MUSEO NACIONAL DE COSTA RICA (MNCR)

- **Informe de Auditoría de Sistemas y Tecnología de Información**
- **Carta de Gerencia TI 2019**
- **Informe Final**

San José, 06 de noviembre del 2020

Señores
Museo Nacional de Costa Rica (MNCR)
Unidad de Informática
Junta Administrativa

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del período 2019 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 2019.

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. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad No. 0116 FIG7
Vence el 30 de setiembre del 2021.

"Timbre de Ley número 6663, por ¢25.00 del Colegio de Contadores Públicos de Costa Rica, adherido y cancelado en el original."

CONTENIDO

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, sobre los siguientes aspectos:

    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.
    o. Gestión de la capacidad y disponibilidad.
    p. Gestión de proyectos de TI.
    q. Desarrollo de software.
    r. Arquitectura de la información.

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 de la parte financiera 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 los meses de octubre y noviembre del año 2020 y corresponde a la auditoría del periodo del 2019.

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 de las tecnologías de información, en todos los casos necesarios solicitamos a los funcionarios las evidencias en formato digital que respaldaran sus afirmaciones.

I. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: AUSENCIA DE UN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el Museo Nacional de Costa Rica (MNCR) no cuenta con un Plan Estratégico Institucional (PEI) vigente, el último plan con el que se cuenta es del periodo 2008-2012, donde su última actualización se realizó en el año 2009. En sustitución de este plan, se elaboran planes de trabajo anuales.

Se consultó si existe una razón por la cual no se cuenta con un Plan Estratégico Institucional actualizado, para lo cual, se indicó que a inicios del 2019 se contrató a una planificadora institucional, sin embargo, dicha empresa se trasladó en concurso a otra Institución y no se finalizó el trabajo.

Se indicó que al no existir un PEI, no se puede desarrollar un Plan Estratégico de Tecnologías de Información (PETI) alineado a dicho PEI. La Unidad de Informática elabora planes de trabajo anuales alineados a los objetivos del Museo y basados en los proyectos estratégicos que lidera dicha Unidad. Estos planes contienen aspectos como las actividades del periodo (donde para cada una de estas se indica la meta planteada, la descripción del indicador utilizado para medir el cumplimiento de cada actividad y la fórmula aplicada para calcular cada indicador), presupuesto de la Unidad y la lista de proyectos de TI que se planearon para el respectivo periodo.

Sin embargo, al no contar con un PETI, existe el riesgo de que la gestión de tecnologías de información tome un enfoque reactivo y no proactivo, lo cual podría mantener la operación de la Institución, pero podría dificultar que se maximice la obtención de beneficios a través de la implementación de estrategias a largo plazo. Además, se desconoce cuál es la situación actual de TI (principales sistemas que soportan a la Institución, ambiente de redes y telecomunicaciones, procesos de TI, análisis FODA de TI), dirección de TI (misión y visión de TI, metas y estrategias, proyectos de TI a desarrollarse con sus respectivos costos, su priorización y beneficios que brindarán al MNCR), entre otros.

CRITERIO:

El apartado **2.1 "Planificación de las Tecnologías de 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 lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes."*

RECOMENDACIONES:

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

1. Elaborar un plan estratégico de tecnologías de información (alineado a los objetivos del MNCR) con el propósito de plasmar la situación actual de TI y la situación deseada, y así poder establecer iniciativas concretas que permitan cerrar las brechas. Para ello, es necesario que el PETI incluya aspectos como los siguientes:

    a. Análisis del negocio (objetivos, procesos de negocio claves, análisis FODA, etc.).
    b. Situación actual de TI (procesos de TI, principales sistemas que soportan al negocio, análisis FODA de TI).
    c. Situación deseada de TI (visión de TI, misión de TI, objetivos de TI).
    d. Iniciativas (corresponden a los proyectos y acciones concretas por realizar para llegar a la situación deseada de TI en el tiempo definido en el PETI). Cada iniciativa puede tener su prioridad, cronograma, recursos, mejoras esperadas por la Institución e indicadores de rendimiento.

2. Asegurarse que el PETI se alinee con el Plan Estratégico Institucional en caso de que se desarrolle.

3. Elaborar informes de seguimiento del PETI al menos cada tres meses, con el fin de dar seguimiento periódico al avance de las iniciativas y corregir posibles desviaciones.

4. Alinear los planes anuales de trabajo con el PETI una vez que se cuente con este.

HALLAZGO 02: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE LOS INVENTARIOS DE LICENCIAS DE SOFTWARE EN EL MNCR. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada en el MNCR relacionada a la gestión del software licenciado, se determinó que actualmente la Unidad de Informática cuenta con los siguientes documentos:

- **Licenciamiento Software Especial:** Este inventario incluye el ID de la licencia, el nombre, el área o departamento donde se está utilizando, responsable y activo en la cual está instalada.
- **Reporte de software instalado:** Incluye el nombre de la licencia y la cantidad de cada una de estas.
- **Reportes del software instalado por equipo:** Se incluye la placa del software, el nombre por cada uno de los equipos y el funcionario responsable del equipo.
- **Reporte de software no instalado:** Se indica el nombre de la licencia y la cantidad que no se encuentran instaladas.

Con base en dicha información suministrada, se procedió a realizar la comparación entre estos reportes. A continuación, se muestra una tabla que contiene algunas de las diferencias encontradas.

Programa	Licencias del reporte de licenciamiento especial	Licencias del reporte de software instalado	Licencias de los reportes de software instalado por equipo	¿Se encuentra en el reporte de software no instalado?
ADOBE PRO DC	15	No se encuentra en este reporte	7	Sí (se indica que hay una licencia sin instalar)
Ms Project 2016	20	3	3	No
Filemaker 10	5	No se encuentra en este reporte	3	No

Cabe destacar que para realizar este análisis, se seleccionó al azar los programas para realizar la comparación. Las cantidades incluidas en las primeras tres columnas se obtuvieron de los reportes que se indican en cada una de ellas. Además, se verificó que dicho software no estuviera incluido en el reporte de **"Software no instalado"**. El resultado de esto se muestra en la columna **"¿Se encuentra en el reporte de software no instalado?**".

Dado lo anterior, se puede observar que existen diferencias entre estos reportes. Esta situación podría dificultar el seguimiento de dichas licencias.

CRITERIO:

El punto **D** de apartado 4.2 "**Administración y operación de la plataforma tecnológica"**, 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: *"Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas."*

RECOMENDACIONES:

A la Unidad de Informática:

1. Identificar las razones por las cuales se están presentando las diferencias entre los reportes que incluyen las licencias de software.

2. Actualizar los respectivos registros, una vez identificadas las razones, con el propósito de mantener una consistencia entre todos los reportes.

3. Realizar revisiones periódicas para determinar qué licencias se encuentran en uso, para determinar la existencia de software no autorizado y para la identificación de necesidades sobre licenciamiento, con el fin de actualizar los respectivos inventarios.

HALLAZGO 03: DEBILIDADES EN LA GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el MNCR cuenta con un manual de contingencias de tecnologías de información, no obstante, carece de fecha de publicación, fecha de actualización y los responsables de la aprobación.

En este manual se incluyen los sistemas que son críticos para la Institución, sin embargo, no se incluye el procedimiento que debe ser seguido para continuar operando estos sistemas en caso de que alguna falla afecte la disponibilidad de su servicio. Además, no se incluyen cuáles son los procesos críticos de la Institución, los servicios de TI que soportan o apoyan dichos procesos, los eventos que podrían afectarlos y qué acciones deben seguirse para su recuperación ante su no disponibilidad.

Por otra parte, no se cuenta con un plan de pruebas para la ejecución del manual y para el periodo 2019 no se realizaron capacitaciones al personal involucrado.

Dada la situación anterior, se evidencia que el manual de contingencias presenta oportunidades de mejora en su estructura, no se han realizado capacitaciones en la ejecución del manual a los respectivos responsables ni se han elaborado pruebas sobre este, por lo tanto, existe el riesgo que ante la materialización de un riesgo relacionado con la continuidad de los servicios de TI, se desconozcan las acciones por realizar para recuperar oportunamente la plataforma tecnológica, afectando la disponibilidad de los servicios de TI y de los procesos de la Institución asociados a estos.

CRITERIO:

El apartado **1.4.7 "Continuidad de los servicios 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 menciona: *"La Organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad."*

RECOMENDACIONES:

A la Unidad de Informática:

1. Valorar si se incluye en el manual de contingencias los siguientes aspectos:

    a. Declarar el alcance, considerando que como mínimo contemple los procesos críticos del negocio que son soportados o apoyados por tecnologías de información.
    b. Identificar los recursos de tecnologías de información que soportan los procesos críticos del MNCCR contemplados en el alcance del manual. Estos recursos pueden ser hardware, software, equipo de red e incluso funcionarios que participan en la ejecución de dichos procesos.
    c. Identificar medidas alternas para recuperar los servicios de TI en caso de que un desastre afecte su disponibilidad, y documentar dentro del manual dichas medidas.
    d. Definir los procedimientos necesarios y los responsables de ejecutarlos para restaurar los servicios de TI en caso de un desastre.
    e. Identificar los actores internos y externos a la organización que pueden eventualmente participar en la ejecución de lo indicado en el manual, especificando los medios para contactarlos.
    f. Definir los procesos posteriores a la recuperación, considerando evaluación de daños y efectividad del manual de continuidad.

2. Establecer un plan de pruebas basado en el manual de contingencia de TI y ejecutarlo al menos una vez al año, donde su resultado quede documentado, con el fin de realizar ajustes necesarios en caso de que se requieran.

3. Realizar capacitaciones, mínimo una vez al año, al personal involucrado en el manual, para que conozcan sus respectivos roles en la ejecución de este.

4. Actualizar o revisar el manual periódicamente y mantener un registro de dichas actualizaciones o revisiones que se realicen.

HALLAZGO 04: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LAS BASES DE DATOS DE ACTIVOS SIBINET Y BOS. RIESGO MEDIO.

CONDICIÓN:

A partir del análisis realizado a las bases de datos de activos del sistema BOS y SIBINET con corte al 31/12/2019, se encontraron inconsistencias en la información almacenada, las cuales se mencionan a continuación:

1. Se identificaron 3 activos en la base de datos del SIBINET que no están registrados en la base de datos del BOS. Del mismo modo, se identificó 57 activos en el BOS que no se encuentra registrado en la base de datos del SIBINET.
2. Se identificaron 7 activos en la base de datos del BOS que se encuentran duplicados. Dichos activos son 804005966, 804006393, 804006394, 804006395, 804006412, 804006521 y 804006525.
3. En la Tabla 1 se muestran las diferencias encontradas entre ambas bases de datos en cuanto al total del valor de compra, depreciación acumulada y valor en libros de los activos.

Tabla 1 Diferencias entre ambas bases de datos.

Sistema	Valor de compra	Depreciación acumulada	Valor en libros
SIBINET	65,468,359,383.63	1,872,470,755.16	63,595,888,628.47
BOS	65,500,460,121.57	2,120,935,976.06	63,379,524,145.52
Diferencia	**-32,100,737.94**	**-248,465,220.90**	**216,364,482.94**

4. Para los 6232 activos registrados en ambas bases de datos (los cuales tienen en común), se encontró una diferencia en el valor de compra, en la depreciación acumulada y en el valor en libros, esto se observa en la Tabla 2.

Tabla 2 Diferencias en la información contenida en ambas bases de datos.

Sistema	Valor de compra	Depreciación acumulada	Valor en libros
SIBINET	65,467,880,286.98	1,872,402,833.23	63,595,477,453.75
BOS	65,466,221,295.30	2,117,257,081.09	63,348,964,214.22
Diferencia	**1,658,991.68**	**-244,854,247.86**	**246,513,239.52**

En las siguientes tablas se detalla el monto en colones de los 57 registros que se encuentran en el BOS y no en el SIBINET, y de los 3 registros que se ubican en SIBINET y no en el BOS.

Tabla 3 Información únicamente en un sistema

Resumen registros solo en el BOS				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
BOS Activos	57	33,629,229.62	3,568,084.58	30,061,145.04

Resumen registros solo en SIBINET				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
SIBINET Activos	3	479,096.65	67,921.93	411,174.72

5. Existen registros que presentan inconsistencias en los atributos de un mismo activo. Dichas inconsistencias corresponden a un mismo activo que posee distintos valores de compra entre ambas bases de datos, o que poseen un mismo valor de compra, pero distinto monto de depreciación acumulada. A continuación, se presentan unos ejemplos.

Tabla 4 Inconsistencias de atributos

	SIBINET				BOS			
Número de placa	**Fecha compra**	**Valor compra**	**Depreciación acumulada**	**Valor en libros**	**Fecha compra**	**Valor compra**	**Depreciación acumulada**	**Valor en libros**
804006335	**09/09/2019**	290,175.75	**9674.6**	**280,501.15**	**09/09/2019**	538,303.71	**53,332.2**	**484,971.51**
804006383	**20/11/2019**	123,934.6	**1,689.5**	**122,245.1**	**20/11/2019**	125,405.2	**10,755.73**	**114,649.47**
917203	**10/01/2006**	75,000	**69,523.2**	**5,476.8**	**10/01/2006**	75,000	**73,085.44**	**1,914.56**
213001293	**20/12/2011**	985,000	**792,869**	**192,131**	**20/12/2011**	985,000	**863,107.37**	**121,892.63**
912501	**02/10/1996**	79,600	**79,100**	**500**	**03/12/2018**	79,600	**79,100**	**500**

En la tabla anterior, se puede mostrar que existen registros con la fecha de compra, la depreciación acumulada o el valor en libros que no coinciden entre las bases de datos.

Al presentarse las inconsistencias mostradas anteriormente, se pierde los principios de integridad y confiabilidad de la información, dado que, dependiendo de la base de datos utilizada, los resultados serán diferentes.

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. En caso de que las inconsistencias no puedan corregirse por alguna situación, justificar el motivo de esto.

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

3. Realizar un proceso periódico de validación y comparación de bases de datos (entre el SIBINET y el BOS) con el propósito de verificar que ambas bases de datos no presenten diferencias. En caso de encontrar diferencias en la información, se debe verificar cuál base de datos posee la información correcta, realizar un análisis de causa raíz para subsanar el problema y actualizar la base de datos errónea. Dicha gestión debe quedar documentada.

HALLAZGO 05: OPORTUNIDADES DE MEJORA DEL MODELO DE ARQUITECTURA DE INFORMACIÓN. RIESGO BAJO.

CONDICIÓN:

Se comprobó que la Unidad de Informática cuenta con un Modelo de Arquitectura de Información e Infraestructura Tecnológica aprobado el 13 de diciembre del año 2019 mediante el acuerdo A-19-1346.

Al respecto con la estructura del Modelo de Arquitectura de Información e Infraestructura Tecnológica se identificó que está conformado por la arquitectura de los sistemas, la tendencia de las tecnologías de información, la arquitectura tecnológica y el modelo de información. Sin embargo, no se logran evidenciar aspectos sobre los procesos de negocio clave, no se especifica como está construido el diccionario de datos, modelo y diagramas de las bases de datos principales, los flujos de información y comunicaciones dentro de toda la organización, y las relaciones entre la tecnología y las aplicaciones que se encuentran desarrolladas o adquiridas por el Museo, así como de un detalle de los diagramas de arquitecturas físicas representando software, hardware, redes y comunicaciones.

Al no contar con un modelo de arquitectura de la información adecuado, se dificulta visualizar la relación entre los procesos de negocio y el flujo de información de la Institución, que resguardada la Unidad de Informática, por lo que no se puede planificar de manera adecuada la estrategia de tecnologías de información, la estrategia del negocio, la seguridad informática, la agilidad de la plataforma y la optimización de los activos, con respecto a los recursos y capacidades de TI.

CRITERIO:

El apartado 2.2 “Modelo de arquitectura de información”, presente en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), menciona lo siguiente: “La organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren.”.

RECOMENDACIONES:

A la Unidad de Informática:

1. Considerar integrar los distintos modelos que conforman el modelo de arquitectura de información, en los siguientes aspectos:

    a. **Modelos de proceso de negocio:** relacionado a identificar la misión, visión, valores y objetivos de la organización. Así como la visión de la arquitectura empresarial y la gestión de los interesados.
    b. **Modelo de datos**: relacionado a la gestión de la información y procesos. Así como la comprobación del ciclo de vida de la información y las trasformaciones recibidas de los datos durante su recepción y procesamiento.
    c. **Modelo de aplicaciones:** relacionado a la gestión de aplicaciones corporativas y externas, desarrollo de aplicaciones y sistemas. Así como la debida gestión de la funcionalidad de cada aplicación encontrada en la organización.
    d. **Modelo de tecnología:** relacionado a la gestión de la tecnología y sistemas de información. Así como la visualización y diagramación de procesos tecnológicos plasmados en la infraestructura, servicios externos o facilitadores del negocio.

2. Revisar el modelo de arquitectura al menos una vez al año.

3. Efectuar las gestiones necesarias para que el modelo de arquitectura cuente con la aprobación formal y sea comunicado a los interesados.

4. Valorar el uso de marcos de referencia como guía para crear un modelo de arquitectura de información robusto. Un ejemplo puede ser:

    a. TOGAF (The Open Group Architecture Framework): es un marco de referencia utilizado como estándar global para la arquitectura empresarial. Dicho estándar permite asegurar que todas las unidades organizaciones manejen un mismo lenguaje de comunicación, ya que proporciona el diseño, planificación, implementación y gobierno de la información a nivel organizacional.

II. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CARTA DE GERENCIA 2018	
HALLAZGO 01: AUSENCIA DE UN MODELO DE ARQUITECTURA DE INFORMACIÓN EN EL MNCR. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 5. Documentar y detallar el modelo de arquitectura, considerando los siguientes aspectos: a. **Modelo de proceso de negocio:** Está relacionado con la identificación de la misión, visión, valores y objetivos de la organización, así como la visión de la arquitectura empresarial. b. **Modelo de datos**: Relacionado con la gestión de la información y los procesos, así como el ciclo de vida de la información y las trasformaciones recibidas de los datos durante su recepción y procesamiento. c. **Modelo de aplicaciones:** Asociado con la gestión de las aplicaciones corporativas y externas, y el desarrollo de aplicaciones. d. **Modelo de tecnología:** Modelo relacionado con la gestión de la tecnología y sistemas de información. 6. Revisar el modelo de arquitectura de información periódicamente para garantizar que este se mantenga actualizado de acuerdo con los cambios presentados en la Unidad de Informática, la información y los procesos de negocio. 7. Valorar el uso de marcos de referencia como guía para crear un modelo de arquitectura de información robusto, un ejemplo puede ser: a. **TOGAF (The Open Group Architecture Framework):** Es un marco de referencia utilizado como estándar global para la arquitectura empresarial. Dicho estándar permite asegurar que todas las unidades organizacionales manejen un mismo lenguaje de comunicación, ya que proporciona el diseño, planificación, implementación y gobierno de la información a nivel organizacional.

COMENTARIOS DE LA ADMINISTRACIÓN	En octubre del 2019 Esteban Quiros finalizó el modelo de Arquitectura.
ESTADO	**CORREGIDO** Se comprobó que la Unidad de Informática cuenta con un Modelo de Arquitectura de Información e Infraestructura Tecnológica aprobado el 13 de diciembre de 2019 mediante el acuerdo A-19-1346. Sin embargo, se identificaron oportunidades de mejora como se detalla en el presente informe en el hallazgo 05.
HALLAZGO 02: INCUMPLIMIENTO DE LA PERIODICIDAD DE LAS SESIONES DE LA COMISIÓN DE INFORMÁTICA. RIESGO BAJO.	
RECOMENDACIÓN	***A la Comisión de Informática:*** 1. Cumplir con la periodicidad de las sesiones establecida en el reglamento o valorar si esta debe cambiarse, según las necesidades del MNCR. 2. Documentar en caso de que se traten temas de interés por la Comisión de Informática en las reuniones de las jefaturas, dichos temas y los acuerdos pactados en la plantilla de las minutas utilizada por la Comisión, con el fin de que se evidencie las reuniones realizadas.
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Durante el periodo 2019 la Comisión de Informática del Museo Nacional ha realizado 4 sesiones en los meses de enero, abril, junio y agosto. Sin embargo, no se identificó la existencia de las sesiones para los meses de febrero, marzo, mayo, julio, setiembre, octubre, noviembre y diciembre.
HALLAZGO 03: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** Considerar, dado que se planea cerrar el área en la cual se encontrará el cuarto de servidores:

	1. Asegurarse que la puerta para acceder a este sea de un material difícil 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. Valorar la adquisición de un aire acondicionado de respaldo, en caso de que se presente una falla en el aire acondicionado principal. 3. Instalar medidores de temperatura y humedad, de modo que se pueda llevar un mejor control del ambiente y que este no dañe los equipos. 4. 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. 5. Mantener un registro del mantenimiento que se realiza a las UPS. 6. Etiquetar la totalidad del cableado del cuarto de servidores para mantener un control adecuado de este. ***A la Comisión de Informática:*** 7. Analizar las vulnerabilidades señaladas, priorizarlas y gestionar su corrección de acuerdo con los recursos y posibilidades que posee el Museo.

COMENTARIOS DE LA ADMINISTRACIÓN	No se han atendido dichas recomendaciones.
ESTADO	**PENDIENTE** De acuerdo con lo indicado por la Unidad de Informática, aún no se han atendido las recomendaciones emitidas en este hallazgo.
HALLAZGO 04: OPORTUNIDADES DE MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN DEL MUSEO NACIONAL DE COSTA RICA. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Unidad de Informática en conjunto con la Dirección General y la Junta Administrativa:*** 1. Crear lineamientos para clasificar la información tomando en cuenta la sensibilidad por divulgación, impacto por pérdida y valor de la información para el Museo (por ejemplo, clasificarla en restringida, pública) y los controles para tratar la información de acuerdo con su clasificación. 2. Valorar si se incluyen los lineamientos asociados con la clasificación de la información en las normas institucionales sobre tecnologías de información o en la política de seguridad que se está desarrollando. 3. Tomar como referencia marcos de razonables prácticas para seguridad de la información tal como la ISO/IEC 27002 para la creación de dichos lineamientos. 4. Aplicar una vez creada la política de seguridad de la información, lo siguiente: a. Comunicarla a todos los funcionarios del Museo, con el fin de que estén enterados sobre su existencia y acatamiento. b. Realizar capacitaciones sobre seguridad de la información, con el fin de crear una cultura de seguridad, se posea un claro entendimiento de la política de seguridad de la información y así evitar o reducir los incidentes asociados con esta. c. Establecer mecanismos de control que ayuden a verificar el cumplimiento de la política tales como actividades de monitoreo de seguridad, pruebas de vulnerabilidades, indicar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

	d. Realizar revisiones periódicas (al menos una vez al año o cuando se requiera) de la política de seguridad de la información, documentando los resultados.
COMENTARIOS DE LA ADMINISTRACIÓN	En noviembre del 2019 Esteban Quiros finalizó el documento Política Clasificación de la Información.
ESTADO	**EN PROCESO** Según lo indicado por la Unidad de Informática se está desarrollando una política de seguridad, a la fecha no se cuenta con dicha política y no se han realizado capacitaciones. Por otra parte, se determinó que cuenta con una Política de Clasificación de la Información aprobada el 13 de diciembre de 2019 mediante el acuerdo A-19-1346 y con respecto a su cumplimiento debe ser valorado en la próxima auditoría del Museo Nacional de Costa Rica.
HALLAZGO 05: AUSENCIA DE CAPACITACIONES PARA EL PERSONAL DE LA UNIDAD DE INFORMÁTICA EN EL PERIODO 2018. RIESGO BAJO.	
RECOMENDACIÓN	***Al Departamento de Recursos Humanos en coordinación con la Unidad de Informática:*** 1. Elaborar un plan de capacitaciones para el personal de la Unidad de Informática con el fin de justificar las necesidades de dichas capacitaciones, el cual cuente con al menos los siguientes puntos: a. Área de conocimiento que se desea abordar. b. Objetivo que se pretende alcanzar con cada capacitación. c. Cronograma de cuándo se planean realizar. d. Indicar los participantes de recibir cada capacitación. e. Lugar en que se realizará la capacitación. f. Costo. 2. Mantener un registro de la ejecución del plan de capacitaciones (listas de asistencia, certificados de participación, entre otros.) de modo que se le pueda dar seguimiento al proceso de capacitación.

COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicho plan de capacitaciones.
ESTADO	**PENDIENTE** Se determinó que no se cuenta con un plan de capacitación para la Unidad de Informática. Para el periodo 2019 no se ha desarrollado capacitaciones para el personal de TI.
HALLAZGO 06: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD DE LA PLATAFORMA TECNOLÓGICA. RIESGO BAJO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Generar un modelo de monitoreo como parte del procedimiento a elaborar considerando al menos los siguientes aspectos: a. Periodicidad del monitoreo. b. Indicadores de rendimiento. c. Herramienta utilizada para el monitoreo. d. Umbrales de monitoreo (gestión de alertas). e. Reportes periódicos (mensuales o según la periodicidad que se defina) de los siguientes aspectos: i. Reportes de disponibilidad. ii. Reportes de capacidad. iii. Reportes de excepciones (situaciones esporádicas que pueden levantar una alerta sobre capacidad o disponibilidad). 2. Generar un plan de capacidad, desempeño y disponibilidad incluyendo un análisis del comportamiento en el consumo de recursos. En el mismo se debe realizar una proyección de los recursos para determinar cuál va a ser el consumo futuro por parte de la Institución y así generar una estrategia para sustentar la necesidad de esos recursos. Además, se debe incluir un plan de trabajo incluyendo los aspectos a realizar durante el periodo, entre ellos:

	a. Componentes que se deben actualizar en el proceso de monitoreo (nuevo equipo, retiro de ítems de configuración). b. Implementación de nuevas herramientas o nuevas configuraciones. c. Identificación de parámetros a monitorear. d. Gestión de acuerdos de nivel de servicio o acuerdos de nivel operativo (en caso de que existan).
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Según lo mencionado por la Unidad de Informática aún no se cuenta con un procedimiento para la gestión de la capacidad y disponibilidad de la plataforma tecnológica.
HALLAZGO 07: AUSENCIA DE UNA METODOLOGÍA PARA LA GESTIÓN DE PROYECTOS DE TI. RIESGO MEDIO.	
RECOMENDACIÓN	***A la Unidad de Informática:*** 1. Documentar una metodología para la administración de proyectos de tecnologías de información, la cual incluya al menos la siguiente estructura: a. Iniciación: Elaborar un acta constitutiva que contenga los elementos principales del proyecto: i. Definición del objetivo y alcance del proyecto. ii. Entregables del proyecto. iii. Descripción del producto final. iv. Presupuesto y costos asociados. v. Personal interesado y sus roles (stakeholders). b. Planeación: Elaborar un plan de trabajo con las tareas y actividades que se deben ejecutar para lograr los alcances definidos: i. Cronograma de trabajo. ii. Criterios de aceptación de los entregables. iii. Riesgos del proyecto. iv. Gestión de cambios del proyecto.

	v. Aprobación del plan de trabajo. c. Ejecución: Realizar cada una de las actividades previstas en el plan de trabajo i. Alinear la ejecución del proyecto a lo establecido en las etapas de iniciación y planeación. ii. Dar seguimiento a la elaboración de los entregables de modo que cumpla con los criterios de aceptación definidos. d. Cierre: Levantar un acta de cierre considerando: i. Aceptación de los entregables. ii. Lecciones aprendidas (mejora continua). iii. Aprobación del proyecto. 2. Valorar el uso de razonables prácticas del mercado para la implementación de una metodología de proyectos como por ejemplo PMBOK y PRINCE2.
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** De acuerdo con lo indicado por la Unidad de Informática, no se cuenta con una metodología establecida de manera institucional para la administración de proyectos.
HALLAZGO 08: DEBILIDADES EN LA ADMINISTRACIÓN DE ACCESOS DE LOS USUARIOS EN LOS SISTEMAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIÓN	***A Recursos Humanos:*** 1. Notificar oportunamente a 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 realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben 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. Valorar si se incluye en el procedimiento DIRG-UI-006_Manual Procedimiento Registro Usuarios Red o se crea uno nuevo, el proceso para la gestión de los usuarios y sus perfiles en los sistemas de información, en el cual se contemplen al menos los siguientes aspectos: a. Actividades para crear, modificar o eliminar un usuario y sus respectivos permisos en los sistemas de información. b. Periodicidad con la cual se debe realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben 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.
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Este hallazgo está pendiente de atenderse, debido a que aún se encuentran las cuentas de los exfuncionarios activas, no se han realizado las revisiones de los roles y perfiles de los usuarios en los sistemas de información (en este caso

	del 2019) y no se ha incluido en un procedimiento el proceso para la gestión de los usuarios y sus perfiles en los sistemas de información.
HALLAZGO 09: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LAS BASES DE DATOS DE ACTIVOS SIBINET Y BOS. RIESGO MEDIO.	
RECOMENDACIÓN	***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. En caso de que las inconsistencias no puedan corregirse por alguna situación, justificar el motivo de esto. 2. Analizar y establecer mecanismos de control que validen los campos donde se presentan las inconsistencias. 3. Realizar un proceso periódico de validación y comparación de bases de datos (entre el SIBINET y el BOS) con el propósito de verificar que ambas bases de datos no presenten diferencias. En caso de encontrar diferencias en la información, se debe verificar cuál base de datos posee la información correcta, realizar un análisis de causa raíz para subsanar el problema y actualizar la base de datos errónea. Dicha gestión debe quedar documentada.
COMENTARIOS DE LA ADMINISTRACIÓN	Esos bienes que no están ingresados en el BOS, no han sido subsanados por la falta de personal en el Área de Bienes.
ESTADO	**NO APLICA** Se procedió a actualizar la condición del hallazgo. Ver hallazgo 04.
CARTA DE GERENCIA 2017	
HALLAZGO 01: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE LA CALIDAD DE LOS PRODUCTOS Y SERVICIOS DE TI. RIESGO MEDIO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Aún no se cuenta con la metodología para la gestión de la calidad de TI.

HALLAZGO 03: OPORTUNIDAD DE MEJORA EN EL PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS. RIESGO BAJO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Se determinó que el procedimiento de control de cambios (DIRG-UI-010) aún no cuenta con las mejoras según recomendaciones emitidas en el hallazgo. Además, la Unidad de Informática indica que no se ha creado un repositorio para cambios.
HALLAZGO 04: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE RIESGOS DE T.I. RIESGO MEDIO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Aún no se ha desarrollado una metodología para la gestión de riesgos de tecnologías de información.
HALLAZGO 05: CUMPLIMIENTO PARCIAL DEL DECRETO EJECUTIVO 37549-JP. RIESGO BAJO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	No se emitieron comentarios de la administración sobre este hallazgo.
ESTADO	**EN PROCESO** Se determinó que un colaborador de la Unidad de Informática elaboró el informe referente a los derechos de autor, el cual fue enviado al Registro de Derechos de Autor y Derechos Conexos. Además, se comprobó la existencia de un software en el cual se gestiona de manera centralizada las licencias y se nos suministró una muestra de los expedientes u hojas de vida de cada equipo. No obstante, debido a que el informe que se envía al Registro de Derechos de Autor y Derechos Conexos fue elaborado por un colaborador de la Unidad de Informática, este hallazgo se encuentra en proceso.
HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE PROBLEMAS. RIESGO BAJO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	En el Manual UI-012 Gestión de Incidentes, se tomaron en cuenta dichas recomendaciones.
ESTADO	**EN PROCESO** Este hallazgo se encuentra en proceso debido a que ya se cuenta con un procedimiento para la gestión de problemas. Sin embargo, no se evidenció la aprobación formal de este. Se sometió a aprobación mediante el oficio Nº UI-2019-O-0142, enviado a la Dirección General del MNCR. Además, no se cuenta con un registro formal de los problemas presentados en el 2019.
HALLAZGO 10: DEFICIENCIAS EN EL SISTEMA DE INFORMACIÓN BOS. RIESGO MEDIO.	
RECOMENDACIÓN	***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 cuentas por pagar y el estado de flujo de efectivo no se están realizando satisfactoriamente, en caso de ser necesario, contactar al proveedor para corregir la causa.
COMENTARIOS DE LA ADMINISTRACIÓN	El Sistema Bos se migró a los servidores de Cultura a inicios de este año. Se desconoce si se resolvieron los problemas descritos en este punto.

ESTADO	**EN PROCESO** Este hallazgo se encuentra en proceso debido a que el estado de flujo de efectivo aún no se genera satisfactoriamente en el sistema, por lo tanto, debe generarse fuera de este.
CARTA DE GERENCIA 2016	
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 cuenta con un inventario de licencias.
ESTADO	**CORREGIDO** Este hallazgo se encuentra corregido dado que se cuenta con un software para gestionar las licencias de una manera centralizada.

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	No se cuenta con dicha información.
ESTADO	**NO APLICA** Se procedió a actualizar la condición de este hallazgo. Ver hallazgo 01.
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	No se ha realizado dicho estudio.
ESTADO	**PENDIENTE** La Unidad de Informática menciona que debido a la sustitución de toda la red de datos, incluyendo los equipos de seguridad, no se han realizado estudios de vulnerabilidad, dado que aún está en proceso de mejoras y actualizaciones.
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	No se cuenta con dicha información.
ESTADO	**PENDIENTE** La Unidad de Informática no cuenta con iniciativas o acciones para la elaboración de un procedimiento para la gestión de bases de datos.
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	No se ha realizado dicho procedimiento.

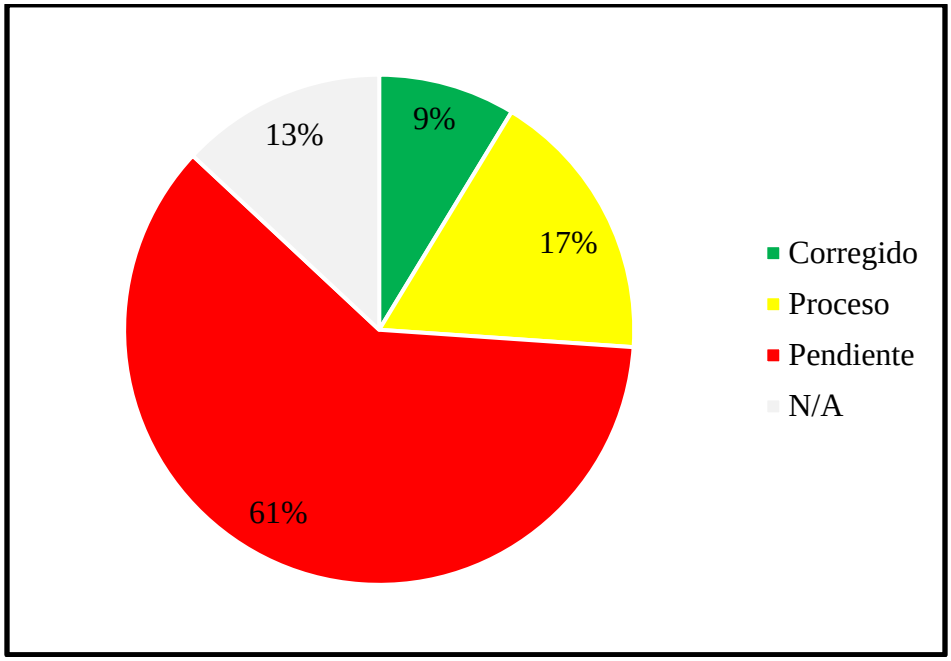
ESTADO	**PENDIENTE** Se determinó que no se ha desarrollado un procedimiento detallado para la elaboración de respaldos y recuperaciones de información. Además, no se cuenta con bitácoras de los respaldos realizados, ni bitácoras de las pruebas realizadas a los respaldos.
HALLAZGO 10: FALTA DE PRUEBAS 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	No se cuenta con dicha información.
ESTADO	**NO APLICA** Se procedió a actualizar la condición de este hallazgo.
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	No se cuenta con dicha información.
ESTADO	**PENDIENTE** Se considera que aún no se ha desarrollado una metodología para la evaluación del control interno de TI.
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 cuenta con dicha información.
ESTADO	**PENDIENTE** Aún no se ha desarrollado un plan para la implementación de las Normas Técnicas de la Contraloría General de la República para la gestión de las TI.

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

Estado / Año	2018	2017	2016	Total por estado
Corregido	1	0	1	**2**
Proceso	1	3	0	**4**
Pendiente	6	3	5	**14**
N/A	1	0	2	**3**
Total por año	**9**	**6**	**8**	**23**



III. ANEXOS

ANEXO A

Análisis de Riesgos TI
Unidad de Informática

Periodo 2019

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	✗		El cuarto de servidores se encuentra ubicado en la Biblioteca, por lo tanto el personal que labora en esta tiene acceso a dicho cuarto, así como el personal de TI.		A
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.		M
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. Además, para acceder al cuarto de servidores tampoco se posee una bitácora.		M
A.5	Acceso restringido a personal de informática definido	✗		Tienen acceso solo personal administrativo y técnico de la unidad de informática, sin embargo, al ubicarse el cuarto de servidores en la Biblioteca, el personal de esta accede a la zona donde este se encuentra localizado.		M
A.6	Una sola vía de acceso		✓	Se cuenta con una sola vía de acceso al cuarto de servidores.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.7	Externos son acompañados por internos		✓	En todo momento los externos son acompañados por personal de informática al ingresar al cuarto de servidores o Unidad de Informática.		B
A.8	Puerta de acceso segura	✗		La puerta del cuarto de servidores es de vidrio y colinda con el exterior.		M
A.9	Acceso con tarjeta electrónica al centro de datos	✗		La entrada del cuarto de servidores posee un llavín simple, se reforzó con una cadena. Además, la puerta es de vidrio.		M
A.10	Alarmas de detección de intrusos		✓	Sí se cuenta con alarmas para detectar intrusos en el cuarto de servidores.		B
A.11	Monitoreo de la entrada por cámara de seguridad		✓	Se cuenta con cámaras de seguridad que monitorea la entrada a las oficinas de informática y de la biblioteca.		B
A.12	Ubicación en un sitio seguro (lugares colindantes)	✗		La puerta de acceso del cuarto de servidores 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		✓	Existe un agujero en el cielo raso del cuarto de servidores, sin embargo, se indicó que es debido a la instalación de la fibra óptica.		B
A.16	Equipos ubicados en rack		✓	Los equipos están ubicados en racks.		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 no se encuentra independiente del cableado de datos.		B
A.19	Cableado entubado y canaleteado		✓	El cableado se encuentra entubado.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.20	Cableado debidamente rotulado	✗		No todo el cableado se encuentra rotulado.		M
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	✗		No es independiente.		M
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 del cuarto de servidores 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)	✗		No se cuenta con un registro del mantenimiento dado a las UPS.		M
B.8	UPS en contrato de mantenimiento preventivo y correctivo	✗		No se cuenta con un registro del mantenimiento dado a las UPS.		M
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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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		✓	Sí se cuenta con un aire acondicionado.		B
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		✓	Se cuenta con un detector de humo.		B
D.8	Sistemas automáticos y manuales de alarma		✓	Se cuenta con una alarma para detección de intrusos en la Biblioteca.		B
D.9	Extintores cercanos portátiles (revisados al día)		✓	Se cuenta con dos extintores y su carga se encuentra al día.		B
D.10	Uso de aspersores	✗		No se cuenta con aspersores.		B
D.11	Pisos falsos		✓	Se cuenta con cielo raso.		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 con antena.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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. Sin embargo, no se cuenta con un procedimiento para la restauración de la información.		M
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 automáticamente.		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 cuenta con una herramienta para la gestión de incidentes. No obstante, no se cuenta con un registro formal de los problemas.		M

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 o a través de la herramienta de solicitudes. Las jefaturas realizan dichas solicitudes.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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 2019 no se brindaron capacitaciones a los colaboradores de la Unidad de Informática.		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 existe un Plan Estratégico de TI ni un Plan Estratégico Institucional. El PEI (su última actualización se realizó en el 2009), por lo cual, no es posible la alineación entre dichos planes.		M
L.2	¿El Plan estratégico ha sido divulgado a los niveles que corresponde?	✗		No se cuenta con un Plan Estratégico de TI.		M
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.		M
L.5	¿Los riesgos que la organización se encuentra dispuesta a aceptar se encuentran aprobados formalmente por la Administración y el Comité de Riesgos?	✗		No se realiza una evaluación de riesgos.		M
L.6	¿El mapa de riesgos es revisado y actualizado periódicamente?	✗		No se realiza una evaluación de riesgos.		M
L.7	¿La evaluación de riesgos considera elementos cualitativos y cuantitativos?	✗		No se realiza una evaluación de riesgos.		M

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.8	¿Los riesgos de TI son revisados con los usuarios del sistema?	✗		No se realiza una evaluación de riesgos.		M
L.9	¿Se han implementado antivirus y firewalls?		✓	Sí se cumple con esta condición.		B
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 y Riesgos?	✗		Se cuenta con un documento denominado "Normas Institucionales sobre tecnologías de información", el cual contiene lineamientos relacionados con la seguridad de la información y este fue comunicado a todo el personal del Museo. Además, se nos indicó que se está desarrollando una política de seguridad de la información. Sin embargo, dado que se está desarrollando una política, 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?		✓	Los procedimientos y políticas de TI que posee actualmente el MNCR se encuentran actualizados.		B
L.13	¿Se tiene definido el perfil para cada cargo de TI y los colaboradores vinculados cumplen con el mismo?		✓	Se basa en el 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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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?		✓	Se cumple con este aspecto.		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
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?	✗		En el 2019 no se brindaron capacitaciones a los colaboradores de la Unidad de Informática.		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. Se mide por medio de la satisfacción del usuario en cuanto al uso.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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?		✓	El equipo eléctrico si posee una póliza con el INS.		B
L.25	¿Cada proyecto de TI tienen definidos y documentados 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.		M
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, el encargado del contrato o del servicio contratado realiza un monitoreo del cumplimiento.		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		✓	Se cumple con este aspecto.		B
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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.8	Se cumplen con los niveles de seguridad físicos para los servidores	✗		No se cumple con esta condición, dado que el cuarto de servidores posee las siguientes deficiencias: 1. No se cuenta con un sitio exclusivo para el cuarto de servidores, si no, que este se ubica dentro de las instalaciones de la Biblioteca del MNCR. 2. La puerta de la entrada es de vidrio y colinda con el exterior. 3. Hay una pared de Gypsum. 4. No se cuenta con un aire acondicionado de respaldo. 5. No se cuenta con medidores de temperatura ni de humedad, los cuales ayuden a identificar los cambios constantes del ambiente del cuarto de servidores. 6. No se cuenta con una bitácora para controlar el acceso al cuarto de servidores. 7. No se cuenta con un registro del mantenimiento brindado a las UPS. 8. No todo el cableado se encuentra etiquetado.		A
M.9	Asignación de usuarios y claves personalizada		✓	Sí se cumple con esta condición.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.10	Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.		✓	Se cumple con este aspecto.		B
M.11	Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.	✗		No se especifica si se envía dicha notificación.		M
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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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
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 bloquean 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 a este. Además, presenta oportunidades de mejora en su estructura.		M

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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
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.		M

--Ultima línea--