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

14 de septiembre de 2023

Informe n.° DFOE-LOC-IAD-00020-2023

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 Escazú 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 Escazú 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 sustancialmente en un sistema de información, el cual soporta la planificación, contabilidad, tesorería y proveeduría, así como la ejecución de procesos de negocio asociados con el desarrollo territorial, seguridad ciudadana, bienes inmuebles, cobros, plataforma de servicios y patentes. A través de dicho sistema 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 Escazú 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, ni ha gestionado capacitación en la materia que perfile la especialización de uno o varios funcionarios en temas avanzados y complejos. Ello dificulta el desarrollo de capacidades del personal que asume esas funciones, e incide en la coordinación de las medidas aplicables, para una gestión efectiva de la seguridad de la información.

Adicionalmente, se presentan debilidades en la formación de una conciencia y cultura de seguridad de la información a nivel institucional, debido a la ausencia de capacitación sobre las políticas de seguridad de la información, así como a la falta de suscripción de acuerdos de confidencialidad con el personal, sobre el uso de información y plataformas tecnológicas. Lo cual impide asegurar que el personal conoce y entiende sus responsabilidades en la materia; a su vez, aumenta la exposición a ataques por medio de técnicas como la ingeniería social.

Asimismo, se identificó que la institución no cuenta con instrumentos para planificar la gestión de seguridad de la información; en línea con lo anterior, no se han definido indicadores ni

acciones para mantener la seguridad en un nivel aceptable. Se carece, además, de protocolos o procedimientos 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.

Por otra parte, se determinó que la Municipalidad carece de esfuerzos a nivel institucional en materia de continuidad de negocio, dado que estos han sido liderados por el Sub-proceso de Tecnologías de Información, que cuenta con un plan de continuidad pero actualmente requiere ser revisado y actualizado. En esta misma línea, se identificó que no se efectúan pruebas para corroborar que los respaldos de información permitan recuperar la información. Asimismo, no se han suscrito acuerdos de nivel de servicio con el proveedor del sistema de información que soporta la mayoría de procesos de negocio institucionales.

Al mismo tiempo, la CGR 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 Escazú; evidencia de ello, es que se identificaron 80 (38 críticas, 39 altas y 3 medias) vulnerabilidades en pruebas internas y 8 (1 crítica y 7 medias) vulnerabilidades 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.

Por último, se evidenciaron 8 deficiencias en materia de seguridad física y ambiental del centro de procesamiento de datos principal y el centro alterno, relacionadas con dispositivos ambientales y de protección contra incendios, sistema eléctrico y sistema de vigilancia. Esas deficiencias podrían comprometer la seguridad y el funcionamiento adecuado de las operaciones.

¿QUÉ SIGUE?

Se emiten disposiciones al Alcalde Municipal, al Coordinador del Sub-proceso de Tecnologías de Información y a la Gerente de Recursos Humanos y Materiales, con el propósito de que se implemente un plan para alinear las capacidades del personal que actualmente se encarga de la seguridad de la información, con el perfil que requiere la institución, además, un plan de concientización al personal institucional en materia de seguridad de la información. Asimismo, se dispone la implementación de un plan de seguridad de la información alineado con las políticas institucionales, junto con acciones tendientes a la gestión de la continuidad de negocio institucional; además de la elaboración e implementación de un procedimiento para la gestión de respaldos, así como los acuerdos de nivel de servicio con el proveedor del sistema integrado institucional. Finalmente, se emiten disposiciones orientadas a la implementación de mecanismos de monitoreo, identificación y atención de riesgos y vulnerabilidades, así como la ejecución de un análisis de riesgos a los que están expuestos el centro de procesamiento de datos principal y el centro alterno.

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La Municipalidad de Escazú ha digitalizado una serie de procesos y servicios institucionales. Como parte de dicho proceso, ha puesto a disposición del público trámites en línea relacionados con el pago de tributos, la gestión de patentes y la gestión urbana. 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 Escazú 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 Escazú, 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.° 5522 (DFOE-LOC-0883) del 28 de abril de 2023. En esa misma fecha, fueron presentados a los funcionarios de la Municipalidad de Escazú Alberto Arias Víquez, Coordinador del Sub-proceso de Tecnologías de Información; y Nadia Valverde Arias, Jefa de la Alcaldía.

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 Escazú, 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 Coordinador del Sub-proceso de Tecnologías de Información, con el fin de indagar sobre aspectos vinculados con la gestión de personas, administración de procesos y uso de la tecnología, 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 Coordinador y un Técnico en Informática del Sub-proceso 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 del informe.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.11. Según datos del Sistema de Información sobre Planes y Presupuestos (SIPP) de la CGR, la Municipalidad de Escazú reporta para el periodo 2022 una ejecución presupuestaria por montos de ₡750,4 millones en partidas asociadas en tecnologías de información, entre las que destacan partidas tales como: servicios de tecnologías de información, mantenimiento y reparación de equipo de cómputo y sistemas de información, equipo de comunicación y equipo y programas de cómputo.

1.12. Para la ejecución de los procesos sustantivos y cumplir sus objetivos institucionales, la Municipalidad de Escazú se apoya sustancialmente en un sistema integrado de información, desarrollado por un tercero y con una antigüedad de más de 30 años. A nivel

de lenguaje de programación está orientado a objetos y presenta una base de datos relacional.

1.13. Este cuenta con un total de 17 módulos que soportan los procesos de planificación, contabilidad, tesorería y proveeduría, así como la ejecución de procesos de negocio asociados con el desarrollo territorial, seguridad ciudadana, bienes inmuebles, cobros, plataforma de servicios y patentes, tal como se muestra en la imagen n.° 1.

Imagen n.° 1. Procesos soportados por el sistema integrado institucional

Fuente: Elaboración CGR, con base en información suministrada por la Municipalidad de Escazú.

1.14. A través de dicho sistema se recopila, procesa y almacena información crítica para el cumplimiento de las funciones y objetivos institucionales, incluyendo datos sobre los contribuyentes.

1.15. 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 los pagos en línea, licencias y patentes municipales, permisos, certificados de uso de suelo, inscripciones y traspasos, entre otros. Ello se ilustra en la imagen n.° 2.

Imagen n.° 2. Trámites en línea ofrecidos por la Municipalidad de Escazú

Fuente: Elaboración CGR, con base en información disponible en el sitio web de la Municipalidad de Escazú.

1.16. Ello implica el despliegue de medidas y controles para 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.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.1. El borrador del presente informe fue remitido a la Municipalidad de Escazú mediante el oficio n.° DFOE-LOC-1479(11582) de fecha 29 de agosto de 2023, dirigido a la Licenciada Karol Tatiana Matamoros Corrales, Vicealcaldesa 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.

1.2. Asimismo, el 30 de agosto 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 Escazú: Karol Tatiana Matamoros Corrales, Vicealcaldesa Municipal; Mario Alberto Arias Víquez, Coordinador del Sub-proceso de Tecnologías de Información; Alma Luz Solano Ramirez, Gerente de Recursos Humanos, y Erick Calderón Carvajal, Auditor Interno.

1.3. En atención a lo solicitado por el Órgano Contralor, se recibió el oficio n.° COR-DA-552-2023 del 6 de septiembre de 2023, suscrito por la Licenciada Karol Tatiana Matamoros Corrales, Vicealcaldesa de la Municipalidad de Escazú, mediante el cual

remitió las observaciones al borrador del informe; mismas que una vez valoradas, fueron atendidas por medio del oficio n.° DFOE-LOC-1649(12494) de fecha 14 de septiembre de 2023.

SIGLAS

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

Siglas	Significado
BIA	Análisis de Impacto al Negocio
BCP	Plan de Continuidad del Negocio
CGR	Contraloría General de la República
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
ISO	Organización Internacional para la Estandarización
RPO	Punto Objetivo de Recuperación
RTO	Tiempo Objetivo de Recuperación

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 Escazú.

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 Escazú 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 Sub-proceso 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. De acuerdo con información suministrada por la Municipalidad, el personal del Sub-proceso de Tecnologías de Información ha recibido capacitación introductoria sobre seguridad de la información y continuidad del negocio; 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. En línea con ello, 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.

2.6. 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.

2.7. 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.

Debilidades en la formación de una conciencia y cultura de seguridad de la información a nivel institucional

2.8. Se determinó que la Municipalidad de Escazú no ha realizado acciones tendientes a la sensibilización o concientización de los funcionarios sobre sus responsabilidades en materia de seguridad de la información. Al respecto, si bien regularmente se remiten correos electrónicos sobre advertencias de estafas y recomendaciones de seguridad, no se ha implementado un proceso de capacitación sobre las políticas de seguridad establecidas por la institución, tanto para el personal actual como para el de nuevo ingreso. Tampoco se han suscrito acuerdos de confidencialidad con el personal, sobre el uso de información y plataformas tecnológicas.

2.9. La norma 1.5 *Responsabilidad de los funcionarios sobre el Sistema de Control Interno* 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, establece que los funcionarios deben realizar las acciones pertinentes y atender los requerimientos de conformidad con las responsabilidades que competen a cada puesto de trabajo, de manera oportuna, efectiva y con observancia a las regulaciones aplicables; mientras que la norma 2.1 *Ambiente de control* establece que se debe fortalecer la ética institucional para propiciar una gestión institucional apegada a altos estándares de conducta en el desarrollo de las actividades, así como mantener el personal comprometido y con competencia profesional para el desarrollo de las actividades.

2.10. Por su parte, la Política de Seguridad de la Información de la Municipalidad de Escazú, versión 2.1, vigente desde el 24 de abril de 2023, en el apartado 4.1 *Entrenamiento de seguridad de la información*, establece que el Proceso de Recursos Humanos, en coordinación con el Sub-proceso de Tecnologías de Información, debe impartir entrenamiento sobre seguridad de la información a todos los empleados, a través de un proceso de inducción, para que comprendan sus responsabilidades. Asimismo, señala que todos sus funcionarios deben aceptar por escrito que conocen y entienden las políticas de seguridad.

2.11. Adicionalmente, el apartado 4.3 de la citada Política establece que la Municipalidad de Escazú, por medio del Proceso de Recursos Humanos, debe gestionar los acuerdos de confidencialidad, que deberá firmar todo el personal que utiliza los activos de información y/o plataformas tecnológicas de la institución.

2.12. Lo anterior se debe a la ausencia de un plan formal de capacitación y sensibilización a los funcionarios municipales sobre las regulaciones en materia de seguridad de la información que ha definido la institución, y los deberes y compromisos que dichas regulaciones les establecen.

2.13. La ausencia de dicho plan, genera falta de aseguramiento sobre el conocimiento del personal y la comprensión que puedan tener de sus responsabilidades en materia de seguridad de la información; con ello aumenta el riesgo de pérdida de la confidencialidad de los datos, así como la facilitación de ciberataques, por ejemplo, utilizando técnicas de ingeniería social.

ADMINISTRACIÓN DE PROCESOS

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

2.14. La Municipalidad de Escazú 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.

2.15. Al respecto, se determinó que, de acuerdo con los informes de labores mensuales, el Sub-proceso de Tecnologías de Información da seguimiento a alertas del software para protección de correos, control antimalware, software de respaldos, el sistema de gestión de actualizaciones, firewall y lleva estadísticas de incidentes reportados y su respectivo estado de atención; sin embargo, no se han formulado indicadores a partir de dichos datos, ni se han definido las acciones para mantener la seguridad en un nivel aceptable y evitar niveles que impliquen una posición de riesgo para los servicios basados en tecnología.

2.16. En línea con lo anterior, 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 y se generan reportes periódicos, 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; no obstante, en caso de ocurrir, podrían tener un impacto directo en la confidencialidad, integridad y disponibilidad de la información institucional.

2.17. Sobre lo anterior, las Políticas de Seguridad de la Información de la Municipalidad de Escazú en el apartado 6 *Seguridad en las operaciones y comunicaciones*, establecen que la organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y de las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

2.18. La Norma ISO 27001 en su apartado 6.1.3 *Tratamiento de riesgo de seguridad de la información*, establece que la organización debe definir y aplicar un proceso de tratamiento

del riesgo de seguridad de la información, entre otros asuntos para formular un plan de tratamiento del riesgo de seguridad de la información.

2.19. Por su parte, las cláusulas A.16.1.1 y A.16.1.5 de la citada Norma referentes a responsabilidades y procedimientos de respuesta a incidentes de seguridad, definen que se deben establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información y esa respuesta a incidentes debe ser de acuerdo con procedimientos documentados.

2.20. 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.

2.21. Las situaciones identificadas se deben a que la Municipalidad de Escazú 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.

2.22. 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.

Debilidades relacionadas con la continuidad del negocio y la disponibilidad de los procesos, los sistemas y la información críticos de la Municipalidad

2.23. La Municipalidad de Escazú cuenta con un plan de continuidad de tecnologías de información versión 0.1, basado en un análisis de impacto tecnológico versión 1.0, ambos elaborados por un tercero en el año 2017. De la revisión de estos documentos se desprende que la institución cuenta con una identificación y clasificación de criticidad de los procesos y actividades de negocio, la infraestructura tecnológica (sistemas, hardware, telecomunicaciones) en los cuales se soportan los procesos críticos. Asimismo, se definen indicadores clave como el tiempo objetivo de recuperación (RTO) y punto objetivo de recuperación (RPO), y se identifica el personal institucional y proveedores críticos.

2.24. No obstante, esta auditoría permitió corroborar que estos esfuerzos de continuidad han sido liderados desde la perspectiva del Sub-proceso de Tecnologías de Información, por lo que no ha tenido un impacto a nivel institucional, al carecer de un documento que evidencie los procedimientos que el negocio debería ejecutar en caso de un evento disruptivo que limite la capacidad de utilizar los sistemas informáticos. Asimismo, el plan de

continuidad de tecnologías de información no ha tenido modificaciones desde que se elaboró en 2017, por lo que actualmente requiere una revisión y actualización.

2.25. Adicionalmente, se identificó que la Municipalidad realiza respaldos diarios de la información a través de una herramienta automatizada y los mismos son trasladados al sitio alterno ubicado en el edificio de la Policía Municipal. Sin embargo, no se realizan pruebas periódicas para determinar si los respaldos se pueden recuperar de forma efectiva en el sitio alterno, por lo que si bien a la fecha no ha sucedido ningún evento adverso que requiera la restauración de información, en caso de presentarse algún evento, existe el riesgo de pérdida o corrupción de datos, o bien incrementos en los tiempos y costos de recuperación.

2.26. A lo dicho se debe sumar el hecho de que la institución carece de acuerdos de niveles de servicio (SLA)[1] con el proveedor del sistema que sirve de soporte para la mayoría de procesos de negocio institucionales y constituye el sistema de mayor criticidad institucional. A la fecha de cierre del presente estudio, únicamente se ha suscrito el acuerdo de confidencialidad, pero no se cuenta con acuerdos que establezcan, por ejemplo, la garantía de disponibilidad del sistema, el tiempo de atención por parte del proveedor en caso de fallos, incidentes o requerimientos, métricas para evaluar el cumplimiento del servicio, entre otros aspectos.

2.27. Al respecto, las Normas de Control Interno para el Sector Público, en la norma 4.4.1. *Documentación y registro de la gestión institucional*, señalan el deber de establecer medidas para garantizar razonablemente la confidencialidad y el acceso a la información pública, según corresponda. Por su parte, la norma 5.4. *Gestión documental* indica el deber de asegurar razonablemente que los sistemas de información propicien el almacenamiento y la recuperación de la información de manera oportuna y eficiente, y de conformidad con las necesidades institucionales.

2.28. Adicionalmente, el objetivo de gestión DSS04 *Gestionar la Continuidad*, de Cobit 2019 de ISACA, indica que las instituciones o empresas tienen la necesidad de establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

2.29. En complemento, la práctica de gestión DSS04.07 *Administrar los acuerdos de respaldo* establece que, como parte de las actividades para mantener la disponibilidad de la información crítica, se debe hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido; definir requisitos para el

[1] De acuerdo con la ISO 20000 y Cobit 2019, un SLA es un acuerdo entre el proveedor del servicio y el cliente, que identifica los servicios y sus objetivos. Describe los servicios que el cliente recibirá, sus requisitos y los plazos de entrega, de manera específica, medible, alcanzable, realista y acotada en el tiempo. Puede ser incluido en un contrato u otro tipo de acuerdo documentado.

almacenamiento de las copias de seguridad en las instalaciones y fuera de ellas, conforme a los requisitos de negocio; así como probar de forma periódica las copias de seguridad.

2.30. Por su parte, la práctica de gestión APO10.03 *Gestionar los contratos y las relaciones con los proveedores*, establece la necesidad de gestionar, mantener y monitorear los contratos y la prestación de servicios y asegurar que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requisitos legales y regulatorios.

2.31. Por último, la Política de Seguridad de la Información de Escazú versión 2.1, en su apartado 6.2 *Protección de información* almacenada en medios, indica que la institución debe identificar la información que debe ser resguardada para mantener la disponibilidad de sus servicios, en cumplimiento de normas legales, de la tabla de conservación, y de acuerdo con la Política de Gestión de Respaldos.

2.32. Las situaciones anteriores se deben a la ausencia de un compromiso a nivel institucional con la continuidad de negocio, en el cual la alta gerencia, en coordinación con el Sub-proceso de Tecnologías de Información y demás procesos municipales, determinen las expectativas, la magnitud y el alcance del esfuerzo de continuidad del negocio que cubra a toda la entidad.

2.33. Ello dificulta la priorización de los recursos y las medidas de protección necesarias para garantizar la continuidad del negocio en caso de interrupciones o incidentes, así como el establecimiento y monitoreo de controles para la protección de la información, de acuerdo con su nivel de sensibilidad o criticidad.

2.34. Por su parte la ausencia de niveles de servicio acordados impacta en la calidad y la eficacia del servicio y dificulta el establecimiento de responsabilidades y prioridades en la atención de posibles eventos que puedan afectar la disponibilidad del sistema, lo cual eventualmente impactaría a su vez en la continuidad de los servicios que brinda la Municipalidad.

USO DE TECNOLOGÍA

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

2.35. Se determinó que la Municipalidad de Escazú no efectúa análisis periódicos de vulnerabilidades internas y externas que permitan una detección temprana y atención oportuna de amenazas de seguridad. 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.

2.36. Asimismo, se carece de un diseño completo de red donde se diagramen los principales elementos de la plataforma tecnológica, que permita identificar las características de dicho

diseño, como los segmentos, zonas de seguridad y los controles de seguridad de red entre los segmentos o zonas. Ello dificulta la identificación de posibles fallos de seguridad en ese diseño, la previsión de eventuales debilidades o fallos al implementar cambios, así como la determinación de dispositivos susceptibles de actualizaciones, mejoras o reemplazos.

2.37. Por otra parte, se encontró que la Municipalidad, por medio del Sub-proceso de Servicios Institucionales, entrega teléfonos celulares a un grupo de funcionarios, para labores municipales. Sin embargo, la seguridad de estos dispositivos no es gestionada por el Sub-proceso de Tecnologías de Información, lo cual impide asegurar que cumplan con las políticas de seguridad institucionales y los controles para garantizar razonablemente los niveles de seguridad establecidos.

2.38. Sobre el particular, 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.

2.39. 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.

2.40. 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.

2.41. 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, que incluya, entre otros aspectos, estrategias de actualización, riesgo, privacidad, análisis de vulnerabilidades y requisitos de seguridad.

2.42. Además la Norma ISO 27002-2013, apartado 13.1.1 indica que se deben gestionar y controlar las redes para proteger la información en los sistemas y aplicaciones, lo cual implica establecer controles especiales para salvaguardar la confidencialidad e integridad de datos que pasan por redes públicas o inalámbricas, aplicar un registro y monitoreo para la detección de acciones que puedan afectar o sean relevantes para la seguridad de la información, así como garantizar que los controles se apliquen de forma coherente en toda la infraestructura de procesamiento de la información.

2.43. Por último, la Política de Seguridad de la Información de la Municipalidad de Escazú, del 18 de abril de 2023, en su apartado 7.11 *Uso de dispositivos móviles* establece que todo funcionario se compromete a hacer uso adecuado de los dispositivos móviles para acceder la infraestructura de red organizacional y los servicios disponibles. El dispositivo deberá

tener el software de antivirus habilitado, y uso de canales seguros para conectarse a la red, en los cuales se autentique como un usuario válido.

2.44. 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 2023-2026 se estableció la “evaluación y monitoreo periódico de protección de tecnología y análisis de vulnerabilidades” como una de las estrategias para atender las amenazas de obsolescencia tecnológica y el incremento de ciberataques.

2.45. 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. Evidencia de ello es que, producto de las pruebas efectuadas por la CGR, se identificaron 80 vulnerabilidades en **pruebas internas**, de las cuales 38 son críticas[2] y se relacionan con obsolescencia de software, actualizaciones de seguridad, algoritmos de cifrado y autenticación de servicios; 39 altas[3] vinculadas con certificados, algoritmos de cifrado, actualizaciones de seguridad y configuración de servidores web y sistemas operativos; así como 3 medias[4] asociadas a autenticación de servicios y algoritmos de cifrado. Lo anterior se muestra en la imagen n.° 3.

2.46. Asimismo, se identificaron 8 vulnerabilidades en **pruebas externas**, de las cuales 1 es crítica y se relaciona con obsolescencia de software; 7 son medias y corresponden a configuraciones de servidores web y sistemas operativos, así como seguridad del sistema de nombres de dominio, y configuraciones por defecto. Ello se muestra en la imagen n.° 4.

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

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

[4] 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.

Imagen n.° 3. Resultados de las pruebas internas

Fuente: Elaboración CGR.

Imagen n.° 4. Resultados de las pruebas externas

Fuente: Elaboración CGR.

Debilidades relacionadas con la seguridad física y ambiental

2.47. Como parte de la auditoría se realizaron inspecciones físicas a las instalaciones de procesamiento de datos principal ubicadas en el Palacio Municipal y al sitio de procesamiento alterno ubicado en el edificio de Policía Municipal. De dichas inspecciones se identificó una serie deficiencias que podrían comprometer la seguridad y el funcionamiento adecuado de las operaciones de esos centros de procesamiento, mismas que se detallan a continuación:

a) Protección contra incendios: Se cuenta con detectores de temperatura y humedad, pero no se cuenta con detectores de humo. Se dispone de un extintor manual tipo ABC, fuera del centro de procesamiento de datos.

b) Aire acondicionado: El aire acondicionado del centro de procesamiento de datos no cuenta con un proceso de revisión y mantenimiento periódico. Asimismo, se carece de un respaldo (duplicado) en caso de falla.

c) Sistema eléctrico: Se carece de una red eléctrica específica para el centro de procesamiento de datos. El sistema de alimentación ininterrumpida (UPS) cuenta con módulos de redundancia y cambio de baterías cada cinco años, pero no con un proceso de revisión y mantenimiento periódico.

d) Controles generales: Existe una cámara de video vigilancia ubicada en el pasillo que da acceso al centro de procesamiento de datos, sin embargo no se cuenta con una vista al interior de manera que se pueda monitorear de forma efectiva lo que sucede al interior.

e) Sitio alterno: La Municipalidad de Escazú cuenta con un sitio alterno ubicado a 2.2 km del centro de procesamiento de datos primario. El ingreso al sitio se encuentra vigilado en el exterior por cámaras de seguridad; sin embargo para el acceso al edificio solo se cuenta con una puerta corrediza de vidrio con un letrero de advertencia de ingreso a particulares. En el interior cuenta con aire acondicionado, fuentes UPS de menor tamaño, canaletas de cableado estructurado, prevista de electricidad. No se ubicó cerca del sitio alterno algún extintor, detectores de humedad o temperatura ni otro tipo de controles ambientales.

2.48. Al respecto, las Normas de Control Interno para el Sector Público, en la norma 4.3 *Protección y conservación del patrimonio*, establece que se debe asegurar razonablemente la protección, custodia, correcto uso y control de los activos pertenecientes a la institución; tomando en cuenta, el bloque de legalidad, la naturaleza de tales activos y los riesgos a los cuales puedan verse expuestos.

2.49. En línea con ello, la práctica de gestión DSS01.04 de Cobit 2019 de ISACA asociada a gestionar el medioambiente, manifiesta la importancia de mantener medidas de protección contra los factores medioambientales, así como instalar equipos y dispositivos especializados para monitorear y controlar el ambiente.

2.50. Por su parte la práctica de gestión DSS05.05 establece la importancia de definir e implantar procedimientos (incluyendo procedimientos de emergencia) para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas, de acuerdo con las necesidades del negocio. El acceso a las instalaciones, edificios y áreas debe estar justificado, autorizado, registrado y supervisado.

2.51. Asimismo, la ISO 27001-2014, en cláusula A.11.1.2, establece que las áreas seguras deben ser protegidas por medio de controles de entrada apropiados para asegurarse de que el acceso sea permitido solamente a personal autorizado; mientras que la cláusula A.11.2.4 define como control para el mantenimiento de equipos, que se debe tener un mantenimiento correcto para asegurarse de su continua disponibilidad e integridad.

2.52. Por otro lado el apartado 5. *Seguridad física y ambiental* señala que la organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, considerando que las oficinas catalogadas como áreas sensibles deben implementar los mecanismos requeridos para que sólo los funcionarios, pasantes o subcontratados autorizados, tengan acceso a las mismas. Además, los activos (de información, físicos y de software) deben ser protegidos de situaciones del entorno que puedan dañarlos, tales como: exposición al polvo, accidentes o amenazas ambientales como descargas eléctricas, inundaciones, etc.

2.53. Las debilidades identificadas obedecen a la ausencia de un análisis de riesgos que contemple la determinación de la probabilidad e impacto de las amenazas a las que están expuestos el centro de procesamiento de datos principal y el centro de procesamiento de datos alterno, así como los controles implementados por la administración para gestionar dichos riesgos y los necesarios lograr un nivel de riesgo aceptable.

2.54. Las situaciones comentadas exponen a la Municipalidad de Escazú a riesgos de seguridad, confiabilidad y disponibilidad de los recursos críticos que se administran en los centros de procesamiento de datos, lo que aumenta la posibilidad de interrupciones de los servicios, pérdida de información, daños de los equipos y posibles accesos no autorizados a la información.

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 Escazú 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, el perfil del personal encargado de gestionarla, así como la capacitación y concientización a nivel institucional sobre la importancia y responsabilidad sobre la seguridad de la información.

3.3. Asimismo, en materia de administración de procesos, se evidenció la necesidad de contar con un marco de seguridad de la información, y el monitoreo de indicadores para mantener la seguridad en niveles aceptables.

3.4. 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. Además, referente a la seguridad física y ambiental de los centros que procesan la información institucional, se requiere de una valoración oportuna de los riesgos identificados, así como las posibles medidas para su tratamiento, dentro de un análisis de costo-beneficio.

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 ARNOLDO BARAHONA CORTÉS EN SU CALIDAD DE ALCALDE DE LA MUNICIPALIDAD DE ESCAZÚ, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. En coordinación con el Sub-proceso de Tecnologías de Información y el Proceso de Gestión de Recursos Humanos y Materiales, 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 2.7):

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 25 de marzo de 2024, 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 21 de junio 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 Escazú que incluya, al menos (ver párrafos del 2.14 al 2.22):

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 12 de febrero 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.

4.6. En coordinación con el Comité de Seguridad de la Información, elaborar, aprobar, comunicar e implementar (ver párrafos del 2.23 al 2.34):

a. La política de continuidad de negocio en la cual se defina el alcance del esfuerzo de continuidad del negocio en la Municipalidad.
b. El análisis de impacto de negocio (BIA).
c. El plan de continuidad de negocio (BCP).

Para el cumplimiento de esta disposición deberá remitir a la Contraloría General de la República, lo siguiente: a) Un oficio a más tardar el 30 de enero de 2024, en el que conste que se elaboró, aprobó y comunicó la política de continuidad del negocio, b) Un oficio a más tardar el 05 de julio de 2024, en el que conste que se elaboró, aprobó y comunicó el análisis de impacto de negocio, c) Un oficio a más tardar el 13 de diciembre de 2024, en el que conste que se elaboró, aprobó y comunicó plan de continuidad de negocio (BCP) y d) Un informe de avance sobre la implementación del plan de continuidad de negocio a más tardar el 14 de febrero de 2025.

4.7. En coordinación con el Sub-proceso de Tecnologías de Información, elaborar, aprobar e implementar los acuerdos de nivel de servicio con el proveedor del sistema integrado institucional (ver párrafos del 2.23 al 2.34).

Para acreditar el cumplimiento de esta disposición deberá remitir a la Contraloría General de la República un oficio a más tardar el 27 de octubre de 2023, en el que conste que se elaboró, aprobó e implementó los acuerdos de nivel de servicio con el proveedor del sistema integrado institucional.

4.8. En coordinación el Sub-proceso de Tecnologías de Información y el Sub-proceso de Servicios Institucionales, elaborar un análisis de riesgos a los que están expuestos el centro de procesamiento de datos principal y el centro de procesamiento de datos alterno, que contemple, al menos (ver párrafos del 2.48 al 2.55):

a. Un diagnóstico de las medidas necesarias para solventar los riesgos identificados.
b. Un cronograma en el que se establezca su prioridad de atención, según el nivel de riesgo y las capacidades institucionales.

Para acreditar el cumplimiento de esta disposición, deberá remitir a la Contraloría General, a más tardar el 24 de noviembre de 2023, un oficio en el que acredite la

elaboración del análisis de riesgos. Asimismo, remitir un informe sobre el avance en la implementación del cronograma de atención, a más tardar el 30 de agosto de 2024.

A LA SEÑORA ALMA LUZ SOLANO RAMÍREZ EN SU CALIDAD DE GERENTE DE RECURSOS HUMANOS DE LA MUNICIPALIDAD DE ESCAZÚ, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.9. En coordinación con el Sub-proceso de Tecnologías de Información, elaborar, oficializar e implementar un plan de concientización al personal institucional en materia de seguridad de la información que contemple tanto a funcionarios actuales como de nuevo ingreso. Este plan debe incluir al menos (ver párrafos del 2.8 al 2.13):

a. Objetivos.
b. Cronograma.
c. Responsables.
d. Participantes del ciclo de formación.
e. Suscripción de acuerdos de confidencialidad para aquellos funcionarios que utilizan los activos de información y/o plataformas tecnológicas de la institución como parte de sus funciones.
f. Definición de indicadores para medir el avance y la cobertura del plan.

Para acreditar el cumplimiento de esta disposición, deberá remitir a la Contraloría General, a más tardar el 24 de enero de 2024, un oficio en el que acredite la elaboración y oficialización del plan de concientización. Con respecto a la implementación, remitir dos informes sobre el avance y la cobertura del plan de concientización; el primero de ellos a más tardar el 31 de julio de 2024, y el segundo a más tardar el 20 de diciembre de 2024.

AL SEÑOR MARIO ALBERTO ARIAS VÍQUEZ EN SU CALIDAD DE COORDINADOR DEL SUB-PROCESO DE TECNOLOGÍAS DE INFORMACIÓN, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.10. Elaborar, oficializar e implementar un procedimiento para la gestión de respaldos de los sistemas institucionales que contemple, al menos (ver párrafos del 2.23 al 2.34):

a. La definición de las actividades.
b. Roles y responsables de efectuar los respaldos.
c. Las medidas para su resguardo.
d. La realización de pruebas para verificar su funcionamiento.

Para acreditar el cumplimiento de esta disposición, deberá remitir a la Contraloría General, a más tardar el 23 de octubre de 2023, un oficio en el que acredite la elaboración y oficialización del procedimiento. Con respecto a la implementación, remitir dos informes de avance, el primero de ellos a más tardar el 15 de enero de 2024, y el segundo a más tardar el 14 de junio de 2024.

4.11. Elaborar, oficializar e implementar mecanismos para monitorear, identificar y atender posibles riesgos y vulnerabilidades relacionados con la seguridad de la información en la infraestructura tecnológica institucional, incluyendo las redes, equipos de cómputo y

dispositivos móviles, 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 2.35 al 2.46):

a. Las acciones.
b. Los responsables.
c. La generación de informes y su periodicidad
d. El seguimiento en la atención de 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 05 de febrero 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 31 de mayo de 2024, y el segundo a más tardar el 15 de octubre 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