MUSEO NACIONAL DE COSTA RICA (MNCR)

- ***Informe de Auditoría de Sistemas y Tecnología de Información***
- ***Carta de Gerencia TI 2018***
- ***Informe final***

San José, 28 de octubre de 2019

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

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del período 2018 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 2018.

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

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)

Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2019.11.21 16:39:11 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad No. 0116 FIG7
Vence el 30 de setiembre del 2020.

"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

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 razonables 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 2019 y corresponde a la auditoría del periodo del 2018.

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 UN MODELO DE ARQUITECTURA DE INFORMACIÓN EN EL MNCR. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el MNCR no cuenta con un modelo de arquitectura de información que refleje un esquema de los procesos organizacionales y sus relaciones con los componentes de TI (servicios, infraestructura, datos, entre otros).

Al no contar con un modelo de arquitectura de la información, se dificulta visualizar la relación de los procesos y el flujo de la información de la Institución, por lo que no se puede planificar de manera adecuada la estrategia de tecnologías de información, la estrategia de la organización, la agilidad de la plataforma y la optimización de los activos, 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. 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.

2. 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.

3. 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.

HALLAZGO 02: INCUMPLIMIENTO DE LA PERIODICIDAD DE LAS SESIONES DE LA COMISIÓN DE INFORMÁTICA. RIESGO BAJO.

CONDICIÓN:

Se determinó que la Comisión de Informática cuenta con un reglamento el cual fue aprobado en enero del año 2018, además, se encuentra conformada por el Director General y por todas las jefaturas de departamento y unidad, y coordinadores de programas del MNCR.

El artículo 6° del reglamento indica que los miembros de la Comisión deben sesionar al menos una vez al mes, no obstante, en un mismo mes se podrá convocar a más de una sesión en caso de ser necesario. Se nos suministraron las minutas del periodo 2018, donde se evidenció que la Comisión sesionó tres veces. Se nos indicó, que en algunas de las reuniones que realizan las jefaturas, se tratan temas de interés de la Comisión, sin embargo, al suministrarse únicamente tres minutas, no se evidencia que los miembros se reúnan al menos una vez al mes, tal como lo indica el reglamento. Por lo tanto, existe un incumplimiento del artículo 6°.

Al no realizar sesiones periódicamente se corre el riesgo de no tratar temas importantes como la priorización de los proyectos de TI, la asignación de recursos y la atención de los requerimientos propios del negocio.

CRITERIO:

El apartado **1.6 "Decisiones sobre asuntos estratégicos 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: *"El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en*

la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización."

Además, el **artículo 6°** del reglamento de la Comisión de Informática indica: *"Sesiones: La Comisión sesionará al menos una vez al mes en el lugar y hora que este cuerpo destine al efecto, sin embargo, en un mismo mes podrá convocarse a más de una sesión de ser necesario".*

RECOMENDACIONES:

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.

HALLAZGO 03: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO.

CONDICIÓN:

Producto de la revisión del cuarto de servidores del MNCR, se determinó que existen debilidades en la seguridad física, las cuales se mencionan a continuación:

1. La puerta de la entrada es de vidrio y colinda con el exterior.
2. Hay una pared de Gypsum.
3. No se cuenta con un aire acondicionado de respaldo.
4. No se cuenta con medidores de temperatura ni de humedad los cuales ayuden a identificar los cambios constantes del ambiente del cuarto de servidores.
5. No se cuenta con una bitácora para controlar el acceso al cuarto de servidores.
6. No se cuenta con un registro del mantenimiento brindado a las UPS.
7. No todo el cableado se encuentra etiquetado.

Además, se comprobó que 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. Se comentó, por parte de la administración del Museo, que se cerrará el área donde está dicho cuarto de servidores, sin embargo, actualmente se comparte el espacio físico, aire acondicionado y la entrada. Dado esto, al no cumplirse con medidas de seguridad física, el MNCR se expone ante las siguientes situaciones:

1. Acceso no autorizado por terceros en caso de que se fuerce la entrada a través de la puerta de vidrio.
2. No se lleva un control adecuado del personal externo que visite el cuarto de servidores, por lo que los equipos pueden quedar vulnerables a intrusiones por terceros no autorizados.
3. No se lleva un adecuado control de los factores ambientales del cuarto de servidores, por lo que podría presentarse deterioro, pérdida o fallas en los equipos.
4. La falta de un respaldo para el aire acondicionado puede comprometer el desempeño de los equipos en caso de que el actual falle.
5. Podría no tenerse un control adecuado del cableado, debido a la ausencia de etiquetas en estos.

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:

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.

HALLAZGO 04: OPORTUNIDADES DE MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN DEL MUSEO NACIONAL DE COSTA RICA. RIESGO MEDIO.

CONDICIÓN:

De acuerdo con lo indicado por la Unidad de Informática, actualmente se está desarrollando una política de seguridad de la información, por lo tanto, a la fecha no se cuenta con esta. Además, no se han realizado capacitaciones a lo interno del MNCR referente a seguridad de la información. Cabe mencionar que mediante el documento **"Normas institucionales sobre Tecnologías de la Información"** se comprobó la existencia de lineamientos relacionados con la seguridad de la información, sin embargo, se determinó que estas normas no contienen lineamientos asociados con la clasificación de la información que se genera, almacena, consulta, modifica, transmite, destruye o utiliza el personal del Museo Nacional de Costa Rica, tanto impresa como digital.

Al no clasificarse la información desde una perspectiva de seguridad, no se puede determinar la manera que la información debería ser tratada y protegida.

CRITERIO:

El apartado **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 garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*
Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

a. La implementación de un marco de seguridad de la información.
b. El compromiso del personal con la seguridad de la información.
c. La seguridad física y ambiental.
d. La seguridad en las operaciones y comunicaciones.
e. El control de acceso.
f. La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
g. La continuidad de los servicios de TI.

Además, debe establecer las medidas de seguridad relacionadas con:

h. El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
i. El manejo de la documentación.
j. La terminación normal de contratos, su rescisión o resolución.
k. La salud y seguridad del personal.
l. Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.".

RECOMENDACIONES:

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.

HALLAZGO 05: AUSENCIA DE CAPACITACIONES PARA EL PERSONAL DE LA UNIDAD DE INFORMÁTICA EN EL PERIODO 2018. RIESGO BAJO.

CONDICIÓN:

Se determinó que en el periodo 2018 los colaboradores de la Unidad de Informática del Museo Nacional de Costa Rica no participaron en capacitaciones. Se nos suministró un documento elaborado en octubre del 2018, con las necesidades de capacitación para el personal de dicha Unidad, con el fin de que se incluyeran en el presupuesto del 2019, sin embargo, según indicó la jefatura de esta Unidad, hasta el momento no se han llevado a cabo capacitaciones.

Las capacitaciones son fundamentales para fomentar y actualizar los conocimientos, habilidades y competencias del personal de dicha Unidad. Al no llevarse a cabo, el personal podría carecer de conocimientos que sean necesarios para apoyar las metas o proyectos del Museo.

CRITERIO:

El apartado 2.4 **"Independencia y recurso humano de la Función 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 asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas. Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones".*

RECOMENDACIONES:

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.

HALLAZGO 06: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD DE LA PLATAFORMA TECNOLÓGICA. RIESGO BAJO.

CONDICIÓN:

Se determinó que la Unidad de Informática del Museo Nacional de Costa Rica no cuenta con un procedimiento para la gestión de la capacidad y disponibilidad de la plataforma tecnológica el cual defina el monitoreo, análisis de la capacidad actual y futura y la gestión de la disponibilidad de la infraestructura de TI, tampoco se cuenta con un plan para el análisis de tendencias y comportamiento en el consumo de recursos.

Al no desarrollar un plan formal de capacidad, desempeño y disponibilidad basándose en un modelo de análisis de comportamiento, no se puede determinar de forma precisa el crecimiento transaccional de la operativa de la Institución. Además, existe el riesgo de que, ante un crecimiento no previsto de la plataforma, la misma no cuente con el rendimiento suficiente afectando la operativa de esta.

CRITERIO:

El apartado **4.2 "Administración y operación de la plataforma tecnológica"**, 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 mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*

a. *Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
b. *Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
c. *Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.*
d. *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.*
e. *Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.*
f. *Mantener separados y controlados los ambientes de desarrollo y producción.*
g. *Brindar el soporte requerido a los equipos principales y periféricos.*
h. *Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.*
i. *Controlar los servicios e instalaciones externos.*".

RECOMENDACIONES:

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).

HALLAZGO 07: AUSENCIA DE UNA METODOLOGÍA PARA LA GESTIÓN DE PROYECTOS DE TI. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada, se determinó que actualmente la Unidad de Informática del Museo Nacional de Costa Rica no cuenta con una metodología de gestión de proyectos de TI documentada y aprobada.

Al no existir una metodología, cada proyecto que se vaya a desarrollar no tendrá una guía estándar de las etapas que se deben realizar para llevarlos a cabo, los productos entregables, los responsables, recursos necesarios, cronograma, entre otros.

CRITERIO:

El apartado **1.5 "Gestión de proyectos"**, 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 administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos."*

RECOMENDACIONES:

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.

HALLAZGO 08: 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 las carpetas compartidas en el servidor, se debe tramitar la solicitud a la Unidad de Informática. Sin embargo, en este procedimiento no se hace referencia a la gestión de los usuarios y sus respectivos permisos en los sistemas de información. Según lo indicado por la jefatura de la Unidad de Informática, esta gestión se realiza por correo electrónico y aún no se ha presentado el procedimiento formal para su aprobación. Además, indicó que hasta el momento no se ha desarrollado un seguimiento relacionado con la revisión de los roles y perfiles por parte de las áreas usuarias.

Por otra parte, 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 Active Directory, correo electrónico institucional y sistemas de información, se identificó la existencia de cuatro cuentas activas de exfuncionarios, las cuales se muestran a continuación:

Funcionario	Fecha de salida	Motivo de salida	Activo en
Armando Azofeifa	01 de octubre del 2018	Cese de interinidad	• Active Directory.
Noelia Tenorio	15 de junio del 2019	Renuncia	• Correo institucional.
Flor Vargas	28 de junio del 2019	Pensión	• Active Directory. • Correo institucional.
Marvin Montero Alfaro	02 de setiembre del 2019	Renuncia	• Active Directory. • Correo institucional.

Al haber cuentas activas pertenecientes a exfuncionarios de la Institución, se corre el riesgo de que estas cuentas sean utilizadas 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. Además, al no realizar la revisión periódica de los privilegios otorgados a los funcionarios en los sistemas de información, podría existir el riesgo de que cuentas de usuario posean más permisos de los necesarios o permisos totales a un usuario, dándose una falta de segregación de funciones a nivel de sistema.

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.".

RECOMENDACIONES:

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.

HALLAZGO 09: 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 31/12/2018, se encontraron inconsistencias en la información almacenada, las cuales se mencionan a continuación:

1. Se identificaron 964 activos en la base de datos del SIBINET que no están registrados en la base de datos del BOS. Del mismo modo, se identificó un activo en el BOS que no se encuentra registrado en la base de datos del SIBINET.
2. 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	65 323 183 309,97	1 562 349 266,21	63 760 834 043,76
BOS	65 096 404 093,97	1 732 207 795,63	63 364 196 298,36
Diferencia	**226 779 216,00**	**-169 858 529,42**	**396 637 745,40**

3. Para los 5007 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	65 095 951 397,32	1 527 797 812,54	63 568 153 584,78
BOS	65 095 251 397,32	1 732 110 663,28	63 363 140 734,06
Diferencia	**700 000,00**	**-204 312 850,74**	**205 012 850,72**

En las siguientes tablas se detalla el monto en colones del registro que únicamente se encuentra en el BOS y no en el SIBINET, y de los 964 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	1	700000	47993,47	652006,53

Resumen registros solo en SIBINET				
Sistema	**Registros**	**Valor de compra**	**Depreciación acumulada**	**Valor en libros**
SIBINET Activos	964	227 231 912,65	34 551 453,67	192 680 458,98

4. Existen registros que presentan inconsistencias en los atributos de un mismo activo, 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**
804006181	**14/12/2018**	421 352,40	**3 918,16**	**417 434,24**	**20/12/2018**	421 352,40	**58 451,72**	**362 900,68**
804006179	**14/12/2018**	205 000,00	**951,66**	**204 048,34**	**20/12/2018**	205 000,00	**14 201,39**	**190 798,61**
804005716	**25/10/2017**	15 683 795,10	**1 855 198,08**	**13 828 597,02**	**13/11/2017**	15 683 795,10	**2 756 270,96**	**12 927 524,14**

En la tabla anterior, se puede mostrar que la fecha de compra, la depreciación acumulada y el valor en libros para los tres activos, es diferente entre ambas 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:

<u>Al Departamento Administrativo y Financiero en conjunto con la Unidad de Informática:</u>

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.

II.MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

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	Se está trabajando en gestionar la definición, aprobación y divulgación de una metodología o procedimiento para gestionar la calidad, con el fin de detallar cómo se llevará a cabo todo el proceso de mejora continua de los servicios y productos que ofrece la Unidad de Informática. Su presentación está planificada para el segundo semestre del 2019.
ESTADO	**PENDIENTE** Aún no se cuenta con la metodología para la gestión de la calidad. Se planea contar con ella a finales de este año (2019).
HALLAZGO 02: AUSENCIA DE UN PROCEDIMIENTO FORMAL PARA LA DIVULGACIÓN DE LA NORMATIVA INTERNA RELACIONADA CON T.I. RIESGO BAJO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	Se desarrolló el procedimiento DIR-UI-011_Manual Procedimiento Divulgación Información, sobre normas, lineamientos, metodologías, políticas, procedimientos, entre otros, relacionadas con la Unidad de Informática.
ESTADO	**CORREGIDO** Se cuenta con un procedimiento para la divulgación de la normativa relacionada con TI (políticas, procedimientos, metodologías, entre otros), el cual empezó a regir en setiembre del 2019. Además, se comprobó la existencia de un repositorio en el cual se almacena dicha normativa para que pueda ser accedida por los funcionarios del MNCR.

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	Se está trabajando en conjunto con estudiantes del TEC los ajustes y modificaciones recomendados por la auditoría externa.
ESTADO	**PENDIENTE** Según lo indicado por la jefatura de la Unidad de Informática, actualmente se está trabajando con estudiantes del TEC las mejoras al procedimiento de cambios, sin embargo, aún no se cuenta con un documento formal que evidencie el avance que se tiene sobre esto. Dado lo anterior, este hallazgo se encuentra pendiente.
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	Se tiene planificado el desarrollo de una metodología formal para la gestión de riesgos de TI. De manera temporal se está utilizando el análisis de riesgos realizado por la auditoría, orientándola hacia el cumplimiento de los objetivos del COBIT.
ESTADO	**PENDIENTE** Aún no se ha elaborado una metodología para la gestión de riesgos de TI.
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	Se implementó un expediente u hoja de vida donde se indica la información del funcionario responsable, fecha de instalación y persona responsable de hacer la instalación.
ESTADO	**EN PROCESO** Se determinó que un colaborador de la Unidad Informática elaboró el informe referente a los derechos de autor, el cual fue enviado al Registro de Derechos de Autor y Derechos Conexos. Por otra parte, se identificó que la Auditoría Interna elaboró un informe similar, el cual fue dirigido a la Junta Administrativa, a la Directora General y a la Jefatura de la Unidad de Informática. 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 06: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	Se realizaron las mejoras indicados por la auditoría externa, entre ellos: reforzar la entrada a TI, se gestionó la compra de un nuevo aire acondicionado, se implementó una bitácora de control de ingreso al cuarto de servidores y se realizó el traslado de los servidores a un nuevo espacio.
ESTADO	**NO APLICA** Se procede a actualizar el hallazgo (Ver hallazgo 03).
HALLAZGO 07: 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 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.
COMENTARIOS DE LA ADMINISTRACIÓN	Se realizaron las mejoras indicadas por la auditoría externa, entre ellos: se deshabilitaron las cuentas de usuario de funcionarios que cesan sus labores para la Institución, además, la oficina de gestión institucional de recursos humanos remite un informe o reporte de los funcionarios que ingresaron y/o dejaron de laborar en ese periodo.
ESTADO	**NO APLICA** Se procede a actualizar el hallazgo (Ver hallazgo 07).
HALLAZGO 08: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LAS BASES DE ACTIVOS SIBINET Y BOS. RIESGO MEDIO.	
RECOMENDACIÓN	***Al Departamento Administrativo y Financiero en conjunto con la Unidad de Informática:*** 4. Realizar una depuración en conjunto con los responsables de la administración de los activos en ambos sistemas, para corregir las inconsistencias detectadas. 5. Analizar y establecer mecanismos de control que validen los campos donde se presentan las inconsistencias.

COMENTARIOS DE LA ADMINISTRACIÓN	Se realizó una depuración en conjunto con los responsables de la administración de los activos en ambos sistemas para corregir las inconsistencias detectadas.
ESTADO	**NO APLICA** Se procedió a actualizar el hallazgo (Ver hallazgo 09).
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	Se está trabajando en conjunto con estudiantes del TEC la elaboración de una guía para la gestión de problemas de TI.
ESTADO	**PENDIENTE** Aún no se cuenta con este procedimiento. Se indicó que se está trabajando con estudiantes del TEC la elaboración de este. Además, se consultó si se cuenta con un avance sobre este, para lo cual se indicó que aún no.
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	Se subsanaron las deficiencias identificadas, por ejemplo, se activaron las siguientes medidas de seguridad en el sistema: • Se activó el vencimiento de las contraseñas cada 30 días. • Se almacena un histórico de las últimas 6 contraseñas. • Las contraseñas deben contener al menos 6 caracteres.
ESTADO	**EN PROCESO** Se corrigieron los siguientes aspectos: • Vencimiento de las contraseñas del BOS (vencen cada tres meses). • Se cuenta con un histórico de claves. • La contraseña exige un formato específico. • El error que se presentaba en el módulo de cuentas por pagar a la hora de registrar una cuenta, ya no se presenta. Sin embargo, durante la revisión del módulo de contabilidad se evidenció que el estado de flujo de efectivo aún no se genera correctamente, por lo tanto, este todavía debe elaborarse en Excel.

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 centralizó el control de las licencias en Informática, lo que permitió incluir toda la información de licencias en un sistema de información para el control y actualización del inventario.
ESTADO	**EN PROCESO** Actualmente se cuenta con un software para gestionar las licencias de una manera centralizada. Sin embargo, se determinaron diferencias entre el software general y el software instalado por equipo.
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	Se desarrolló el documento de normas institucionales sobre tecnologías de información.
ESTADO	**NO APLICA** Se procede a actualizar el hallazgo (Ver hallazgo 04).
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 un plan estratégico de tecnologías de información, alineados a los objetivos del Museo Nacional, esto por cuanto no se cuenta con un plan estratégico institucional.
ESTADO	**EN PROCESO** De acuerdo con las recomendaciones 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. Se indicó que dicho plan fue presentado ante las diferentes jefaturas, donde se está a la espera de su aprobación oficial. Por tal motivo, esta condición se encuentra en proceso, puesto que solo faltaría su aprobación. • El PAO 2018 se encuentra alineado al PETI. Por lo tanto, esta condición se encuentra cumplida. • El seguimiento al PAO se da a través de informes que se le presentan a la administración de forma anual, por lo tanto, esta condición se encuentra cumplida. Basado en lo anterior, el hallazgo está en proceso debido a que, existen recomendaciones pendientes y en proceso.
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 cuenta con una red nueva, por el proceso de mantenimiento y garantía, se planificó el primer estudio de vulnerabilidad para finales del 2019 e inicios del 2020.

ESTADO	**PENDIENTE** Se indicó que debido a toda la sustitución de la red de datos, no se han realizado estudios de vulnerabilidad, dado que aún se está en proceso de mejoras y actualizaciones. Además, se planea el primer estudio de vulnerabilidad para finales del 2019 e inicios del 2020, por lo tanto, esto evidencia que en el 2018 no se llevaron a cabo.
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 actualizaron los procedimientos relacionados a las bases de datos.

ESTADO	**PENDIENTE** De acuerdo con lo indicado por la jefatura de la Unidad 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, este hallazgo se encuentra 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 ajustó el procedimiento de respaldos a fin de generar bitácoras para los respaldos y restauraciones realizadas.
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

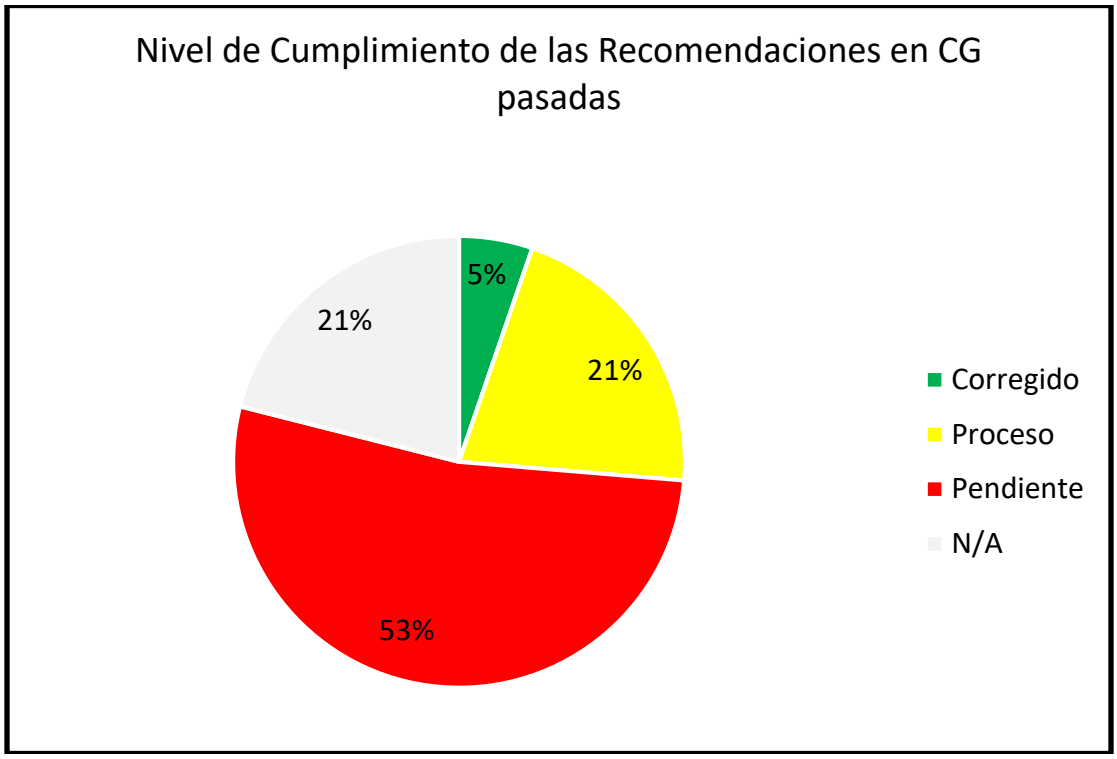
	los respaldos, el tipo de respaldo a realizar, periodicidad, procedimiento para llevar a cabo la restauración de los respaldos de información, etc. Además, tampoco se generaron las bitácoras que evidencien tanto los respaldos como las pruebas realizadas a dichos respaldos en el periodo 2018. Dado lo anterior, este hallazgo se encuentra pendiente.
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	Pendiente la elaboración de un plan de pruebas que abarque todas las actividades de continuidad definidos en el plan.
ESTADO	**PENDIENTE** Se indicó que aún se encuentra pendiente la elaboración de pruebas a todas las actividades incluidas en el plan, además, no se han realizado capacitaciones al personal encargado de la ejecución del manual de contingencias.
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.

	Ya se implementó un sistema de información para el control interno, se está en proceso de pruebas.
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** 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 nos indicó que esto no se iniciado debido a que primero se debía consolidar la Unidad de Informática, definir los procesos y procedimientos.

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

Estado / Año	2017	2016	Total por estado
Corregido	1	0	**1**
Proceso	2	2	**4**
Pendiente	4	6	**10**
N/A	3	1	**4**
Total por año	**10**	**9**	**19**



III. ANEXOS

ANEXO A

Análisis de Riesgos TI
Unidad de Informática

Periodo 2018

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	✗		Actualmente, 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.		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. Además, la puerta es de vidrio.		M
A.10	Alarmas de detección de intrusos		✓	Sí se cuenta con alarmas para detectar intrusos.		M
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 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, 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
A.20	Cableado debidamente rotulado	✗		No todo el cableado se encuentra 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	✗		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 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
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.		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		✓	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.FALLASHARDWARE

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
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.		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 o a través de la herramienta de solicitudes. Las jefaturas realizan dichas 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 2018 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, 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 Riesgos?	✗		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

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
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 2018 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
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.		M
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
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

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
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.		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
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--