Museo Nacional

Informe Auditoría de Sistemas y Tecnologías de Información.

Carta de Gerencia

CG-TI 2023

Informe final

San José, 08 de noviembre de 2024

Señores
Museo Nacional de Costa Rica
Unidad de Informática.

Presente

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2023 al Museo Nacional y con base en el examen efectuado, observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en las normas técnicas para la gestión y control de las tecnologías de la información del MICITT, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2023.

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 de tecnologías de información.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)

Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2024.11.22 10:00:18 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado No. 1649
Póliza de Fidelidad Nº 0116 FIG 7
Vence el 30 de setiembre del 2025.

Nombre del CPA: GERARDO MONTERO MARTINEZ
Carné: 1649
Cédula: 302880821
Nombre del Cliente: MUSEO NACIONAL DE COSTA RICA
Identificación del cliente: 3007075500
Dirigido a: MUSEO NACIONAL DE COSTA RICA
Fecha: 22-11-2024 09:49:38 AM
Tipo de trabajo: INFORME AUDITORÍA DE SISTEMAS Y TECNOLOGÍAS DE INFORMACIÓN.

Timbre de ¢25 de la Ley 6663 adherido y cancelado en el original.

GERARDO MONTERO MARTINEZ
Contador Público Autorizado No. 1649
COSTA RICA

COSTA RICA TIMBRE
25 COLONES 25

Código de Timbre: CPA-25-395905

TABLA DE CONTENIDO

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN

I. INTRODUCCIÓN

ORIGEN DEL ESTUDIO

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

La evaluación la realizamos basados en las normas técnicas para la gestión y control de las tecnologías de la información del MICITT y los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés), y en general las mejores prácticas de la industria de Tecnología de Información.

OBJETIVO DEL ESTUDIO

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

ALCANCE

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

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

PERIODO DEL ESTUDIO

El estudio se realizó durante los meses de octubre y noviembre del 2024 y corresponde a la auditoría del periodo del 2023.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones en el estudio realizado.

METODOLOGÍA

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

II. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: AUSENCIA DE UN MARCO DE GOBIERNO Y GESTIÓN DE TI DOCUMENTADO. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada a la documentación proporcionada como evidencia durante el proceso de auditoría, se identificaron aspectos que carecen de ciertos puntos fundamentales, como la falta de documentación formal sobre el Marco de Gobierno y Gestión de TI, así como la ausencia de implementación de dicho marco.

Por otra parte, evidenciamos la existencia de un documento no formal denominado "Propuesta Proyecto Implementación Normas TI" donde se indica que, como objetivo general se pretende implementar las Normas Técnicas para la Gestión y Control de Tecnologías de Información en el Museo Nacional de Costa Rica (MNCR), para garantizar la seguridad, disponibilidad y eficiencia de los recursos tecnológicos utilizados en la preservación y difusión del patrimonio cultural, natural y arqueológico.

1. Gobernanza de TI.
2. Planificación Tecnologiza Institucional.
3. Gestión de TI.
4. Contratación y Adquisición de Bienes y Servicios Tecnológicos.
5. Gestión de Riesgos Tecnológicos.
6. Seguridad y Ciberseguridad.
7. Desarrollo, Implementación y Mantenimiento de sistema de Información.
8. Arquitectura Empresarial.
9. Administración Infraestructura Tecnológica.
10. Continuidad y Disponibilidad Operativa de los Servicios.
11. Aseguramiento.
12. Recursos Humanos.
13. Calidad de los procesos tecnológicos.
14. Gestión de Proyectos que implementan Recursos tecnológicos.

No contar con un marco de gobierno de TI conlleva el riesgo de desalineación estratégica, donde los proyectos tecnológicos pueden no alinearse con los objetivos organizacionales, generando un uso ineficiente de recursos e inversiones en soluciones de poco valor. Esto afecta la eficiencia operativa, limita la innovación y aumenta el riesgo de incumplimiento normativo, impactando negativamente la reputación de la organización.

CRITERIO:

En las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el MICITT se encuentra el proceso **I. Gobernanza de TI**, donde se menciona: "La institución debe disponer de un marco orientador que permita la definición de la acción institucional con un enfoque de valor público. Asimismo, debe considerar en la estrategia institucional la incorporación de iniciativas habilitadas por tecnologías de información.".

RECOMENDACIONES:

A la Unidad de Informática:

1. Aprobar y comunicar la aprobación del Marco de Gobierno y Gestión de TI para el Museo Nacional.

2. Comenzar con la implementación de las iniciativas establecidas en Plan de Implementación del Marco de Gobierno y Gestión de TI.

3. Realizar al menos una vez al año revisión de los procedimientos establecidos.

4. Revisar el marco de gobierno y gestión de TI regularmente (al menos una vez al año), con el fin de garantizar que éste se mantenga actualizado de acuerdo con los cambios presentados en la organización, sus necesidades y procedimientos del negocio.

HALLAZGO 02: EXISTEN DEBILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN DEL MUSEO NACIONAL DE COSTA RICA. RIESGO ALTO.

CONDICIÓN:

Producto de la revisión efectuada a la estructura organizacional del Museo Nacional, hemos identificado la ausencia de un Comité de Seguridad de la Información (TI) formalmente constituido. Dicha omisión ha llevado a la falta de un marco regulatorio claro que defina aspectos fundamentales como la conformación del comité, sus objetivos, roles, funciones, y la periodicidad con la que deberían realizarse las sesiones. Asimismo, se evidencia la ausencia de un plan de ciberseguridad formalmente establecido.

El no contar con un plan de ciberseguridad no permite asegurar una correcta gestión de la ciberseguridad, lo cual coloca en una posición vulnerable a la información, esto debido a las recientes situaciones de ataques cibernéticos en el país.

CRITERIO:

En las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el MICITT se encuentra el siguiente proceso del Marco de Gestión de TI: **XI. Seguridad y Ciberseguridad** cita: "La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados".

RECOMENDACIONES:

A la Unidad de Informática:

1. Establecer un Comité de Seguridad de la Información y/o definir un equipo para la Gestión de la Ciberseguridad.

2. Establecer un reglamento formal para el Comité de TI, asegurando que incluya al menos los siguientes elementos:
    a. Disposiciones generales.
    b. Objetivo y funciones del Comité de TI.
    c. Roles y responsabilidades del Comité de TI.
    d. Limitaciones del Comité de TI.
    e. Políticas o marco de trabajo.
    f. Participantes de las sesiones.
    g. Condiciones de las sesiones.
    h. Periodicidad de las sesiones.
    i. Composición de las actas.

3. Presentar el reglamento ante la gerencia para su respectiva aprobación, y una vez aprobada comunicarla a todas las áreas involucradas.

4. Comunicar y divulgar al personal respectivo sobre la existencia del reglamento.

5. Definir responsables de gestionar el reglamento, frecuencia de la revisión y actualización de este.

6. Establecer mecanismos de control que ayuden a verificar el cumplimiento de los lineamientos establecidos, así como las acciones a seguir en caso de incumplir con el reglamento.

7. Valorar la necesidad de elaboración de un plan de ciberseguridad para la institución, de manera que se respalde con la política de seguridad de la información y servicios de seguridad existentes, tomando en cuenta las actividades que actualmente se realizan para gestionar la ciberseguridad.

HALLAZGO 03: EXISTEN DEBILIDADES EN EL SISTEMA DE INFORMACIÓN BOS. RIESGO MEDIO.

CONDICIÓN:

Producto del seguimiento dado a los hallazgos de periodos anteriores identificamos uno relacionado con deficiencias en los sistemas de información, a continuación, se indica el hallazgo y una descripción del estado al periodo auditado.

HALLAZGO 10-2017. DEFICIENCIAS EN EL SISTEMA DE INFORMACIÓN BOS.

En cuanto a la atención y seguimiento del hallazgo, se verificó que no se han realizado gestiones para atender el hallazgo, por el contrario, se nos indicó que este ya no aplicaba. Pero pese a la solicitud de requerimientos adicionales, no se recibió evidencia que permitiera validar el motivo por el cual ya no aplica el hallazgo.

Debido a la falta de evidencia para determinar que el hallazgo no aplica y producto de la antigüedad del hallazgo, se procede a realizar una actualización de las recomendaciones.

CRITERIO:

En las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el MICITT se encuentra el siguiente proceso del Marco de Gestión de TI**: XI. SEGURIDAD Y CIBERSEGURIDAD** que indica: “La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.”.

RECOMENDACIONES:

<u>A la Unidad de Informática en conjunto con Financiero Contable:</u>

1. Subsanar las deficiencias identificadas, con el fin de evitar posibles vulnerabilidades en la seguridad lógica del sistema, estas corresponden a aspectos como:
    a. No se realiza un proceso de revisión periódico de las pistas de auditoría por parte de las áreas usuarias.
    b. Existen usuarios que no les vence la contraseña.
    c. No se cuenta con un histórico de claves.
    d. El sistema no exige un tamaño de la contraseña mínimo.

III. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CARTA DE GERENCIA 2021	
HALLAZGO 01: EXISTE INCUMPLIMIENTO DE LA PERIODICIDAD DE LAS SESIONES DE LA COMISIÓN DE INFORMATICA. RIESGO BAJO.	
RECOMENDACIÓN	**A la Comisión de Informática:** 1. Cumplir con la periodicidad de las sesiones establecida en el reglamento o valorar si esta debe cambiarse, según las necesidades del MNCR. 2. Documentar en caso de que se traten temas de interés por la Comisión de Informática en las reuniones de las jefaturas, dichos temas y los acuerdos pactados en la plantilla de las minutas utilizada por la Comisión, con el fin de que se evidencie las reuniones realizadas.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** Como seguimiento del hallazgo se nos indicó que la Unidad de Informática ha realizado solicitudes para cumplir con las sesiones de la Comisión de Informática, sin embargo, no se han realizado convocatorias por parte de la Dirección General, dado lo anterior, no es posible remitir evidencias de seguimiento del periodo 2023, el hallazgo se mantiene pendiente de atender.
HALLAZGO 02: AUSENCIA DE UN CATÁLOGO DE SERVICIOS Y SLAs POR PARTE DE LA UNIDAD DE INFORMÁTICA DEL MUSEO NACIONAL. RIESGO ALTO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Elaborar un catálogo de servicios de TI, identificando los servicios proporcionados por el departamento de informática y documentar cada uno de ellos. Al menos el catálogo de servicios debe contener lo siguiente: a. Descripción del servicio. b. Horas del servicio. c. Contactos. d. Disponibilidad.

	e. Características del servicio. 2. Elaborar un procedimiento para la gestión de acuerdos de nivel de servicio, con los siguientes lineamientos: a. La estructura que debe cumplir cada SLAs. b. La periodicidad con la cual se deben revisar los SLAs. c. El responsable que monitorea el cumplimiento de los SLAs. 3. Elaborar los correspondientes acuerdos de nivel de servicio (SLAs), tomando en consideración los requerimientos y demandas de cada una de las áreas usuarias. Asegurar que los acuerdos de nivel de servicio cuenten con al menos lo siguiente: a. Descripción del servicio. b. Alcance del acuerdo (Se incluye lo que abarca el acuerdo y lo que se excluye). c. Horas en las cuales el servicio estará disponible, incluyendo condiciones especiales para excepciones (por ejemplo, fines de semana, feriados). d. Métricas del servicio tales como: i. Disponibilidad (Nivel de disponibilidad del servicio dentro de las horas acordadas, el cual generalmente es expresado en forma de porcentaje). ii. Confiabilidad (Número máximo de interrupciones del servicio que pueden tolerarse). iii. Rendimiento (Detalles de la capacidad de respuesta esperada del servicio, por ejemplo, número de transacciones a procesar). e. Seguridad (Descripción de las políticas de seguridad asociadas). f. Soporte al cliente. g. Contactos donde el cliente puede llamar o enviar consultas con respecto al servicio. h. Responsabilidades de las distintas partes involucradas en el servicio. 4. Revisar periódicamente los acuerdos de nivel de servicio para asegurar que son efectivos, actuales y que los cambios en los requisitos se tienen en cuenta cuando sea apropiado. 5. Comunicar y divulgar al personal respectivo sobre la existencia del catálogo y procedimiento.

	6. Definir responsables de gestionar el catálogo de servicios y procedimiento, la frecuencia de la revisión y actualización de estos. 7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** Se nos suministró el documento de gestión de incidentes que incluye una sección que lista los servicios de la institución llamada "catálogo de servicios" pero no cumple con la estructura de catálogo mínima requerida solo es una lista de servicios, tampoco se nos suministró un procedimiento específico para la gestión de acuerdos de nivel de servicios. En conclusión, no se adjuntó evidencia que permitiera verificar la atención del hallazgo, además, la administración nos indicó que el hallazgo se encuentra pendiente.
HALLAZGO 03: AUSENCIA DE UN PLAN DE ADQUISICIÓN DE TI. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Elaborar un plan de adquisición de tecnología de información, este plan debe tener como mínimo los siguientes puntos: a. Definir los objetivos o metas de TI y cómo contribuirán a los objetivos del negocio. b. Identificar las necesidades de compra. c. Definir las actividades. d. Responsables. e. Establecer prioridades según las necesidades y áreas más críticas. f. Contemplar el presupuesto. g. Tiempo estimado. h. Enumerar los proveedores potenciales. i. Valorar los riesgos asociados a la adquisición y al recurso propiamente. j. Analizar la flexibilidad que posee el recurso de TI para añadir capacidad y tolerar cambios a futuro. 2. Comunicar y divulgar al personal respectivo sobre la existencia del plan de adquisición de TI.

	3. Definir responsables de gestionar el plan de adquisición, la frecuencia de la revisión y actualización de este. 4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Plan de adquisición de TI, registrado en el Banco de Proyectos MIDEPLAN
ESTADO	**EN PROCESO** Se nos suministró el documento Excel Plan Anual Adquisiciones - Anteproyecto-2024-F_UI, este detalla el plan de adquisiciones que aplican para el 2024, lo cual evidencia que para el periodo auditado la atención del hallazgo estuvo en proceso. Adicionalmente, la Unidad de Informática nos indicó que la atención de recomendaciones comenzaría en 2024, entonces en la auditoría que se realice para ese periodo las recomendaciones del hallazgo ya quedarían atendidas.
HALLAZGO 04: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE DESARROLLO DE SOFTWARE. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Crear y mantener una metodología -o equivalente- que guíe todas las etapas del ciclo de vida del desarrollo de software y su implementación, ya sea basada en una metodología ágil o diseñando una propia, considerando el menos los siguientes aspectos: a. Análisis y toma de requerimientos funcionales y no funcionales. b. Desarrollo de diseños (diagrama de componentes, de clases, de despliegue, paquetes), tomando en cuenta la integración con otros sistemas. c. Programación de acuerdo con estándares, buenas prácticas y metodología de desarrollo utilizada, así como la gestión de control de versiones. d. Desarrollo y ejecución de plan de pruebas (pruebas unitarias, de integración, de aceptación funcional y no funcional), tanto en entorno de pruebas como en entorno de producción. e. Desarrollo de manuales técnicos y de usuario. f. Plan de implementación de sistemas y actualizaciones.

	g. Plan de mantenimiento a los sistemas. 2. Comunicar y divulgar al personal respectivo sobre la existencia de la metodología. 3. Definir responsables de gestionar la metodología, la frecuencia de la revisión y actualización de este. 4. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**EN PROCESO** Se nos suministró la metodología actual de desarrollo de software, pero contiene una estructura muy general, también la metodología SCRUM que según lo indicado se utiliza para gestionar los desarrollos en el Museo Nacional. Sin embargo, estos documentos requieren actualizaciones por su antigüedad y para asegurar que su estructura esté en cumplimiento con las recomendaciones del hallazgo. Por tanto, el hallazgo se encuentra en proceso.
HALLAZGO 05: EXISTEN DEFICIENCIAS EN LA GESTIÓN DE RESPALDOS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Desarrollar un procedimiento detallado para la elaboración de respaldos y recuperaciones de información, o realizar la actualización de los procedimientos existentes en caso de ser necesario, asegurando que contemplen al menos los siguientes aspectos: 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. 4. Revisar periódicamente el procedimiento para asegurar que cumple con lo requerido. 5. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 6. Definir responsables de gestionar el procedimiento, la frecuencia de la revisión y actualización de este. 7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** Los procedimientos para respaldos de información y de bases de datos suministrados siguen manteniendo una estructura inadecuada, con respecto a las bitácoras de respaldo, estas no fueron suministradas. Además, en solicitud de requerimientos adicionales se nos indicó que, a la fecha, no se han atendido las recomendaciones del hallazgo. Por tanto, se encuentra pendiente.
HALLAZGO 06: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD DE LA PLATAFORMA TECNOLÓGICA. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Elaborar un procedimiento para gestionar la capacidad y disponibilidad de la plataforma tecnológica.

	2. 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). 3. 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 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). 4. Revisar periódicamente el procedimiento, los planes y el modelo de monitoreo. 5. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 6. Definir responsables de gestionar el procedimiento, planes y modelo, la frecuencia de la revisión y actualización de estos.

	7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	A la fecha no se han aplicado las recomendaciones.
ESTADO	**PENDIENTE** Se nos suministró una matriz con los comentarios de la administración en respuesta a los requerimientos adicionales; en donde se menciona que a la fecha no se ha aplicado ninguna acción para subsanar las recomendaciones emitidas en el hallazgo. Por lo tanto, se determina el estado del hallazgo en pendiente.
HALLAZGO 07: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE RIESGOS DE T.I. RIESGO MEDIO.	
RECOMENDACIÓN	**A la Unidad de Informática en coordinación con el comité de riesgos:** 1. Elaborar 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	Sin comentarios.
ESTADO	**EN PROCESO** Según la respuesta a los requerimientos iniciales, en el año 2023, se remitió la Propuesta de Plan de Gestión de Riesgos de TI; sin embargo, esta fue rechazada debido a que se comentó que debía utilizarse el instrumento sobre directrices generales para el establecimiento y funcionamiento del SEVRI, y que el plan debía ajustarse al formato específico para estos efectos. Se menciona por parte de la Unidad de Informática que actualmente se está elaborando una nueva propuesta. Por lo anterior, el estado del hallazgo se encuentra en proceso, ya que se están trabajando en las recomendaciones emitidas.
HALLAZGO 08: 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. 3. Revisar periódicamente el procedimiento para asegurar que cumple con lo requerido. 4. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 5. Definir responsables de gestionar el procedimiento, la frecuencia de la revisión y actualización de este. 6. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**EN PROCESO** Como parte del seguimiento al hallazgo se nos suministró un documento con las actividades clave para asegurar la calidad de los servicios informáticos, se cuenta con un total de 10 actividades y para cada una se detalla la forma de realizar dicha actividad. Lo anterior permite comprobar que se han realizado avances en

	la atención del hallazgo, sin embargo, aún no se cuenta con un procedimiento formalmente establecido y aprobado.
HALLAZGO 09: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LOS CONTRATOS DE PROVEEDORES DE TI. RIESGO MEDIO.	
RECOMENDACIÓN	**A la Unidad Informática:** 1. Gestionar la definición de un procedimiento o modelo para la gestión de los seguimientos de los contratos de los proveedores externos. Dicha documentación puede contemplar: a. Contratos que se tiene con proveedores. b. Periodicidad del seguimiento. c. Indicadores de incumplimiento. d. Pruebas de cumplimiento para realizar. e. Documentar los seguimientos realizados. 2. Presentar el procedimiento o modelo ante la comisión de Informática para su respectiva aprobación. 3. Revisar periódicamente el procedimiento para asegurar que cumple con lo requerido. 4. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 5. Definir responsables de gestionar el procedimiento, la frecuencia de la revisión y actualización de este. 6. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Según lo remitido se cumple parcialmente, en este momento iniciamos con el Catálogo Proveedores.
ESTADO	**EN PROCESO** Se nos suministró una matriz con los comentarios de la administración en respuesta a los requerimientos adicionales. Como parte del seguimiento, se menciona que el cumplimiento es parcial y se ha iniciado la creación del catálogo de proveedores. La evidencia presentada incluye el catálogo de proveedores que está

	en desarrollo, lo que demuestra que se están realizando acciones para subsanar el hallazgo. Por lo tanto, se considera que el estado del hallazgo está en proceso de ser atendido.
HALLAZGO 10: OPORTUNIDADES DE MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN DEL MUSEO NACIONAL DE COSTA RICA. RIESGO MEDIO.	
RECOMENDACIÓN	**Al encargado de la seguridad de la información:** 1. Gestionar la definición, aprobación y divulgación de una política de seguridad de la información. 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. 2. Definir responsables de gestionar la política, la frecuencia de la revisión y actualización de este documento. 3. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	En respuesta a la primera consulta, a la fecha no se han aplicado las recomendaciones.
ESTADO	**PENDIENTE**

	Se nos suministró una matriz con los comentarios de la administración en respuesta a los requerimientos adicionales; en donde se menciona que a la fecha no se ha aplicado ninguna acción para subsanar las recomendaciones emitidas en el hallazgo. Por lo tanto, se determina el estado del hallazgo en pendiente.
HALLAZGO 11: EXISTEN DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL MNCR. RIESGO ALTO.	
RECOMENDACIÓN	**A la Unidad de Informática:** Considerar los siguientes aspectos en el área en la cual se encuentra el cuarto de servidores: 1. Asegurarse que la puerta para acceder a este sea de un material difícil de vulnerar y con un tipo de llavín apropiado para garantizar la seguridad del sitio, de ser factible agregar mecanismos automáticos como alarmas en caso de ser forzada la puerta. 2. Valorar la adquisición de un aire acondicionado de respaldo, en caso de que se presente una falla en el aire acondicionado principal. 3. Instalar medidores de temperatura y humedad, de modo que se pueda llevar un mejor control del ambiente y que este no dañe los equipos. 4. Implementar una bitácora de control de ingreso al cuarto de servidores en donde se registren las visitas de externos y se documente como mínimo lo siguiente: a. Nombre del visitante. b. Fecha de la visita. c. Motivo de la visita. d. Hora de ingreso y hora de salida. e. Firma del visitante. 5. Mantener un registro del mantenimiento que se realiza a las UPS.

	6. Etiquetar la totalidad del cableado del cuarto de servidores para mantener un control adecuado de este. **A la Comisión de Informática:** 7. Analizar las vulnerabilidades señaladas, priorizarlas y gestionar su corrección de acuerdo con los recursos y posibilidades que posee el Museo.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** En la respuesta a la matriz de seguimiento se menciona que el hallazgo está en proceso, sin embargo, no se nos suministró evidencia que respalde lo indicado por la Unidad Informática; además, en la respuesta a la solicitud de información adicional se nos indicó que las recomendaciones no se han aplicado. Dado lo anterior, el hallazgo se considera pendiente.
HALLAZGO 12: OPORTUNIDAD DE MEJORA EN EL PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Elaborar y documentar los procedimientos realizados por la Unidad de Informática para la gestión de cambios. Para ello, se debe considerar: 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). 2. 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. 3. 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. 4. Revisar periódicamente el procedimiento para asegurar que cumple con lo requerido. 5. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 6. Definir responsables de gestionar el procedimiento, la frecuencia de la revisión y actualización de este.
COMENTARIOS DE LA ADMINISTRACIÓN	A la fecha no se han aplicado las recomendaciones.
ESTADO	**PENDIENTE** Se nos suministró una matriz con los comentarios de la administración en respuesta a los requerimientos adicionales; en donde se menciona que a la fecha no se ha aplicado ninguna acción para subsanar las recomendaciones emitidas en el hallazgo. Por lo tanto, se determina el estado del hallazgo en pendiente.

HALLAZGO 13: 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: 2. Revisar periódicamente el procedimiento para asegurar que cumple con lo requerido.

	3. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 4. Definir responsables de gestionar el procedimiento, la frecuencia de la revisión y actualización de este. 5. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** Se nos suministró una matriz con los comentarios de la administración sobre las acciones realizadas para subsanar los hallazgos; como parte del seguimiento se menciona que está en proceso, aunque no se nos presentó documentación que respalde el progreso alcanzado. Adicionalmente, en solicitud de requerimientos adicionales se nos indicó que a la fecha las recomendaciones del hallazgo no han sido atendidas. Por lo anterior, se determina que el hallazgo permanece pendiente, debido a la falta de evidencia que permita verificar las acciones correctivas implementadas.
HALLAZGO 14: AUSENCIA DE UNA METODOLOGÍA FORMAL PARA LA GESTIÓN DE ROLES Y PERFILES. RIESGO MEDIO.	
RECOMENDACIÓN	**A Recursos Humanos:** 1. Notificar oportunamente a la Unidad de Informática, el cambio en las condiciones laborales de una persona, con el fin de que se proceda con la debida actualización o eliminación de su cuenta de usuario asociada en la plataforma tecnológica. **A las áreas usuarias en conjunto con la Unidad de Informática:** 2. Definir la periodicidad con la cual se debe realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben generar.

	A la Unidad de Informática: 3. Deshabilitar las cuentas de usuario de funcionarios que cesan sus labores para la Institución según lo informe Recursos Humanos. 4. Valorar si se incluye en el procedimiento DIRG-UI-006_Manual Procedimiento Registro Usuarios Red o se crea uno nuevo, el proceso para la gestión de los usuarios y sus perfiles en los sistemas de información, en el cual se contemplen al menos los siguientes aspectos: a. Actividades para crear, modificar o eliminar un usuario y sus respectivos permisos en los sistemas de información. b. Periodicidad con la cual se debe realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben generar, según lo acordado con las áreas usuarias. 5. Modificar la introducción, el objetivo general y los objetivos específicos del procedimiento contenido en DIRG-UI-006_Manual Procedimiento Registro Usuarios Red, de modo que sean alusivos a este.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**EN PROCESO** Fue posible evidenciar los manuales para el control de acceso web y registro de usuarios de red, estos documentos se crearon en junio de 2017; además se nos suministraron las Normas Institucionales sobre Tecnologías de Información del Museo Nacional de Costa Rica, este documento tiene una fecha correspondiente a junio 2019; como parte de los documentos suministrados se incluye la creación de cuentas nuevas, los accesos a la red interna, accesos y uso al servicio de correo electrónico; sin embargo, la documentación suministrada no profundiza en cuanto a la gestión de los usuarios en los sistemas de información.

	Dado lo anterior, se evidenció que se cuenta con documentación referente a la gestión de usuarios, pero esta debe ser actualizada. Además, existe un usuario que dejó de laborar para el MNCR que se encuentra en el listado de usuarios activos en el Active Diretory, esto se relaciona con la primera recomendación del hallazgo. Por lo tanto, el hallazgo se considera en proceso de ser atendido.
HALLAZGO 15: EXISTEN DEFICIENCIAS EN EL PROCEDIMIENTO DE REVISIÓN DE PISTAS DE AUDITORÍA. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática en conjunto con las Áreas usuarias:** 1. Definir, documentar, aprobar y divulgar una metodología o procedimiento para la gestión y revisión de pistas de auditorías de los sistemas. 2. Definir y documentar las pistas de auditoría en los sistemas utilizados por la Institución. 3. Actualizar regularmente (al menos una vez al año) el documento para el procedimiento de la gestión y revisión de pistas de auditorías de los sistemas. 4. Realizar revisiones periódicas de las pistas de auditoría de los sistemas de información.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** No se nos suministró evidencia que permita verificar la gestión de las pistas de auditoría, tampoco fue posible verificar que exista documentación que permita comprobar que el hallazgo asociado se encuentra en proceso, aunado a esto, en la respuesta a la solicitud de información adicional se confirmó que las recomendaciones no se han aplicado. De acuerdo con lo anterior, las recomendaciones se encuentran pendientes.
HALLAZGO 16: 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 realizó Análisis de Seguridad "SOPHOS Cybersecurity Assessment" NIST Cybersegurity Framework en el 2022.
ESTADO	**CORREGIDO** Se nos suministró una matriz con los comentarios de la administración en respuesta a los requerimientos adicionales; como parte del seguimiento se menciona que está corregido y se realizó un Análisis de Seguridad "SOPHOS Cybersecurity Assessment" NIST Cybersegurity Framework en el 2022, asimismo, se evidencia la existencia de dicho documento el cual respalda lo previamente mencionado y subsana las recomendaciones emitidas. Por lo anterior, se determina el estado del hallazgo en corregido.
HALLAZGO 17: INEXISTENCIA DE UNA METODOLOGÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN TECNOLOGÍAS DE INFORMACIÓN DEL MUSEO NACIONAL DE COSTA RICA. RIESGO MEDIO.	
RECOMENDACIÓN	**A la Unidad de Informática en conjunto con Auditoría Interna:** 1. Definir, documentar, aprobar un procedimiento que permita supervisar, evaluar y valorar el sistema de control interno en la unidad de informática, que contemple modelos de monitoreo de rendimiento. **A la Unidad de Informática** 2. Definir y aprobar planes de acción diferentes para subsanar o atender las recomendaciones presentadas en los hallazgos de las auditorías anteriores, ya sean tanto internas como externas. 3. Realizar avances en los planes de acción definidos para subsanar las oportunidades de mejora identificados anteriormente.

	4. Revisar periódicamente el procedimiento, los planes y el modelo de monitoreo. 5. Comunicar y divulgar al personal respectivo sobre la existencia del procedimiento. 6. Definir responsables de gestionar el procedimiento, planes y modelo, la frecuencia de la revisión y actualización de estos. 7. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** Se presentaron informes de auditoría interna, sin embargo, no se nos suministró la metodología para evaluar control interno en la unidad de informática, ni información que permitiera validar avances en la atención del hallazgo, en la solicitud de requerimientos adicionales se indicó que a la fecha las recomendaciones no han sido atendidas. Por tanto, se encuentra pendiente.
HALLAZGO 18: AUSENCIA DE CAPACITACIONES PARA EL PERSONAL DE LA UNIDAD DE INFORMÁTICA EN EL PERIODO 2021. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática en conjunto con el departamento de RH:** 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. 3. Revisar periódicamente el cumplimiento del plan y el registro de ejecución del plan. 4. Comunicar y divulgar al personal respectivo sobre la existencia del plan. 5. Definir responsables de gestionar el plan y el registro de ejecución del plan, la frecuencia de la revisión y actualización de estos. 6. Tomar en cuenta la normativa nacional e institucional vigente en materia de TI, y marcos de referencia como lo es COBIT.
COMENTARIOS DE LA ADMINISTRACIÓN	Se remiten en Hallazgo 18-2021.
ESTADO	**EN PROCESO** Se nos suministró una matriz con los comentarios de la administración en respuesta a los requerimientos adicionales. Como parte de la evidencia presentada, se incluyeron capacitaciones, certificados y formularios de solicitudes, lo que demuestra que se realizan capacitaciones. Por lo tanto, el hallazgo se considera en proceso de ser atendido.
CARTA DE GERENCIA 2019	
HALLAZGO 01: AUSENCIA DE UN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIÓN	**A la Unidad de Informática en conjunto con las áreas usuarias:** 1. Elaborar un plan estratégico de tecnologías de información (alineado a los objetivos del MNCR) con el propósito de plasmar la situación actual de TI y la situación deseada, y así poder establecer iniciativas concretas que permitan cerrar las brechas. Para ello, se recomienda que el PETI incluya aspectos como los siguientes:

	a. Análisis del negocio (objetivos, procesos de negocio claves, análisis FODA, etc.). b. Situación actual de TI (procesos de TI, principales sistemas que soportan al negocio, análisis FODA de TI). c. Situación deseada de TI (visión de TI, misión de TI, objetivos de TI). d. Iniciativas (corresponden a los proyectos y acciones concretas por realizar para llegar a la situación deseada de TI en el tiempo definido en el PETI). Cada iniciativa puede tener su prioridad, cronograma, recursos, mejoras esperadas por la institución e indicadores de rendimiento. 2. En caso de que se desarrolle un Plan Estratégico Institucional, asegurarse que el PETI se alinee con este. 3. Elaborar informes de seguimiento del PETI al menos cada tres meses, con el fin de dar seguimiento periódico al avance de las iniciativas y corregir posibles desviaciones. 4. Una vez que se cuente con el PETI, alinear los planes anuales de trabajo con este.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** En el documento UI-2024-O-146 (Respuesta Requerimientos Auditoría Externa 2023 TI) se nos indicó que no cuentan con un PETI en la institución, además, en la matriz de seguimiento de hallazgos la administración indicó que se encuentra pendiente de atención. Por tanto, el estado es pendiente.
HALLAZGO 02: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE LOS INVENTARIOS DE LICENCIAS DE SOFTWARE EN EL MNCR. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Identificar las razones por las cuales se están presentando las diferencias entre los reportes que incluyen las licencias de software.

	2. Una vez identificadas las razones, actualizar los respectivos registros con el propósito de mantener una consistencia entre todos los reportes. 3. Realizar revisiones periódicas para determinar qué licencias se encuentran en uso, para determinar la existencia de software no autorizado y para la identificación de necesidades sobre licenciamiento, con el fin de actualizar los respectivos inventarios.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**CORREGIDO** Como parte de la evidencia para el seguimiento del hallazgo, se nos suministró el informe **AI-2023-Inf-02-Auditoría-Licenciamiento-Equipo-Cómputo-2023**, en dicho documento se incluye el seguimiento a los inventarios de licencias de software, en el estudio realizado la auditoría indicó que no se determinaron diferencias entre la cantidad de licencias registradas y la cantidad de licencias instaladas, por lo tanto, no existen inconsistencias. De acuerdo con lo anterior, las recomendaciones del hallazgo se cumplen de manera satisfactoria.
HALLAZGO 03: DEBILIDADES EN LA GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIÓN	**<u>A la Unidad de Informática:</u>** 1. Valorar si se incluye en el manual de contingencias los siguientes aspectos: a. Declarar el alcance, considerando que como mínimo contemple los procesos críticos del negocio que son soportados o apoyados por tecnologías de información. b. Identificar los recursos de tecnologías de información que soportan los procesos críticos del MNCCR contemplados en el alcance del manual. Estos recursos pueden ser hardware, software, equipo de red e incluso funcionarios que participan en la ejecución de dichos procesos. c. Identificar medidas alternas para recuperar los servicios de TI en caso de que un desastre afecte su disponibilidad, y documentar dentro del manual dichas medidas.

	d. Definir los procedimientos necesarios y los responsables de ejecutarlos para restaurar los servicios de TI en caso de un desastre. e. Identificar los actores internos y externos a la organización que pueden eventualmente participar en la ejecución de lo indicado en el manual, especificando los medios para contactarlos. f. Definir los procesos posteriores a la recuperación, considerando evaluación de daños y efectividad del manual de continuidad. 2. Establecer un plan de pruebas basado en el manual de contingencia de TI y ejecutarlo al menos una vez al año, donde su resultado quede documentado con el fin de realizar ajustes necesarios en caso de que se requieran. 3. Realizar capacitaciones, mínimo una vez al año, al personal involucrado en el manual, para que conozcan sus respectivos roles en la ejecución de este. 4. Actualizar o revisar el manual periódicamente y mantener un registro de dichas actualizaciones o revisiones que se realicen.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**PENDIENTE** En la respuesta a la matriz de seguimiento se menciona que el hallazgo se encuentra en proceso, sin embargo, no fue posible verificar si existe documentación que respalde lo indicado, por otra parte, en la respuesta a la solicitud de requerimientos iniciales se mencionó que el Museo se encuentra en definición del Plan de Continuidad y a la fecha no hay uno formalizado. Dado lo anterior, el hallazgo se considera pendiente de atender.
HALLAZGO 04: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LAS BASES DE DATOS DE ACTIVOS SIBINET Y BOS. RIESGO MEDIO.	
RECOMENDACIÓN	**Al Departamento Administrativo y Financiero en conjunto con la Unidad de Informática:**

	1. Realizar una depuración en conjunto con los responsables de la administración de los activos en ambos sistemas, para corregir las inconsistencias detectadas. En caso de que las inconsistencias no puedan corregirse por alguna situación, justificar el motivo de esto. 2. Analizar y establecer mecanismos de control que validen los campos donde se presentan las inconsistencias. 3. Realizar un proceso periódico de validación y comparación de bases de datos (entre el SIBINET y el BOS) con el propósito de verificar que ambas bases de datos no presenten diferencias. En caso de encontrar diferencias en la información, se debe verificar cuál base de datos posee la información correcta, realizar un análisis de causa raíz para subsanar el problema y actualizar la base de datos errónea. Dicha gestión debe quedar documentada.
COMENTARIOS DE LA ADMINISTRACIÓN	El sistema BOS es administrado por el Ministerio de Cultura y el SIBINET por Hacienda, en ambos sistemas los usuarios del Museo Nacional son usuarios finales, y desde TI no tenemos ninguna tarea o actividad técnica en estos.
ESTADO	**PENDIENTE** En la respuesta a la matriz de seguimiento se menciona lo siguiente "El sistema BOS es administrado por el Ministerio de Cultura y el SIBINET por Hacienda, en ambos sistemas los usuarios del Museo Nacional son usuarios finales, y desde TI no tenemos ninguna tarea o actividad técnica en estos". Debido a lo indicado, se comprobó que la Unidad Informática no tiene responsabilidades sobre los sistemas y sus bases de datos, ya que están a cargo de otros ministerios, sin embargo, las recomendaciones se deben atender en conjunto con los responsables, dado lo anterior y debido a que no se entregó información, el hallazgo se mantiene pendiente.
HALLAZGO 05: OPORTUNIDADES DE MEJORA DEL MODELO DE ARQUITECTURA DE INFORMACIÓN. RIESGO BAJO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Considerar integrar los distintos modelos que conforman el modelo de arquitectura de información, en los siguientes aspectos:

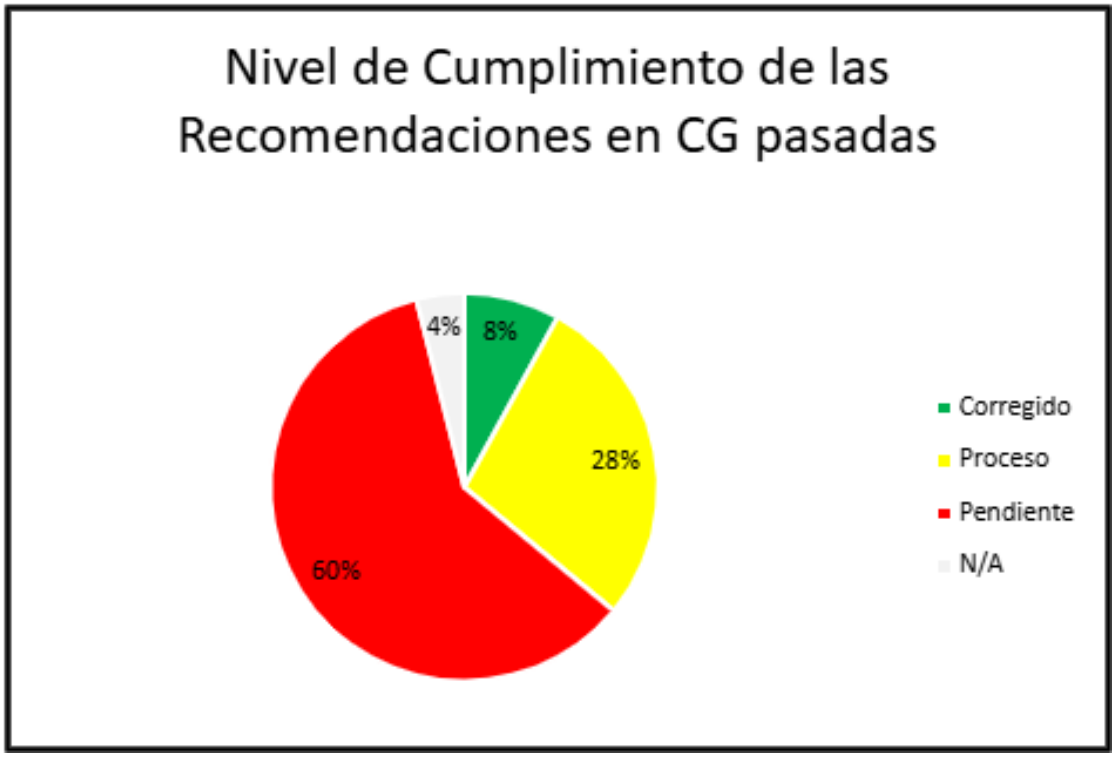
	a. **Modelos de proceso de negocio:** relacionado a identificar la misión, visión, valores y objetivos de la organización. Así como la visión de la arquitectura empresarial y la gestión de los interesados. b. **Modelo de datos**: relacionado a la gestión de la información y procesos. Así como la comprobación del ciclo de vida de la información y las trasformaciones recibidas de los datos durante su recepción y procesamiento. c. **Modelo de aplicaciones:** relacionado a la gestión de aplicaciones corporativas y externas, desarrollo de aplicaciones y sistemas. Así como la debida gestión de la funcionalidad de cada aplicación encontrada en la organización. d. **Modelo de tecnología:** relacionado a la gestión de la tecnología y sistemas de información. Así como la visualización y diagramación de procesos tecnológicos plasmados en la infraestructura, servicios externos o facilitadores del negocio. 2. Revisar el modelo de arquitectura al menos una vez al año. 3. Efectuar las gestiones necesarias para que el modelo de arquitectura cuente con la aprobación formal y sea comunicado a los interesados. 4. Valorar el uso de marcos de referencia como guía para crear un modelo de arquitectura de información robusto. Un ejemplo puede ser: a. TOGAF (The Open Group Architecture Framework): es un marco de referencia utilizado como estándar global para la arquitectura empresarial. Dicho estándar permite asegurar que todas las unidades organizaciones manejen un mismo lenguaje de comunicación, ya que proporciona el diseño, planificación, implementación y gobierno de la información a nivel organizacional.
COMENTARIOS DE LA ADMINISTRACIÓN	El sistema BOS es administrado por el Ministerio de Cultura y el SIBINET por Hacienda, en ambos sistemas los usuarios del Museo Nacional son usuarios finales, y desde TI no tenemos ninguna tarea o actividad técnica en estos.
ESTADO	**PENDIENTE**

	Como parte de la respuesta a los requerimientos adicionales se menciona que el Modelo se encuentra en la lista de los procesos que se deben actualizar, aún no se ha iniciado. Dado que no se ha iniciado con la actualización del Modelo aún no se subsana la recomendación. Por lo anterior, el estado del hallazgo se encuentra pendiente, debido a que no existe ninguna acción por parte de la Unidad de Informática para subsanar las recomendaciones emitidas.
CARTA DE GERENCIA 2018	
HALLAZGO 07: AUSENCIA DE UNA METODOLOGÍA PARA LA GESTIÓN DE PROYECTOS DE TI. RIESGO MEDIO.	
RECOMENDACIÓN	**A la Unidad de Informática:** 1. Documentar una metodología para la administración de proyectos de tecnologías de información, la cual incluya al menos la siguiente estructura: a. Iniciación: Elaborar un acta constitutiva que contenga los elementos principales del proyecto: i. Definición del objetivo y alcance del proyecto. ii. Entregables del proyecto. iii. Descripción del producto final. iv. Presupuesto y costos asociados. v. Personal interesado y sus roles (stakeholders). b. Planeación: Elaborar un plan de trabajo con las tareas y actividades que se deben ejecutar para lograr los alcances definidos: i. Cronograma de trabajo. ii. Criterios de aceptación de los entregables. iii. Riesgos del proyecto. iv. Gestión de cambios del proyecto. v. Aprobación del plan de trabajo. c. Ejecución: Realizar cada una de las actividades previstas en el plan de trabajo i. Alinear la ejecución del proyecto a lo establecido en las etapas de iniciación y planeación. ii. Dar seguimiento a la elaboración de los entregables de modo que cumpla con los criterios de aceptación definidos.

	d. Cierre: Levantar un acta de cierre considerando: i. Aceptación de los entregables. ii. Lecciones aprendidas (mejora continua). iii. Aprobación del proyecto. 2. Valorar el uso de razonables prácticas del mercado para la implementación de una metodología de proyectos como por ejemplo PMBOK y PRINCE2.
COMENTARIOS DE LA ADMINISTRACIÓN	Sin comentarios.
ESTADO	**EN PROCESO** Como evidencia para la gestión de proyectos se nos suministró un procedimiento para el diseño y desarrollo de software, aprobado el 23 de junio del 2017. El documento suministrado solamente abarca proyectos relacionados con desarrollo de software, por lo que cualquier otro tipo de proyecto referente a TI no está contemplado en el alcance de dicho procedimiento. Además, el procedimiento no se encuentra actualizado. Por otra parte, se nos suministró evidencia de los proyectos de inversión, lo cual incluye la matriz de proyectos y documentación relacionada a los proyectos de licenciamiento y equipamiento; también se cuenta con la programación del proyecto de licenciamiento lo cual incluye el detalle del presupuesto. Dado lo anterior, se evidencia que se ha trabajado en la gestión de proyectos, por lo tanto, se considera que el hallazgo aún se encuentra en proceso.
CARTA DE GERENCIA 2017	
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	Sin comentarios.

ESTADO	**NO APLICA** Debido a que el hallazgo se emitió aproximadamente hace 6 años, se procede a actualizarlo, con tal de brindar un mejor seguimiento en las mejoras recomendadas.

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



La siguiente tabla muestra el cumplimiento de recomendaciones por periodo.

Estado de Recomendaciones	2017	2018	2019	2021	Total
Corregidas	0	0	1	1	**2**
En Proceso	0	1	0	6	**7**
Pendiente	0	0	4	11	**15**
No Aplica	1	0	0	0	**1**
Total	**1**	**1**	**5**	**18**	**25**

IV. ANEXO I

Análisis de Riesgos T.I.

Unidad Informática
Periodo 2023

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

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

I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene definido un plan estratégico de TI formalmente aprobado y alineado a los objetivos organizacionales.	✗		No cumple con la condición. Tiene un hallazgo en seguimiento asociado.	M
A.2.	Se le da seguimiento al PETI por parte del Comité de TI.	✗		No cumple con la condición. Tiene un hallazgo en seguimiento asociado.	M
A.3.	Se define anual un plan anual operativo de TI con los proyectos y actividades que realiza el área de TI y se encuentra alineado a las iniciativas y objetivos del PETI.	✗		Cuentan con PAO, pero no está alineado al PETI, ya que no tienen uno establecido.	M
A.4.	Se le da seguimiento periódico al cumplimiento del PAO.		✓	Se cumple con la condición.	B

B. GESTIÓN DEL PRESUPUESTO DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se genera un plan anual presupuestario de TI formalmente aprobado.		✓	Se cumple con la condición.	B
B.2.	El presupuesto se encuentra categorizado y priorizado según las actividades críticas del plan anual operativo de TI.		✓	Se cumple con la condición.	B
B.3.	Se mantiene alineado el plan presupuestario de TI con el plan anual operativo.		✓	Se cumple con la condición.	B

C. GESTIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con un modelo de arquitectura de información formalmente establecido y aprobado.	X		Cuentan con un documento que contiene el modelo de arquitectura de información e infraestructura tecnológica del Museo Nacional. No obstante, existe un hallazgo relacionado, hallazgo 05 del periodo 2019.	B
C.2.	Se le realizan revisiones anuales al modelo de arquitectura para garantizar su actualización de acuerdo con los cambios generados a nivel organizacional.	X		No se cumple con la condición.	M

D. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.1.	Se establecen contratos formales para los servicios que son brindados por terceros.	X		Se cuenta con un catálogo de proveedores, pero no se nos suministró el procedimiento para la gestión de los proveedores de TI.	M
D.2.	Para los contratos de servicios de TI, se establecen acuerdos de nivel de servicio con los respectivos indicadores de capacidad, disponibilidad, confiabilidad, etc.	X		No se cumple con la condición.	M
D.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.	X		No se cumple con la condición.	M

E. GESTIÓN DE LA CALIDAD DE LOS SERVICIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.1.	Se cuenta con una política, metodología o procedimiento para la gestión de la calidad de los servicios de TI.	X		No existe una metodología o procedimiento formal, solo se tienen mapeadas las actividades de calidad.	M
E.2.	Se han definido indicadores clave de los procesos de TI realizados para determinar el rendimiento de los servicios brindados.	X		No se cumple con la condición.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.3.	Se realizan evaluaciones periódicas de la calidad de los servicios de TI para determinar las principales deficiencias y mejoras, y se genera el respectivo plan de acción.	X		No se cumple con la condición.	M
E.4.	La normativa y demás documentación de TI es revisada y actualizada periódicamente.	X		No se cumple con la condición.	M

F. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.	X		Se cuenta con un procedimiento no formal para la gestión de riesgos, sin embargo, esta aún se encuentra establecida como una propuesta, asimismo existe un hallazgo relacionado, hallazgo 07 del periodo 2021.	M
F.2.	La evaluación de riesgos de TI es periódica y se encuentra revisada y aprobada por la administración (de acuerdo con el nivel de tolerancia al riesgo organizacional).	X		No se cumple con la condición.	M

G. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se cuenta con un catálogo de servicios de TI actualizado y aprobado por el Comité de TI.	X		No se cumple con la condición.	M
G.2.	Se cuenta con una política o procedimiento para la gestión de los acuerdos de nivel de servicio (SLAs) de TI.	X		No se cumple con la condición.	M
G.3.	Se tiene definido acuerdos de nivel de servicio para cada uno de los servicios activos que se encuentran definidos en el catálogo.	X		No se cumple con la condición.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.4.	Cada uno de los SLAs tiene establecido las responsabilidades de las partes, indicadores (disponibilidad, capacidad, confiabilidad, etc.) y requerimientos de soporte.	X		No se cumple con la condición.	M
G.5.	Se verifica el cumplimiento, validez y actualización de los SLAs establecidos con las áreas usuarias de manera periódica.	X		No se cumple con la condición.	M

II. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

H. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.1.	Se cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.	X		No se cuenta con una metodología para gestionar proyectos, el hallazgo asociado a dicha situación (hallazgo 07 del 2021) se encuentra en proceso de ser atendido.	M
H.2.	Se documenta cada una de las fases del ciclo de vida del proyecto para cada uno de los proyectos ejecutados por el área de TI (constitución, estimación de recursos, responsabilidades, cronograma, desempeño, riesgos, calidad, cambios y cierre del proyecto.)	X		No se cumple con la condición.	M

I. GESTIÓN DE DESARROLLOS DE SOFTWARE.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.1.	Se cuenta con una metodología para el desarrollo e implementación del software.	X		No se cumple con la condición.	M
I.2.	Las bases de datos poseen logs para registrar los cambios y mantener una trazabilidad de estos.	X		No se cumple con la condición.	M
I.3.	Se cifra la información más sensible de las bases de datos.	X		No se cumple con la condición.	M

J. GESTIÓN DE CAMBIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.1.	Se cuenta con una política y/o procedimiento para la gestión de cambios de TI.	✗		Se cuenta con un procedimiento para la gestión de cambios, sin embargo, existe un hallazgo relacionado, hallazgo 12 del periodo 2021.	M
J.2.	Los cambios se realizan a través de solicitudes formales y se documenta todo el proceso realizado (ciclo de vida).	✗		No se cumple con la condición.	M
J.3.	La documentación de los cambios se mantiene de forma centralizada (mesa de servicios).	✗		No se cumple con la condición.	M
J.4.	Se evalúa periódicamente el estado de los cambios para verificar que todas las solicitudes hayan sido atendidas.	✗		No se cumple con la condición.	M

K. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
K.1.	Se mantienen controles para el ingreso y salida de equipo tecnológico a la organización.		✓	Se cumple con la condición.	B
K.2.	Se cuenta con un inventario de activos de TI (equipo en uso y desuso, periféricos, equipo de comunicación, dispositivos móviles, etc.), junto con información de su ubicación y responsable.		✓	Se cumple con la condición.	B
K.3.	Se mantiene un inventario actualizado de las licencias de software, así como un catálogo de software permitido en la organización.	✗		Se cuenta con un inventario de licencias, pero no se nos suministró evidencia del software permitido.	M
K.4.	Se verifica periódicamente que el software instalado en los equipos corresponda a las licencias adquiridas y al software permitido en la organización.		✓	Se cumple con la condición, se evidencia con la auditoría de licenciamiento realizada en 2023.	B

III. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

L. GESTIÓN DE INCIDENTES.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
L.1.	Se cuenta con un procedimiento para la gestión de incidentes de TI.		✓	Se cumple con la condición.	B
L.2.	La gestión de incidentes se mantiene centralizada (mesa de servicios).		✓	Se cumple con la condición.	B
L.3.	Se verifica periódicamente el estado de los incidentes para determinar si se atienden oportunamente los incidentes registrados.		✓	Se cumple con la condición.	B

M. GESTIÓN DE PROBLEMAS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
M.1.	Se cuenta con un procedimiento para la gestión de problemas de TI.		✓	Se cumple con la condición.	B
M.2.	Se identifica, clasifica y analiza la causa raíz de los problemas de TI.		✓	Se cumple con la condición.	B

N. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
N.1.	Se cuenta con un plan de continuidad del negocio (con el componente de TI), formalmente establecido y aprobado por la administración o el Comité de TI.	✗		No se cumple con la condición.	A
N.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗		No se cumple con la condición.	A
N.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.	✗		No se cumple con la condición.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
N.4.	Se realizan pruebas a los respaldos de información.	✗		No se cumple con la condición.	M
N.5.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).	✗		No se cumple con la condición.	M

O. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
O.1.	Se cuenta con una política de seguridad de la información formalmente aprobado por la administración y divulgado a nivel organizacional.	✗		No se cumple con la condición.	A
O.2.	Se le brinda seguimiento al cumplimiento de la política de seguridad de la información (se aplican medidas correctivas) y se le comunica los resultados a la administración.	✗		No se cumple con la condición.	A
O.3.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.	✗		No se cumple con la condición.	M
O.4.	Se revisan periódicamente los perfiles de los usuarios para determinar si estos poseen la cantidad de accesos mínimos necesarios.	✗		No se cumple con la condición.	M
O.5.	Se inhabilitan las cuentas de los usuarios que cesan funciones en la organización (despidos, renuncias, jubilaciones, vacaciones, permisos, etc.).	✗		No se cumple con la condición.	M

IV. EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

P. VALORAR EL CONTROL INTERNO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
P.1.	Se han establecido normas para la evaluación del control interno de TI.	✗		No se cumple con la condición.	M
P.2.	Se realizan autoevaluaciones periódicas para que TI identifique de manera proactiva las debilidades de control.		✓	Se cumple con la condición.	B
P.3.	Se ejecutan estudios de auditoría periódicos (internos o externos) para identificar debilidades en el cumplimiento de obligaciones con normativas relativas a TI.		✓	Se cumple con la condición.	B

V. SISTEMAS DE INFORMACIÓN.

Q. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
Q.1.	Existencia de pistas de auditoría o bitácoras en los sistemas de información que permitan tener una trazabilidad en las transacciones realizadas por los usuarios.	✗		No se cumple con la condición.	M
Q.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.	✗		No se cumple con la condición.	M

--Fin del documento--