24 de octubre de 2024

MUNICIPALIDAD DE CARTAGO
AUDITORÍA INTERNA

AI-INF-004-2024

Informe Final

Auditoría de Carácter Especial de Tecnología de Información y Comunicaciones sobre:
La Administración de la Infraestructura Tecnológica

SERVICIOS DE AUDITORIA

www.muni-carta.go.cr Tel.: (506) 2550-4400 (506) 2550-4600 Fax: (506) 2551-1057Apdo.: 298-7050
Auditoría Interna Ext.: 4439/4440/4441 auditoriainterna@muni-carta.go.cr

CONTENIDO

1 INTRODUCCIÓN 1
1.1 Origen del estudio 1
1.2 Objetivo General 1
1.3 Alcance y Período del estudio 1
1.4 Criterios de Auditoría 2
1.5 Metodología aplicada 3
1.6 Generalidades sobre el ejercicio de la Auditoría Interna 3
1.7 Limitaciones que afectaron la ejecución de la auditoría 4
1.8 Antecedentes del estudio 4
1.9 Comunicación preliminar de los resultados 5
2 RESULTADOS DEL ESTUDIO **7**
2.1 Debilidades de control en el registro y control del Inventario de Infraestructura Tecnológica 7
2.2 Debilidades en el proceso de gestión de la Configuración (CMDB) 14
2.3 Debilidades en el proceso de Gestionar las operaciones 17
3 CONCLUSIONES 22
4 RECOMENDACIONES 24
4.1 Al Alcalde Municipal 24
4.2 Al Encargado del Área de Informática 24
5 ANEXOS AL INFORME 27

RESUMEN EJECUTIVO

¿Qué examinamos?

La efectividad y suficiencia del sistema de control interno en el Área de Informática respecto de los procesos de gestión de activos de TI, gestión de la configuración, gestión de la operaciones, gestión de Incidentes, asignación y ejecución presupuestaria, que están relacionados con la Administración de la Infraestructura de TI según la normativa y buenas prácticas aplicables, esto con el propósito de establecer posibles desviaciones y de esta manera confrontarlas con dichos criterios y poder realizar las recomendaciones respectivas. El estudio abarcó los ejercicios económicos 2022-2023 y se extendió cuando así se requirió.

¿Por qué es importante?

La "ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLOGICA" es un proceso de relevancia dentro de las operaciones de la Institución, que en los últimos años ha presentado un incremento considerado en la adquisición de nuevos recursos tecnológicos (hardware- Software, licenciamientos, otros), principalmente por el cambio tan acelerado en el uso de las Tecnologías de Información, invirtiéndose grandes cantidades de dinero con el fin de garantizar un funcionamiento óptimo de la infraestructura de TIC´s, con el objetivo de asegurar la disponibilidad, seguridad y rendimiento de los recursos tecnológicos que dan soporte a la operativa de la Institución y que permita brindar un mejor servicio a la ciudadanía Cartaginesa.

¿Qué encontramos?

La revisión efectuada permitió determinar importantes debilidades vinculadas a las tareas y actividades asociadas al proceso de administración de la infraestructura tecnológica, específicamente para los procesos relacionados con gestión de los activos, gestión de la configuración y gestión de las operaciones; además, de las consideraciones referentes a las debilidades del marco normativo interno establecido por la Municipalidad.

Al respecto, se comprobó que aunque la Institución cuenta con prácticas formales para gestionar todos los Activos Municipales, incluyendo los Activos de TI; se presentan deficiencias en el control diseñado para su registro, así como inconsistencias en la información almacenada de algunos activos referente a computadoras, servidores, router, modem, que no tienen registrados algunas características como detalle, marca, modelo, serie, lo que impide conocer con exactitud toda la información de dichos recursos tecnológicos.

Aunado a lo anterior, se determinó que el Área de Informática, carece de prácticas formales como políticas, procedimientos, directrices para gestionar los activos de TI, gestionar la configuración y gestionar las operaciones, según lo establece el Marco de Gobierno y gestión de la Tecnologías de Información, limitando dicho procesos a herramientas de Ofimática de Microsoft Office en el programa en Excel, con muy escasos controles sobre el detalle técnico (Inventario de Activos de TI) contrario a lo sugieren las mejores prácticas, asimismo la carencia de un repositorio de configuración (CMDB) que contenga los registros de configuración a lo largo de su ciclo de vida de los servicios, activos de TI, infraestructura y registro de elementos de configuración (CI), incluidos las relaciones entre ellos los elementos TIC (servidores, firewall, routers), los servicios de proveedores, el software, las personas, documentación.

En esa línea, se denota la ausencia de bitácoras sobre la realización de la ejecución de las tareas operativas asignadas a los profesionales de Infraestructura, la cual establezca las actividades a realizar, su frecuencia y el responsable de ejecutarlas, lo que ayudaría a determinar cualquier evento detectable que sea de importancia para la Administración de la Infraestructura de TI y que pueda interrumpir la continuidad del Negocio, lo cual, se debería canalizarse a través del sistema automatizado de gestión de Incidentes, creando el respectivo incidente que ayudaría a documentar su ciclo de vida, hacer la gestión más eficiente, además de poder monitorearlo de manera adecuada posteriormente.

En síntesis, el proceso de administración de la infraestructura tecnológica, en lo que refiere a los procesos de gestión de activos de TI, gestión de la configuración y gestión de las operaciones, no se realiza en observancia razonable al marco técnico y buenas prácticas rige la materia, y presenta importantes oportunidades de mejora en relación a asuntos de marco normativo interno, diseño e implementación de controles y demás gestiones administrativas que fortalezcan el proceso bajo estudio, lo que indica que, la Administración debe fortalecer las labores del proceso, considerando la necesidad de establecer procesos formales conforme al marco normativo y las buenas prácticas, que permitan bajo procedimientos adecuados y técnicamente estructurado, garantizar que la infraestructura tecnológica institucional sea administrada adecuadamente, y con ello, efectuar las operaciones con eficiencia, eficacia y economía, salvaguardándose y protegiendo la utilidad de los activos, la seguridad de la información y la continuidad de la operación municipal.

¿Qué sigue?

Al Alcalde Municipal, se le recomienda que: 1. Gire las instrucciones que correspondan, orientadas al cumplimiento de las recomendaciones emitidas por la Auditoría Interna; y 2. Apruebe conforme sus competencias, la propuesta de procedimientos y prácticas formales que se determinen del análisis realizado por el Área de Informática.

Al Encargado del Área de Informática, se le recomienda 1- a) Establecer, documentar, y divulgar las políticas, procedimientos y directrices formales referente al proceso de Gestión de Activos de TI, Gestión de la Configuración y Gestionar las operaciones, ya que son procesos primarios para realizar una adecuada Administración de la Infraestructura Tecnológica; 2- Implementar soluciones automatizadas como herramientas para administrar el inventario de TI y el repositorio de configuración (CMDB), y 3- Eleve a aprobación del Alcalde según corresponda, las políticas, procedimientos y directrices formales referentes a la gestión de los activos, gestión de la configuración y gestión de las operaciones.

1 INTRODUCCIÓN

1.1 Origen del estudio

Con fundamento en el Plan Anual de Trabajo de Auditoría Interna para el año 2024, específicamente el aparte 5.2. referente a "Servicios de auditoría y/o preventivos en tecnologías de información y comunicaciones planificados para el periodo 2024."; así como, las atribuciones conferidas en la Ley General de Control Interno[1], las Normas Generales de Auditoría para el Sector Público[2] emitidas por la Contraloría General de la República; así como, el Reglamento de Organización y Funcionamiento de la Auditoría Interna de la Municipalidad del Cantón Central de Cartago[3], este Despacho dispuso llevar a cabo una "**Auditoría de Carácter Especial de Tecnología de Información y Comunicaciones sobre la Administración de la Infraestructura Tecnológica**."

1.2 Objetivo General

- ✓ Verificar la implementación, cumplimiento y seguimiento de prácticas formales para una adecuada administración de los recursos tecnológicos instalados en la institución, administrados interna y externamente.

1.3 Alcance y Período del estudio

El estudio se llevó a cabo en el Área de Informática en relación con el proceso de Administrar la Infraestructura de TI, realizado durante el periodo 2022 y 2023 y se extendió en los casos que se requirió. Adicionalmente se involucró a otros departamentos y funcionarios asociados o que en el estudio se determinaron involucrados con el proceso

[1] Publicada en La Gaceta 169 del 04/09/2002
[2] Publicadas en La Gaceta 184 del 25/09/2014
[3] Publicada en La Gaceta 130 del: 07/07/2009

auditado; abarcando lo relacionado a: 1. gestionar los activos de TI, 2. gestionar la configuración, 3. gestionar las operaciones, 4. plan efectivo de capacitación, formación y actualización tecnológica, así como 5. ejecución Presupuestaria para los recursos de Infraestructura Tecnológica.

Lo anterior, fue comunicado a la Administración Activa través del oficio AI-OF-174-2024, fechado 05 de Julio del 2024 y remitido al Lic. Mario Redondo Poveda, Alcalde Municipal y al Lic. Daniel Ramírez Gonzalez, Encargado a.i. Área de Informática.

1.4 Criterios de Auditoría

La comunicación de los criterios de evaluación aplicados en la presente auditoría se efectuó el día 05 de Julio del 2024, según consta en oficio número AI-OF-174-2024, concediendo un plazo de dos (2) días hábiles para la remisión de observaciones a los criterios auditores; del cual no se obtuvo respuesta con observaciones referentes al fondo del tema comunicado.

Para la ejecución de la presente auditoría se emplearon principalmente, los siguientes criterios: Ley General de Control Interno Ley N° 8292; Normas de control interno para el Sector Público (N-2-2009-CO-DFOE) emitidas por la Contraloría General de la República; Marco Normativo Gobierno y Gestión TI del MICITT, emitido mediante Oficio MICITT–DGD-OF-215-2021 el 11 de noviembre del 2021; COBIT (Objetivos de Control para Información y Tecnologías Relacionadas), en su versión 2019; Procedimiento 7P04 Gestión de TI; Normas Técnicas de Gobierno y Gestión de las Tecnologías de Información para la Municipalidad de Cartago; procedimientos e instructivos internos vigentes, manuales internos, entre otras normas y criterios aplicables que se definieron durante el desarrollo del estudio.

1.5 Metodología aplicada

Para efectos del presente estudio se llevaron a cabo entrevistas, reuniones y consultas por correo con el personal destacado en el Área de Informática y otra Áreas o departamentos relacionados con el tema de estudio, con el propósito de validar la información suministrada, así como, la aplicación de pruebas de auditoría y muestreos conforme los criterios de auditoría comunicados a la Administración.

Respecto a los muestreos, se utilizaron del tipo no probabilístico y conveniencia/selectivo/juicio-criterio, según lo determinó el Encargado de Estudio, por la necesidad de cada procedimiento de auditoría en particular y por el tipo y cantidad de información que se requirió analizar.

De igual manera, se remitieron oficios y correos electrónicos, mediante los cuales se solicitaron reportes y/o informes de gestión, expedientes conformados, accesos a sistemas informáticos, entre otros; relacionados con las actividades propias del proceso objeto de estudio, con el fin de llevar a cabo el respectivo análisis, verificación, revisión y corroboración, tanto física como digital, de dicha información, insumos que, resultan necesarios para la determinación de posibles hallazgos de auditoría.

1.6 Generalidades sobre el ejercicio de la Auditoría Interna

El trabajo se efectuó de conformidad con lo dispuesto en las Normas Generales de Auditoría para el Sector Público, dictadas por la Contraloría General de la República, el Reglamento de Organización y Funcionamiento de la Auditoría Interna de la Municipalidad del Cantón Central de Cartago y, demás normativa aplicable.

Se recuerda que, en materia de informes de Auditoría Interna, prevalecen los artículos N° 12 inciso c), N°35, N° 36, N°37 y N° 38 de la Ley General de Control Interno, conocidos ampliamente por la Administración Activa.

1.7 Limitaciones que afectaron la ejecución de la auditoría.

Durante el desarrollo del estudio, se presentaron limitaciones que afectaron la ejecución de las actividades relacionadas a las actividades de planificación y examen, así como, los procedimientos de auditoría inmersos en estas; principalmente debido a que el Área de Informática se encuentra en proceso de implementada la Normativa de Gobierno y Gestión de la Tecnologías de Información, alineada a las mejores prácticas de COBIT 2019, además que dicha Área continua en un estado invariable en el cual aún no logran implementar o adaptarse a las mejores prácticas en cuanto a la gestión de TI; en ese sentido al momento de solicitarse la información correspondiente, no se obtenía lo solicitado o se entregaba otra información que no se estaba solicitando, lo cual, dificultó en el avanzar en la revisión, ya que se tuvo que recurrir a otros medios (consulta/cotejo directo en Sistemas Informáticos) o solicitándose nuevamente la información.

1.8 Antecedentes del estudio

El proceso de Administrar la Infraestructura de Tecnología de Información forma parte del nuevo Marco Normativo de Gobierno y Gestión de las Tecnologías de Información, el cual orienta a la institución en la implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos, de forma tal que se garantice la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, entrega de valor y el cumplimiento normativo.

En ese sentido dicha normativa estableció el proceso es el XII. ADMINISTRACIÓN INFRAESTRUCTURA TECNOLÓGICA, asimismo para su implementación se agrupa con otros procesos de implementación de las buenas prácticas tales:

1- **Gestionar los activos** a lo largo de su ciclo de vida para asegurarse de que su uso proporcione valor a un costo óptimo, permanezcan operativos (adecuados para su propósito) y están contabilizados y protegidos físicamente.

2- **Gestionar la Configuración** busca definir y mantener descripciones y relaciones entre recursos y capacidades claves necesarios para brindar servicios habilitados para TI, incluir información de configuración, estableciendo líneas base, verificando y auditando la información de configuración y actualizando el repositorio de configuración.

3- **Gestionar las operaciones** busca coordinar y ejecutar las actividades y procedimientos operativos necesarios para brindar servicios de TI internos y subcontratados. Incluye la ejecución de procedimientos operativos estándar predefinidos y las actividades de seguimiento requeridas.

4- **Gestión de Incidentes** Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda gestionarse de forma eficaz y pueda mantenerse un registro histórico completo.

1.9 Comunicación preliminar de los resultados

La comunicación preliminar de los resultados, conclusiones y recomendaciones producto de la auditoría a la que alude el presente informe, se convocó para las once horas del 17 de octubre del 2024, según consta en oficio Nro. AI-OF-263-2024 de fecha 15 de octubre cursado a: Lic. Mario Redondo Poveda, Alcalde Municipal y al Lic. Daniel Ramírez González Encargado a.i. Área de Informática.

Así las cosas y conforme al ACTA COMPARECENCIA EXPOSICIÓN DE RESULTADOS número ACE-002-2024, se realizó la conferencia en las Oficinas de la Auditoría Interna, contándose con la asistencia de los funcionarios municipales Licda. Silvia Navarro Gómez,

Vicealcaldesa Municipal, Lic. Daniel Ramírez González, Encargado a.i., Área de Informática, y Lic. Juan Arias Artavia, Sub Encargado a.i., Área de Informática.

El borrador de este informe se comunicó mediante oficio No. AI-OF-265-2024 del 18 de octubre del 2024 y fue dirigido a: Lic. Mario Redondo Poveda, Alcalde Municipal y al Lic. Daniel Ramírez González, Encargado a.i. Área de Informática; esto con el propósito de que, formularan y remitieran a esta Auditoría Interna, en un plazo no mayor a tres días (3) hábiles, las observaciones y/o comentarios que consideraran pertinentes sobre su contenido, con la respectiva documentación de respaldo.

Mediante Oficio AIN-OF-198-2024, fechado el 21 de octubre del 2024, se reciben observaciones del informe borrador, dichas observaciones no modifican el contenido del informe borrador, sino se indica en términos generales cómo van a implementar cada recomendación.

2 RESULTADOS DEL ESTUDIO

Una vez realizada la recopilación de la documentación necesaria para llevar a cabo el estudio y efectuado el análisis de la información, considerando tanto el marco jurídico y técnico, así como el sistema de control interno, y las actividades administrativas del Área de Informática relacionados con la Administración de la Infraestructura Tecnológica, específicamente en asuntos relacionados con la gestión de Activos de TI, gestión de la configuración, gestión de la operaciones, gestión de incidente , se procedió a elaborar el presente informe, que contiene los hallazgos de relevancia a ser comunicados, respecto a las actividades evaluadas para los ejercicios económicos 2022 y 2023 ampliándose en aquellos casos que se consideró pertinente.

2.1 Debilidades de control en el registro y control del Inventario de Infraestructura Tecnológica

Producto del examen realizado, para lo cual se pretendió validar que la Institución contara con prácticas formales para gestionar todos los Activos Municipales Informáticos (Activos de TI), aplicando controles adecuados para esa tarea, se determinó que el Área de Informática, carece de prácticas formales y técnicas para gestionar los activos de TI a través de un sistema o aplicación informática, limitando el registro y control de dicho proceso en un archivo en la herramienta Ofimática de Microsoft Office en el programa Excel; el cual carece de controles y aspectos de seguridad que si brinda un sistema informático, situación que pone en riesgo la perdida, sustracción o mal manejo de la información ahí consignada.

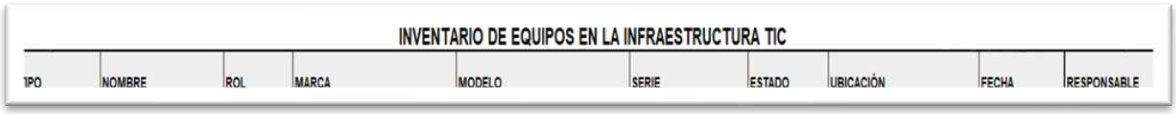
En línea con lo anterior, se observó que se cuenta con dos documentos en formato Excel que integran el inventario de activos de TI, uno denominado "*Inventario para el Hardware Municipal de Cartago*" y otro "I*nventario de equipos en la infraestructura TIC*", sobre los cuales se evidenció lo siguiente:

✓ Se gestiona el inventario en una herramienta de Ofimática de Microsoft Office en el programa Excel, lo cual carece de controles de seguridad de la Información (Integridad, Disponibilidad, Confidencialidad), que podría ser manipulado adicionando o eliminando información, perdiéndose la integridad de los datos, sin asegurarse el acceso oportuno a los datos por parte de las personas autorizadas en el momento que lo requieran, ni garantizarse que la información contenida en dicho inventario no va sea accedida ni divulgada por personas no autorizadas; en esa misma línea, la herramienta utilizada no permite disponer de pistas de auditoría, en las cuales se pueda documentar cualquier modificación, actualización, eliminación u otros realizado en los registros con el fin de poder identificar posibles inconsistencias.

✓ Los controles de inventarios llevados por el Área de Informática, no mantienen uniformidad en los registros de información que se llevan; como se observó, el Inventario de Hardware Municipal de Cartago, contiene registro sobre los siguientes aspectos: Departamento, Nombre de Equipo, Usuario, Marca, Modelo, Serie, Tipo, Disco Duro, Windows, Office, Placa CPU, Placa Monitor (1), Placa monitor (2), Año Compra, Condición, Observaciones; mientras que el inventario de equipos en la infraestructura TIC, contiene registro sobre los siguientes aspectos: Tipo, nombre, rol, marca, modelo, serie, estado, ubicación, fecha, responsable.

✓ El control “Inventario de equipos en la Infraestructura TIC”, no consigna el registro del identificador único o número de placa del activo, lo que obstaculiza la oportuna individualización del activo y su identificación en el inventario Institucional llevado en el sistema de Wizdom.

Imagen No. 01
Municipalidad de Cartago
Auditoría Interna
Control "INVENTARIO DE EQUIPOS EN LA INFRAESTRUCTURA TIC"
Octubre de 2023



Fuente: Control "Inventario equipos en la Infraestructura TIC" facilitado por el Área de Informática.

✓ Tanto el "Inventario de Hardware Municipal de Cartago" como el "Inventario de equipos en la infraestructura TIC", carecen de controles que se establecen en mejores prácticas como COBIT 2019, ITIL, referentes al tema de Inventario de Activos de TI, en los cuales deben contener como se muestra en el siguiente cuadro:

Cuadro No. 01
Municipalidad de Cartago
Auditoría Interna
Comparativo de controles de acuerdo con las mejores prácticas, relacionadas con el inventario de Activos Institucional y del Área de Informática
Octubre de 2023

Controles definidos según las mejores prácticas COBIT 2019, ITIL.	Inventario TI (hardware)	Inventario TI (infraestructura)	Inventario Wizdom
Id Activo	X	X	✓
Nombre	✓	✓	✓
Descripción	X	X	✓
Oficina donde está asignado el Activo	✓	✓	✓
Fecha de Ingreso del Activo al registro o inventario	X	X	✓
Fecha de ultima conciliación de estado físico vrs Lógico	X	X	X
Criticidad del Activo (Confidencialidad, Integridad, disponibilidad)	X	X	X
Riesgo (bajo, medio, alto) de los activos de TI en caso de fallos.	X	X	X
Se aplica un mantenimiento preventivo regularmente a los activos de TI.	X	X	X
Fecha del último mantenimiento preventivo	X	X	X
Etiquetas físicas (código de barras o Metálicas)	✓	X	✓
Responsable (Propietario del Activo)	✓	✓	✓
Custodio (Custodio del Activo)	X	X	✓

Estado asignación de Activo	X	X	✓
Dirección de red (si es estática)	X	X	X
Dirección del MAC adres	X	X	X
Valor original (compra)	X	X	✓
Valor unitario actual	X	X	✓
Estado del Activo (Depreciado, Activo)	✓	✓	✓
Estado conservación del activo (malo, regular, bueno, excelente)	X	X	X
Estado de uso (son adecuados para su propósito)	X	X	X
Licencias o software instalado.	✓	X	X

Fuente: Elaboración propia de la Auditoría Interna.

✓ El control denominado “Inventario de Hardware Municipalidad de Cartago”, no es llenado completamente a pesar de disponer registros para Modelo, Año de compra; en esos campos no se adiciona información alguna.

Imagen No. 02
Municipalidad de Cartago
Auditoría Interna
Control “INVENTARIO DE HARDWARE MUNICIPALIDAD DE CARTAGO”
Octubre de 2023

Inventario de Hardware Municipalidad de Cartago

Departamento	Nombre Equipo	Usuario	Marca	Modelo	Serie	Tipo	Memoria	Disco Duro	Windows	Office	Placa CPU	Placa Monitor (1)	Placa Monitor (2)	Año Compra	Condición	Observaciones
Acueductos	DFCCPAC01	Roberto Valderramos Sanchez	HP		MXL2510DH9	Escritorio	8 GB	1TB	Windows 10	2016	6275	6270				
Acueductos	PFCCPAC07	Cassius Bonilla Lopez	DELL		CTQSDK3	Portátil	32 GB	1TB	Windows 10	365	18953	6340	6736		CADUCADO	
Acueductos	DFCCPAC04	POR ASIGNAR	HP		NO POSEE	Escritorio	4 GB	500 GB	Windows 10	2016	6075	11763			2024	
Acueductos	DFCCPAC06	Raul Hidalgo Maroto	HP		MXL746269C	Escritorio	8 GB	1TB	Windows 10	2016	13265	12025			ACTIVO	
Acueductos	PFCCPAC01	Julio Urbina Rojas	LENOVO		PF39JY75	Portátil	16 GB	500 GB	Windows 10	365	18320					
Acueductos	PFCCPAC19	Gerardo Fernandez Calderon	DELL		ir76ik3	Portátil	32 GB	1TB	Windows 10	2016	18939					
Acueductos	DFCCPAC02	Carlos Salas Gould	HP		MXL746283J	Portátil	8 GB	1TB	Windows 10	2016	12050	6090			CADUCADO	
Acueductos	PFCCPAC04	Allan Araya Bienes	DELL		7785DK3	Portátil	32 GB	1TB	Windows 10	365	18931	6751				
Acueductos	PFCCPAC05	Alejandro Arce Gonzalez	HP		5CG9055YDV	Portátil	32 GB	1TB	Windows 10	365	13275				ACTIVO	
Acueductos	PFCCPAC06	Wendy Aguilar Ulloa	HP		5CB9055YBR	Portátil	32 GB	500 GB	Windows 10	2016	13273				CADUCADO	
Acueductos	PFCCPAC08	Milagro Serrano Cortes	HP		5CG9055YG7	Portátil	32 GB	1TB	Windows 10	365	13284					
Acueductos	PFCCPAC10	Kevin Sanchez Barrantes	Sony		2752447-3000183	Portátil	6 GB	500 GB	Windows 10	2016	6170				CADUCADO	
Acueductos	PFCCPAC12	Luis Morales Alvarado	DELL		2T3VDK3	Portátil	32 GB	1TB	Windows 10	2016	18942	11767				
Acueductos	PFCCPAC14	Andres Solano Sanmamaria	LENOVO		PF39SQVL	Portátil	16 GB	500 GB	Windows 10	2016	18327				CADUCADO	
Acueductos	PFCCPAC16	Jossue Solis Flores	HP		5CG9055YGZ	Portátil	32 GB	1TB	Windows 10	2016	13281				ACTIVO	
Acueductos	SCADA-02	SCADA-02	HP		CND5081378	Portátil	8 GB	1TB	Windows 8.1	2010	5158				ACTIVO	
Acueductos	SCADA-03	SACADA-03	HP		MXL6010D49	Escritorio	8 GB	1TB	Windows 7	2010	6782	12024				
Acueductos	SCADA-01	SCADA-01	HP		CND5081377	Portátil	8 GB	1TB	Windows 8.1	2013	5157					
Acueductos	PFCCPAC03	Cristin Prez Rios	LENOVO		PF2VRER6	Portátil	16 GB	500 GB	Windows 10	2016	17369	11768			CADUCADO	
Acueductos	PFCCPAC15	Jossue Centro Control	HP		5CG9055YG2	Portátil	32 GB	1TB	WINDOWS 10	365	13281				CADUCADO	
Acueductos	PFCCPAC03	Mayela Sanabria Portuguez	LENOVO		PF43KAVV	Portátil	16 GB	500 GB	WINDOWS 10	365	18908					
Acueductos	PFCCPAC02	Oscar Fernandez Segura	HP		4Q76DK3	Portátil	32 GB	1TB	Windows 10	365	18943					

Fuente: Control “Inventario de Hardware Municipalidad de Cartago” facilitado por el Área de Informática.

✓ Respecto al Inventario Institucional que se lleva en el sistema de Wizdom, al menos para los activos de TI revisados, se logra evidenciar que a pesar de que contienen registros relacionados a detalle, marca, modelo y serie; no se le adiciona información del activo a esos campos, lo que impide conocer con exactitud todas las características de ese.

Imagen No. 03
Municipalidad de Cartago
Auditoría Interna
Control "INVENTARIO INSTITUCIONAL SISTEMA WIZDOM"
Octubre de 2023

Activo fijo	Ubicación física	Descrip Activo fijo	Detalle	Marca	Modelo	Serie	Identificador Placa
15242	Cuarto de servidores de TI	SWTCH DE VIDEO	NULL	BELKIN	N/A	N/A	694
15243	Cuarto de servidores de TI	ANALIZADOR DE ING	NULL	FORNITER	N/A	N/A	695
15244	Cuarto de servidores de TI	FIREWALL	NULL	N/A	N/A	N/A	7406
15245	Cuarto de servidores de TI	FIREWALL	NULL	N/A	N/A	N/A	7407
15246	Cuarto de servidores de TI	SWITCH DE COMUNICACION	NULL	N/A	N/A	N/A	12207
17287	Cuarto de servidores de TI	SWITCH	NULL	N/A	N/A	N/A	3912
17288	Cuarto de servidores de TI	SWITCH	NULL	N/A	N/A	N/A	3915
17289	Cuarto de servidores de TI	SWITCH	NULL	N/A	N/A	N/A	3917
17290	Cuarto de servidores de TI	CONTROLADOR WIFI	NULL	N/A	N/A	N/A	19469
17291	Cuarto de servidores de TI	CONTROLADOR WIFI	NULL	N/A	N/A	N/A	19468
17292	Cuarto de servidores de TI	SERVIDOR	NULL	N/A	N/A	N/A	3922
17293	Cuarto de servidores de TI	SWITCH	NULL	N/A	N/A	N/A	3933
17294	Cuarto de servidores de TI	SWITCH	NULL	N/A	N/A	N/A	3931

Fuente: Control "INVENTARIO INSTITUCIONAL SISTEMA WIZDOM" facilitado por el Área de Informática.

✓ La revisión en sitio de los activos ubicados en el Data Center o Cuarto de Servidores para validar el inventario Institucional llevado en el sistema Wizdom, permitió evidenciar que por su ubicación física, para algunos activos se obstaculizaba observar el número de placa, impidiendo para ello su verificación y cotejo con los registros de inventario, por lo que al recurrirse a consultar su número de serie, este en muchos casos no constaba registrado en el reporte emitido del Inventario Institucional gestionado en el sistema Wizdom.

✓ Según se observó, tanto el Sistema Wizdom como el inventario de equipos en la infraestructura TIC, dispone de registros relacionados a Marca, Modelo y Serie de cada

Activo; pero a razón del Sistema Wizdom esa información no es llenada para todos los activos; y en el caso del inventario de infraestructura, este no contempla el registro del número de placa del activo; todo lo anterior, impide conciliar adecuadamente la información contenida en los inventarios, tanto el de TI como el Institucional.

Cuadro No. 02
Municipalidad de Cartago
Auditoría Interna
Muestra de activos con información incompleta respecto de sus características
Octubre de 2023

Muestra inventario de Wizdom								Muestra inventario de Infraestructura de TI						
Activo fijo	Ubicación física	Descrip Activ	Detalle	Marca	Modelo	Serie	Identificador	TIPO	NOMBRE	ROL	MARCA	MODELO	SERIE	Placa localizada por Auditoria
	15244 Cuarto de servidores de TI	FIREWALL	NULL	N/A	N/A	N/A	7406	Firewall	Muni_Carta_MASTER	APLIANCE SEGURIDAD	FORTIGATE	800D	FG800D3916801131	7406
	15245 Cuarto de servidores de TI	FIREWALL	NULL	N/A	N/A	N/A	7407	Firewall	Muni_Carta_SLAVE	APLIANCE SEGURIDAD	FORTIGATE	800D	FG800D3916801119	7407
	15246 Cuarto de servidores de TI	SWITCH DE C	NULL	N/A	N/A	N/A	12207	Switch	SW-MCINTERNET-01	Switch Acceso	CISCO	WS-C2960X-24PS-L	FJC2224W072	1207
	15258 Cuarto de servidores de TI	UPS	NULL	VERTIV	LIEBET APS	N/A	17518	Ups	UPS_DATACENTER	Alimentacion electrica	LIEBERT	UPS APS, 16 BAY, 20 KVA	1819600012AU053	17518
	16558 Bodega de TI	COMPUTADC	COMPRA DE HARDWARE P	LENOVO	THINK PAD- E15-GEN2	PF3XN6M7	18920	1	LENOVO	18920	NUEVA	SI		
	17288 Cuarto de servidores de TI	SWITCH	NULL	N/A	N/A	N/A	3912	Enclosure	MC_BL_ENC-01	HP BladeSystem c7000	HP	C7000	USE8058P2K	3912
	17386 Cuarto de servidores de TI	SERVIDOR CC	NULL	HP	HPE-DL360GEN10+	MXQ3040KM	19536	Servidor	NFCHVTI09	Server DL	HP ProLiant	G11	MXQ3040KMR	
	17387 Cuarto de servidores de TI	SERVIDOR CC	Tipo de cambio del sector	HP	HPE-DL360GEN10+	MXQ3040KM	19537	Servidor	NFCHVTI07	Server DL	HP ProLiant	G11	MXQ3040KMQ	
	17388 Cuarto de servidores de TI	SERVIDOR	NULL	HP	HPE-DL360GEN10	MXQ3040KM	19538	Servidor	NFCHVTI08	Server DL	HP ProLiant	G11	MXQ3040KMP	

Fuente: Elaboración propia de la Auditoría Interna.

Estas situaciones expuestas, representan faltas al marco técnico que rige la gestión de los activos de TI, conforme lo indicado en las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de la Información de la Municipalidad de Cartago, aprobadas por el Concejo Municipal en sesión ordinaria N° 127-2021 del 14 de diciembre de 2021, específicamente en su apartado relacionado a Administración Infraestructura Tecnológica, el cual indica *"La institución debe implementar prácticas formales que permitan mantener identificados y actualizados los activos de TI, mediante inventarios de recursos tecnológicos instalados en la organización (hardware, software, aplicaciones, comunicaciones), clasificados según el nivel de criticidad, características, configuración, servicios y medidas de protección asociadas".*

En línea con lo anterior, se estima la inobservancia a las buenas prácticas de gestión de activos de TI indicadas en COBIT 2019 de ISACA, según se indica en el proceso "*AI09 Gestionar los Activos",* el cual expresa "*Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento*

(acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. (…) "

Por otra parte, se deja de lado la consideración del marco de referencia ITIL V4, que en el tema de gestión de activos de TI establece "*Planificar y gestionar el ciclo de vida integral de todos los activos de TI para maximizar el valor, controlar los costes, gestionar los riesgos, apoyar a la toma de decisiones relacionadas con compras, reutilización y sustitución, y satisfacer los requerimientos contractuales y reguladores*"

Las deficiencias de control antes mencionadas, parecen encontrar su causa principalmente en que el Área de Informática no ha diseñado, implementado, documentado e incorporado en su función, un proceso formal que ayude a gestionar de manera más eficaz y eficiente los activos de TI, que permita a la Institución a tener bien identificados todos los activos de TI y su estado actual; para comprobar que los activos se adecuan a sus objetivos (si están en condiciones utilices), si estos todavía están proporcionado valor según su vida útil, además de identificar si son críticos según el servicio brindado, lo que permitiría monitorear su rendimiento y en caso necesarios tomar las medidas para reparar o reemplazarlo considerando el riesgo de fallo, esto ayudaría a mantener la resiliencia de los activos mediante la aplicación de un mantenimiento preventivo regular, además de contribuir a una mejor planificación y asignación presupuestaria.

En ese sentido, no contar con un proceso formal de gestión de activos de TI, incrementa los riesgos operativos de la Institución, al ser este un proceso vital para la prestación de servicios, además, no se podría asegurar que los equipos tecnológicos se administren de la manera más eficiente dentro de la Institución, lo que afectaría además la planificación y la asignación presupuestaría para la adquisición de nuevos recursos Tecnológicos.

Por otra parte, se incrementan los riesgos de Seguridad de la Información, al ser que no se tiene identificados los activos por su criticidad y, en base a ello, determinar qué medidas de seguridad debemos implementar para reducir el nivel de riesgos de exposición

de cada activo asociados; así como se incrementan los riesgos de obsolescencia Tecnológica y de incumplimiento normativo que exigen la normativa aplicable.

2.2 Debilidades en el proceso de gestión de la Configuración (CMDB)

Producto del examen realizado, para lo cual se pretendió validar que la Institución contara con prácticas formales para gestionar la configuración (CMDB), se determinó que el Área de Informática, administra el control de la gestión de la configuración en la herramienta de Ofimática de Microsoft Office en el programa en Excel, en un documento denominado “CONTROL DE EXPEDIENTE DE SERVIDORES”, la cual es utilizada como repositorio de la configuración (CMDB), no obstante, este documento carece de algunos controles con los que debería contar un repositorio o base de datos de configuración, según lo que indican las mejores prácticas como COBIT 2019, ITIL; en los cuales deben contener como se muestra en el siguiente cuadro.

Cuadro No. 03
Municipalidad de Cartago
Auditoría Interna
Cumplimiento del repositorio de la configuración respecto de las características definidas en las mejores prácticas
Octubre de 2023

Controles definidos según las mejores prácticas COBIT 2019, ITIL.:	**Porcentaje cumplimiento (1)**
Clasificación 1- Categoría (por ej. Servicio, Equipo, Aplicación, Documento, Personal ...) 2- Tipo (por ej. Servidor, Impresora, .)	0%
Identificador único (ID)	0%
Nombre	100%
Descripción	0%
Propietario del CI / persona a cargo	37%
Tipos de elementos de Configuración (CI)	100%
Id de Elementos de Configuración	0%
Tiene una línea base de configuración de un servicio, aplicación o infraestructura	0%

Información del fabricante 1. Nombre del Fabricante, 2. Número de serie 3. Número de licencia/referencia al contrato de licencia	0%
Información de la Versión	0%
Ubicación 1. Localización física, si aplica 2. Localización lógica, si aplica (por ej. directorio del servidor)	0%
Relaciones con otros Elementos de Configuración; ejemplo: 1. "Es un componente de", 2. "Está asociado con", 3. "Usos" 4. "Es una nueva versión de", 5. "Será reemplazado por", 6. incluidas las relaciones con los servicios respaldados por la CI.	0%
Información sobre licencias	0%
Referencias del documento 1.Documentación contractual, 2. Documentación de funcionamiento 3.Documentación del usuario, 4. Documentación relevante para emergencias	4%
Historial de modificaciones del Registro de Elementos de Configuración 1. Fecha de creación del registro Elementos de Configuración 2. Modificaciones: 1. Fecha, 2. Persona a cargo, 3. Descripción de la modificación	15%
Aprobación de control de cambios de los elementos de configuración (CI)	0%
Control de cambios de elementos de Configuración	0%
Actualización de la Configuración de los cambios aprobados en los Elementos de Configuración (CI)	0%
Se validan los Elementos de configuración real con los elementos de configuración lógica(repositorio)	0%
Historial de estado 1.Estado actual y versión 2. Historial de estado y versiones (cambios históricos en el estado del CI o cambios planificados para el futuro): 1. Cambio de estado, 2. Descripción, 3. Hora y fecha del cambio de estado	0%

Nota (1): porcentaje de cumplimiento obtenido de la valoración de una muestra de 27 actividades de control de servidores
Fuente: Elaboración propia de la Auditoría Interna.

Aunado a lo anterior, se logró determinar que a pesar de que el archivo “CONTROL DE EXPEDIENTE DE SERVIDORES” dispone de los campos denominados “Fecha última actualización/revisión”, “Responsable” y “Documentación de contenido de servidores y procesos”; en la mayoría de los casos revisados, no se asigna información en esos, perdiéndose así la integridad en los datos almacenados.

Estas situaciones expuestas, representan faltas al marco técnico que rige la gestión de los activos de TI, conforme lo indicado en las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de la Información de la Municipalidad de Cartago, aprobadas por el

Concejo Municipal en sesión ordinaria N° 127-2021 del 14 de diciembre de 2021, específicamente en su apartado relacionado a Administración Infraestructura Tecnológica, el cual indica *"El Área de TIC debe establecer prácticas formales para la gestión de la entrega de servicios a través de los recursos tecnológicos instalados en la institución, administrados interna y externamente, gestionando la configuración y mantenimiento del desempeño y capacidad de los activos de TI, de manera que a través de monitoreos y actualizaciones se mantenga el uso óptimo de los recursos y brinden una garantía razonable sobre la continuidad de las operaciones institucionales, establecidos a través de niveles de operación y sostenibilidad para brindar los servicios requeridos."*.

Asimismo, se estima la inobservancia a las buenas prácticas de gestión de activos de TI indicadas en COBIT 2019 de ISACA, según se indica en el proceso "*BAI10 Configuración gestionada",* el cual expresa *"Definir y mantener descripciones y relaciones entre recursos y capacidades clave necesarios para brindar servicios habilitados para TI. incluir coleccionar información de configuración, estableciendo líneas de base, verificando y auditando la información de configuración y actualizando el repositorio de configuración."*

Corolario a lo anterior, se dejan de lado las buenas prácticas para la gestión de servicios de tecnologías de la información según ITIL V4 (Biblioteca de Infraestructura de Tecnologías de Información), que en su apartado "Gestión de la configuración de servicios" establece "*Recopila y gestiona información sobre una amplia gama variedad de CI, que suelen incluir hardware, software, redes, edificios, personas, proveedores y documentación. El servicio también se trata como CI, y la gestión de la configuración ayuda a la organización a comprender cómo funcionan en conjunto los numerosos CI que contribuyen a cada servicio."*

Las deficiencias de control antes mencionadas, parecen encontrar su causa principalmente en que el Área de Informática no ha diseñado, implementado, documentado e incorporado en su función, un proceso formal que ayude a gestionar de manera más eficaz y eficiente la administración de la configuración, el cual defina el alcance y nivel de detalle sobre la gestión de la configuración. Asimismo la ausencia de un adecuado repositorio de configuración (CMDB), que ayude a mejorar la eficacia operativa de la

Institución, estableciendo y manteniendo un modelo lógico que contenga los registros de configuración a lo largo de su ciclo de vida de los servicios, activos, infraestructura y registro de elementos de configuración (CI), incluidos las relaciones entre ellos; no solo que contenga los elementos TIC (servidores, firewall, routers), sino que incluya los servicios de proveedores, el software, las personas, documentación, que se consideran necesarios para gestionar los servicios de forma eficaz y proporcionar una descripción única y fiable de los activos en un servicio, entre los cuales.

En ese sentido, no contar con un proceso formal de gestión de la configuración, incrementa los riesgos operativos de la Institución, dado que ese proceso es parte vital para la prestación de servicios, donde es fundamental tener registrado y documentado las configuraciones tanto del hardware como del software que están presentes en el entorno Institucional, máxime que los cambios no controlados pueden provocar fallas en el sistema, causando considerables interrupciones y tiempos de inactividad que pueden incidir negativamente en la continuidad de las operaciones.

Por otra parte, se incrementan los riesgos de Seguridad de la Información, ya que una mala configuración sería una de las causas principales en posibles fallas de seguridad, en el sentido que, un sistema operativo sin parches puede exponer a toda la Institución a vulnerabilidades de accesos no autorizados, fugas de datos y ciberataques, asimismo se incrementa los riesgos de cumplimiento normativo lo que podría acarrear en sanciones de todo tipo y daños a la imagen institucional.

2.3 Debilidades en el proceso de Gestionar las operaciones

Producto del examen realizado, para lo cual se pretendió validar que la Institución contara con prácticas formales para gestionar las operaciones de la infraestructura, se evidenció que el Área de Informática no tiene implementados controles referentes a ejecutar los procedimientos operativos entre los que se establezca un cronograma de las actividades operativas a realizar, su frecuencia y el responsable de realizarlas y de supervisarlas; la

implementación y uso de una bitácora sea (física o digital) para el registro y control de la ejecución de las tareas operativas asignadas a los profesionales de Infraestructura referente al monitoreo realizado.

En esa línea, se determinó que no se dispone de una bitácora de monitoreo que registre los controles correspondientes así como la información cronológica de los registros de operaciones que permitan reconstruir y revisar secuencias de tiempo de operaciones y otras actividades que rodean dicha operación; tampoco se logró determinar que se cuente con un control para la creación del tiquete de Incidentes sobre eventos reportados en el monitoreo de infraestructura tecnológica, ni se logra evidenciar que existan tiquetes sobre incidentes reportados por el personal a cargo de la Infraestructura.

Conforme a lo indicado en las mejores prácticas como COBIT 2019, ITIL; se observó una carencia de controles que se deben establecer como se muestra en el siguiente cuadro.

Cuadro No. 04
Municipalidad de Cartago
Auditoría Interna
Cumplimiento de controles definidos en las mejores prácticas referentes a gestionar las operaciones de la infraestructura
Octubre de 2023

Controles definidos según las mejores prácticas COBIT 2019, ITIL:	**Porcentaje cumplimiento**
Se tiene un cronograma de las actividades operativas a realizar, la frecuencia y el responsable	**0%**
Se tiene una bitácora de las labores realizadas	**0%**
Id del Activo	**0%**
Nombre del Activo	**100%**
Identificación del funcionario responsable de realizar el proceso	**83%**
Fecha de ejecución del proceso	**100%**

Descripción del trabajo ( ) Optimización de consultas ( ) Sistema Operativo Instalado ( ) Arquitectura de Procesamiento Configurada ( ) Aplicaciones Instaladas (Web Server, WebServices) ( ) Bibliotecas instaladas ( ) Sistema operativo actualizado a fecha ( ) Licencias utilidades de Seguridad y monitoreo ( ) IP's asignados ( ) Dominios asignados ( ) Usuarios y privilegios ( ) Política de Respaldos ( ) Contrato ( ) Versionamiento	0%
Se registra en una bitácora de monitoreo, la información cronológica de los registros de operaciones para reconstruir y revisar secuencias de tiempo de operaciones y otras actividades que rodean la operaciones de apoyo.	0%
Se crean tickets de incidentes de los eventos reportados en el monitoreo a infraestructura tecnológica	0%
Se mantiene un monitoreo constante sobre las medidas de protección contra factores ambientales, tales como detectores de humo	17%
Se mantiene un monitoreo constante sobre las medidas de protección contra factores ambientales, tales como Aire Acondicionado	33%
Se mantiene un monitoreo sobre mantienen medidas de protección que podrían afectar el Data Center, como las UPS,	0%
Se mantiene un monitoreo sobre mantienen medidas de protección que podrían afectar el Data Center, tales como Planta eléctrica	0%

Fuente: Elaboración propia de la Auditoría Interna.

En esa misma línea, tampoco se evidencia los controles sobre el monitoreo constante sobre la protección contra factores ambientales tales como detectores de humo, aire acondicionado, como también del monitoreo sobre las medidas de protección que podrían afectar el Data Center, tales como UPS, Planta Eléctrica.

Estas situaciones expuestas, representan faltas al marco técnico que rige la gestión de los activos de TI, conforme lo indicado en las Normas Técnicas para el Gobierno y Gestión de las Tecnologías de la Información de la Municipalidad de Cartago, aprobadas por el Concejo Municipal en sesión ordinaria N° 127-2021 del 14 de diciembre de 2021, específicamente en su apartado relacionado a Administración Infraestructura Tecnológica, el cual indica *"El Área de TIC debe establecer prácticas formales para la gestión de la entrega de servicios a través de los recursos tecnológicos instalados en la institución, administrados interna y externamente, gestionando la configuración y mantenimiento del desempeño y capacidad de los*

activos de TI, de manera que a través de monitoreos y actualizaciones se mantenga el uso óptimo de los recursos y brinden una garantía razonable sobre la continuidad de las operaciones institucionales, establecidos a través de niveles de operación y sostenibilidad para brindar los servicios requeridos.".

Asimismo, se estima la inobservancia a las buenas prácticas de gestión de activos de TI indicadas en COBIT 2019 de ISACA, según se indica en el proceso "*DSS01 Operaciones gestionadas",* el cual expresa *"Coordinar y ejecutar las actividades y procedimientos operativos necesarios para brindar servicios de TI internos y subcontratados. Incluye la ejecución de procedimientos operativos estándar predefinidos y las actividades de seguimiento requeridas."*

Por otra parte, se deja de lado la consideración del marco de referencia ITIL V4, que en el tema de monitorización y gestión de eventos establece *"Observar de manera sistemática los servicios y sus componentes, y registrar y crear informes sobre determinados cambios de estado identificados como eventos. Esta práctica identifica y prioriza los eventos y establece su respuesta adecuada, incluyendo la respuesta a condiciones que podrían comportar errores o incidencias potenciales"*

Corolario a lo anterior, se inobservan los procedimientos internos aprobados para el Área de Informática, específicamente el número 7P04 denominado "Gestión de TI", el cual establece un procedimiento operativo denominado "Monitorear la infraestructura de TI (3.1.1)", el cual contempla el monitoreo a la Plataforma tecnológica y virtual, donde se expone que los colaboradores de infraestructura ingresan a los servidores de forma local y remota desde la red del edificio y desde fuera por medio de un acceso VPN, para verificar que todos los equipos a monitorear se encuentren activos y se encuentran en los segmentos de red correspondientes; lo anterior según lo especificado para cada uno de los subapartados 3.1.1.1 Monitoreo de la plataforma tecnológica y virtual, 3.1.1.2. Monitoreo de Antivirus y 3.1.1.3. Monitoreo de servicio de correo.

Las deficiencias de control antes mencionadas, parecen encontrar su causa principalmente en que el Área de Informática no ha diseñado, implementado, documentado e incorporado en su función, un proceso formal que ayude a gestionar de manera más eficaz y eficiente la gestión de la operación de la infraestructura de TI, que coadyuve a mejorar la eficacia en el control de la ejecución de los procesos y funciones operativas y de monitoreo del área de Informática, que representan el día a día del personal, que permita determinar cualquier evento detectable que sea de importancia para la gestión de la Infraestructura de TI. Por otra parte, no se ha implementado un control documentado de monitoreo, que permita se detecten alertas operacionales generadas por los distintos elementos de configuración ya sean automatizadas o manuales; siendo que el monitoreo es la herramienta que brinda valiosa información para la toma de decisiones en cuanto a la identificación de vulnerabilidades técnicas.

En ese sentido, no contar con un proceso formal de gestión de las operaciones de TI (política, procedimientos, directrices) según las mejores prácticas, incrementa los riesgos operativos del área de Informática, al carecerse de controles o los que existen no son los adecuados en pro de una correcta ejecución de los procedimientos y tareas operativas de monitoreo y soporte, de forma que no se garantiza que estos sean confiables, oportunos y consistentes; pues no se dispone de un registro cronológico documentado tanto de las acciones operativas realizadas como de la relación de los eventos reportados en la infraestructura tecnológica, incluyendo como fallas en eléctricas en el centro el data center, fallas en el equipo de aire acondicionado, UPS o planta Eléctrica.

3 CONCLUSIONES

En general, el proceso de Administración de la Infraestructura llevado a cabo por el Área de Informática, no se realiza con observancia del Marco Normativo que rige la materia de Tecnologías de Información, a pesar de mantener implementados algunas prácticas formales para la gestión de activos de TI (Inventario), estas no están alineados con el marco normativo ni las mejores prácticas; producto de ello, se determinaron debilidades e inconsistencia de control que afectan y/o pueden afectar negativamente el uso apropiado de los activos de TI, sin que garantice ello una contribución real a la eficiencia operativa y la seguridad de la información a nivel institucional, sino que también, el cumplimiento normativo que nos regula, y que se realice una gestión basada en los principios de eficacia, eficacia y economía perseguidos por la gestión pública.

Así las cosas, la Administración Municipal no ha llevado a cabo las gestiones necesarias para implementar la normativa técnica que regula los procesos de infraestructura tecnológica, siendo que el proceso tal como se lleva actualmente, presenta inexactitud en la información o esa está incompleta; además, existen incongruencias entre procedimientos Institucionales formales y aprobados y lo ejecutado por el Área de Informática, sin dejar de lado las limitaciones que se presentan en los controles técnicos que deberían llevarse por parte del área técnica y que no están implementados; todo lo anterior, afecta la regulación y ejecución de las actividades de control propias del proceso que, además, delimitan aspectos importante que son insumos para otros procesos relacionados.

Aunado a lo anterior, las falencias determinadas en la gestión de la Configuración, relacionadas al almacenamiento, los controles generales y específicos que deben contener los registros de configuración, a lo largo de su ciclo de vida y las relaciones entre ellos, no solamente los con los elementos TIC (servidores, firewall, routers), sino los servicios de proveedores, el software, las personas y documentación. En este sentido, la base de datos CMDB, no debe considerarse solo como un repositorio donde almacenar elementos, sino que, tiene como característica principal la interrelación de todos los elementos, lo que debe

permitir trazabilidad de los procesos, de un elemento inicial a uno final a través de las relaciones que existen entre cada uno de ellos.

Es esa misma línea, la falta de los controles o bitácoras pertinentes para el registro de la ejecución y monitoreo de las actividades o tareas operativas de los profesionales de infraestructura de TI, incrementa los riesgos operativos tanto del área de Informática, como la continuidad de las operaciones Institucionales, de ahí, la importancia de mantener un soporte que sea confiable y consistente, como aspecto fundamental para disponer de un registro cronológico documentado, que permita identificar tanto las acciones operativas realizadas como la relación de los eventos reportados en la infraestructura tecnológica, por medio del tiquetes en la herramienta correspondiente.

Finalmente, los resultados de auditoría obtenidos ponen en evidencia que el Área de Informática debe fortalecer las labores y actividades de control y seguimiento relacionadas al proceso de administración de la infraestructura tecnológica, considerando la necesidad de establecer procesos formales conforme al marco normativo y las buenas prácticas, que permitan bajo procedimientos adecuados y técnicamente estructurado, garantizar que la infraestructura tecnológica institucional sea administrada adecuadamente, y con ello, efectuar las operaciones con eficiencia, eficacia y economía, salvaguardándose y protegiendo la utilidad de los activos, la seguridad de la información y la continuidad de la operación municipal.

4 RECOMENDACIONES

4.1 Al Alcalde Municipal

a) Girar las instrucciones pertinentes al Encargado del Área de Informática, con el fin de cumplir las recomendaciones emitidas por la Auditoría Interna. Para la atención de dicha recomendación se cuenta con un plazo de quince (15) días hábiles contados a partir del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

b) Analizar y aprobar conforme a sus competencias, la propuesta de procedimientos y prácticas formales que se determinen del análisis realizado por el Área de Informática respecto a manuales institucionales y procedimientos que rigen el proceso de administración de la infraestructura tecnológica, según la recomendación número 4.2.f) del presente informe. Para la atención de dicha recomendación se cuenta con un plazo de cinco (5) meses calendario contados a partir del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

4.2 Al Encargado del Área de Informática

a) Establecer, documentar, aprobar y divulgar las políticas, procedimientos y directrices formales referentes al proceso de Gestión de Activos de TI, en los cuales se definan los funcionarios responsables, roles, responsabilidades, criterios de clasificación y valoración de los activos, y demás requisitos específicos de cumplimiento regulatorio para dicha gestión; así como la periodicidad de las evaluaciones del cumplimiento de las políticas de gestión de Activos de TI y la verificación de la exactitud de los registros ingresados en los respectivos controles de activos. Para la atención de dicha recomendación se cuenta con un plazo de cinco (5) meses calendario contados a partir

del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

b) Implementar mediante el uso de una herramienta automatizada el Inventario de Activos de TI, que permita contar con información completa, oportuna y actualizada respecto de esos activos, y que considera incluir aspectos como la criticidad del Activo (Confidencialidad, integridad, disponibilidad), valoración del Riesgo (bajo, medio, alto) del activo en caso de fallas, Fecha de ultimo mantenimiento preventivo, fecha de ultima conciliación Físico Vr Lógico, dirección de red (si es estática), dirección Mac, Estado de conservación del activo (malo, regular, bueno, excelente), estado de Uso (son adecuados para su propósito) y demás características específicas de cumplimiento regulatorio para dicha gestión; que además permita contar con pistas de auditoría tendientes a reflejar los cambios referentes a adquisiciones, traspasos de responsables y custodios, bienes en desuso, y otros aspectos. Para la atención de dicha recomendación se cuenta con un plazo de cinco (5) meses calendario contados a partir del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

c) Establecer, documentar, aprobar y divulgar las políticas, procedimientos y directrices formales referentes al proceso de gestión de la configuración, donde se defina un modelo de configuración conforme al marco normativo y buenas prácticas, que permita determinar el alcance y detalle de los elementos de configuración a registrar. Para la atención de dicha recomendación se cuenta con un plazo de cinco (5) meses calendario contados a partir del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

d) Diseñar e implementar un repositorio de configuración (CMDB) cuyo desarrollado sea a partir del Modelo de Configuración definido en la recomendación 4.2.c), que permita identificar todos los elementos de Configuración (CI) y sus relaciones conforme al marco normativo y buenas prácticas. Para la atención de dicha recomendación se

cuenta con un plazo de cinco (5) meses calendario contados a partir del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

e) Establecer, documentar, aprobar y divulgar las políticas, procedimientos y directrices formales referentes al proceso de gestión de las operaciones, en la cual se definan aspectos como el desarrollo de calendarización de las tareas operativas relacionadas al monitoreo de los servicios de TI, la frecuencia y responsables de ejecutarlos, los Activos a monitorear (servidores, UPS, Aires Acondicionado), numero de Incidente, la creación de tiquetes de incidentes asociados con los eventos identificados producto de la ejecución de las actividades operativas de monitoreo propias del área, y demás requisitos específicos de cumplimiento regulatorio para dicha gestión. Para la atención de dicha recomendación se cuenta con un plazo de cinco (5) meses calendario contados a partir del acuse de recibo del informe final. Cumplida la recomendación remitir a esta Auditoría Interna documentación donde conste su observancia.

f) Someter a aprobación del Alcalde Municipal según corresponda, las políticas, procedimientos y directrices formales referentes a la gestión de los activos, gestión de la configuración y gestión de las operaciones, producto del cumplimiento de las recomendaciones números 4.2.a), 4.2.c) y 4.2.d). Para la atención de dicha recomendación se cuenta con un plazo de cinco (5) meses calendario contados a partir del acuse de recibo del informe final. Cumplida la recomendación, remitir a esta Auditoría Interna documentación donde conste su observancia.

DENNIS DAMIAN VEGA REDONDO (FIRMA)
Firmado digitalmente por DENNIS DAMIAN VEGA REDONDO (FIRMA)
Fecha: 2024.10.25 15:26:52 -06'00'

Lic. Dennis Vega Redondo
Auditor Interno a.i.

RICARDO ASDRUBAL CHAVES RODRIGUEZ (FIRMA)
Firmado digitalmente por RICARDO ASDRUBAL CHAVES RODRIGUEZ (FIRMA)
Fecha: 2024.10.25 15:26:20 -06'00'

Lic. Ricardo Chaves Rodriguez
Asistente de Auditoría en Informática

5 ANEXOS AL INFORME

Anexo #1
Municipalidad de Cartago
Auditoría Interna

HERRAMIENTA EA-CR-VOA-01 VALORACIÓN OBSERVACIONES DEL INFORME DE AUDITORÍA
Octubre de 2024

MUNICIPALIDAD DE CARTAGO

AUDITORÍA INTERNA

C_{180}-1/1-1

VALORACIÓN DE OBSERVACIONES AL BORRADOR DEL INFORME DE AUDITORIA
HERRAMIENTA EA-CR-VOA-01

Área auditada	Área TICS	Dependencia/ Unidad auditada	Área TICS
Nombre del estudio	Auditoría de Carácter Especial de Tecnología de Información y Comunicaciones sobre la Administración de la Infraestructura Tecnológica.		
Número de Estudio	AI-EST-CE001-2024	Número de Informe	AI-INF-004-2024

¿Se reciben observaciones al borrador de informe de auditoria?		SI☐ *(Se completan los apartados I., II., III.)*	NO☐ *(Se completan los apartados II.,III.)*
Documento recibido	AIN-OF-198-2024	Fecha	21 de Octubre 2024
Fecha acuse recibo	23-oct-24	Anexos	No tiene

I. OBSERVACIONES DE LA ADMINISTRACIÓN

Observaciones relacionadas al hallazgo 4.1 al Alcalde Municipal, referente a la recomendación 4.1 a)			
Observaciones Administración	Este comentario lo debe dar la Alcaldía municipal		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto.		
Observaciones relacionadas al hallazgo 4.1 al Alcalde Municipal, referente a la recomendación 4.1 b)			
Observaciones Administración	Este comentario lo debe dar la Alcaldía municipal		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto.		
Observaciones relacionadas al hallazgo 4.2 al Encargado del Área de Informatica, referente a la recomendación 4.2 a)			
Observaciones Administración	Como parte del proceso ya iniciado de la implementación de la normativa técnica de las TIC y en conjunto con la administración municipal se establecerán, documentaran, aprobaran y divulgaran las políticas, procedimientos y directrices formales referentes al proceso de Gestión de Activos de TI. Al ser un proceso que integra varios departamentos y coordinación no solo de TIC se intentara cumplir en el plazo asignado.		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto, del como van a implemetar la recomendación.		
Observaciones relacionadas al hallazgo 4.2 al Encargado del Área de Informatica, referente a la recomendación 4.2 b)			
Observaciones Administración	Desde la dirección se TIC ya se han brindado las instrucciones para desarrollar nuevos módulos que permitan mejorar los inventarios de la infraestructura de TIC según las recomendaciones indicadas en este punto. Se tomarán como base las recomendaciones del proceso de implementación de la norma técnica de las TIC y las realizadas por los señores de la auditoria interna.		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto, del como van a implemetar la recomendación.		
Observaciones relacionadas al hallazgo 4.2 al Encargado del Área de Informatica, referente a la recomendación 4.2 c)			
Observaciones Administración	Como parte del proceso ya iniciado de la implementación de la normativa técnica de las TIC y en conjunto con la administración municipal se establecerán, documentaran, aprobaran y divulgaran las políticas, procedimientos y directrices para la configuración de la Base de datos de la gestión de configuración (CMDB) institucional		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐

MUNICIPALIDAD DE CARTAGO AUDITORÍA INTERNA			C_{180}-1/1-1
VALORACIÓN DE OBSERVACIONES AL BORRADOR DEL INFORME DE AUDITORIA HERRAMIENTA EA-CR-VOA-01			
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto, del como van a implemetar la recomendación.		
Observaciones relacionadas al hallazgo 4.2 al Encargado del Área de Informatica, referente a la recomendación 4.2 d)			
Observaciones Administración	Desde la dirección se TIC ya se han brindado las instrucciones para desarrollar nuevos módulos que permitan mejorar el registro la Base de datos de la gestión de configuración (CMDB) institucional, para esto se desarrollara un módulo que permita llevar la información, así como el histórico de la misma.		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto, del como van a implemetar la recomendación.		
Observaciones relacionadas al hallazgo 4.2 al Encargado del Área de Informatica, referente a la recomendación 4.2 e)			
Observaciones Administración	Como parte del proceso ya iniciado de la implementación de la normativa técnica de las TIC y en conjunto con la administración municipal se establecerán, documentaran, aprobaran y divulgaran las políticas, procedimientos y directrices para la calendarización de tareas calendarización de las tareas operativas relacionadas al monitoreo de los servicios de TI, la frecuencia y responsables de ejecutarlos, los Activos a monitorear (servidores, UPS, Aires Acondicionado), numero de incidente, la creación de tiquetes de incidentes asociados con los eventos identificados producto de la ejecución de las actividades operativas de monitoreo propias del área de TIC		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto, del como van a implemetar la recomendación.		
Observaciones relacionadas al hallazgo 4.2 al Encargado del Área de Informatica, referente a la recomendación 4.2 f)			
Observaciones Administración	En cuanto se terminen las políticas y desarrollos de software necesarios para el cumplimiento de los hallazgos se remitirá a los compañeros del Area de Planeamiento para inclusión en el sistema de gestión municipal y la aprobación por parte del señor alcalde		
¿Se acoge?	SI ☐	NO ☐	PARCIAL ☐
Argumentos Auditoria Interna	La observación indicada por la Administración, no modifica el contenido del informe o de la recomendación, por lo cual, solo se toma nota al respecto, del como van a implemetar la recomendación.		
II.OBSERVACIONES GENERALES			
Al no presentarse observaciones específicas sobre el contenido del informe borrador, sino observaciones del cómo van a implementar las recomendaciones, esta unidad de control y fiscalización da por cerrada esta etapa de valoración de observaciones del informe borrador.			
III. ELABORACIÓN			
Hecho por:	Lic. Ricardo Chaves Rodriguez	Fecha	24/10/2024
Revisado por:	Lic. Dennis Vega Redondo	Fecha	24/10/2024
Aprobado por:	Lic. Dennis Vega Redondo	Fecha	24/10/2024