MUNICIPALIDAD DE CARTAGO

AUDITORÍA INTERNA

Auditoría de Carácter Especial sobre la Gestión de Riesgos de Tecnologías de Información.

INFORME NÚMERO AI-TIC´s- INF-002-2021

Julio, 2021

CONTENIDO

.

1 INTRODUCCIÓN 1

1.1 Origen del estudio 1

1.2 Objetivo General 1

1.3 Objetivos Específicos 2

1.4 Alcance y período del estudio 2

1.5 Metodología aplicada 2

1.6 Generalidades sobre el ejercicio de la Auditoría Interna. 3

1.7 Comunicación de resultados 3

2 RESULTADOS DEL ESTUDIO 6

2.1 Carencia de un marco de gestión de TI, alineado con la gestión de riesgos de TI. 6

2.2 Falta de integración de la gestión de riesgos de TI con las Directrices Contraloras referentes al establecimiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI). 8

2.3 Ausencia de una ejecución periódica del proceso de gestión de riesgos de TI. 10

2.4 Designación de un Coordinador de gestión de riesgos de TI sin competencias e idoneidad. 12

2.5 Escaso conocimiento en las sesiones respecto a temas asociados a la gestión de riesgos de TI, por parte de la Comisión de Tecnologías de Información y Comunicaciones (CTIC); ente asesor del Alcalde Municipal. 15

3 CONCLUSIONES **18**

4. RECOMENDACIONES **20**

Auditoría Interna
auditoriainterna@muni-carta.go.cr
Teléfonos: 2550-4439/40/41
Tel. Fax: 2552-73-32

RESUMEN EJECUTIVO

¿Qué examinamos?

La auditoría de carácter especial sobre la gestión de riesgos de las tecnologías de información analizó la alineación del marco normativo teórico al Sistema Específico de Valoración del Riesgo Institucional (SEVRI), además de comprobar la aplicación y seguimiento de la metodología de gestión de riesgo para la toma de decisiones y la planificación de la función de las Tecnologías de Información.

Esta auditoría abarcó el periodo comprendido entre el 01 de enero de 2019 al 31 de diciembre de 2020, ampliándose cuando se consideró necesario.

¿Por qué es importante?

Al vivirse actualmente en un entorno evolutivo, donde el incremento en el uso de las tecnologías de Información se encuentra inmersa en toda la organización, desde su estrategia institucional hasta en la ejecución de sus procesos operativos, nace la necesidad de las organizaciones de gestionarse dentro de gestión de riesgos de TI, donde se administren los eventuales riesgos (naturales, técnicos o humanos) que podrían afectar los procesos involucrados en el proceso de TI y por consiguiente, afectar la continuidad de negocio, el logro de los objetivos y planes estratégicos institucionales, además de, los incumplimientos regulatorios que involucra.

Auditoría Interna
auditoriainterna@muni-carta.go.cr
Teléfonos: 2550-4439/40/41
Tel. Fax: 2552-73-32

Con ese norte y, considerando la importancia que dicho proceso representa para este Gobierno Local, la Auditoria Interna conforme la Planificación Estratégica 2019-2023 dispuso en su Plan Anual de Trabajo para el presente año llevar a cabo el citado estudio de auditoria, en materia de gestión de riesgos de Tecnologías de Información.

¿Qué encontramos?

Se determinó que el Área de Tecnologías de Información y Comunicaciones, cuenta con una metodología de gestión de riesgos desde el año 2018, la cual toma como marco referencia el COBIT[1] 4.1, específicamente en su proceso "*P09 Evaluar y Administrar los Riesgos de TI*", el cual es desarrollado de forma independiente de otros procesos, contrario a lo establecido en la citada mejor práctica, en cuanto a establecer un marco integral para todos los procesos y dominios que tienen que ver con la gestión de TI.

Asimismo, esta Unidad de Control y Fiscalización identificó debilidades durante la ejecución del proceso de gestión de riesgos, dado que, la identificación, análisis, evaluación, administración y revisión de los riesgos no se está realizando en forma cíclica en un periodo de tiempo establecido, siendo que, el Area de TIC's únicamente brinda seguimiento a los riesgos incorporados en la metodología de gestión de riesgos presentada en el año 2018.

Por otra parte, considerando que la gestión de la Tecnología de la Información en la Corporación Municipal debe orientarse principalmente a lograr que la tecnología de información sea congruente con las estrategias y objetivos de

[1] Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas dirigida al control y supervisión de tecnología de la información (TI).

Auditoría Interna
auditoriainterna@muni-carta.go.cr
Teléfonos: 2550-4439/40/41
Tel. Fax: 2552-73-32

la Municipalidad de Cartago y que, los riesgos relacionados con tecnología de información sean debidamente conocidos y administrados; no logro esta instancia auditora evidenciar participación por parte de la Comisión de Tecnologías de Información, como Órgano asesor de la Alcaldía Municipal en la coadyuvancia de la gestión de las TIC con la estrategia institucional, en temas relacionados a riesgos asociados con la gestión tecnológica de la institución, de forma tal que contribuya en la consecución de los beneficios esperados, eficiencia, productividad y competitividad de su gestión.

¿Qué sigue?

Se dispuso a la Administración Activa, una serie de oportunidades de mejora para subsanar las deficiencias expuestas en el presente estudio de auditoria con el fin de definir e implementar una metodología para la gestión de los riesgos aplicables al Area de Tecnologías de Información y Comunicaciones en la Municipalidad de Cartago, que permita una mejora en la periodicidad del ciclo que incluye su identificación, análisis, evaluación, administración y revisión, con apoyo de la Comisión de Tecnologías de Información y Comunicaciones, como órgano asesor del Alcalde Municipal conforme sus competencias y funciones normadas; así como, coadyuvar en el fortalecimiento del conocimiento técnico e idoneidad del personal destacado en el Area de TIC's involucrado en dicho proceso.

Auditoría Interna
auditoriainterna@muni-carta.go.cr
Teléfonos: 2550-4439/40/41
Tel. Fax: 2552-73-32

1 INTRODUCCIÓN

1.1 Origen del estudio

Las tecnologías de información (TI) constituyen uno de los principales instrumentos que apoyan la gestión institucional, de ahí que, la institución tenga que administrar las amenazas que pueden afectar la gestión de Tecnologías de Información, esto mediante una gestión de riesgos, debidamente integrada al Sistema Específico de Valoración de Riesgos Institucional[2]

Con ese norte, con fundamento en el Plan Anual de Trabajo de Auditoria Interna para el año 2021, así como las atribuciones conferidas en la *Ley General de Control Interno*[3], las *Normas Generales de Auditoría para el Sector Público*[4] dictadas por la Contraloría General de la República y el *Reglamento de Organización y Funcionamiento de la Auditoria Interna de la Municipalidad del Cantón Central de Cartago*[5]; este Despacho dispuso llevar a cabo un estudio titulado ***"Auditoría de Carácter Especial sobre la Gestión de Riesgos de Tecnologías de Información".***

1.2 Objetivo General

Evaluar el marco normativo teórico, la metodología (aplicación y seguimiento) de la gestión del riesgo de las Tecnologías de la Información (TI) integrada al Sistema Específico de Valoración del Riesgo Institucional (SEVRI).

---

[2]Conjunto organizado de elementos que interaccionan para la **identificación**, **análisis**, **evaluación**, **administración**, **revisión**, **documentación** y **comunicación** de los **riesgos** institucionales. Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) Nº Gaceta: 134 del: 12/07/2005

[3] Ley N° 8292 Publicada en La Gaceta N° 169 del 04 de setiembre del 2002.

[4] Resolución Contralora N-2-2009-CO-DFOE Publicada en La Gaceta N° 26 del 06 de febrero del 2009.

[5] Resolución Contralora N° R-DC-119-2009 Publicada en La Gaceta Nº 28 de 10 de febrero de 2010.

1.3 Objetivos Específicos

- ✓ Revisar el Marco Normativo Teórico de la gestión de Riesgos.
- ✓ Comprobar la corrección, aplicación, seguimiento la metodología de gestión de riesgo de TI integrada al SEVRI Institucional.
- ✓ Evaluar la integridad del uso del SEVRI para la toma de decisiones y planificación de la función de las Tecnologías de Información.
- ✓ Emitir recomendaciones de mejora para el proceso de gestión de riesgos en pro de su efectividad.

1.4 Alcance y período del estudio

El estudio abarcó del 01 de enero de 2019 al 31 de diciembre del 2020, ampliándose en los casos que se consideró necesarios. Dicho estudio se llevó a cabo en el Área de Tecnologías de Información y Comunicaciones, Área de Planeamiento Estratégico y Unidad de Control Interno. Lo anterior, fue comunicado a la Administración Activa a través del oficio número AI-OF-008-2021 fechado 25 de enero 2021 y remitido al Lic. Mario Redondo Poveda, en su condición de Alcalde Municipal.

El trabajo se efectuó de conformidad con lo dispuesto en las **Normas Generales de Auditoría para el Sector Público**[6] dictadas por la Contraloría General de la República y el *Reglamento de Organización y Funcionamiento de la Auditoria Interna*[7],

1.5 Metodología aplicada

Para efectos del presente estudio se efectuaron entrevistas y reuniones con colaboradores destacados en la Unidad de Control Interno y Area de Tecnología de Información y Comunicaciones, con el propósito de validar la información suministrada; así

[6] Resolución R-DC-64-2014 Publicada en La Gaceta No. 184 de 25 de setiembre del 2014
[7] Publicado en La Gaceta No. 130 de 7 de julio del 2009

como, así como, la aplicación de pruebas de auditoría conforme los criterios de auditoría comunicados previamente a la Administración Municipal.

De igual manera, se cursaron oficios y correos electrónicos a las dependencias municipales involucradas, mediante los cuales se solicitó información, relacionada con las actividades propias del proceso de gestión de riesgos objeto de estudio,

1.6 Generalidades sobre el ejercicio de la Auditoría Interna.

Se les recuerda que, en materia de informes de auditoría interna, prevalecen los artículos N° 12 inciso c), N°35, N° 36 y N° 38 de la Ley General de Control Interno[8], conocida ampliamente por la Administración Activa.

1.7 Comunicación de resultados

La comunicación preliminar de los resultados, conclusiones y recomendaciones producto de la auditoría realizada, se llevó a cabo el día 09 de julio del 2021 en mediante la plataforma de comunicación Microsoft Teams, según convocatoria realizada día 29 de junio del 2021 mediante oficio número AI-OF-115-2021 y remitido a: Lic. Mario Redondo Poveda, Alcalde Municipal; Licda. Laura Fernández Delgado, Jefa Despacho de Alcaldía Municipal; Licda. Silvia Alvarado Martinez, Vice Alcaldesa Municipal y Coordinadora de Comisión de Tecnología de Información y Comunicaciones (CTIC); Lic. Miguel Sanchez Leandro, Jefe de la Unidad de Control Interno y Lic. Daniel Ramirez Gonzalez, Sub director del Area de Tecnologías de Información y Comunicaciones.

Dicha presentación contó con la participación de los funcionarios de la Administración Activa que se detalla seguidamente.

[8] Ley Número 8292 publicada en La Gaceta No. 169 de 4 de setiembre del 2002

Área/Departamento/Unidad	Nombre del Funcionario	Cargo/Puesto
Alcaldía Municipal	Lic. Mario Redondo Poveda	Alcalde Municipal
Alcaldía Municipal	Licda. Laura Fernández Delgado	Jefa Despacho de Alcaldía Municipal
Coordinadora de Comisión de Tecnología de Información y Comunicaciones (CTIC)	Licda. Silvia Alvarado Martinez	Vice Alcaldesa Municipal
Unidad de Control Interno	Lic. Miguel Sanchez Leandro	Jefe de la Unidad de Control Interno
Área de Tecnologías de Información y Comunicaciones	Lic. Daniel Ramirez Gonzalez	Subdirector de Tecnologías de Información y Comunicaciones
Área de Tecnologías de Información y Comunicaciones	Lic. Gilberto López López	Coordinador de la gestión de riesgos de TI

El borrador de este informe se comunicó mediante oficio número AI-OF-123-2021 de fecha 12 de julio de 2021 y dirigido a: Lic. Mario Redondo Poveda, Alcalde Municipal; Licda. Silvia Alvarado Martinez, Vicealcaldesa Municipal y Coordinadora de Comisión de Tecnología de Información y Comunicaciones (CTIC); Lic. Miguel Sanchez Leandro, Jefe de la Unidad de Control Interno y Lic. Daniel Ramirez Gonzalez, Sub director del Área de Tecnologías de Información y Comunicaciones; con copia para conocimiento de la Licda. Laura Fernández Delgado, Jefa Despacho de Alcaldía Municipal; donde se les concede un plazo improrrogable de tres (3) días hábiles, sea hasta el jueves 15 de julio del 2021 para que, realicen las observaciones y/o comentarios que estimen pertinentes, en forma escrita,

debidamente justificados y/o documentados; así como, posibles alternativas de solución a los hallazgos de auditoría consignados en el presente informe.

En ese sentido, habiendo transcurrido el plazo concedido para la remisión de observaciones y/o comentarios por parte de la Administración Activa, este Despacho Auditor al no recibir respuesta alguna, da por aceptado el borrador de informe en los términos ahí expuestos y, procede con la oficialización y remisión del informe final para lo de su competencia.

2 RESULTADOS DEL ESTUDIO

La gestión de riesgos de las Tecnologías de Información, forma parte del capítulo I "*Normas de aplicación general*" de las Normas técnicas para la gestión y el control de las Tecnologías de Información[9], las cuales señalan que la institución debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al Sistema Específico de Valoración del Riesgo Institucional y que, considere el marco normativo que le resulte aplicable.

Así las cosas, una vez realizada la recopilación y análisis de la información, se procedió a elaborar el presente informe, que abarca los principales hallazgos de auditoría, conforme se comenta a continuación:

2.1 Carencia de un marco de gestión de TI, alineado con la gestión de riesgos de TI.

El marco teórico metodológico para la gestión de riesgos de TI se basa principalmente en el documento "*Plan para la gestión de los riesgos del área de TIC*", el cual, sirve de guía o herramienta para la identificación, análisis y evaluación de riesgos que permite generar el plan de continuidad para el área involucrada, garantizando por consiguiente el cumplimiento de los objetivos operativos. Dicho plan se basa en el marco de referencia "*Objetivos de Control para Información y Tecnología relacionada*" versión COBIT 4.1, en su proceso "*P09. Evaluar y Administrar los Riesgos de TI"* y sus 6 objetivos de control ("*Marco de Trabajo de Administración de Riesgos, Establecimiento del Contexto del Riesgos, Identificación de Eventos, Evaluación de Riesgos de TI, Respuesta a los Riesgos, Mantenimiento y Monitoreo de un Plan de Acción de Riesgos"*).

Con base en lo expuesto, esta instancia auditora logra evidenciar que, aunque el proceso de gestión de riesgos de TI se ajusta a lo indicado en citado marco de referencia;

[9] R-CO-26-2007.-Contraloría General de la República. - Despacho de la Contralora General. -San José a las diez horas del siete de junio del 2007.

no incorporó la administración de los riesgos asociados a TI en otros procesos tales como: planificación estratégica de TI, Seguridad de la información, Continuidad de los servicios de TI, gestión de proyectos, entre otros, los cuales coadyuban a la gobernanza de TIC. Lo anterior, considerando que dicha mejor práctica se orienta en un modelo de dominios y procesos que se interrelacionan entre sí, ofreciendo una visión integral de las tecnologías de información.

En este mismo orden, es preciso mencionar que para el año 2018, ya existían versiones más actualizadas de los "*Objetivos de Control para Información y Tecnología relacionada*" que la utilizada como referencia para desarrollar el citado proceso.

En ese sentido las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por la Contraloría General de la República de Costa Rica, indican en el punto N° 1.3 referente a *"Gestión de riesgos"*:

> *"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."*

Por su parte, Ley General de Control Interno N° 8292, en su artículo 2 inciso f) señala:

> *"Valoración del riesgo: identificación y análisis de los riesgos que enfrenta la institución, tanto de fuentes internas como externas relevantes para la consecución de los objetivos."*

Las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgo Institucional emitidas por el Ente Contralor, define la "Valoración del Riesgo" como la: *"…Identificación, análisis, evaluación, administración y revisión de los riesgos institucionales, tanto de fuentes internas como externas, relevantes para la consecución de los objetivos. (En normativas técnicas este proceso también se denomina "gestión de riesgos").*

Lo anterior denota que, el proceso de gestión de riesgos de TI presenta errores de conceptualización en la implementación de mejores prácticas en forma integral y de

desarrollo; situación que afecta la eficiencia de la gestión de TIC, la consecución del logro de objetivos institucionales, debilitamiento en el Sistema de Control Interno Institucional e incumplimientos regulatorios.

2.2 Falta de integración de la gestión de riesgos de TI con las Directrices Contraloras referentes al establecimiento del Sistema Específico de Valoración de Riesgos Institucional (SEVRI).

El marco teórico metodológico para la gestión de riesgos de TI, se basa principalmente en el documento: *"Plan para la gestión de los riesgos del área de TIC",* el cual contiene la estructura para: identificación (identificador del riesgo, proceso, origen, causa del riesgo, riesgo), análisis de los riesgos identificados (análisis cuantitativo de los riesgos identificados, que incluye: categoría, probabilidad, impactó, calificación), análisis cualitativo de los riesgos identificados (calificación, severidad, IVM , Acción), planificar la respuesta (tipo de control, tipo de medida, descripción de medida actual, frecuencia de aplicación) controlar y monitorear controles propuestos, responsables, periodo de implementación, porcentaje de avance); no obstante, la identificación del riesgo, no se vincula con los objetivos del Área de TIC, ni con los eventos y su consecución.

Así las cosas, a pesar de que el Área de Tecnologías de Información y Comunicaciones administra su propio proceso de gestión de riesgos, conforme lo regulado en las Normas Técnicas para la gestión y el control de las Tecnologías de Información, este no consideró lo normado por el Ente Contralor en las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional, en lo que corresponde a: Valoración del riesgo. Identificación, análisis, evaluación, administración y revisión de los riesgos institucionales, tanto de fuentes internas como externas, relevantes para la consecución de los objetivos. (En normativas técnicas este proceso también se denomina "gestión de riesgos").

En ese sentido las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional emitidas por la Contraloría General de la República, estipulan en el punto 4 referente a *"Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional"* que:

> *"4.2 Identificación de riesgos. Se deberá identificar por áreas, sectores, actividades o tareas, de conformidad con las particularidades de la institución, lo siguiente:*
>
> *a) Los eventos que podrían afectar de forma significativa el cumplimiento de los objetivos institucionales. Estos deberán organizarse de acuerdo con la estructura de riesgos institucional previamente establecida.*
>
> *b) Las posibles causas, internas y externas, de los eventos identificados y las posibles consecuencias de la ocurrencia de dichos eventos sobre el cumplimiento de los objetivos.*
>
> *c) Las formas de ocurrencia de dichos eventos y el momento y lugar en el que podrían incurrir.*
>
> *d) Las medidas para la administración de riesgos existentes que se asocian con los riesgos identificados.*
>
> *La identificación de riesgos debe vincularse con las actividades institucionales de planificación-presupuestario, estrategia, evaluación y monitoreo del entorno".*

La debilidad referente a la inobservancia de las directrices generales emitidas por la Contraloría General de la Republica, se asocia al desconocimiento técnico y legal durante el establecimiento del proceso de gestión de riesgos, dada la carencia de personal debidamente especializado o capacitado en esta materia a nivel institucional y, del área objeto de estudio.

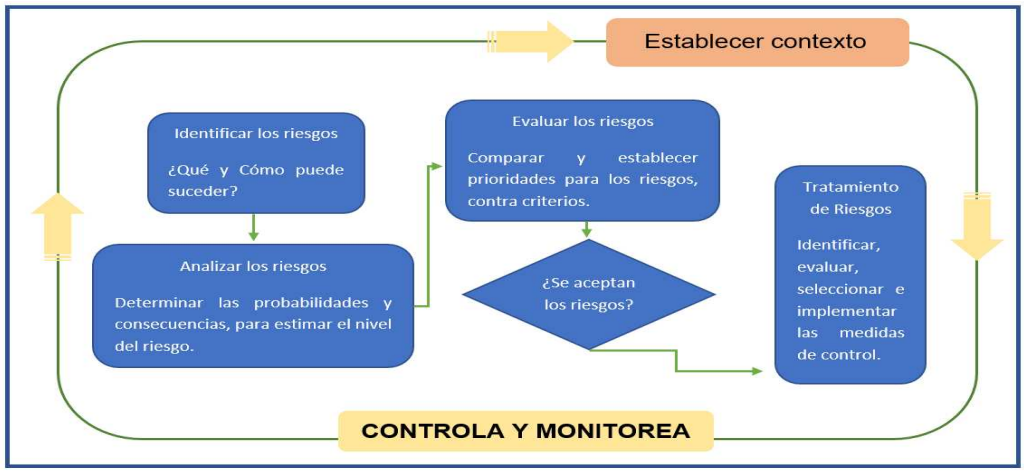
Tal situación, afectaría el logro de los objetivos institucionales relacionados a la eficiencia de la gestión de TIC, así como, de continuidad del negocio; por consiguiente, provocando el debilitamiento del Sistema de Control Interno e incumplimientos de carácter regulatorio.

2.3 Ausencia de una ejecución periódica del proceso de gestión de riesgos de TI.

El documento denominado "*Plan para la gestión de los riesgos del área de TI"*, estableció dentro de su lineamiento que la valoración de riesgos es un proceso constante, íntegro y participativo, dónde el primer levantamiento de riesgos del área objeto de estudio se efectúo en el año 2018, identificándose (66) riesgos provenientes de los procesos estructurados y definidos en el Área de TIC's (Infraestructura y Arquitectura, Soporte técnico, Base de Datos, Desarrollo, administración), con su respectivo proceso de análisis y valoración; así las cosas, para cada riesgo se tienen asignados: controles, responsables, periodo de implementación (entre el II semestre 2018 y I semestre 2019) y su avance de implementación.

Ahora bien, en dicha área se designó un "*Coordinador de la gestión de riesgos de TI",* funcionario que confecciono un documento denominado: "*Tabla consolidada inicial administración de riesgos de TI"*, donde procedió a agrupar toda la información que le suministran los responsables de implementar los controles correspondientes de cada riesgo y, posteriormente, se procedió con la inclusión de la información obtenida en el módulo denominado, "Gestión Integral de riesgos de TIC", del software DELPHOS CONTINUUS.

No obstante, a la fecha del presente estudio, no se tiene evidencia de auditoria que demuestra que la Administración Activa, haya realizado un nuevo levantamiento de riesgos de TIC´s; denotándose que, en la etapa relativa al monitoreo durante los años 2019 y 2020, únicamente han realizado un seguimiento de forma continua al mismo listado de riesgos identificados en el año 2018, provocando que el proceso de gestión de riesgos de TI no se esté ejecutando, tal como lo planificado tendiente a administrar de manera integral el factor riesgo, sea, en forma cíclica y secuencial conforme a las etapas relacionadas entre sí, tal como se demuestra en la siguiente imagen:



Fuente: Plan para la gestión de los riesgos del Área de TIC.

Bajo ese esquema, es importante la identificación de nuevos riesgos en el proceso de gestión de TI (internos y externos), que podrían afectar no solo el logro de sus objetivos estratégicos sino institucionales, con repercusiones en la operativa diaria de los procesos del Área de Tecnologías de Información y Comunicaciones o bien, el cumplimiento regulatorio.

En ese orden de ideas, la Ley General de Control Interno N° 8292, en la Sesión II indica:

> *Artículo 18. —Sistema específico de valoración del riesgo institucional. Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo.*

Por otra parte, las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional emitidas por el Ente Contralor al texto manifiestan en lo de interés:

> *2.4. Productos del SEVRI. El SEVRI deberá constituirse en un instrumento que apoye de forma continua los procesos institucionales. En este sentido, se deberá generar a través del SEVRI:*
>
> *a) Información actualizada sobre los riesgos institucionales relevantes asociados al logro de los objetivos y metas, definidos tanto en*

los planes anuales operativos, de mediano y de largo plazos, y el comportamiento del nivel de riesgo institucional.

Asimismo, las Normas de Control Interno para el Sector Público en su apartado 3.3, refieren a la vinculación con la planificación institucional expresando*:*

"La valoración del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión institucionales, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones, y en consecuencia, de los riesgos correspondientes".

"Asimismo, los resultados de la valoración del riesgo deben ser insumos para retroalimentar ese proceso de planificación, aportando elementos para que el jerarca y los titulares subordinados estén en capacidad de revisar, evaluar y ajustar periódicamente los enunciados y supuestos que sustentan los procesos de planificación estratégica y operativa institucional, para determinar su validez ante la dinámica del entorno y de los riesgos internos y externos".

La situación antes descrita es producto de una incorrecta ejecución de la gestión de riesgos que se tiene establecido a lo interno del Área de TIC´s, ya que dicho proceso no se caracteriza por ser dinámico, es decir, en constante revisión del contexto, tanto interno como externo, que le permita conocer factores que podrían afectar la operativa y la continuidad de TI, identificar nuevos riesgos y por ende, establecer controles, preventivos, defectivos o correctivos, de manera que estos no se materialicen y afecten el cumplimiento de la planificación estratégica Institucional.

2.4 Designación de un Coordinador de gestión de riesgos de TI sin competencias e idoneidad.

Como parte de los controles establecidos al riesgo TIC-R66 "*No se tiene documentado la gestión de riesgos de TIC No existe la administración basada en riesgos. No se tienen los recursos humanos necesarios para mantener documentado los riesgos*", el Encargado del Área de Tecnología de Información en mes de junio del año 2018, asignó al funcionario municipal Lic. Gilberto López López, quien desempeña el puesto de Analista de Sistemas (*análisis, diseño, programación, desarrollo, implementación de los sistemas que se*

desarrollan a lo interno del Municipio), como "*Coordinador de la gestión de riesgo de TI"*, designación con alcances tanto en funciones internas del área, como, el constituirse en enlace con la Unidad de Control interno para integrar la gestión de riesgos de TI con el Sistema Específico de Valoración de Riesgos Institucional(SEVRI).

En esa misma línea, la Unidad de Control Interno en el año 2019, realizo una serie de charlas de culturización referentes a: "*Metodología de SEVRI, Uso de las herramientas para la gestión del SEVRI-DELPHOS, resultados procesos anteriores, Plan de trabajo 2019 y siguientes ciclos de evaluación*", en las cuales participaron tres colaboradores del área objeto de estudio a saber: MsC. Eduardo Jiménez González, Encargado; Lic. Daniel Ramírez González Sub Encargado y Lic. Juan Arias Artavia, Analista de Sistemas; no obstante, a pesar de con un funcionario designado como Coordinador del proceso de gestión de Riesgos de TI, este no participó de dicha charla, ni ha recibido algún tipo de capacitación relacionada al proceso de gestión de riesgos de tecnologías de Información, denotándose que no posee el conocimiento técnico necesario para llevar a cabo dicha labor, ni la idoneidad necesaria que garantice el cumplimiento del proceso de gestión de riesgos, ni posee la idoneidad necesaria que garantice el cumplimiento del proceso de gestión de riesgo (identificación, análisis, evaluación, seguimiento) en apego a la normativa que rige la materia.

Lo antes indicado, contraviene las Normas de control interno para el Sector Público emitidas por la Contraloría General de la Republica, en su apartado 2.4 Idoneidad del personal, donde se indica:

> *2.4 Idoneidad del personal El personal debe reunir las competencias y valores requeridos, de conformidad con los manuales de puestos institucionales, para el desempeño de los puestos y la operación de las actividades de control respectivas. Con ese propósito, las políticas y actividades de planificación, reclutamiento, selección, motivación, promoción, evaluación del desempeño, capacitación y otras relacionadas con la gestión de recursos humanos, deben dirigirse técnica y profesionalmente con miras a la contratación, la retención y la actualización de personal idóneo en la cantidad que se estime suficiente para el logro de los objetivos institucionales.*

En ese mismo sentido las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgo Institucional (SEVRI)) indica en lo de interés:

> *"3.4. Recursos. El SEVRI deberá contar con los recursos financieros, humanos, técnicos, materiales y demás necesarios para su establecimiento, operación, perfeccionamiento y evaluación, según lo dispuesto en esta normativa.*
>
> *(…)*
>
> *En el diseño, operación, evaluación y seguimiento del SEVRI se deberán seleccionar y capacitar los recursos humanos que garanticen el cumplimiento del objetivo del Sistema.*
>
> *El presupuesto institucional deberá contemplar los recursos financieros necesarios para la implementación de la estrategia del SEVRI y las provisiones y reservas para la ejecución de las medidas para la administración de riesgos."*

En ese mismo norte, el Marco Orientador del Sistema Específico de Valoración de Riesgos Institucional (SEVRI) del año 2019, manifiesta en sus lineamientos:

> *" …*
> *La Municipalidad desarrollará la estrategia capacitación-acción, para generar pericia en la metodología para la administración del riesgo, paralelamente a la automatización de la implementación del SEVRI, mediante el software DELPHOS CONTINUUM; capacitación en el uso de la herramienta, que permita ir desarrollando en forma gradual y progresiva, los conocimientos y experiencia en la implementación del SEVRI para que la Municipalidad soporte su operación y administración en forma cada vez más robusta.*
> *Mantenimiento del SEVRI*
> *"Proceso continuo de capacitación en torno a diferentes temas relacionados con el SEVRI y la ley de Control Interno."*

La debilidad determinada se relaciona con la necesidad de personal especializado en la materia o bien, carencia de un plan para capacitación del personal destacado en el Area de TIC' que permita obtener una curva de aprendizaje sobre nuevas funciones asignadas, sus procesos y procedimientos.

Tal situación incrementa el riesgo de incumplimiento normativo, pudiéndose presentar factores de riesgo derivados de la carencia de idoneidad de conocimientos y/o capacitación, provocando una potencial afectación de la ejecución de las actividades, a la comunicación apropiada de las labores a los funcionarios involucrados y, a los mecanismos de control sobre la gestión de riesgos de TIC's que desempeñan.

2.5 Escaso conocimiento en las sesiones respecto a temas asociados a la gestión de riesgos de TI, por parte de la Comisión de Tecnologías de Información y Comunicaciones (CTIC); ente asesor del Alcalde Municipal.

La Comisión de Tecnologías de Información y Comunicaciones (CTIC), funge como un órgano asesor de la Alcaldía de la Municipalidad para coadyuvar a mantener la concordancia de la gestión de las TIC's con la Estrategia Institucional, esto según lo estipulado en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República. En esa línea, la Corporación Municipal publicó un Reglamento Interno de Gestión de la Comisión de Tecnologías de Información y Comunicaciones (CTIC), cuerpo normativo que fue modificado según consta en el acuerdo del Concejo Municipal de Sesión Ordinaria realizada el día 28 de agosto del 2018, artículo XXVI del Acta N° 180-2018.

Dentro de las disposiciones generales del citado reglamento, se define que la gestión de la Tecnologías de Información, es la estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar las tecnologías de información, sus riesgos asociados y su vinculación con las estrategias y objetivos de la Municipalidad de Cartago, también se indica dentro de las funciones y responsabilidades de la Comisión de Tecnologías de Información y Comunicaciones, el recomendar a la persona que ocupe la Alcaldía Municipal, la política Institucional en TIC con sujeción al Plan Estratégico Institucional vigente, así como, el asegurar la gestión y la actualización de los documentos al Plan Estratégico de Tecnologías de Información y Comunicaciones (PETIC).

Tal como se observa, la Comisión de Tecnologías de Información y Comunicaciones, asume un rol determinante en asuntos de materia tecnológica y en los riesgos asociados a asuntos estratégicos, que permitan a la Institución lograr sus objetivos; sin embargo, para los años 2019-2020, dicha comisión, únicamente conoció un documento denominado "Metodología de Gestión de Riesgos de TI", según consta en la Sesión Ordinaria N°5-2019 celebrada el 15 de octubre del 2019, misma que fue presidia por el

señor Rolando Rodríguez Brenes como Coordinador de la Comisión de turno, acordándose en los puntos números 1 y 2:

> *"ARTÍCULO VIII. – METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TI.*
>
> *El señor Rolando Rodriguez Brenes, les solicita a los miembros de la comisión que estén de acuerdo con indicar que se dio a conocer la metodología para la gestión de riesgos de TI que procedan a levantar la mano esta Comisión acuerda por unanimidad:*
>
> *1. Se dio a conocer la metodología para la gestión de riesgos de TI.*
>
> *2.Acuerdo definitivamente aprobado."*

Cabe mencionar que, el acta en cita no se encuentra debidamente firmada ni por el Presidente (a) ni por el Secretario (a) de la comisión; aunado a que, el documento "*Metodología para la gestión de riesgos de TI"*, no cumple con el formato que se tiene establecido en: *"7I01 Instructivo desarrollo de documentos"* y *"7I02 Lineamientos para la normalización de documentos"*, incluidos en el Sistema de Gestión de Calidad.

En este sentido, esta instancia auditora consultó a la actual Coordinadora de la Comisión de Tecnología de Información y Comunicaciones, Licda. Silvia Alvarado Martínez, Vice Alcaldesa Municipal, respecto a los acuerdos contenido en actas del citado órgano Colegiado donde se hubiesen tratado "…*asuntos relacionados a la gestión de riesgos atinentes al Área de Tecnologías de Información y Comunicaciones entre el periodo 2019 y 2020";* obteniéndose por respuesta que, no consta que el tema consultado haya sido conocido en alguna sesión.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información emitidas por la Contraloría General de la República,

> *"1.6 Decisiones sobre asuntos estratégicos de TI*
>
> *El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización. "*

Lo anterior obedece a que, la Comisión de Tecnologías de Información y Comunicaciones en sus sesiones, no está conociendo temas relacionados con la gestión de TI, incluidos en los informes productos de: auditoría interna y externa, Autoevaluaciones del Sistema de Control Interno (ASCI) y seguimientos al Sistema Específico de Valoración de Riesgos (SEVRI) u otros entes gubernamentales con competencia en la materia; los cuales podrían comunicar debilidades que afecten el cumplimiento del Plan Estratégico de Tecnologías de Información (PETIC) e impactar los objetivos del área objeto de estudio y por ende, el Plan Estratégico Institucional y objetivos fijados en los planes de gobierno.

Tal situación podría causar incumplimientos por parte de la Comisión de Tecnologías de Información y Comunicaciones, al no estar ejerciendo sus funciones y responsabilidades acorde a lo normado en el citado marco normativo, en cuanto a asesorar para la toma de decisiones estratégicas concernientes a TI, pudiendo materializarse riesgos tecnológicos asociados al funcionamiento normal del Gobierno Local y por ende, el logro de los objetivos Institucionales.

3 CONCLUSIONES

3.1. El marco de gestión de TI, no se encuentra alineado con la gestión de riesgos de TI en cuanto a la: planificación estratégica de TI, Seguridad de la información, Continuidad de los servicios de TI, gestión de proyectos, entre otros, los cuales coadyuban a la gobernanza de TIC.

3.2. El Área de Tecnologías de Información y Comunicaciones administra su propio proceso de gestión de riesgos, conforme lo regulado en las Normas Técnicas para la gestión y el control de las Tecnologías de Información, sin embargo, esta no consideró lo normado por el Ente Contralor en las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional, en lo que corresponde a: Identificación, análisis, evaluación, administración y revisión de los riesgos institucionales, tanto de fuentes internas como externas, relevantes para la consecución de los objetivos.

3.3. La Administración Activa, específicamente para el Area de TIC's ha realizado durante los años 2019 y 2020, únicamente un seguimiento o monitoreo del listado de riesgos identificados en el año 2018, omitiéndose la identificación de nuevos riesgos en el proceso de gestión de TI (internos y externos), que podrían afectar no solo el logro de sus objetivos estratégicos sino institucionales, con repercusiones en la operativa diaria de los procesos del Área de Tecnologías de Información y Comunicaciones o bien, el cumplimiento regulatorio.

3.4. Como parte de los controles establecidos al riesgo TIC-R66 *"No se tiene documentado la gestión de riesgos de TIC No existe la administración basada en riesgos. No se tienen los recursos humanos necesarios para mantener documentado los riesgos"*, se designó un *"Coordinador de la gestión de riesgo de TI"*, el cual no posee el conocimiento técnico necesario para llevar a cabo dicha labor, ni posee la idoneidad necesaria que garantice el cumplimiento del proceso de gestión de riesgos

(identificación, análisis, evaluación, seguimiento) en apego a la normativa que rige la materia.

3.5. La Comisión de Tecnologías de Información y Comunicaciones no está conociendo en sus sesiones, temas relacionados con la gestión de TI, incluidos en los informes productos de: auditoría interna y externa, Autoevaluaciones del Sistema de Control Interno (ASCI) y seguimientos al Sistema Específico de Valoración de Riesgos (SEVRI) u otros entes gubernamentales con competencia en la materia; los cuales podrían comunicar debilidades que afecten el cumplimiento del Plan Estratégico de Tecnologías de Información (PETIC) e impactar los objetivos del área objeto de estudio y por ende, el Plan Estratégico Institucional y objetivos fijados en los planes de gobierno.

4. RECOMENDACIONES

Conforme a los hallazgos expuestos en el aparte 2 del presente informe, esta instancia auditora gira las siguientes recomendaciones de índole administrativo, orientadas hacia la Alcaldia Municipal y la Comisión de Tecnologías de Información y Comunicaciones, las cuales deberán estar implementadas en un plazo máximo de dos meses, contados a partir del día hábil siguiente, a la recepción del informe final, según se detalla:

Se recomienda al **Lic. Mario Redondo Poveda, en su condición de Alcalde Municipal** o a quien en su lugar ocupe el cargo:	
Nº	**Detalle de Recomendación**
1	Adoptar un marco de buenas prácticas para la gestión de TI, el cual permita desarrollar el proceso de gestión de riesgos relacionados a TI de forma integrada con otros procesos institucionales de la misma índole; de manera que, los riesgos relacionados con TI estén debidamente identificados, analizados y evaluados, que permita generar información útil para tomas de decisiones en benefició del logro de los planes estratégicos de TI y, por ende, corporativos. **Refiérase al hallazgo Nro.2.1**
Se recomienda al **Lic. Mario Redondo Poveda,** en su condición de **Alcalde Municipal** o a quien en su lugar ocupe, girar las instrucciones a la **Jefatura de la Unidad de Control Interno** en coordinación con **el Encargado del Area de Tecnologías de Información y Comunicaciones** para que procedan a:	
Nº	**Detalle de Recomendación**
2	Revisar y ajustar la valoración de riesgos de TI, conforme lo establecido en la Directrices generales para el establecimiento y funcionamiento del sistema específico de riesgo institucional (SEVRI), de manera que dicho marco teórico metodológico se encuentre alineado con las citadas directrices, así como al Marco Orientador

	Institucional. **Refiérase al hallazgo Nro.2.2**

Se recomienda al **Lic. Mario Redondo Poveda,** en su condición de **Alcalde Municipal** o a quien en su lugar ocupe, girar las instrucciones al **Encargado del Area de Tecnologías de Información y Comunicaciones** para que proceda a:

Nº	**Detalle de Recomendación**
3	Definir mediante documento formal, la periodicidad del ciclo o proceso atinente a la gestión de riesgos de TI, que permita cumplir con lo normado en las Directrices establecidas para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos (SEVRI) en lo concerniente a: identificación, análisis, evaluación, administración, revisión, documentación y comunicación. **Refiérase al hallazgo Nro.2.3**
4	Gestionar ante quien corresponda, la elaboración y ejecución de un diagnóstico que permita definir los tópicos y recursos a utilizar, necesarios para fortalecer y actualizar las competencias de los funcionarios del Area de TIC's involucrados en el proceso gestión de riesgos, de modo que se asegure su idoneidad en el proceso. **Refiérase al hallazgo Nro.2.4**

Se recomienda a la **Comisión de Tecnología de Información y Comunicaciones** para que proceda a:

Nº	**Detalle de Recomendación**
5	Elaborar y presentar ante el Alcalde Municipal, una propuesta de ajustes al Reglamento interno de gestión de la Comisión de Tecnologías de Información y Comunicaciones, que permita alinear tanto sus funciones y responsabilidades, así como su participación, al marco de gestión de TI definido por este Gobierno Local, que incluye el proceso de gestión de riesgos (identificación, análisis, evaluación,

	administración, revisión, documentación y comunicación). **Refiérase al hallazgo Nro.2.5**
6	Solicitar al Alcalde Municipal Lic. Mario Redondo Poveda o quien ocupe su lugar, mediante acuerdo de CTIC, girar las instrucciones a quien corresponda para que, los documentos relacionados al proceso de gestión de TI, que incluyen: Plan Estratégico de TIC´s, informes productos de: auditoría interna, auditoría externa, autoevaluaciones de control interno y seguimiento a la gestión de valoración de riesgos relacionados con el Area de TIC´s, entre otros; sean elevados a conocimiento de la citada comisión, de manera que permita obtener un conocimiento más amplio y oportuno de su gestión y así, asesorar en temas de carácter tecnológico para el logro de los objetivos Institucionales. **Refiérase al hallazgo Nro.2.5**

RICARDO ASDRUBAL CHAVES RODRIGUEZ (FIRMA)
Firmado digitalmente por RICARDO ASDRUBAL CHAVES RODRIGUEZ (FIRMA)
Fecha: 2021.07.16 11:21:12 -06'00'

Lic. Ricardo Chaves Rodríguez
ENCARGADO DEL ESTUDIO

ALFREDO ARAYA LEANDRO
Firmado digitalmente por ALFREDO ARAYA LEANDRO
Fecha: 2021.07.16 14:23:50 -06'00'

Lic. Alfredo Araya Leandro,MBA.
COORDINADOR DEL ESTUDIO