INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DE CARTAGO

14 de septiembre de 2023

Informe n.° DFOE-LOC-IAD-00019-2023

Contraloría General de la República
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización para el Desarrollo Local
Auditoría de Carácter Especial - Compromiso de informe directo

CONTENIDO

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos de la Municipalidad de Cartago responde al marco regulatorio y buenas prácticas aplicables. El periodo evaluado comprende desde 01 de enero de 2022 al 31 de julio de 2023.

¿POR QUÉ ES IMPORTANTE?

La Municipalidad de Cartago como administradora de los intereses y servicios públicos, cumple un papel determinante en la promoción del desarrollo local. Para la ejecución de los procesos sustantivos y cumplir sus objetivos institucionales, la Municipalidad se apoya en varios sistemas de información, dentro de los cuales destacan el sistema tributario, para la recaudación, cobro, plataforma de servicios y patentes; el sistema financiero, para la administración del presupuesto institucional, el control de órdenes de compra, la gestión de inventario, la gestión de caja chica y generación de asientos contables de egresos; y el sistema de bienes inmuebles. Por medio de dichos sistemas se recopilan, procesan y almacenan datos sobre los contribuyentes; ello plantea la necesidad de proteger la plataforma tecnológica institucional contra el uso fraudulento, acceso no autorizado, pérdida, alteración o difusión; de manera que se garantice en forma razonable la protección de la información crítica.

¿QUÉ ENCONTRAMOS?

De conformidad con el objetivo de la auditoría, se concluye que la seguridad de la información de los sistemas críticos de la Municipalidad de Cartago no responde razonablemente al marco regulatorio y buenas prácticas aplicables. Lo cual genera que la institución se exponga a diferentes riesgos, y por lo tanto se deben ejecutar acciones oportunas que permitan la atención y corrección de los temas que se detallarán en los siguientes párrafos.

En ese sentido, se determinó que la Municipalidad no cuenta con un área o persona encargada formalmente de la seguridad de la información y tampoco se ha gestionado capacitación en la materia que perfile la especialización de uno o varios funcionarios en temas avanzados y complejos, para una gestión efectiva de la seguridad de la información. Ello dificulta el desarrollo de capacidades internas en el personal que asume esas funciones, e incide en la coordinación de las medidas de seguridad aplicables en la organización.

Asimismo, se identificó que la institución no cuenta con instrumentos divulgados, validados y aprobados por la Alcaldía, que permitan planificar la gestión de seguridad de la información. Se carece, además, de protocolos o procedimientos específicos para atender al menos los incidentes de seguridad más conocidos o bien más comunes. Dichas situaciones elevan la exposición a incidentes, y potencian el riesgo de que estos afecten de manera significativa la seguridad de la información y la continuidad de los procesos institucionales.

Adicionalmente, se evidenciaron deficiencias en la calidad de la información respecto a las solicitudes que se tramitan a través de la mesa de ayuda, dado que no se hace una distinción clara entre requerimientos de servicios e incidentes, ni se cuenta con una categoría específica

para catalogar incidentes de seguridad. Lo anterior de conformidad con un reporte generado entre enero de 2022 y julio de 2023 en el que se contabilizan 1.242 eventos catalogados como incidentes. Ello desvía la atención hacia temas que no son urgentes, y dificulta la priorización, asignación de recursos y respuesta oportuna de los eventos que efectivamente corresponden a incidentes.

Finalmente, la Contraloría General determinó vulnerabilidades, tanto en la red interna como en los servicios expuestos a Internet. Estas situaciones pueden comprometer la integridad, disponibilidad y confidencialidad de la información de la Municipalidad de Cartago; evidencia de ello, es que se identificaron 269 vulnerabilidades (91 críticas, 167 altas, 11 medias) en pruebas internas y 9 vulnerabilidades (3 críticas, 2 altas y 4 medias) en pruebas externas.

En el transcurso de la auditoría, la institución ha solucionado algunas de las situaciones identificadas, sin embargo, a la fecha existen otras que continúan en proceso de atención.

¿QUÉ SIGUE?

Se emiten disposiciones al Alcalde Municipal, con el propósito de que, en coordinación con el Área de Tecnologías de Información y Comunicación y el Departamento de Recursos Humanos, se implemente un plan para alinear las capacidades del personal que actualmente se encarga de la seguridad de la información, con el perfil que efectivamente requiere la Municipalidad.

También, se dispone a dicho Alcalde la implementación de un plan de seguridad de la información alineado con las Políticas de Seguridad de la Información institucionales, que permita contar con indicadores y acciones definidas para la gestión eficaz de la seguridad de la información, así como la atención oportuna de situaciones que pongan en riesgo los activos de información y la continuidad de los procesos institucionales.

Finalmente, se emiten disposiciones al Área de Tecnologías de Información y Comunicación para que implemente mecanismos de monitoreo, identificación y atención oportuna de riesgos y vulnerabilidades relacionados con seguridad de la información.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DE CARTAGO

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La Municipalidad de Cartago ha digitalizado una serie de procesos y servicios institucionales. Como parte de dicho proceso, ha puesto a disposición del público trámites en línea, canales digitales de pago mediante portales y aplicaciones móviles, así como campañas de alfabetización digital. Todo lo anterior, en procura del cumplimiento de sus funciones asociadas con la prestación de servicios municipales y el desarrollo territorial.

1.2. Para ello, la institución se apoya en sistemas de información, que le facilitan la captura, el procesamiento y custodia de la información. Por lo anterior, resulta necesario analizar las medidas con que cuenta esa institución para garantizar la confidencialidad, integridad y disponibilidad de los datos que gestiona por medio de dichos sistemas.

1.3. La presente auditoría se realizó en cumplimiento del Plan Anual Operativo de la DFOE y sus modificaciones, con fundamento en las competencias que le son conferidas a la Contraloría General de la República en los artículos 183 y 184 de la Constitución Política y los artículos 12, 17 y 21 de su Ley Orgánica, n.° 7428.

OBJETIVO GENERAL

1.4. La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos de la Municipalidad de Cartago responde al marco regulatorio y buenas prácticas aplicables.

ALCANCE

1.5. La auditoría comprendió el análisis del marco normativo y buenas prácticas relacionadas con la seguridad de la información aplicadas por la Municipalidad de Cartago, con el fin de fortalecer la capacidad de gestión institucional. El período de análisis comprendió del 1 de enero de 2022 al 31 de julio de 2023.

CRITERIOS DE AUDITORÍA

1.6. Los criterios de evaluación aplicados en la presente auditoría, y la escala de cumplimiento utilizada para llegar a las conclusiones de este informe, se comunicaron mediante oficio n.° 5596 (DFOE-LOC-0891) del 02 de mayo de 2023. En esa misma fecha, fueron presentados a los funcionarios de la Municipalidad de Cartago, Mario Redondo Poveda, Alcalde Municipal; Daniel Ramírez González, Director del Área de Tecnologías de Información; y Juan Arias Artavia, Subdirector del Área de Tecnologías de Información.

METODOLOGÍA APLICADA

1.7. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR, el Procedimiento de Auditoría vigente, establecido por la DFOE, que está basado en la ISSAI 100: Principios Fundamentales de Auditoría del Sector Público, y los principios de la ISSAI 400: Principios de la Auditoría de Cumplimiento de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI por sus siglas en inglés).

1.8. Para el desarrollo de esta auditoría, se utilizó la información suministrada en las entrevistas a funcionarios de la Municipalidad de Cartago, así como las respuestas a las consultas planteadas por escrito a esa institución.

1.9. Asimismo, se realizaron pruebas sustantivas para validar la efectividad operativa de controles específicos tanto a nivel de aplicaciones como a nivel de gestión de TI; por otra parte, se remitió una herramienta de consulta al Director del Área de Tecnologías de Información, con el fin de indagar sobre aspectos vinculados con la gestión de personas, administración de procesos y uso de tecnologías, y una carpeta compartida en la cual se solicitó adjuntar la información de respaldo que se considerara pertinente. Al respecto, se efectuó una sesión previa para explicar la herramienta, y una sesión posterior para validar los resultados.

1.10. Finalmente, se realizó un ejercicio con el Director y el Subdirector del Área de Tecnologías de Información, con el fin de conocer causas y opciones de solución sobre las temáticas encontradas en la auditoría, las cuales fueron consideradas para la elaboración de este informe.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.11. De conformidad con los datos extraídos del Sistema de Información sobre Planes y Presupuestos (SIPP) de la CGR, la Municipalidad de Cartago reporta para el periodo 2022 una ejecución presupuestaria por montos de ₡1.050 millones en partidas asociadas en tecnologías de información, entre las que destacan partidas tales como: mantenimiento y reparación de equipo de cómputo y sistemas de información, equipo y programas de cómputo, servicios de desarrollo de sistemas informáticos, servicio de telecomunicaciones y servicios de tecnologías de información.

1.12. Para la ejecución de los procesos sustantivos y cumplir sus objetivos institucionales, la Municipalidad se apoya en el uso de sistemas de información, por medio de los cuales captura, procesa y almacena información crítica para el cumplimiento de las funciones y objetivos institucionales, incluyendo datos sobre los contribuyentes.

1.13. Dentro de dichos sistemas, destacan el sistema tributario, para la recaudación, cobro, plataforma de servicios y patentes; el sistema financiero, para la administración del presupuesto institucional, el control de órdenes de compra, la gestión de inventario, la gestión de caja chica y generación de asientos contables de egresos; y el sistema de bienes inmuebles.

Imagen n.° 1. Principales sistemas de información de la Municipalidad de Cartago

Fuente: Elaboración CGR

1.14. Asimismo, la Municipalidad ha desarrollado una plataforma digital, por medio de la cual ofrece a los ciudadanos del cantón facilidades para realizar trámites en línea, a través del sitio web institucional. Dentro de dichos trámites se encuentran el pago de tributos en línea, la solicitud y consulta de certificados de uso de suelo, el envío de la declaración jurada de patentes, entre otros.

1.15. Para un correcto aprovechamiento de dichas facilidades, la Municipalidad ha emprendido acciones orientadas a la alfabetización digital y concientización de sus funcionarios y de los pobladores del cantón, por medio de cursos sobre temáticas como ciberseguridad, robótica y ofimática, así como la emisión de comunicados sobre medidas de protección contra estafas.

1.16. Aunado a lo anterior, la digitalización de los procesos y servicios institucionales implica el despliegue de medidas y controles, para proteger la plataforma tecnológica contra el uso fraudulento, acceso no autorizado, pérdida, alteración o difusión; de manera que se garantice en forma razonable la protección de la información.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.17. El borrador del presente informe fue remitido a la Municipalidad de Cartago mediante el oficio n.° DFOE-LOC-1476 (11550) de fecha 29 de agosto de 2023, dirigido al Licenciado Mario Redondo Poveda, Alcalde Municipal. Lo anterior, con el propósito de que se formularan y remitirieran a la Contraloría General, en un plazo no mayor de seis días hábiles, las observaciones que se consideraran pertinentes sobre su contenido, con la respectiva documentación de respaldo.

1.18. Asimismo, el 04 de septiembre de 2023 se presentaron los resultados de la auditoría en reunión virtual realizada por medio de la plataforma Google Meet. En la reunión participaron los siguientes representantes de la Municipalidad de Cartago: Mario Redondo Poveda, Alcalde; Daniel Ramírez González, Director del Área de Tecnologías de Información y Comunicación; y Juan Arias Artavia, Subdirector del Área de Tecnologías de Información y Comunicación.

1.19. En atención a lo solicitado por el Órgano Contralor, se recibió el oficio n.° AM-OF-829-2023 de fecha 04 de septiembre de 2023 y recibido por la Contraloría General el 05 de septiembre de 2023, suscrito por el Licenciado Mario Redondo Poveda, Alcalde de la Municipalidad de Cartago, mediante el cual remitió las observaciones al borrador del informe; mismas que una vez valoradas, fueron atendidas por medio del oficio n.° DFOE-LOC-1648(12493) de fecha 14 de septiembre de 2023.

SIGLAS Y ABREVIATURAS

1.20. A continuación, se indica el detalle de las siglas utilizadas en este informe:

Siglas / Abreviaturas	Significado
CGR	Contraloría General de la República
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas, por sus siglas en inglés
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
ISO	Organización Internacional para la Estandarización, por sus siglas en inglés

2. RESULTADOS

2.1. A continuación se exponen los resultados obtenidos en la auditoría de carácter especial sobre la seguridad de la información en la Municipalidad de Cartago.

GESTIÓN DE PERSONAS

Ausencia de roles y responsabilidades vinculados con la seguridad de la información que permitan el desarrollo de capacidades internas en esa materia

2.2. Se determinó que la Municipalidad de Cartago no cuenta con un área o persona encargada formalmente de seguridad de la información, que lidere, entre otros asuntos, el análisis de riesgos de seguridad de la información, políticas de seguridad, concienciación y capacitación del personal, monitoreo y respuesta de incidentes, entre otros. En su defecto, las funciones de seguridad de la información y ciberseguridad han sido asumidas por personal del Área de Tecnologías de Información, sin una definición oficial de sus roles y responsabilidades.

2.3. En adición a lo anterior, se carece de una gestión de capacitación en seguridad de la información para el personal que actualmente asume dichas funciones. El Área de Tecnologías de Información elaboró en 2022 un diagnóstico de necesidades de capacitación para su personal, dentro del cual incluyó el tema de ciberseguridad. En respuesta a dicho diagnóstico, actualmente todos los funcionarios de esa dependencia recibieron una capacitación introductoria de ciberseguridad; sin embargo, no se cuenta con una planificación detallada que perfile la especialización de uno o varios funcionarios en temáticas más avanzadas y complejas, requeridas para una efectiva gestión de la seguridad de la información institucional.

2.4. Al respecto, la norma 2.4 *Idoneidad del personal*, de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) del 6 de febrero de 2009, publicado en La Gaceta n.° 26 del 6 de febrero de 2009, señala que el personal debe reunir las competencias y valores requeridos, de conformidad con los manuales de puestos institucionales, para la operación de las actividades de control respectivas; y que las políticas y actividades de capacitación deben dirigirse técnica y profesionalmente con miras a la contratación y actualización de personal idóneo para el logro de los objetivos institucionales.

2.5. Por su parte, el apartado *Recursos Humanos* de 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, establecen el deber de contar con funcionarios que dispongan de un perfil técnico de acuerdo con sus responsabilidades.

2.6. Asimismo, las buenas prácticas de Cobit 2019 de ISACA, en la práctica de gestión APO07.03 *Mantener las habilidades y competencias del personal*, establecen dentro de sus actividades el identificar las habilidades y competencias disponibles actuales; identificar las brechas entre las habilidades requeridas y las disponibles; y desarrollar planes de acción, como capacitación, contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas.

2.7. Las situaciones anteriores se deben a la ausencia de perfiles oficiales en materia de seguridad de la información, en los que se definan las funciones a ejecutar y los conocimientos requeridos. Ello impide el desarrollo de un plan de capacitación que permita cerrar las brechas de conocimiento entre el perfil actual del personal encargado de la seguridad y el perfil requerido.

2.8. La ausencia de un perfil de personal en materia de seguridad de la información incide en la coordinación de las medidas de seguridad aplicables en la organización. Dichas medidas comprenden la formulación, implementación y seguimiento de acciones preventivas, el monitoreo de la infraestructura de TI y la respuesta oportuna ante incidentes de seguridad. Lo anterior incrementa el tiempo de respuesta, el costo de atención ante eventuales incidentes de seguridad, así como el riesgo de exposición y pérdida de información.

ADMINISTRACIÓN DE PROCESOS

Necesidad de mejorar los procesos de planificación y monitoreo del sistema de gestión de la seguridad de la información

2.9. La Municipalidad de Cartago no cuenta con instrumentos divulgados, validados y aprobados por la Alcaldía, que permitan planificar la gestión de la seguridad de la información. Por lo tanto, no se han establecido las medidas que implementará la organización para proteger la información y los activos asociados contra las amenazas y riesgos identificados, aunado a que no se cuenta con un proceso de seguimiento y cumplimiento de tales acciones.

2.10. Asimismo, la Municipalidad carece de protocolos o procedimientos específicos para atender al menos los incidentes de seguridad más conocidos o bien más comunes. Si bien, la institución cuenta con mecanismos para identificar eventuales incidentes de seguridad, no se tiene claridad sobre la forma de atender un eventual incidente. Cabe aclarar que, a la fecha, no se han presentado incidentes de seguridad de la información; sin embargo, en caso de ocurrir, podrían tener un impacto directo en la confidencialidad, integridad y disponibilidad de la información institucional.

2.11. En adición a lo anterior, se identificaron deficiencias en la calidad de la información que se obtiene del Sistema de Administración de Requerimientos (mesa de ayuda), dado que no se hace una distinción clara entre requerimientos de servicios e incidentes, ni se cuenta con una categoría específica para catalogar incidentes de seguridad.

2.12. Al respecto, las Políticas de Seguridad de la Información de la Municipalidad de Cartago (7M16) del 30 de mayo de 2022, establecen en el apartado 1.2. *Plan sobre establecimiento de medidas de seguridad*, que "se deben establecer medidas de seguridad que funcionen de manera óptima para proteger la información que se maneja dentro de la Municipalidad. Estas deben contar con protocolos que puedan repeler una amenaza ya sea de hardware o software". En dicho apartado se establece, además, que entre las medidas de seguridad es importante contar con una identificación del conjunto de activos de la organización, a saber, personal, hardware, software, sistemas y todos los datos dentro de los sistemas informáticos; además, de identificar las amenazas que pueden poner en peligro la información, tales como virus, daños físicos, hackers y errores del personal de TI; también indica que se debe evaluar el daño de cada amenaza, y establecer las medidas de protección.

2.13. En línea con ello, la práctica de gestión APO13.03 *Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)*, de Cobit 2019, indica que se debe mantener y comunicar periódicamente la necesidad y los beneficios de una mejora continua de seguridad de la información, recopilar y analizar datos sobre el sistema de gestión de seguridad de la información (SGSI), mejorar su efectividad, y corregir los incumplimientos para evitar la recurrencia.

2.14. Las situaciones identificadas se deben a que la Municipalidad de Cartago ha concentrado sus esfuerzos en definir las acciones reactivas para recuperarse posterior a un incidente de seguridad; pero carece de un enfoque preventivo respaldado en un plan de seguridad de la información, que permita la definición de acciones para gestionar la seguridad como un proceso continuo, así como atender oportunamente incidentes de seguridad y evitar que lleguen a constituirse en desastres.

2.15. La ausencia de un plan de seguridad de la información eleva el riesgo de exposición a incidentes, y a su vez, la ausencia de protocolos para la atención oportuna de incidentes potencia el riesgo de que estos se transformen en desastres y afecten de manera significativa la seguridad de la información y continuidad de los procesos institucionales.

2.16. Asimismo, respecto a las deficiencias en la calidad de la información del Sistema de Administración de Requerimientos, en un reporte generado por dicho sistema entre el 1 de enero de 2022 y el 21 de julio de 2023, se registraron 1.242 eventos catalogados como incidentes; sin embargo, al hacer una revisión de los casos, algunos de ellos no constituyen incidentes. Por ejemplo, cambios de tinta o atascos de papel en impresoras, traslado de equipos entre oficinas, aumento del espacio de almacenamiento, entre otros.

2.17. Ello desvía la atención hacia temas que no son urgentes, y dificulta la priorización, asignación de recursos y respuesta oportuna de los eventos que efectivamente corresponden a incidentes. Además, imposibilita la definición y medición de indicadores

para monitorear los controles de seguridad, y la definición de acciones a realizar, según el comportamiento de dichos indicadores.

USO DE TECNOLOGÍAS

Debilidades en la gestión de la seguridad de la información y ciberseguridad para garantizar la protección de los activos críticos de la Municipalidad

2.18. Se determinó que la Municipalidad de Cartago no efectúa análisis periódicos de vulnerabilidades internas y externas, ya sea por parte de personal municipal o contratadas a terceros. Al respecto, se han efectuado contrataciones para ejecutar algunos análisis; sin embargo la última contratación para los efectos fue realizada en el año 2020, producto de la cual se reportaron 10 vulnerabilidades relativas a aspectos como la seguridad de servidores, el sitio web y cumplimientos regulatorios.

2.19. En línea con lo anterior, como parte de la auditoría, la Contraloría General efectuó una serie de pruebas de vulnerabilidades de seguridad que permitieron identificar oportunidades de mejora relacionadas con la integridad, disponibilidad y confidencialidad de la información. A la fecha de cierre de este estudio, la Municipalidad reportó que algunas de las situaciones han sido atendidas, mientras otras continúan en proceso de atención.

2.20. Al respecto, el artículo 12 *Deberes del jerarca y de los titulares subordinados en el sistema de control interno*, de la Ley General de Control Interno, n.° 8292, señala el deber de tomar acciones correctivas ante cualquier evidencia de desviaciones.

2.21. Por su parte, las normas 5.7.4 *Seguridad* y 5.8 *Control de Sistemas de Información*, de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), indican el deber de instaurar controles para proteger la información, según su grado de sensibilidad y confidencialidad, así como disponer de controles para que los sistemas de información garanticen razonablemente su calidad, la seguridad, administración de niveles de acceso y garantía de confidencialidad de la información que ostente ese carácter.

2.22. En línea con ello, el marco de buenas prácticas de Cobit 2019, en la práctica de gestión DSS05.07 *Gestionar las vulnerabilidades y monitorear la infraestructura para detectar eventos relacionados con la seguridad*, indica que se deben gestionar las vulnerabilidades y monitorear la infraestructura para detectar accesos no autorizados, mediante el uso de un portafolio de herramientas y tecnologías.

2.23. Asimismo, la práctica de gestión BAI03.10 *Mantener las soluciones,* indica que se debe desarrollar y ejecutar un plan para mantener los componentes de la solución tecnológica, que incluya, entre otros aspectos, estrategias de actualización, riesgo, privacidad, análisis de vulnerabilidades y requisitos de seguridad.

2.24. Lo anterior obedece a la ausencia de mecanismos permanentes para monitorear e identificar en forma periódica posibles riesgos y vulnerabilidades que permitan tomar decisiones oportunas sobre la aplicación de parches de seguridad, mejoras en la

configuración, actualización de equipos y sistemas, entre otros. Ello a pesar de que en el Plan Estratégico de Tecnologías de Información 2022-2024 se estableció el objetivo de "mejorar la seguridad de la información de la Municipalidad y proteger los datos sensibles de los ciudadanos" y como parte de los resultados clave se definió "mejorar en un 20% la detección temprana de amenazas y vulnerabilidades".

2.25. La ausencia de un proceso de detección y atención oportuna de vulnerabilidades pone en riesgo la seguridad de la información que se captura, procesa y almacena en los sistemas de información institucionales. Evidencia de ello es que, producto de las pruebas de campo efectuadas por la Contraloría General de la República, se identificaron 296 vulnerabilidades en **pruebas internas**, de las cuales 91 son críticas[1] y se relacionan con la obsolescencia de software, actualizaciones de seguridad, algoritmos de cifrado y controles de acceso; 167 altas[2] vinculadas con certificados, algoritmos de cifrado, actualizaciones de seguridad y configuración de servidores web y sistemas operativos; así como 11 medias[3] asociadas a transmisión de texto sin cifrar, denegación de servicio, actualizaciones de seguridad, y algoritmos de cifrado.

Imagen n.° 2. Resultados de las pruebas internas

Fuente: Elaboración CGR

[1] Vulnerabilidad que puede poner en riesgo explotación de otras vulnerabilidades, podría poner en riesgo los servidores o los dispositivos de infraestructura de forma sencilla.

[2] Vulnerabilidad que requiere un nivel mayor de complejidad para ser explotada y como consecuencia podría darse pérdida de información (datos).

[3] Para explotar este tipo de vulnerabilidad, el usuario malicioso puede manipular a potenciales víctimas mediante técnicas de ingeniería social, proporciona un acceso limitado; sin embargo el fin de este ataque es escalar en privilegios dentro de los sistemas.

2.26. Asimismo, se identificaron 9 vulnerabilidades en **pruebas externas**, de las cuales 3 son críticas y se relacionan con obsolescencia de software; 2 son altas y corresponden a configuraciones de servidores web y sistemas operativos, así como seguridad del sistema de nombres de dominio; y 4 son medias, relativas a configuraciones por defecto, obsolescencia de software y configuraciones de servidores web y sistemas operativos.

Imagen n.° 3. Resultados de las pruebas externas

Fuente: Elaboración CGR

3. CONCLUSIÓN

3.1. Una vez obtenidos los resultados, con base en la recopilación de la evidencia suficiente y apropiada, se concluye que la seguridad de la información de los sistemas críticos de la Municipalidad de Cartago no cumple, en todos sus aspectos significativos, con los criterios de auditoría. Ello expone a la institución a diferentes riesgos, por lo que resulta necesario que se ejecuten acciones para la atención y corrección oportuna de los temas abordados en el presente informe.

3.2. Lo anterior por cuanto, en lo referente a la gestión de personas, es relevante fortalecer la estructura organizativa de seguridad de la información y el perfil del personal encargado de gestionarla.

3.1. Asimismo, en materia de administración de procesos, se evidenció la necesidad de contar con un marco de seguridad de la información, así como la formulación de indicadores que permitan el monitoreo de incidentes.

3.3. Por último, en lo referente al uso de tecnologías, resulta necesario fortalecer las prácticas de seguridad de información vinculadas con el establecimiento de mecanismos para identificar, de forma oportuna, vulnerabilidades en la infraestructura institucional.

4. DISPOSICIONES

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, n.° 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los “Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría”, emitidos mediante resolución n.° R-DC-144-2015, publicados en La Gaceta n.° 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016

4.3. Este Órgano Contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

AL SEÑOR MARIO REDONDO POVEDA EN SU CALIDAD DE ALCALDE DE LA MUNICIPALIDAD DE CARTAGO, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. En coordinación con el Área de Tecnologías de Información y el Departamento de Recursos Humanos, elaborar, oficializar e implementar un plan para alinear las capacidades del personal de seguridad con el perfil que efectivamente requiere la Municipalidad. Dicho plan debe contener, al menos (ver párrafos del 2.2 al 2.8):

a. Una identificación del perfil actual de las personas encargadas de la seguridad de la información.
b. Una definición del perfil requerido, un diagnóstico de las brechas existentes entre los perfiles actuales y el perfil requerido.
c. Un cronograma de capacitación con plazos, responsables e indicadores para medir el avance y la cobertura.

Para acreditar el cumplimiento de esta disposición, deberá remitir a la Contraloría General, a más tardar el 22 de diciembre de 2023, un oficio en el que acredite la elaboración y oficialización del plan. Con respecto a la implementación, remitir dos informes sobre el avance y la cobertura del cronograma de capacitación; el primero de ellos a más tardar el 31 de mayo de 2024, y el segundo a más tardar el 29 de noviembre de 2024.

4.5. Elaborar, oficializar e implementar un plan de seguridad de la información alineado con las Políticas de Seguridad de la Información de la Municipalidad de Cartago que incluya, al menos (ver párrafos del 2.9 al 2.17):

a. Objetivos.
b. Medidas y controles a aplicar.
c. Definición de indicadores para el monitoreo de controles de seguridad.
d. Roles y responsables.

Para acreditar el cumplimiento de esta disposición, deberá remitir a la Contraloría General, a más tardar el 31 de enero de 2024, un oficio en el que acredite la elaboración y oficialización del plan de seguridad. Asimismo, remitir dos informes sobre el avance en la implementación del plan de seguridad; el primero de ellos a más tardar el 28 de junio de 2024, y el segundo a más tardar el 31 de octubre de 2024.

AL SEÑOR DANIEL RAMÍREZ GONZÁLEZ EN SU CALIDAD DE DIRECTOR DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA MUNICIPALIDAD DE CARTAGO, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.6. Elaborar, aprobar e implementar mecanismos para monitorear, identificar y atender posibles riesgos y vulnerabilidades relacionados con la seguridad de la información, que permitan tomar decisiones oportunas para reducir el impacto de estos riesgos en los procesos del negocio. Dichos mecanismos deben considerar al menos (ver párrafos del 2.18 al 2.26):

a. Acciones
b. Responsables
c. Generación de informes y su periodicidad
d. Seguimiento en la atención de vulnerabilidades señaladas como resultado de la aplicación de pruebas internas y externas del presente informe.

Para acreditar el cumplimiento de esta disposición, deberá remitir a la Contraloría General, a más tardar el 30 de noviembre de 2023, un oficio en el que acredite la elaboración y oficialización de los mecanismos. Asimismo, remitir dos informes sobre el avance en la implementación de los mecanismos, en los cuales conste la atención de las vulnerabilidades señaladas como resultado de la aplicación de pruebas internas y

externas del presente informe; el primero de ellos a más tardar el 29 de marzo de 2024, y el segundo a más tardar el 31 de julio de 2024.

Licda.Vivian Garbanzo Navaro
Gerente de Área
Contraloría General de la República

M.Sc. Yorleny Rojas Ortega
Asistente Técnico
Contraloría General de la República

Lic. Kevin Rodríguez Muñoz
Coordinador
Contraloría General de la República

Lic. Alex Fabián Ramírez Alpízar
Colaborador
Contraloría General de la República

CGR | Firmado digitalmente
Valide las firmas digitales