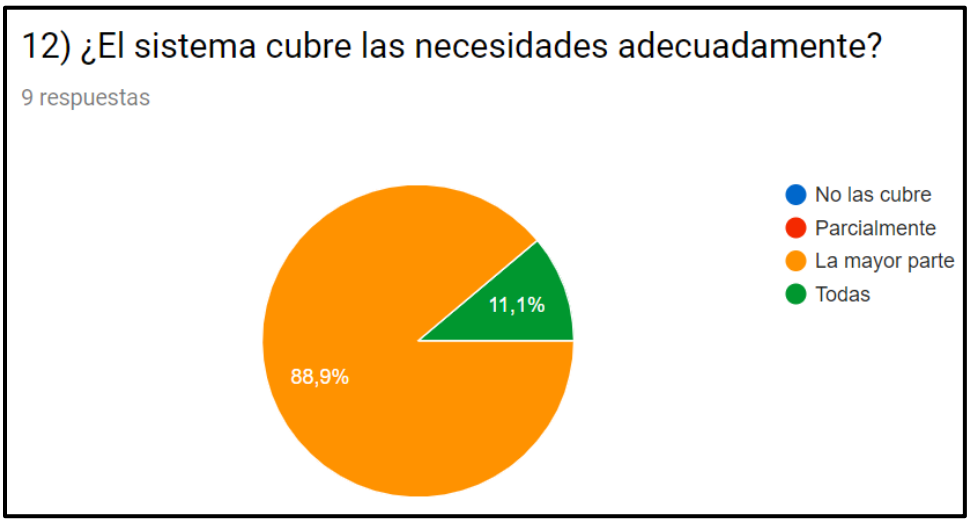
4. **Trabajos entregados con puntualidad:** Las opciones de respuesta para evaluar este criterio fueron "Nunca", "Rara vez", "Regularmente" o "Siempre". Se puede observar que el 55.6% de los usuarios indicó que los trabajos realizados por la Unidad de Informática regularmente son entregados con puntualidad y el 44.4% indicó que siempre.

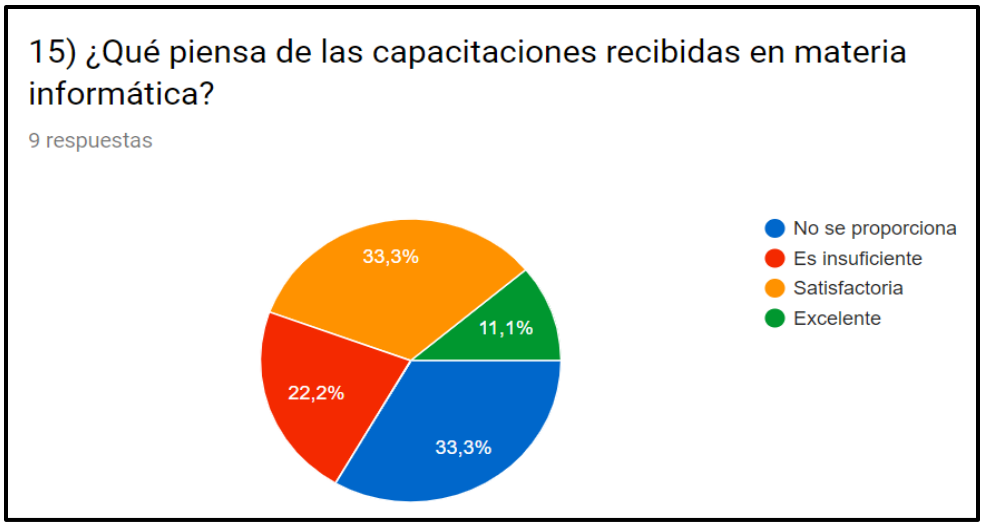
Se puede observar que la mayoría de las respuestas fueron positivas respecto al servicio brindado por la Unidad de Informática. Además, se emitieron comentarios respecto a su labor los cuales se mencionan a continuación:

1. Solo un funcionario de la Unidad de Informática tiene conocimiento del sistema BOS, por lo que se tiene dependencia de esta persona. En caso de que él no esté, si se requiere resolver alguna situación con el sistema, la respuesta es más lenta.
2. En ocasiones cuesta comunicarse vía telefónica con la Unidad.

Lo anterior refleja algunos puntos de mejora que puede tener dicha Unidad.

Además, en el cuestionario se aplicaron las siguientes dos preguntas:





1. **Necesidades cubiertas por el sistema:** Para este criterio las opciones de respuesta fueron "No las cubre", "Parcialmente", "La mayor parte" o "Todas". El 89.9% de los usuarios indicó que la mayor parte de las necesidades son cubiertas y el 11.1% indicó que sí cubre todas sus necesidades laborales.
2. **Capacitaciones recibidas en informática:** Las posibles opciones de respuesta para evaluar este criterio fueron "No se proporcionan", "Es insuficiente", "Satisfactoria" o "Excelente". El 33.3% de los usuarios indicó que no se han proporcionado capacitaciones, otro 33.3% indicó que son satisfactorias, un 22.2% indicó que son insuficientes y un 11.1% indicó que son excelentes.

En el caso del criterio "necesidades cubiertas por el sistema" se puede observar que el sistema satisface la mayoría de las funciones que estos requieren para realizar sus labores. En el caso de las capacitaciones recibidas en materia informática, se puede observar que los resultados no fueron muy positivos, dado que, de acuerdo con comentarios emitidos por los usuarios, estos indicaron que hacen falta capacitaciones en el uso del sistema.

Los comentarios o mejoras expresados por parte de los usuarios referentes al sistema BOS son los siguientes:

1. Integrar el BOS con SICOP.
2. Generar el analítico de cuentas antes de contabilizar para su revisión.
3. Generar el flujo de efectivo.
4. Permitir realizar correcciones antes de contabilizar.
5. Integración adecuada del módulo de planillas con presupuesto.
6. En caso de que se vaya a incluir varios activos de una misma clase, hacer que el sistema conserve los datos para solo incluir el número de patrimonio.
7. Notificar al personal cuando se realizan correcciones o nuevas actualizaciones al sistema.
8. Brindar capacitaciones.

RECOMENDACIONES

Basado en los resultados anteriores, se puede observar que el sistema presenta principalmente debilidades en cuanto a seguridad lógica y la falta de capacitación en el uso de este, por lo cual se debe de dar un mayor énfasis en mejorar estos aspectos, además de tomar en consideración los comentarios emitidos por los usuarios.

En el hallazgo 10 también se mostraron algunas recomendaciones para el BOS.

Además, es recomendable que se propicie una reunión entre los usuarios de las áreas involucradas o se habilite algún medio (tal como un formulario), con el propósito de conocer con mayor detalle las necesidades o debilidades del sistema, de modo que se puedan llevar a cabo las mejoras que correspondan según el grado de importancia y/o urgencia.

Se podrían realizar preguntas como las siguientes:

1. ¿Cuáles problemas presenta con el sistema actualmente?
2. ¿Cuáles funciones o necesidades no son cubiertas por el sistema?

Lo anterior también ayudará a que la mayoría de los resultados sobre las evaluaciones a los criterios sean excelentes en lugar de buenos y regulares.

ANEXO B

Análisis de Riesgos TI
Unidad de Informática

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		✓	Solo el personal de TI tiene acceso, se colocó un candado extra en la entrada de las oficinas para garantizar el ingreso de solo personal de TI.		B
A.2	Personal interno y externo debidamente identificado (gafete)	✗		Se cuenta con gafete, no obstante, algunos funcionarios no lo tienen a la vista y el personal externo no lo porta.		B
A.3	Revisión de equipos de ingreso y salida		✓	Se cuenta con una boleta de recibido para la aceptación del servicio, se tiene un inventario físico y cuando se retira el equipo se genera una boleta y un oficio con el equipo que se retira. Los equipos por parte de externos no se registran en una bitácora.		B
A.4	Bitácoras de acceso al edificio y centro de cómputo	✗		No se cuenta con bitácoras para ingresar a la Unidad de Informática, para ingresar al edificio el personal externo si se debe registrar.		B
A.5	Acceso restringido a personal de informática definido		✓	El equipo es monitoreado por el encargado de informática.		B
A.6	Una sola vía de acceso		✓	Se cuenta con una sola vía de acceso.		B
A.7	Externos son acompañados por internos		✓	En todo momento los externos son acompañados por personal de informática.		B
A.8	Puerta de acceso segura	✗		La puerta es de vidrio y colinda con el exterior.		M
A.9	Acceso con tarjeta electrónica al centro de datos	✗		La entrada posee un llavín simple, se reforzó con una cadena, la cual solo informática posee acceso.		M
A.10	Alarmas de detección de intrusos	✗		No se cuenta con alarmas para detectar intrusos.		M

A.11	Monitoreo de la entrada por cámara de seguridad		✓	Se cuenta con una cámara de seguridad que monitorea la entrada a las oficinas de informática.		B
A.12	Ubicación en un sitio seguro (lugares colindantes)	✗		La puerta de acceso colinda con una entrada del museo, la puerta es de vidrio.		M
A.13	Lugar completamente cerrado	✗		Es cerrado, pero la puerta de vidrio da directamente a un sitio externo.		M
A.14	Paredes de concreto	✗		Una de las paredes es de gypsum.		B
A.15	Cielo raso sellado		✓	Se cuenta con cielo raso sellado.		B
A.16	Equipos ubicados en rack		✓	Los equipos están ubicados en racks, el equipo encontrado fuera de los racks se indicó por parte de informática que se encontraba en revisión.		B
A.17	Los racks están asegurados		✓	Cada rack posee su propio seguro y están fijados al piso.		B
A.18	Cableado de datos independiente del eléctrico		✓	El cableado eléctrico es independiente al cableado de datos.		B
A.19	Cableado entubado y canaleteado		✓	El cableado se encuentra entubado y canaleteado.		B
A.20	Cableado debidamente rotulado		✓	El cableado está rotulado.		B
A.21	Hay un sitio alterno	✗		No se cuenta con un sitio alterno.		A

B. INSTALACIÓN ELÉCTRICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
B.1	Hay pararrayos		✓	El sistema eléctrico del museo posee pararrayos.		B
B.2	Circuito eléctrico independiente		✓	Sí es independiente.		B
B.3	Interruptor de emergencia en la sala de cómputo (palanca)		✓	Se cuenta con caja de breaker en TI.		B
B.4	Cableado eléctrico debidamente entubado o cubierta contra incendios		✓	El cableado está entubado.		B

B.5	Conexión de los equipos a UPS		✓	Los equipos están conectados a UPS.		B
B.6	UPS ubicada en un sitio seguro		✓	Las UPS se ubican en un sitio seguro.		B
B.7	Pruebas periódicas de la UPS (bitácora)	✗		Sí se realizan pruebas periódicas a las UPS, sin embargo, no se mantiene un registro de estas.		B
B.8	UPS en contrato de mantenimiento preventivo y correctivo		✓	El mantenimiento se da a lo interno.		B
B.9	Conexión a planta eléctrica	✗		No se cuenta con planta eléctrica.		M
B.10	Planta eléctrica ubicada en un sitio seguro	✗		No se cuenta con planta eléctrica.		M
B.11	Pruebas periódicas de la planta eléctrica	✗		No se cuenta con planta eléctrica.		M
B.12	Planta eléctrica en contrato de mantenimiento preventivo y correctivo	✗		No se cuenta con planta eléctrica.		M
B.13	Luces de emergencia en el centro de cómputo o cercanías	✗		No se cuenta con luces de emergencia.		B
B.14	Pruebas periódicas de sistema de iluminación de emergencias	✗		No se cuenta con luces de emergencia.		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	✗		El aire acondicionado es compartido entre el centro de datos y las oficinas de informática.		M
C.2	Equipo de respaldo para el aire acondicionado	✗		No se cuenta con un aire acondicionado de respaldo.		M
C.3	Contrato de mantenimiento preventivo y correctivo		✓	Sí se le da mantenimiento bajo un contrato.		B
C.4	Control y monitoreo de humedad y temperatura	✗		No se cuenta con medidores para monitorear la temperatura y humedad.		M

D. DESASTRES NATURALES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
D.1	Brigada de emergencias		✓	Sí se cuenta con una brigada.		B
D.2	Capacitación del personal		✓	Se han brindado capacitaciones de primeros auxilios.		B
D.3	Rutas de evacuación y salidas de emergencia		✓	Se cuenta con rutas de evacuación y salidas de emergencia.		B
D.4	Señalización		✓	Las rutas de evacuación, salidas de emergencia y sitios restringidos están señalizados.		B
D.5	Simulaciones periódicas		✓	Se realizan simulaciones periódicas.		B
D.6	Fácil acceso por Unidades de Bomberos		✓	No se detectaron condiciones que imposibiliten la entrada de los bomberos.		B
D.7	Sistemas de detección de humo/calor/fuego	✗		No se cuenta con sistemas de detección de humo, ya se iniciaron las gestiones para adquirirlos.		M
D.8	Sistemas automáticos y manuales de alarma	✗		No se cuenta con ninguno de los dos sistemas de alarmas.		M
D.9	Extinguidores cercanos portátiles (revisados al día)		✓	Se cuenta con extintor y su carga se encuentra al día.		B
D.10	Uso de aspersores	✗		No se cuenta con aspersores.		B
D.11	Pisos falsos		✓	No, pero el cableado se maneja por canastas.		B
D.12	Desnivel en el piso		✓	No se tiene desnivel en el piso, no hay riesgo de inundación.		B

E. FALLAS HARDWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
E.1	Redundancia de servidores críticos	✗		No se cuenta con redundancia en los servidores críticos.		M
E.2	Mantenimiento preventivo		✓	El mantenimiento preventivo se brinda a lo interno.		B
E.3	Mantenimiento correctivo		✓	El mantenimiento correctivo se brinda a lo interno.		B

F. FALLAS SOFTWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
F.1	Política de uso de recursos (prioridades en procesos)		✓	Se cuenta con una política de uso de recursos.		B
F.2	Control de cambios		✓	Se cuenta con un procedimiento para gestionar cambios en sistemas de información.		B

G. FALLAS EN COMUNICACIONES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
G.1	Redundancia de equipos y enlaces		✓	Si hay redundancia en equipos de red. Hay dos enlaces de Internet con el ICE, por Fibra Óptica y por SHDSL.		B
G.2	Mantenimiento preventivo		✓	El mantenimiento preventivo se brinda a lo interno.		B
G.3	Mantenimiento correctivo		✓	El mantenimiento correctivo se brinda a lo interno.		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 procedimientos para el respaldo de información.		B
H.2	Procedimientos para respaldo y recuperación	✗		Se cuenta con procedimientos para el respaldo de información. No se cuenta con un procedimiento para la restauración de la información.		B
H.3	Almacenamiento de información		✓	Se almacena una copia en el servidor ubicado en el sitio principal, en un disco duro externo y en otro servidor ubicado en la sede de Pavas.		B
H.4	Traslado de respaldos		✓	Se envían a la sede de Pavas a través de una VPN.		B
H.5	Configuración de programas para respaldo		✓	Los respaldos se realizan dos veces a la semana y se utiliza el programa Iperious backup.		B

I. ATAQUES POR VIRUS

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
I.1	Política de antivirus		✓	Se cuenta con política de antivirus.		B
I.2	Programa antivirus		✓	Actualmente se cuenta con ESSET.		B
I.3	Actualización del antivirus		✓	Son automáticas y se instalan desde internet o desde la red interna.		B
I.4	Administración de incidentes y problemas	✗		Se gestionan por correo electrónico.		B

J. INTRUSIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
J.1	Política de acceso lógico		✓	Se tiene una política de acceso lógico.		B
J.2	Control de acceso a aplicaciones		✓	Las solicitudes se realizan por correo electrónico. Las jefaturas realizan las solicitudes.		B
J.3	Monitoreo de usuarios y accesos	✗		Las jefaturas son las encargadas de realizar la solicitud a la Unidad de Informática para crear o deshabilitar un usuario, asignar, modificar, o eliminar los permisos sobre un módulo o programa determinado. Sin embargo, no se realizan monitoreos periódicos de los usuarios y sus permisos en los sistemas.		M

K. ADMINISTRACIÓN DE OPERACIONES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
K.1	Capacitación personal técnico		✓	En el periodo 2017 los funcionarios de la Unidad de Informática participaron en charlas de actualización en materia de transparencia y gestión de sitios web.		B
K.2	Segregación de funciones		✓	Se apega a lo establecido al manual de funciones del Servicio Civil.		B

L. RIESGOS DE LA GESTIÓN DE TI

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.1	¿Se tienen definido un plan estratégico para TI alineado con el de la organización?	✗		No, dado que no existe un Plan Estratégico Institucional vigente (su última actualización se realizó en el 2009), por lo cual, no es posible la alineación entre dichos planes.		A
L.2	¿El Plan estratégico ha sido divulgado a los niveles que corresponde?	✗		Se cuenta con un PETI del periodo 2018-2021, sin embargo, este aún no ha sido aprobado formalmente.		A
L.3	¿Se tienen definidas las políticas y procedimientos para TI?	✗		Se identificaron deficiencias en algunos procedimientos y la ausencia de otros. Dentro de ellas, se encuentra la ausencia de: un marco para la gestión de control interno de TI, procedimiento para evaluar el cumplimiento de la política de seguridad de la información, una metodología para la gestión de la calidad y una metodología para la gestión de riesgos de TI.		M
L.4	¿Se tiene definido el apetito de riesgos para TI? (Nivel de riesgo que la institución quiere aceptar)	✗		No se realiza una evaluación de riesgos.		A
L.5	¿Los riesgos que la organización se encuentra dispuesta a aceptar se encuentran aprobados formalmente por la Administración y el Comité de Auditoría?	✗		No se realiza una evaluación de riesgos.		A
L.6	¿El mapa de riesgos es revisado y actualizado periódicamente?	✗		No se realiza una evaluación de riesgos.		A
L.7	¿La evaluación de riesgos considera elementos cualitativos y cuantitativos?	✗		No se realiza una evaluación de riesgos.		A
L.8	¿Los riesgos de TI son revisados con los usuarios del sistema?	✗		No se realiza una evaluación de riesgos.		A
L.9	¿Se han implementado antivirus y firewalls?		✓	Sí se cumple con esta condición.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.10	¿Se han establecido los protocolos para la realización de copias de seguridad?	✗		Se realizan respaldos de información, no obstante, no se cuenta con las bitácoras respectivas.		B
L.11	¿La seguridad de la información es un tema de seguimiento para la alta gerencia como para el Comité de Auditoría?	✗		No se ha realizado una evaluación de la política de seguridad de la información. Además, no se cuenta con un procedimiento para validar su cumplimiento.		M
L.12	¿Las políticas y procedimientos relacionados con TI son revisados y actualizados periódicamente, considerando los cambios en la industria y la regulación externa?	✗		Se comprobó que el reglamento de tecnologías de información no se actualiza desde el 2008. Además, se carecen de varios procedimientos de gestión de TI, por lo que, no se puede determinar su revisión y actualización.		M
L.13	¿Se tiene definido el perfil para cada cargo de TI y los colaboradores vinculados cumplen con el mismo?		✓	Se basa en manual de puestos del Servicio Civil.		B
L.14	¿Se tienen definidas y divulgadas las funciones y responsabilidades de cada colaborador del área?		✓	Sí se tienen definidos las funciones y responsabilidades de cada colaborador.		B
L.15	¿Las responsabilidades de cada nivel y colaborador, parten del principio de segregación de funciones?		✓	De acuerdo con el manual de puestos del Servicio Civil.		B
L.16	¿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 solicitan los permisos a través de correo electrónico.		B
L.17	¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de estas?		✓	Se cuenta con manuales de usuario y capacitaciones según sea necesario.		B
L.18	¿Las herramientas de TI permiten tener la trazabilidad de las operaciones realizadas, así como de los usuarios (logs)?		✓	Los sistemas de información poseen pistas de auditoría.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.19	¿Se monitorea el estado de los equipos (Hardware)?		✓	Sí se realiza. Se dan mantenimientos preventivos al equipo.		B
L.20	¿La seguridad física de las instalaciones donde operan los equipos y personas de TI, es evaluada y revisada periódicamente, cumpliendo con los protocolos establecidos?		✓	Durante el proceso de revisión de la auditoría externa.		B
L.21	¿La organización desarrolla un plan de formación integral tanto para los miembros de TI como para los usuarios de la herramienta, orientado al uso, seguridad y ética en la utilización de estas?		✓	De acuerdo con las necesidades, se brindan las capacitaciones requeridas.		B
L.22	¿Se han establecido indicadores de gestión que permitan medir el desempeño de las herramientas como de los colaboradores del área?	✗		No se han establecido indicadores de gestión que permitan medir el desempeño.		B
L.23	¿Se han implementado planes de acción correctivos, para aquellos casos en que los indicadores presentar resultados inferiores a los esperados?	✗		No se cuenta con planes de acción correctivos.		B
L.24	¿Se han adquirido pólizas de seguro para eventos de riesgos en el área de TI?	✗		No se cuenta con póliza de seguros para eventos de riesgos en el área de informática, sin embargo, el equipo eléctrico si posee una póliza con el INS.		M
L.25	¿Cada proyecto de TI tienen definidos y documentos los riesgos tanto de su desarrollo como de la puesta en marcha, así como tiene la proyección de recursos financieros a invertir?	✗		No se realiza de manera formal.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.26	¿Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de TI y dicho seguimiento es documentado?		✓	Sí se realiza un seguimiento del cumplimiento, pero no se lleva documentado, más que por las boletas y aceptaciones de servicio.		B
L.27	¿Todos los cambios desarrollados en las aplicaciones y/o software son documentados y custodiados?	✗		No se posee un registro de los cambios realizados.		M
L.28	¿Se ha establecido el plan de continuidad para los procesos de TI?	✗		Se cuenta con un plan de continuidad, sin embargo, no se han realizado pruebas ni capacitaciones.		M
L.29	¿Se solicita el apoyo de consultores externos para los proyectos estratégicos?		✓	En el caso de ser necesario, se acude a consultores externos.		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		✓	Son solicitados por las jefaturas.		B
M.2	Los accesos otorgados son revisados periódicamente	✗		No se realiza un monitoreo periódico de los accesos que poseen los usuarios en los sistemas de información.		M
M.3	La asignación de los accesos parte de la segregación de funciones		✓	Sí, se realiza según el puesto desempeñado.		B
M.4	Cada usuario tiene asignada una clave de composición alfanumérica y de mínimo 8 caracteres	✗		El sistema BOS no exige el tamaño de la contraseña. Tampoco se debe cambiar periódicamente. Se verificó en las entrevistas con los usuarios del sistema.		M

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.5	Se pueden rastrear las operaciones realizadas por los usuarios por medio de los logs		✓	Existen pistas de auditoría.		B
M.6	Se cuenta con una política de copias de seguridad y de restauración	✗		Se cuenta con procedimientos para el respaldo de información. No se cuenta con un procedimiento para la restauración de información.		M
M.7	La información sensible se encuentra protegida de modificaciones no autorizadas		✓	Sí se cumple con esta condición.		B
M.8	Se cumplen con los niveles de seguridad físicos para los servidores	✗		No se cumple con esta condición, dado que el cuarto de servidores posee las siguientes deficiencias: la puerta tiene llavín tipo convencional, se utiliza una puerta de vidrio que colinda con el exterior, se cuenta con una ventana, hay una pared de Gypsum, no se cuenta con un aire acondicionado de respaldo, no posee detectores de humo, no se cuenta con medidores de temperatura y humedad, no se cuenta con una bitácora de accesos, el aire acondicionado se encontraba goteando en el momento de la revisión y se cuenta con un tanque de agua dentro de las instalaciones del cuarto de servidores.		A
M.9	Asignación de usuarios y claves personalizada		✓	Sí se cumple con esta condición.		B
M.10	Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.	✗		En el procedimiento no se especifica cuáles son los usuarios que pueden solicitar los cambios. Además, se indica que la Unidad de Informática es la encargada de aprobar y realizar los cambios, no obstante, no se especifica quienes son los encargados.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.11	Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.	✗		No se especifica si se envía dicha notificación.		B
M.12	Las modificaciones en las bases de datos son realizadas por un área independiente a la que utiliza la información.		✓	Se tiene personal específico para cada función.		B
M.13	Los cambios en la base de datos permiten tener la trazabilidad de quien los realiza por medio de los logs.		✓	Sí se cuenta con logs para dar trazabilidad a los cambios en la base de datos.		B
M.14	Se tiene un número reducido de administradores.		✓	Sí se tiene un número reducido de 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.		✓	Sí se cuenta con diccionarios de datos.		B
M.16	Definición y documentación de la Política de Cambios		✓	Sí se cuenta con un procedimiento.		B
M.17	Segregación de funciones entre el desarrollador, aprobador y responsable de administrar en producción		✓	Se cuenta con personal independiente para cada etapa.		B
M.18	Aprobación del usuario final de los cambios.	✗		En el procedimiento no se indica si los usuarios finales aprueban los cambios.		M
M.19	Asignación usuarios y permisos, previo requerimiento y aprobación del director y/o Responsable del área que utiliza la aplicación.		✓	Las jefaturas solicitan los accesos.		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.	✗		No se tiene un registro de los cambios.		M

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.21	Validación periódica de los cambios en permisos y asignación de usuarios por parte del nivel autorizador.		✓	Las jefaturas son las encargadas de solicitar a la Unidad de Informática la creación, modificación de los permisos que poseen los usuarios en los sistemas de información, o deshabilitar un usuario.		B
M.22	Bloqueo de usuarios retirados, previa comunicación de Gestión Humana.	✗		Se bloquen bajo solicitud de las jefaturas, sin embargo, se identificó cuentas de exfuncionarios activas.		M
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.	✗		No se realiza un monitoreo periódico de los usuarios y sus permisos en los sistemas de información.		M
M.24	Bloqueo de usuarios en vacaciones		✓	Se bloquean bajo solicitud de las jefaturas.		B
M.25	Identificación de los usuarios que realizan las transacciones, por medio de los Logs.		✓	Se cuentan con pistas de auditoría.		B
M.26	Certificaciones externas sobre la calidad del servicio prestado.		✓	Anualmente se realizan auditorías externas.		B
M.27	Suscripción de un acuerdo sobre privacidad con el proveedor.		✓	Dentro de las contrataciones se coloca un apartado sobre la confidencialidad.		B
M.28	Plan de contingencia para migrar a otro servidor	✗		Se cuenta con un plan de continuidad, pero no se han dado capacitaciones o realizado pruebas.		M
M.29	Plan de capacitaciones en seguridad, para los usuarios con accesos más vulnerables.		✓	Se dan inducciones a los usuarios.		B
M.30	Cifrar las bases de datos más sensibles, junto con controles de monitoreo.		✓	Las bases de datos están cifradas y requieren de un software y un token para visualizarlas.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.31	Limitar el acceso a los datos y/o solicitar mayores autenticaciones, de acuerdo con el dispositivo y al lugar desde donde se ingresa.		✓	No se puede ingresar a la información desde fuera de la institución.		B
M.32	Instalar en los dispositivos móviles parches que permitan aislar los datos de la compañía de los personales.		✓	No se puede ingresar a la información desde dispositivos móviles.		B
M.33	Se realizan pruebas periódicas sobre la recuperación de datos.	✗		Se realizan pruebas, pero no se documentan.		B

--Ultima línea--