INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SISTEMAS CRÍTICOS DE LA MUNICIPALIDAD DE SAN JOSÉ

23 de febrero de 2023

Informe n°. DFOE-LOC-IAD-00001-2023

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

IMÁGENES

TABLAS

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos de la Municipalidad de San José responde al marco regulatorio y buenas prácticas aplicables de manera que se promueva el logro de sus objetivos. El periodo evaluado comprende desde 01 de enero de 2021 al 31 de julio de 2022, y se extendió cuando se consideró pertinente.

¿POR QUÉ ES IMPORTANTE?

La municipalidad de San José cumple un papel relevante en la gestión y administración de los intereses y servicios públicos locales y es la encargada de promover el desarrollo local del cantón mediante la recaudación de ingresos y ejecución de inversiones. El soporte de esos procesos sustantivos y el cumplimiento de sus objetivos institucionales, conlleva el uso de varios sistemas de información, siendo uno de los más importantes el sistema que soporta los procesos de servicios urbanos, bienes inmuebles, patentes, recaudación, cobro y plataforma de servicios, así como el Sistema Integrado Autorización Patentes (SIAP), encargado de registrar y dar seguimiento a trámites varios de patentes y órdenes de trabajo de inspección.

La utilización de sistemas con datos de los contribuyentes, plantea la necesidad de garantizar de forma razonable la seguridad de la información de los sistemas sustantivos, pues contienen información de carácter crítico para la prestación de los servicios y cumplimiento de las competencias municipales, así como datos de los contribuyentes, y por lo tanto, requieren ser protegidos ante cualquier uso fraudulento, accesos no autorizados, pérdida, alteración o difusión.

¿QUÉ ENCONTRAMOS?

Se determinó que la gestión de la continuidad de negocio carece de la documentación que respalde la planificación, implementación, seguimiento y mejora de la continuidad de negocio municipal, debido a que no se ha implementado un Sistema de Gestión de la Continuidad del Negocio a nivel institucional, para dar respuesta a incidentes, por lo tanto no es posible alinear los esfuerzos de la Dirección de Tecnologías de Información y demás direcciones municipales en esa misma materia.

Además, para el plan de recuperación ante desastres de la Dirección de Tecnología de la municipalidad, no se cumplen la totalidad de las premisas establecidas necesarias para la recuperación correspondiente, también carece de los procedimientos necesarios para establecer la declaración de un desastre, así como de los criterios de activación del plan. Adicionalmente, no se han realizado simulacros o pruebas de manejo de incidentes ni se ha actualizado la definición de los tiempos de recuperación (RTO y RPO).

Por su parte, la matriz de riesgos no contempla de forma integral una evaluación de la seguridad de la información en aspectos asociados a integridad y confidencialidad de la información y no se establecen controles asociados a la ciberseguridad.

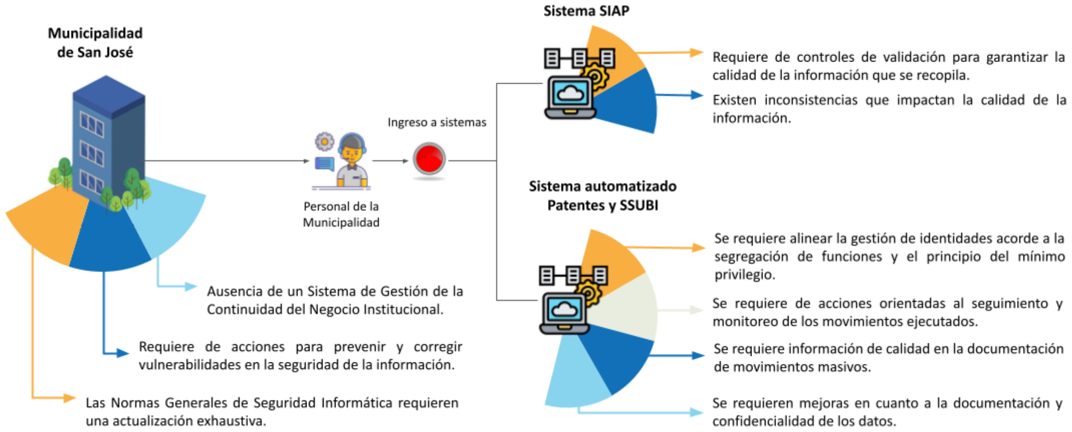
Asimismo, se evidenció que el sistema automatizado donde se tramitan los procesos de patentes y servicios urbanos y bienes inmuebles no cumple con varios aspectos necesarios para garantizar de forma razonable la disponibilidad, integridad y confidencialidad, tales como: la carencia de documentación de sistemas, la ausencia de gestión de identidades basada en el principio del mínimo privilegio y segregación de funciones, el mantenimiento de usuarios conforme al tipo de permisos asignados para las funciones migradas, así como aspectos que afectan la razonabilidad de la confidencialidad de los datos.

En el ámbito operativo, se determinó que las unidades de negocio no ejecutan procesos de monitoreo sobre las funciones a su cargo, debido a que no cuentan con acceso a visualizar las bitácoras en el sistema; además, se logró evidenciar que se asignan permisos que incumplen el principio del mínimo privilegio en funcionalidades de riesgo alto dentro del proceso de bienes inmuebles como lo es el control de aprobación de propiedades.

Asimismo, se identificó que el 53% de los funcionarios con permisos en el módulo de patentes y el 22% de los funcionarios con permisos en la Sección servicios urbanos y bienes inmuebles ya no deberían contar con dicho acceso, por cuanto no laboran para la Municipalidad y que en el caso de un 5% funcionarios, la Municipalidad no logró establecer su vinculación o desvinculación laboral.

Adicionalmente, la Municipalidad no ha uniformado para las diferentes unidades de negocio, los controles que permiten salvaguardar la integridad de los datos de las propiedades de los contribuyentes y sus tributos, siendo que se identificó que existe personal en diferentes unidades que no se adhiere ni cumplen con las mismas directrices y controles establecidos para salvaguardar la integridad y veracidad de esta información.

Imagen n°. 1 Resumen de Resultados



Fuente: Elaboración CGR.

Finalmente, la Contraloría General determinó vulnerabilidades en la red interna que pueden comprometer la integridad, disponibilidad y confidencialidad de la información de la Municipalidad de San José, por lo tanto, remitió el oficio n°. DFOE-LOC-OI-00001-2023 (DFOE-LOC-268) del 01 de febrero de 2023, con el propósito de que esa información sea valorada por la Municipalidad en la toma de decisiones relacionados con la identificación, protección, detección, respuesta y recuperación sobre las situaciones comunicadas.

¿QUÉ SIGUE?

Se emiten disposiciones al Alcalde Municipal, al Director de Tecnologías de Información y Comunicación y al Jefe de la Sección de Patentes, con el propósito de que se implemente el Sistema de Gestión de la Continuidad del Negocio a nivel institucional, que se actualicen las Normas Generales de Seguridad Informática y se implementen controles para salvaguardar la integridad de los datos de las propiedades de los contribuyentes y sus tributos, así como medidas específicas para alinear la gestión de identidades acorde a la segregación de funciones y el principio del mínimo privilegio. Asimismo, que se implemente un plan de remediación de las vulnerabilidades sobre seguridad de la información que permita subsanar las situaciones identificadas y un programa de sensibilización en esta materia.

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN PARA EL DESARROLLO LOCAL

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD LA INFORMACIÓN DE LOS SISTEMAS CRÍTICOS DE LA MUNICIPALIDAD DE SAN JOSÉ

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. 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°. 7 428.

OBJETIVO

1.2. El propósito de la auditoría fue determinar si la seguridad de la información de los sistemas críticos de la Municipalidad de San José responden al marco regulatorio y buenas prácticas aplicables de manera que se promueva el logro de sus objetivos.

ALCANCE

1.3. La auditoría comprenderá el análisis de la gestión de las tecnologías de información, en relación con la preparación y controles de la Municipalidad de San José para el resguardo de la información de los sistemas críticos que apoyan la gestión municipal. El período de análisis comprendió del 1 de enero de 2021 al 31 de julio de 2022.

CRITERIOS DE AUDITORÍA

1.4. El 7 de octubre de 2022, se presentaron los criterios de auditoría a los funcionarios de la Municipalidad de San José: señor Johnny Araya Monge, Alcalde Municipal; señora Paula Vargas Ramírez, Vicealcaldesa Municipal; señor Rodney Zúñiga Guzmán, Jefe Despacho Alcaldía; señor Edgar Sandoval Montero, Gerente Administrativo Financiero y DTIC; señor Carlos Garita Cabezas, Director DTIC y señor Erick Gutierrez Desanti, Subauditor interno. Además, dichos criterios fueron comunicados mediante oficio n°. DFOE-LOC-1940 (16 301) del 10 de octubre de 2022.

METODOLOGÍA APLICADA

1.5. 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 Contraloría General y el Procedimiento de Auditoría vigente, establecido por la DFOE.

1.6. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas al personal de la Municipalidad de San José, así como las respuestas a las consultas planteadas por escrito ante diferentes instancias de esa municipalidad.

1.7. Asimismo, se realizó una visita a los centros de datos de la Municipalidad de San José para verificar el cumplimiento de mejores prácticas en la seguridad física, se realizaron pruebas de penetración modalidad “caja gris” no intrusivas a dispositivos en distintos segmentos de la red interna, como servidores y estaciones de trabajo a nivel de escaneo de puertos, análisis de vulnerabilidades y explotación de vulnerabilidades, para ello se contó con la colaboración de los funcionarios de la Dirección de Tecnologías de Información y Comunicación (DTIC) para obtener un acceso cableado a la red interna y simular acciones de un atacante que obtenga acceso a la red interna, lo anterior sin generar afectación en los servicios brindados por la institución.

1.8. Se utilizaron los datos del personal municipal con corte al 11 de enero de 2023, el detalle de personas pensionadas del Sistema Centralizado de Recaudación (SICERE) al mes de julio de 2022 y el detalle de las personas fallecidas del Registro Civil del Tribunal Supremo de Elecciones (TSE) con corte al mes de febrero de 2022. Se realizó un análisis, en el cual se relacionó la información del personal de la Municipalidad con los usuarios registrados en el servicio de directorio (Active Directory).

1.9. La auditoría abarcó el análisis de la información contenida en las tablas de los sistemas que albergan los datos de los procesos de patentes, servicios urbanos y bienes inmuebles, así como el detalle del personal de la Gerencia Gestión Municipal y Desarrollo Urbano y la Gerencia Administrativa Financiera y T.I.C, al 24 de agosto de 2022, para lo cual se utilizó un software de extracción y análisis de datos, así como el estudio de las acciones llevadas a cabo por la administración en lo que respecta a la funcionalidad de los módulos de patentes y servicios urbanos y bienes inmuebles.

1.10. Finalmente, se realizaron talleres con personal de la DTIC y la Gerencia de la Dirección Administrativa y Financiera y DTIC, para identificar las causas y soluciones de las situaciones que se comunican en este informe, lo que contribuyó a lograr una visión integral de las causas, los desafíos, retos y oportunidades de mejora.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.11. La Sección de bienes inmuebles y servicios urbanos tiene entre sus funciones el mantenimiento de los datos de las propiedades de los contribuyentes, con el propósito de mantener actualizada su información para el cálculo y cobro de los diferentes impuestos y servicios, para ello se cuenta con el control denominado “Movimiento Estadístico Censal (MEC)”, mediante el cual los funcionarios deben incluir las observaciones sobre el trámite ejecutado; además se implementó, en febrero 2021, una notificación a la jefatura o personas autorizadas para que apruebe de forma automatizada la modificación de la propiedad o sus condiciones.

1.12. Con respecto, al análisis de la red externa los resultados revelan que no existen hallazgos o vulnerabilidades, por lo tanto, las aplicaciones web se encuentran en un estado razonablemente seguro y protegido contra posibles ataques o intrusiones. Sin embargo, es importante seguir monitoreando y revisando regularmente la seguridad para asegurarse de que no haya cambios o nuevos riesgos que puedan afectar la seguridad en el futuro.

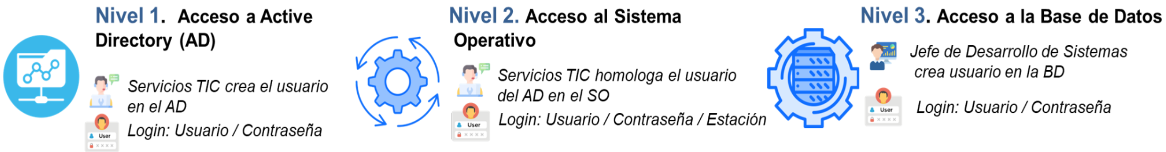
1.13. Adicionalmente, se han realizado acciones para fortalecer la infraestructura considerando mejoras en el centro de cómputo y en los dispositivos de seguridad de red que detectan y bloquean amenazas, filtrado web, políticas de bloqueo, entre otras.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.14. El proceso de cobro del impuesto sobre bienes Inmuebles está normado mediante la Ley n°. 7509, en la cual se establece que son objeto del impuesto por bienes inmuebles los terrenos, las instalaciones o las construcciones fijas y permanentes que allí existan. Al respecto, las municipalidades tendrán el carácter de administración tributaria, esto les permite realizar valoraciones de bienes inmuebles, facturar, recaudar y tramitar el cobro judicial y de administrar, en sus respectivos territorios, los tributos que genera la Ley.

1.15. En la actualidad la Municipalidad cuenta con el sistema monolítico[1] de información automatizado[2] que le permite recopilar, procesar y comunicar los datos necesarios para llevar a cabo los trámites relacionados con los procesos para establecer y cobrar los impuestos de patentes, bienes inmuebles y servicios urbanos, el cual cuenta con su propio sistema operativo (Master Control Program-MCP) y base de datos (DMS II), accesible por red interna y cuenta con tres niveles para su acceso:

Imagen n°. 2 Niveles de acceso del Sistema



Fuente: Elaboración CGR con base en entrevista con la DTIC

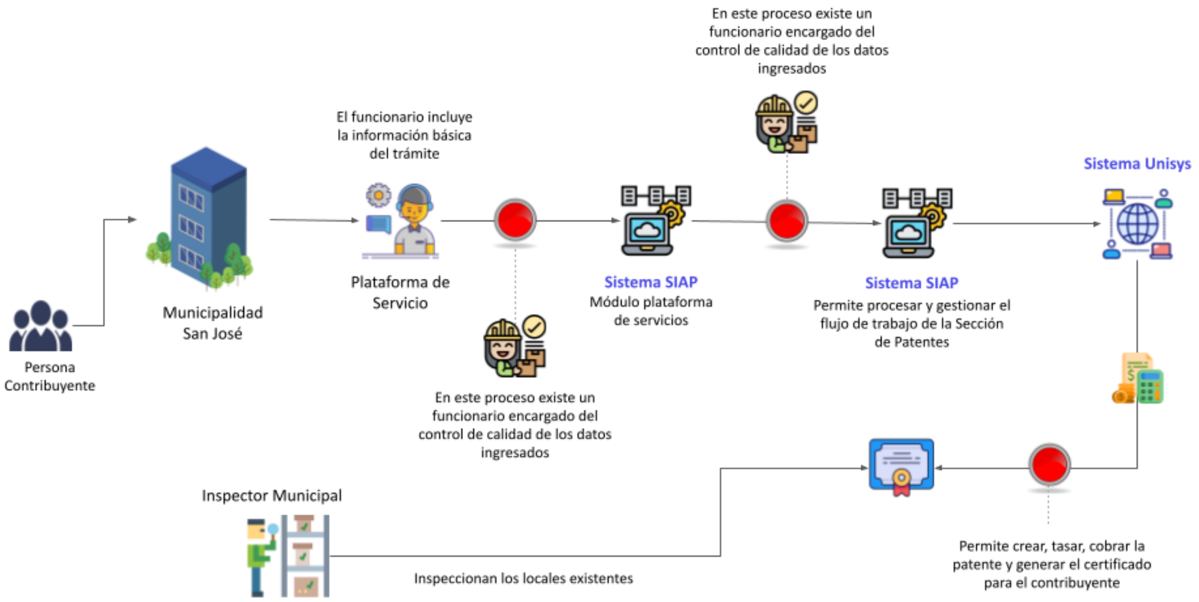
1.16. Además cuenta con el sistema denominado SIAP, implementado por la DTIC en el año 2021 para registrar y dar seguimiento a trámites varios de patentes y órdenes de trabajo de inspección.

---

[1] Los sistemas monolíticos agrupan la funcionalidad y sus servicios en una base de código única.

[2] Sistema con una antigüedad de más de 30 años, en infraestructura EAD / LINC y cuenta con un Sistema de Gestión de Base de Datos (DBMS) en DMSII cuya estructura de base de datos es de tipo jerárquica.

Imagen n°. 3 Descripción de la intervención de los sistemas en los procesos de patentes y SSUBI



Fuente: Elaboración CGR.

MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA

1.17. Durante la ejecución del taller de causas y soluciones, la DTIC detalló que se han realizado depuraciones en los usuarios del Active Directory, mejora en las políticas del dominio y remediación del 56% de las vulnerabilidades detectadas, lo que ha permitido mejorar las condiciones identificadas en la presente auditoría.

1.18. Adicionalmente, la municipalidad implementó una herramienta de Detección de Brechas (sBDS)[3], para detectar y responder a diferentes tipos de ataques y amenazas de red mediante el uso de tecnología tradicional basada en firmas o basada en reglas y modelado de datos para inteligencia de amenazas.

---

[3] Servidor de Sistema de Detección de Brechas (sBDS) es una plataforma de detección de amenazas que identifica las amenazas avanzadas que violan el perímetro de defensa y que están al acecho dentro de una red interna de la empresa.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.19. El borrador del presente informe fue remitido a la Municipalidad de San José mediante oficio n.°DFOE-LOC-0328 del 10 de febrero de 2023, dirigidos al Sr. Johnny Araya Monge, Alcalde Municipal y al Sr. Lenin Barrantes Villareal, Presidente del Concejo Municipal, respectivamente; con el propósito de formular y remitir a la Contraloría General, las observaciones pertinentes sobre su contenido, con la respectiva documentación de respaldo.

1.20. El 13 de febrero de 2023 se presentaron los resultados de la auditoría en reunión virtual con los representantes de la Municipalidad: Sr. Johnny Araya Monge, Alcalde Municipal; Sr. Lenin Barrantes Villareal, Presidente del Concejo Municipal, Rodney Zúñiga Guzmán, Asesor Alcaldía; Edgar Sandoval Montero, Gerente Administrativo Financiero y TIC; Carlos Garita Cabezas, Director de Tecnologías de Información y Comunicación; Carlos Montero Paniagua, Jefe Sección de Patentes e Israel Barrantes Sánchez, Auditor Interno.

1.21. Las observaciones al borrador de informe fueron remitidas por la Municipalidad de San José mediante el oficio ALCALDIA-00430-2023 de 17 de febrero de 2023. Lo resuelto sobre las observaciones efectuadas se comunicó mediante el oficio 01978(DFOE-LOC-0379) del 23 de febrero de 2023.

SIGLAS Y ABREVIATURAS

1.22. En el cuadro n°. 1 se indican las principales siglas utilizadas en este informe y su significado.

Siglas / Abreviaturas	Significado
DFOE	División de Fiscalización Operativa y Evaluativa
DTIC	Dirección de Tecnologías de Información y Comunicación
SSUBI	Sección de Servicios Urbanos y Bienes Inmuebles
SIAP	Sistema Integrado Autorización Patentes
BIA	Análisis de Impacto de Negocio, por sus siglas en inglés
DRP	Plan de Recuperación de Desastres, por sus siglas en inglés
RPO	Objetivo de Punto de Recuperación, por sus siglas en inglés
RTO	Objetivo de Tiempo de Recuperación, por sus siglas en inglés

2. RESULTADOS

SEGURIDAD DE LA INFORMACIÓN

2.1. El gobierno de la seguridad de la información comprende impulsores de valor específicos como la confidencialidad, integridad y disponibilidad de la información, la continuidad de los servicios y la protección de los activos de la información. La ausencia de una estrategia en esta temática, reduce la capacidad de una organización para mitigar el riesgo y aprovechar las oportunidades de las tecnologías de información en el mejoramiento del proceso de negocio. Por lo tanto, la seguridad y sus impulsores son un aspecto significativo sujeto de evaluación ante las amenazas y vulnerabilidades a las que están expuestas las instituciones del país.

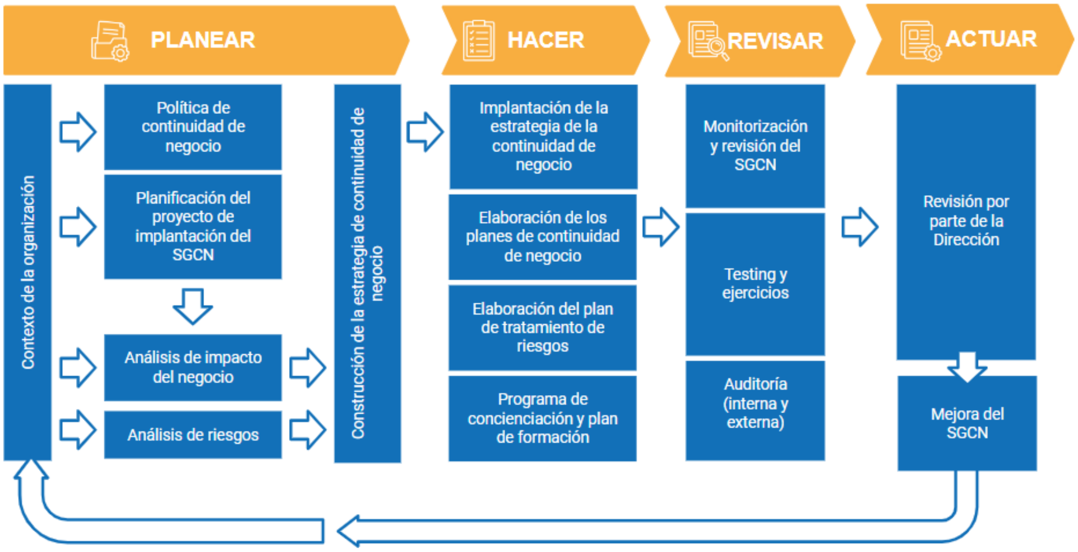
2.2. En atención a lo anterior, la DTIC de la Municipalidad de San José ha ejecutado acciones tales como la formalización de las Normas Generales de Seguridad Informática donde se detalla un conjunto de reglas que buscan la integridad, confidencialidad y disponibilidad de la información y recursos informáticos. Adicionalmente, se han realizado acciones para fortalecer la infraestructura considerando mejoras en el centro de cómputo y en los dispositivos de seguridad de red que detectan y bloquean amenazas, filtrado web, políticas de bloqueo, entre otras.

2.3. No obstante, se identificaron debilidades relacionadas con la disponibilidad, integridad y confidencialidad de la información de los sistemas críticos municipales, las cuales requieren de acciones correctivas que permitan a la Municipalidad fortalecer esta temática debido a su vinculación con el logro de los objetivos institucionales:

Debilidades relacionadas con la continuidad del negocio y su impacto en la disponibilidad de la información de los sistemas críticos municipales

2.4. La continuidad del negocio permite que una organización continúe ofreciendo los servicios críticos en caso de que se presenten eventos que provoquen una interrupción. Para esos efectos, es necesario contar con un proceso de planificación y un compromiso riguroso de los recursos para prever tales eventos de forma adecuada, a través de un Sistema de Gestión de la Continuidad de Negocio, siendo que dicho proceso debe iniciar con la identificación de los aspectos clave responsables del crecimiento y la consecución de las metas del negocio. Basado en esos aspectos clave, se evalúan los riesgos para identificar los recursos humanos, datos, infraestructura que los respaldan, las vulnerabilidades, probabilidad de ocurrencia de las amenazas así como la eficacia eficiencia de los controles.

Imagen n°. 4 Sistema de Gestión de la Continuidad del Negocio



Fuente: Elaboración CGR con base en la ISO 22301

2.5. La DTIC de la MSJ, desarrolló e implementó las Normas Generales de Seguridad Informática[4] en las cuales se incorpora el apartado 18 denominado “Normas para la elaboración de planes de continuidad y contingencias de la gestión de tecnologías de información y comunicaciones”; además, cuenta un Plan de recuperación de desastres (DRP)[5] y una matriz de riesgos, documentos necesarios para dar respuesta a incidentes de forma que se propicie un impacto positivo en las personas y en la capacidad de las operaciones.

2.6. La revisión de los citados documentos permitió identificar oportunidades de mejora que impactan la continuidad del negocio en la disponibilidad y confidencialidad de la información relacionados con:

a) No se establece o regula la obligatoriedad de que los planes de continuidad y contingencias de las diferentes unidades de la institución sean debidamente probados para garantizar razonablemente su efectividad.
b) El DRP carece de los procedimientos necesarios para establecer la declaración de un desastre, así como de los criterios de activación del plan. Además, no se cumple la totalidad de las premisas establecidas en el documento para la recuperación correspondiente.
c) No se han realizado simulacros o pruebas de manejo de incidentes ni se ha actualizado en 6 años la definición de los tiempos de recuperación (RTO y RPO).

---

[4] Aprobada el 17 de enero de 2022, por el Director DTIC y la Alcaldesa a.i., en su versión 2.0

[5] Denominado internamente como “Manual de instrucciones para la recuperación de tecnologías de información ante desastres” en su versión 4.0 del año 2022.

d) La matriz de riesgos no contempla de forma integral una evaluación de la seguridad de la información en aspectos asociados a integridad y confidencialidad de la información y no se establecen controles asociados a la ciberseguridad; además, no es posible identificar y administrar el riesgo por activo y tipo de atributo (disponibilidad, confidencialidad e integridad).

e) Las Normas Generales de Seguridad Informática presentan errores en la redacción dado que hacen referencia externa a una serie de documentos que no se encuentran como adjuntos, sino que fueron incorporados dentro del cuerpo de la normativa.

2.7. La Municipalidad de San José (MSJ), contrató en el año 2017 la elaboración del documento Análisis de Impacto de Negocio (BIA)[6], para identificar los servicios, sistemas y la infraestructura tecnológica que da sustento a los procesos o procedimientos críticos de la Municipalidad de San José, sin embargo, esta auditoría permitió identificar que los esfuerzos en la continuidad de negocio no tuvieron impacto a nivel de toda la institución, dado que se carece de la documentación que respalde la planificación, implementación, seguimiento y mejora continua de la continuidad de negocio municipal.

2.8. En línea con lo anterior, la Municipalidad carece de un modelo de clasificación de activos de información que permita, entre otros asuntos, identificar los activos de información relacionada con los procesos clave de negocio[7]. Además, no se ha desarrollado un plan de continuidad de negocio municipal que defina cómo deben actuar las unidades de negocio y el personal operativo en caso de que se presente un evento disruptivo, esto a pesar de las alertas efectuadas por la DTIC.

2.9. Asimismo, se identificó que el BIA contratado por la institución no presenta actualizaciones desde su creación, por lo que corre el riesgo de estar desactualizado o no se ajuste a la realidad institucional actual, en razón de que la infraestructura tecnológica ha sufrido variaciones a través del tiempo.

2.10. De acuerdo con la norma DSS04 Gestionar la Continuidad de COBIT 5 de ISACA, 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".

2.11. En esta mejor práctica, se establecen prácticas para poder dar continuidad de las operaciones críticas para el negocio y mantener la disponibilidad de la información, tales como: definir la política de continuidad del negocio, objetivos y alcance; mantener una estrategia de continuidad; desarrollar e implementar una respuesta a la continuidad del negocio; ejercitar, probar y revisar el plan de continuidad; revisar, mantener y mejorar el plan de continuidad; proporcionar formación en el plan de continuidad; gestionar acuerdos de respaldo y ejecutar revisiones post-reanudación.

---

[6] Contratado a empresa externa, versión 3.0 del año 2017.

[7] Los informes de Auditoría Interna y externa emitieron alertas desde el año 2015 sobre la necesidad de establecer e implementar una calificación de activos de información que contemple al menos el propietario, ubicación, función y su relevancia.

2.12. Por otro lado, la norma ISO 27001, sobre Gestión de Seguridad de la Información, en su cláusula A.8.2.1, indica que para la gestión de la seguridad de la información, la información debe clasificarse en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

2.13. Las situaciones evidenciadas tienen origen en la ausencia de un compromiso institucional con la continuidad de negocio, que debiera estar plasmado en la implementación del Sistema de Gestión de la Continuidad del Negocio que cubra a toda la entidad, mediante el cual la alta gerencia determine las expectativas, la magnitud y el alcance del esfuerzo de continuidad del negocio en la institución, de forma tal que se alineen el resto de los esfuerzos de la DTIC y demás direcciones municipales.

2.14. Al respecto, se resalta que la continuidad de negocio es responsabilidad de la alta gerencia[8], dado que es esta a quien se le confía la protección de los activos; en ese sentido la planificación de la continuidad del negocio en la Municipalidad de San José ha sido iniciativa de la Dirección de Tecnologías de Información y Comunicaciones quienes han realizado esfuerzos aislados en materia de continuidad del negocio, por lo que las expectativas del negocio y la estrategia institucional no se encuentran alineados con los esfuerzos del área técnica. Es necesario un mayor compromiso de la alta gerencia con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del sistema de gestión de la continuidad del negocio.

2.15. Además, las debilidades asociadas con las Normas Generales de Seguridad Informática tienen también su origen en que las aprobaciones periódicas que ha realizado la DTIC, no ha considerado una revisión exhaustiva de las modificaciones necesarias para que esta normativa cumpla con el propósito para el que fue creada, que se resume en regular la implementación y actualización de la estrategia de Tecnologías de Información, para administrar y dirigir los recursos de acuerdo con la estrategia del negocio y sus prioridades.

2.16. Las debilidades asociadas a la planificación de la continuidad del negocio y la atención de incidentes, atentan contra la disponibilidad, integridad y confidencialidad de los sistemas críticos y los procesos de negocio vinculados a éstos; y por consiguiente en la gestión institucional, con el consecuente riesgo de afectación a la oportuna prestación de los servicios municipales y la recaudación de impuestos municipales.

Debilidades en los sistemas que impactan en la confidencialidad e integridad de la información de los sistemas críticos municipales

2.17. La auditoría realizada permitió determinar que la seguridad de la información del sistema de automatizado donde se tramitan los procesos de patentes y SSUBI no cumple con varios aspectos necesarios para garantizar, de forma razonable, la disponibilidad, integridad y confidencialidad, tales como la documentación de sistemas, la gestión de

---

[8] La alta dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGCN estableciendo una política de continuidad del negocio, 5.2 Compromiso de la dirección de la ISO 22301.

identidades, el principio del mínimo privilegio[9], el mantenimiento de usuarios y la confidencialidad de los datos, tal y como se detalla seguidamente:

a) La DTIC no cuenta con ninguna documentación del sistema y su base de datos, situación que toma relevancia si se considera que la estructura del código y las tablas han sido modificadas por los diferentes funcionarios que han trabajado en esa unidad durante los últimos 30 años.
b) Tampoco se documentan las mejoras o ajustes efectuados sobre este sistema y su base de datos, ni se ha tomado una decisión contundente para que se documente lo correspondiente sobre los cambios efectuados.
c) Se identificó que el módulo mediante el cual se asignan los permisos para el sistema, no cuenta con el "enmascaramiento" de las claves de los funcionarios, por lo tanto, en el sistema se puede visualizar en texto plano la contraseña de cada módulo y usuario del sistema. Al respecto, también se logró evidenciar que estas claves no se encuentran encriptadas a la hora de guardarse en la base de datos de los usuarios del sistema.
d) Los puntos c) y d) toman relevancia al considerar que para el segundo nivel de acceso al sistema se debe ingresar la combinación del usuario, la clave y la estación, sin embargo, para todos los funcionarios la clave de acceso es el mismo nombre de su usuario.
e) Se determinó que no se realiza mantenimiento de la tabla de los usuarios, ni de los catálogos de claves, dado que después de migrar varias funciones a otros sistemas, no se ha depurado la información correspondiente a los usuarios y tipo de permisos que se asignaban para las funciones migradas. Cabe detallar que para el catálogo de claves, la documentación de los tipos de accesos del módulo de patentes no permite identificar claramente los permisos reales que obtienen los usuarios al establecer los campos denominados "módulo", "nivel", "tipo" y "opción", ya que para el 78% (7 de 9 descripciones) de las combinaciones la descripción es la misma.
f) En cuanto a la gestión de identidades, se determinó que si bien existen procedimientos para que las unidades soliciten a la DTIC la creación o modificación de los permisos de los usuarios, los mismos no cuentan con una estructura estandarizada para detallar los accesos requeridos, dado que la costumbre es indicar que se den los permisos al funcionario con base en los de otro funcionario. Al respecto, se logró evidenciar que se asignan permisos que incumplen el principio del mínimo privilegio en funcionalidades de riesgo alto dentro del proceso de bienes inmuebles como lo es el control de aprobación de propiedades.
g) Adicionalmente, se identificó que 8 (53%) de los funcionarios con permisos en el módulo de patentes y 29 (22%) de los funcionarios con permisos en la sección SSUBI ya no deberían contar con dicho acceso, por cuanto ya no laboran para la Municipalidad. Además, se determinó que para 7 (5%) funcionarios de SSUBI la DTIC no logró establecer su vinculación o desvinculación con la municipalidad.
h) Asimismo, se pudo constatar que el Departamento de Gestión Tributaria tiene como función modificar y depurar las bases de datos para las actualizaciones de los saldos de las cuentas de los tributos municipales, no obstante, la asignación de permisos en el

---

[9] El principio de privilegio mínimo (POLP) es un concepto de seguridad informática que limita los derechos de acceso de los usuarios a lo estrictamente necesario para realizar su trabajo. Los usuarios tienen permiso para leer, escribir o ejecutar solo los archivos o recursos necesarios para realizar su trabajo.

sistema para ejecutar dicha función incumple el principio del mínimo privilegio, al respecto, la jefatura de ese departamento, indicó en repetidas ocasiones que solamente 2 funcionarios son los autorizados para ejecutar los movimientos al pendiente de patentes, no obstante, se identificaron 84575 (82%) modificaciones al pendiente que fueron ejecutadas por 15 funcionarios que no figuran en la autorización definida por la jefatura consultada.

2.18. El jerarca y de los titulares subordinados, como responsables[10] del buen funcionamiento del sistema de información, deben asegurarse de contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno. También se establece que se deben armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficientes de los recursos públicos, y se considera la necesidad de establecer las políticas, los procedimientos y recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico.

2.19. Adicionalmente, se debe disponer[11] de los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.

2.20. Finalmente, las actividades de control[12] deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación.

2.21. En cuanto a la existencia de usuarios que ya no pertenecen a la Municipalidad, las jefaturas usuarias tienen la responsabilidad[13] de informar a la DTIC, sobre cualquier movimiento de su personal (cambio de funciones, dependencia, o renuncia) para proceder a eliminar los derechos o accesos a los sistemas, sin embargo, la DTIC también puede ser proactiva y ejecutar ciertas depuraciones periódicas.

2.22. Asimismo, las Normas Generales de Seguridad Informática cuentan con incisos donde se regulan temas como la documentación de sistemas, indicando que el desarrollo y mantenimiento de toda aplicación deberá contemplar y dejar documentado, en sus distintas etapas, los aspectos de seguridad que permitan la disponibilidad, confidencialidad e integridad de los datos. También se regula que los usuarios utilicen los recursos de acuerdo con los derechos que se les asignen de conformidad con sus

---

[10] Ley n°. 8292, Ley General de Control Interno, Artículo 16

[11] Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) Artículo 5.8 Control de sistemas de información.

[12] Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) Artículo 4.2 Requisitos de las actividades de control.

[13] Normas Generales de Seguridad Informática de la Municipalidad de San José, Sección 21; Normas para el final de la relación laboral, 21.3 Normas.

funciones, aunado a que conozcan y cumplan con las regulaciones en materia de Seguridad de la Información. Finalmente, esta norma también regula el correcto uso de contraseñas donde se enfatiza que la contraseña por adoptar no podrá ser igual o similar a su respectivo nombre de usuario.

2.23. Las debilidades detalladas tienen origen en que la DTIC no ha sido rigurosa en el acatamiento de las Normas Generales de Seguridad Informática en lo que corresponde al sistema donde se tramitan los procesos de patentes y SSUBI, dado que no ha habido claridad en las decisiones concernientes a si seguir invirtiendo esfuerzos en mejorar la herramienta actual, o bien optar por su eliminación. No es hasta enero del año 2021 que la Municipalidad decide que la DTIC sea la encargada del proyecto para desarrollar el sistema tributario, el cual ya cuenta con la justificación tanto técnica, financiera y cuenta con el levantamiento de los requerimientos.

2.24. Además, la DTIC no ha definido una estructura estándar para la gestión de las identidades que le permita a las jefaturas usuarias cumplir con las citadas normas y evitar los errores evidenciados. En cuanto a las debilidades en el mantenimiento de los usuarios, tampoco se han establecido mecanismos para monitorear y propiciar que las unidades de la Municipalidad cumplan con informar lo correspondiente, o bien ejecutar procesos automatizados y proactivos que impacten de forma positiva en esta gestión.

2.25. En cuanto a la condición expresada sobre el Departamento de Gestión Tributaria, las causas no se asocian en sí a la gestión tecnológica, sino a la ausencia de controles que permitan monitorear la ejecución y aprobación de estos ajustes, así como la revisión periódica de los responsables de ejecutar estos procesos en los sistemas.

2.26. Las situaciones evidenciadas potencian los riesgos relacionados con la pérdida de disponibilidad, confidencialidad e integridad de la información de la Municipalidad, comprometen la capacidad técnica de dar mantenimiento a los sistemas, promueven la pérdida de la trazabilidad tanto transaccional como documental de los procesos y de los ajustes realizados en sistemas o bases de datos, con la afectación en la rendición de cuentas a que está sometida toda dependencia.

2.27. La falta de claridad en cuanto a los funcionarios que pueden ejecutar movimientos en el pendiente de patentes, es un riesgo para la confiabilidad de la información que se registra en el sistema, por cuanto no existe certeza si los movimientos corresponden a transacciones legítimas.

Debilidades relacionadas con la estandarización de las bitácoras que respaldan los sistemas críticos y con la documentación del sistema SIAP

2.28. La revisión de las bitácoras del sistema donde se tramitan los procesos de patentes y servicios urbanos y bienes inmuebles para el proceso de patentes permitió determinar que no se cuenta con el detalle documental sobre la cantidad de bitácoras existentes, su utilidad y si se encuentran disponibles para el funcionario, tampoco se ha documentado la lógica de su programación, la estructura de los campos, ni su interpretación. Lo anterior se agrava al considerar que los creadores de algunas de estas bitácoras ya han dejado de ser funcionarios de la Municipalidad.

2.29. Por otra parte, los datos registrados en esas bitácoras reflejan que si bien los sistemas registran datos como la fecha, el usuario que ejecuta el movimiento, el tipo de movimiento realizado, el programa mediante el cual se ejecutó y el documento u oficio que lo justifica, los registros de esas tablas presentan las siguientes inconsistencias:

a) Se identificaron debilidades en la integridad de la información de las bitácoras de patentes: "PAREPL1383-Bitácora de Movimientos Pendientes" y "PAREPL1384-Bitácora de Movimientos Maestro de Patentes", específicamente en los campos "usuario" y "programa", en los cuales se registra información inconsistente como espacios en blanco, números de oficio o nombres de reportes o sistemas, siendo lo correcto que estos datos se ingresen el campo denominado "documento", y que los campos usuario y programa registren el "usuario" que ejecutó el movimiento y el "programa" del sistema mediante la cuál se ejecutó, respectivamente.

b) La tabla "PAREPL1383-Bitácora de Movimientos Pendientes" exhibe 674635 (76%) de registros inconsistentes en el campo "usuario" y entre las inconsistencias se observan datos en blanco, así como número de oficio o reportes que no deben ser registrados en el campo del usuario que ejecuta el movimiento.

c) La tabla "PAREPL1383-Bitácora de Movimientos Pendientes" exhibe 66611 (8%) de registros inconsistentes en el campo "programa", dado que se incluyeron números de oficio que no corresponden con la lógica del campo en la bitácora.

d) La tabla "PAREPL1383-Bitácora de Movimientos Pendientes" cuenta con 388471 (54%) registros con el campo "documento" en blanco, siendo que se consideraron los registros en los que el campo programa sea diferente a las pantallas del sistema, es decir, no se está registrando para estos casos en el campo correspondiente el documento que justifica esos movimientos.

e) Finalmente, la tabla "PAREPL1384-Bitácora de Movimientos Maestro de Patentes" exhibe 2536 (3%) registros inconsistentes en el campo "codigo_usuario", 1065 (1%) en el campo programa y 2282 (90%) registros con el campo documento en blanco (en este caso para la revisión por documento, se consideraron solo los registros con números de oficio o reportes en el campo codigo_usuario).

2.30. Adicionalmente, se evidenció que si bien la DTIC cuenta con bitácoras donde se registran las transacciones relacionadas con los estadísticos, movimientos, inclusiones y exclusiones al pendiente y créditos de bienes inmuebles, servicios urbanos y patentes, a la fecha no se han implementado mecanismos de visualización dentro del sistema mediante el cual los funcionarios dueños de esos procesos puedan tener acceso a las mismas sin intervención de la DTIC, lo anterior exceptúa la visualización de la bitácora del movimiento estadístico censal (MEC) de la sección SSUBI.

2.31. Mediante el análisis de los sistemas de la municipalidad, se identificó que se cuenta con otro sistema denominado SIAP, implementado por la DTIC en el año 2021 para registrar y dar seguimiento a trámites varios de patentes y órdenes de trabajo de inspección. Al respecto, la revisión de los datos de este sistema permitió evidenciar que no cuenta con controles de validación y automatización para el registro de la información, por lo tanto, esta información no cumple con los atributos de integridad y disponibilidad conforme al marco regulatorio aplicable.

2.32. En línea con lo anterior, existen 28 (13%) campos en la tabla del SIAP que presentan inconsistencias básicas como campos en blanco, es decir, para ninguno de esos campos existe un control que obligue al usuario a incluir los datos correspondientes al proceso de patentes, esta situación toma relevancia si consideramos que existen campos como el “correo electrónico” que son considerados como un requisito obligatorio para el trámite, pues se requiere que el contribuyente presente una dirección de correo electrónico como medio de notificación.

Tabla n°. 1 Inconsistencias en datos del sistema SIAP

Datos del Sistema SIAP para el registro y seguimiento de trámites de patentes		
	Campo según SIAP	**Campos en blanco**
1	Medio de Notificaciones de la sociedad (correo)	5 671(88%) de 6475
2	Número de cédula jurídica	536 (17%) de 3085
3	Dirección del establecimiento de la sociedad	1 372 (44%) de 3085
4	Tipo de identificación	14 (0,5%) de 3044
5	Nombre del solicitante	23 (1%) de 3044
6	Télefono	4 210 (65%) de 6475
7	Celular	1457 (22%) de 6475
8	Email	437 (7%) de 6475
9	Nombre del Establecimiento	349 (5%) de 6475
10	Dirección Local Comercial	720 (11%) de 6475
11	Clase de trámite	118 (2%) de 6475
13	Plano	3 783 (58%) de 6475
14	Localización	3 796 (59%) de 6475
15	Área Útil	3 913 (60%) de 6475
16	Código CIIU	5 799 (90%) de 6475

17	Régimen tributario	5 968 (92%) de 6475
18	Código CIIU Salud	3 285 (51%) de 6475
19	Tipo de Riesgo	3 236 (50%) de 6475
20	Fecha de vencimiento Salud	3 262 (50%) de 6475
22	Fecha de Vencimiento SENASA	13 (19%) de 79
23	Fecha de vencimiento CAI (Centros de Atención Integral)	1 (33%) de 3
24	Número de póliza	3 817 (59%) de 6475
25	Hasta (vencimiento póliza del INS)	83 (3%) de 2658
	Campo según SIAP	**Dirección de correo electrónico no válida**
26	Email	268 (33%) de 6475
	Campo según SIAP	**Número de cédula jurídica no válida (Se registró un nombre en lugar del número)**
27	Número de Cédula Jurídica	70 (2%) de 3085
	Campo según SIAP	**INS (No existe número de póliza)**
28	Póliza exonerado	635 (17%) de 3 817, casos que se marcaron como exonerados pero el registro del número de póliza se encuentra en blanco

Fuente: Elaboración CGR, con base en los datos aportados por la MSJ

2.33. En cuanto proceso de inspección se detallan las siguientes inconsistencias:

Tabla n°. 2 Inconsistencias en datos del sistema SIAP (módulo inspección)

Datos del Sistema SIAP para el registro y seguimiento de trámites de Inspección		
	Campo según SIAP	**Campos en blanco**
1	Identificador de ingreso SIAP	6 714 (60%) de 11 284
2	Nombre Comercial	7 205 (64%) de 11 284
3	Teléfono	7 735 (69%) de 11 284
4	Dirección	7 345 (65%) de 11 284
5	Indicaciones	8 451 (75%) de 11 284
6	Fecha de inspección	931 (8%) de 11 284
7	Motivo de inspección	50 (5%) de 11 284

8	Nombre del Inspector	493 (4%) de 11 284
9	Nombre Comercial	1 539 (14%) de 11 284
10	Nombre del Patentado	1 499 (13%) de 11 284
11	Cédula del Patentado	1 727 (15%) de 11 284
12	Distrito	742 (7%) de 11 284
13	Localización	4 737 (42%) de 11 284
14	Permiso de Salud	6 116 (54%) de 11 284
15	Fecha de Vencimiento Salud	6 568 (58%) de 11 284
16	Área Útil	1 138 (10%) de 11 284
17	Dirección Verificada	93 (1%) de 11 284
18	Teléfono	1 476 (13%) de 11 284
19	Correo Electrónico	1 469 (13%) de 11 284
20	Informe de la inspección	1 949 (17%) de 11 284

Fuente: Elaboración CGR, con base en los datos aportados por la MSJ

2.34. Al respecto, las Normas Generales de Seguridad Informática[14] de la municipalidad establecen que se debe verificar que todos los sistemas de información que se desarrollen contengan el manual técnico y de usuario correspondiente y que dichos manuales sean actualizados constantemente.

2.35. El jerarca y los titulares subordinados, según sus competencias, deben asegurar[15] razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios, así como velar por que la información se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente.

2.36. Con respecto a la visualización de las bitácoras, se debe considerar que las unidades de negocio están llamadas a ejercer la supervisión constante[16] sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos.

2.37. Las debilidades en la documentación e integridad de las bitácoras del sistema donde se tramitan los procesos de patentes y servicios urbanos y bienes inmuebles, obedecen a que en los casos en que las áreas de negocio solicitan a la DTIC la aplicación de ajustes en patentes o bienes inmuebles, estos movimientos se aplican mediante fragmentos de

---

[14] Sección 10; Normas para el Desarrollo, Mantenimiento, y actualización de Sistemas de Información Institucionales, 10,3 Normas.

[15] Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE). Norma 5.6 Calidad de la información.

[16] Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE). 4.5.1 Supervisión constante

código (scripts) directamente en la base de datos, es decir, no se realiza por medio del sistema, aunado a que la DTIC no ha establecido un mecanismo para estandarizar la forma en que se generan y aplican estos códigos.

2.38. Estas debilidades también encuentran sustento en que las modificaciones a los datos de la municipalidad no deberían estar siendo ejecutadas de esta forma por la DTIC, dado que la responsabilidad de estas funciones corresponde a las unidades de negocio, aunado a que la DTIC no puede tener certeza de que los ajustes que tramita por este medio se encuentren libres de errores, defectos, omisiones y/o modificaciones no autorizadas, aún cuando se tenga un oficio que lo respalde.

2.39. Por su lado, la ausencia de un medio para visualizar las bitácoras dentro del sistema se debe a que la mayoría de las unidades de negocio no han solicitado este tipo de ajustes en el sistema, sino que la práctica común ha sido solicitar a la DTIC la investigación específica de los casos inconsistentes o bien reportes desarrollados a partir de los datos de esas bitácoras.

2.40. La causa de las debilidades evidenciadas en la integridad de la información del sistema SIAP es la ausencia de controles de validación programados en el código desarrollado para la aplicación, asimismo, la sección de patentes no fundamentó los requerimientos originales del sistema en un análisis que contemple lineamientos para la estandarización y validación de esa información.

2.41. La situación identificada se materializó en las bitácoras de los movimientos al pendiente de patentes[17]; en consecuencia tuvieron que ser reemplazadas en agosto de 2020, dado que la DTIC identificó debilidades en su estructura y dificultad en su interpretación, aunado a que fueron creadas por una ex funcionaria que tampoco las documentó.

2.42. Las debilidades comentadas impactan la gestión de las bitácoras, por cuanto, se disminuye su capacidad para proporcionar información útil sobre las actividades realizadas por los usuarios en los sistemas y aplicaciones, además se dificulta monitorear las actividades de carácter sospechoso.

2.43. Lo anterior toma relevancia para la municipalidad, si se considera el tipo de transacciones que se realizan diariamente, aunado a las debilidades del sistema en cuanto a la visualización de reportes para el control, seguimiento y monitoreo de las acciones de los funcionarios sobre las patentes y las propiedades de los contribuyentes.

2.44. Por otra parte, la ausencia de controles de validación en el sistema SIAP trae como efecto que los datos recopilados mediante esta herramienta se encuentren inconsistentes, además, repercute en la agilidad de los trámites de patentes por cuanto se debe tomar tiempo en su inclusión, no es amigable a la hora de incluir datos.

---

[17] PAREPL1424-AUPIE Bitácora inclusiones y exclusiones al Maestro de patentes, PAREPL1424-AUPCD bitácora de cargos y descargo al pendiente y PAREPL1424-AUPMM Bitácora Modificaciones Maestro de patente

Debilidades en los controles implementados para asegurar la seguridad de la información en los procesos operativos

2.45. La sección de servicios urbanos y bienes inmuebles (SSUBI) cuenta con dos controles automatizados en el sistema para salvaguardar razonablemente la integridad de los datos de los tributos de los contribuyentes. El primer control es el que establece la obligatoriedad de contar con una aprobación para poder ejecutar cambios en las características de las propiedades o tributos; el segundo control, denominado “MEC”, hace obligatoria la inclusión de las observaciones que respalden y justifiquen los movimientos ejecutados en las propiedades o tributos. Si bien esta Sección ha promovido un mayor control de los procesos desde el año 2019, se identificaron debilidades relacionadas con su aplicación y funcionalidad.

2.46. Con respecto a la aprobación requerida para modificar las propiedades o tributos, se logró comprobar que existen 13 usuarios realizando aprobaciones, de los cuales 7 no coinciden con la lista de personas autorizadas para ello; al respecto, la jefatura de SSUBI detalló que son 6 los funcionarios con el perfil y permisos para dar las autorizaciones al resto de los compañeros.

2.47. Adicionalmente, se determinó[18] que para 1319 contribuyentes se hicieron exclusiones en el pendiente de cobro[19] sin contar con la autorización correspondiente en el control establecido por SSUBI (cabe aclarar que éstos no son necesariamente movimientos irregulares, sino que no cumplen con los controles establecidos para esos movimientos). Al respecto, 68 de esos contribuyentes fueron modificados por usuarios de la Sección SSUBI, mientras que 1260 fueron modificados por otros usuarios de otras unidades.

2.48. En cuanto al MEC, cabe destacar que a partir del año 2018 se realizaron ajustes para que los campos donde se registran las observaciones de los funcionarios cuenten con al menos 6 caracteres, para que no sea posible que se dejen en blanco de forma intencional, sin embargo, la revisión de la tabla[20] permitió determinar que existen 2795 registros que no cuentan con ningún dato en las observaciones, de los cuales 1 685 (60%) son trámites a nombre de personal de la sección SSUBI, por consiguiente, existen debilidades en la aplicación de este control que impactan el cumplimiento de las directrices de esa sección así como la adecuada documentación y justificación del trámite ejecutado.

2.49. Adicionalmente, se revisó el proceso que ejecutan para aplicar los pagos parciales (mal denominados recibos manuales), al respecto, se logró evidenciar que la pantalla utilizada despliega el desglose de los pendientes de cobro por servicios y sus intereses con el monto registrado, pero éstos se encuentran habilitados para ser modificados por el

---

[18] Mediante un cruce de datos entre las tablas “BIREP00006 Inclusiones y exclusiones al Pendiente” que registra los movimientos al pendiente de bienes inmuebles y la tabla “EXTRAAUHCT Bitácora de accesos finca cédula localización” la cual almacena las autorizaciones para modificar las fincas a partir del 01 de marzo de 2021.

[19] Datos del período comprendido entre el 01 de marzo de 2021 y el 21 de noviembre de 2022.

[20] EXTRAURMEC MOVIMIENTOS ESTADÍSTICOS CENSAL cuenta con 156417 registros y 5 campos para que los funcionarios incluyan las observaciones de los trámites ejecutados.

funcionario, situación que puede prestarse para fraudes o errores. Además, en el sistema no se deja evidencia de la documentación que respalda el origen de ese movimiento ni del visto bueno que otorga la jefatura para su aplicación.

2.50. El jerarca y los titulares subordinados[21], deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.

2.51. Asimismo, se deben disponer los elementos y condiciones[22] necesarias para que de manera organizada, uniforme, consistente y oportuna se ejecuten las actividades de obtener, procesar, generar y comunicar, en forma eficaz, eficiente y económica, y con apego al bloque de legalidad, la información de la gestión institucional y otra de interés para la consecución de los objetivos institucionales.

2.52. Estas inconsistencias en los datos y su relación con el proceso establecido en SSUBI, permiten evidenciar que la Municipalidad no ha uniformado los controles que permiten salvaguardar la integridad de los datos de las propiedades de los contribuyentes y sus tributos en las diferentes unidades de negocio; por lo tanto, existen otros usuarios en otras unidades que no se adhieren ni cumplen con las mismas directrices y controles establecidos para salvaguardar la integridad y veracidad de esta información.

2.53. Las situaciones evidenciadas sobre los pagos parciales, tienen origen en que la Sección de cobro administrativo no ha establecido controles automatizados e integrados que le permitan vincular los movimientos al pendiente con los recibos, pagos o depósitos que los justifican, además, no se realiza monitoreo o seguimiento de las transacciones que se ejecutan mediante esta función del sistema.

2.54. En consecuencia, los datos de los trámites reflejan que existe la libertad de ejecutar movimientos sobre las propiedades y sus tributos, sin autorización y sin registrar observaciones que los justifiquen. Esta situación atenta contra el control, monitoreo y seguimiento que se implementó en la sección de SSUBI para evitar y disminuir la probabilidad e impacto de posibles irregularidades.

---

[21] Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) Artículo 5.8 Control de sistemas de información.

[22] Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE). Norma 5.1 Sistemas de información.

Debilidades en la gestión de la ciberseguridad para garantizar la protección de los activos críticos de la municipalidad

2.55. La revisión efectuada permitió identificar que la Municipalidad tiene oportunidades de mejora relacionadas con la seguridad de la información; al respecto, la Contraloría General determinó que esas debilidades pueden comprometer la integridad, disponibilidad y confidencialidad de la información de la Municipalidad de San José, por lo tanto, se remitió el oficio N.° DFOE-LOC-OI-00001-2023 (DFOE-LOC-268) del 01 de febrero de 2023, en el cual se detallan los aspectos técnicos así como los riesgos identificados, considerando su clasificación y recomendaciones.

2.56. Por otra parte, se revisó el servicio de directorio Active Directory (AD), que almacena información acerca de las cuentas de usuario, como nombres, contraseñas, políticas y permite autenticar a los usuarios; al respecto, la Municipalidad tiene 5282 cuentas de usuario creadas y la revisión permitió determinar que existen 89 cuentas de usuario que no corresponden a cuentas de funcionarios activos. De estas, 53 cuentas corresponden a exfuncionarios y a un usuario que aparece fallecido en el Tribunal Supremo de Elecciones y 72 cuentas para las cuales no se tiene evidencia de que correspondan a personas que hayan trabajado para la Municipalidad.

2.57. Por otro lado, se determinó que la Municipalidad no ha realizado acciones tendientes a la sensibilización o concientización de los funcionarios en materia de seguridad de la información, tales como cursos, charlas, talleres, recordatorios, y otros medios de comunicación, que permitan alcanzar un nivel de entendimiento y de compromiso del personal, en relación con sus responsabilidades en materia de seguridad.

2.58. Al respecto, en el Código Nacional de Tecnologías Digitales del MICITT se establece el deber de administrar la infraestructura desarrollando procedimientos para la actualización frecuente de firmware, controladores y parches del sistema operativo, aplicaciones y dispositivos, así como que el desarrollo de la ciberseguridad en la infraestructura tecnológica debe de contar con un inventario de software oficial y actualizado periódicamente.

2.59. Además, en el mismo cuerpo normativo se señala que el acceso a los activos físicos y lógicos e instalaciones asociadas debe estar limitado a los usuarios, procesos y dispositivos autorizados, que los mecanismos de autenticación deben garantizar la veracidad de la identidad del usuario y seguir las mejores prácticas para prevenir el mal uso o el abuso por parte de usuarios o sistemas no autorizados. Asimismo, sugiere el uso de mecanismos de cifrado para proteger la información de acceso restringido, así como la validación, filtrado y codificación de la información recibida por las aplicaciones, para prevenir los riesgos relacionados con la posible captura de información de la municipalidad.

2.60. En cuanto a la sensibilización de los funcionarios, la institución debe[23] tener en cuenta la necesidad de recomendar programas de formación y concienciación en seguridad de la información, divulgar[24] acerca de software malicioso y forzar procedimientos y responsabilidades de prevención así como realizar regularmente formación[25] sobre seguridad física.

2.61. De forma complementaria, las Normas Generales de Seguridad Informática establece la responsabilidad de la DTIC así como departamentos y jefaturas institucionales, de buscar los medios para lograr la concientización en seguridad informática de los usuarios mediante boletines, charlas, afiches o capacitaciones[26].

2.62. Se debe considerar que en las Normas de control interno para el Sector Público[27], se detalla que cuando se detecte alguna deficiencia o desviación en la gestión o en el control interno, se deben emprender oportunamente las acciones preventivas o correctivas pertinentes para fortalecer el SCI, de conformidad con los objetivos y recursos institucionales.

2.63. Por consiguiente, las debilidades identificadas obedecen a la ausencia de mecanismos para monitorear e identificar posibles riesgos y vulnerabilidades que les permitan tomar decisiones oportunas sobre la aplicación de parches de seguridad, mejoras en la configuración, actualización de equipos y sistemas, entre otros.

2.64. Si bien las debilidades identificadas corresponden a equipos de la red interna institucional, las mismas pueden impactar en la seguridad de la información, en particular, si se considera que la Municipalidad planea poner en producción nuevos sistemas publicados en Web, por lo tanto, es importante atender esas vulnerabilidades antes de implementar futuros sistemas.

2.65. Al respecto, las situaciones comentadas potencian el riesgo de accesos no autorizados, pérdida o modificación de información y degradación parcial o total de los servicios. Cabe mencionar que este tipo de debilidades no corregidas permiten que la Municipalidad se encuentre susceptible a fallos de seguridad, o vulnerabilidades que pueden ser aprovechadas para intentar acceder a los sistemas y obtener información sensible o confidencial de la institución.

3. CONCLUSIÓN

3.1. La Municipalidad de San José, como administradora de los intereses y servicios locales del cantón sustenta sus procesos de negocio sustantivos en sistemas de información para la recaudación de impuestos municipales, la prestación de servicios al ciudadano y la

---

[23] Cobit 5. Práctica APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
[24] Cobit 5. Práctica DSS05.01 Proteger contra software malicioso (malware).
[25] Cobit 5. Práctica DSS05.05 Gestionar el acceso físico a los activos de TI.
[26] Sección 5. Normas para la concientización en seguridad informática.
[27] Norma 6.4 Acciones para el fortalecimiento del SCI de la Norma N-2-2009-CO-DFOE (NCISP).

generación de información crítica para la toma de decisiones. Al respecto, en el Plan de Desarrollo Municipal 2020-2024, se establece como pilar de la municipalidad, una conducta ética orientada al apego a la legalidad, a la mejora continua y la eficiencia operativa, en la cual se busca aplicar la innovación para brindar soluciones más efectivas a los clientes y partes interesadas.

3.2. De conformidad con lo anterior, es relevante que la institución disponga de los controles necesarios para garantizar razonablemente la seguridad de la información de sus clientes, conforme al marco regulatorio y prácticas aplicables, en procura del uso eficiente de los recursos asignados y el cumplimiento de los objetivos pretendidos.

3.3. Sin embargo, con base en los resultados obtenidos, se determinaron debilidades en la seguridad de la información relacionadas con la disponibilidad, integridad y confidencialidad de la información, las cuales requieren de acciones correctivas que permitan a la Administración fortalecer la continuidad de negocio municipal, los sistemas de información en temas tales como la documentación, la gestión de identidades, el principio del mínimo privilegio y segregación de funciones, el mantenimiento de usuarios, la confidencialidad de los datos y la estandarización de la bitácoras de las transacciones. Además, se identificaron debilidades relacionadas con los controles implementados para asegurar la seguridad de la información en los procesos operativos, por cuanto, no existe uniformidad en su aplicación en diferentes unidades de negocio que cuentan con habilitación por medio del sistema para la ejecución de trámites.

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, JOHNNY ARAYA MONGE, ALCALDE DE LA MUNICIPALIDAD DE SAN JOSÉ O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Elaborar, aprobar y divulgar el Sistema de Gestión de la Continuidad del Negocio, que contemple al menos: 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 plan de continuidad de negocio (BCP), c) el plan de recuperación de desastre (DRP), d) el análisis de impacto de negocio (BIA) e) plan de continuidad de negocio de forma tal que se subsanen las debilidades comentadas en este informe (Ver párrafos del 2.4 a 2.16). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) El cronograma debidamente aprobado y divulgado, que contenga las acciones, plazos y responsables para la planificación, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Continuidad del Negocio solicitado a más tardar el 31 de marzo de 2023.

ii) Informes semestrales, a más tardar el 31 de julio de 2023, 22 de diciembre de 2023 y 28 de junio de 2024, donde se haga constar el avance respecto a la implementación del Sistema de Gestión de la Continuidad del Negocio.

iii) Un oficio en el que se haga constar que se elaboró, se aprobó y se divulgó el Sistema de Gestión de la Continuidad del Negocio solicitado a más tardar el 20 de diciembre de 2024.

4.5. Actualizar, aprobar y divulgar las Normas Generales de Seguridad Informática, considerando al menos lo relacionado con a) la continuidad de negocio (Ver párrafos del 2.4 a 2.16), b) la documentación de sistemas, c) la gestión de identidades y el principio del mínimo privilegio, d) el mantenimiento de usuarios y permisos, e) la confidencialidad de los datos de los sistemas y f) las herramientas que permitan dar seguimiento del cumplimiento por parte del personal, de forma tal que se subsanen las debilidades comentadas en este informe (Ver párrafos del 2.17 a 2.27). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el que se haga constar que se elaboraron, aprobaron y divulgaron las Normas Generales de Seguridad Informática a más tardar el 31 de julio de 2023.

ii) Un oficio en el que se haga constar el avance respecto a la implementación de las Normas Generales de Seguridad Informática a más tardar el 30 de noviembre de 2023.

4.6. Definir, aprobar, divulgar e implementar los controles para salvaguardar la integridad de los datos de las propiedades de los contribuyentes y sus tributos, considerando acciones para garantizar que esos controles sean aplicados de manera uniforme y consistente por todas las unidades de negocio que tengan funciones vinculadas a los procesos de bienes inmuebles y servicios urbanos (Ver párrafos del 2.45 a 2.54). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el que se haga constar que se definieron, se aprobaron y se divulgaron los controles solicitados a más tardar el 31 de mayo de 2023.

ii) Un oficio en el que se haga constar el avance respecto a la implementación de los controles solicitados a más tardar el 31 de octubre de 2023.

4.7. Definir e implementar medidas específicas para: a) revisar la asignación de roles y perfiles de los procesos correspondientes a la gestión de patentes, bienes inmuebles y servicios urbanos de conformidad con la segregación de funciones y el principio del mínimo privilegio, b) solicitar a la DTIC el ajuste de los roles o permisos inconsistentes en los usuarios actuales (Ver párrafos del 2.17 a 2.27). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el que se haga constar que se definieron las medidas específicas solicitadas a más tardar el 31 de marzo de 2023.

ii) Un oficio en el que se haga constar el avance en la implementación de las medidas solicitadas a más tardar el 31 de julio de 2023.

4.8. Elaborar, aprobar y divulgar un procedimiento que contemple las acciones, plazos y responsables para: a) determinar cuáles son las bitácoras y reportes que se requiere visualizar para realizar las funciones de seguimiento y control de los procesos correspondientes a la gestión de patentes, bienes inmuebles y servicios urbanos, b) gestionar con la DTIC su visualización en sistemas y c) gestionar con las unidades usuarias su implementación en el seguimiento y control de sus funciones, de forma tal que se subsanen las debilidades comentadas en este informe (Ver párrafos del 2.28 a 2.44). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el que se haga constar que se elaboró, se aprobó y se divulgó el procedimiento solicitado a más tardar el 30 de junio de 2023.

ii) Un oficio en el que se haga constar el avance respecto a la implementación del procedimiento aprobado a más tardar el 31 de octubre de 2023.

4.9. Definir, aprobar e implementar los mecanismos de control para revisar que la asignación de roles y perfiles de todos los funcionarios del sistema cumpla con el principio del mínimo privilegio (PoLP) y la segregación de funciones (Ver párrafos del 2.45 a 2.54). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el cual se haga constar que se definieron y aprobaron los mecanismos de control solicitados, a más tardar el 31 de mayo de 2023.

ii) Un oficio donde se detalle el avance de su implementación a más tardar el 31 de octubre de 2023.

4.10. Realizar un informe que contemple los resultados del análisis de las transacciones ejecutadas sobre el pendiente de patentes y bienes inmuebles para determinar si los movimientos corresponden a lo definido según los procedimientos, roles y perfiles asignados a los usuarios (Ver párrafo 2.17 y párrafos 2.45 a 2.54). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República un oficio en el que conste que se elaboró el informe citado, a más tardar el 28 de abril de 2023.

4.11. Definir, aprobar e implementar los controles automatizados e integrados que le permitan vincular los movimientos al pendiente con los recibos, pagos o depósitos (Ver párrafos del 2.45 a 2.54). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el cual se haga constar que se definieron y aprobaron los controles solicitados a más tardar el 31 de mayo de 2023.

ii) Un oficio en el cual se detalle el avance de su implementación a más tardar el 30 de noviembre de 2023.

AL SEÑOR, CARLOS MONTERO PANIAGUA, JEFE DE LA SECCIÓN DE PATENTES DE LA MUNICIPALIDAD DE SAN JOSÉ O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.12. Elaborar, formalizar e implementar un procedimiento para la depuración y revisión periódica de la calidad de la información almacenada en el sistema SIAP con el fin de asegurar la confiabilidad, integridad, utilidad y oportunidad de la información mediante la identificación de errores o desviaciones en la información ingresada en el sistema, su corrección oportuna, actividades de depuración mediante los cuales se subsanen las situaciones identificadas en este informe (Ver párrafos del 2.28 a 2.44). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el que se haga constar que se elaboró y se formalizó el procedimiento solicitado a más tardar el 30 de junio de 2023.

ii) Un oficio en el que se haga constar el avance respecto a la implementación del procedimiento aprobado a más tardar el 31 de octubre de 2023.

AL SEÑOR, CARLOS GARITA CABEZAS, DIRECTOR DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA MUNICIPALIDAD DE SAN JOSÉ O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.13. Elaborar, formalizar e implementar un procedimiento para estandarizar la aplicación de movimientos masivos que se tramitan en los procesos de patentes y servicios urbanos y bienes inmuebles en el cual se definan, al menos, las actividades, responsables y estructura de los campos con el fin de evitar el ingreso de información inconsistente en las bitácoras y subsanar las debilidades de este informe (ver párrafos del 2.28 a 2.44). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General de la República:

i) Un oficio en el que se haga constar que se elaboró y se formalizó el procedimiento solicitado a más tardar el 31 de julio de 2023.

ii) Un oficio en el que se haga constar el avance respecto a la implementación del procedimiento aprobado a más tardar el 30 de noviembre de 2023.

4.14. Elaborar, aprobar e implementar un plan de remediación de las vulnerabilidades sobre seguridad de la información comunicadas mediante el oficio n°. DFOE-LOC-OI-00001-2023 (DFOE-LOC-268) del 01 de febrero de 2023, considerando al menos las acciones requeridas para subsanar las debilidades identificadas y los planes de mitigación cuando corresponda, así como los plazos de ejecución, los responsables y los mecanismos para supervisar el avance en dicha remediación (Ver párrafos del 2.55 al 2.65). Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Un oficio en el cual se haga constar que se elaboró el plan solicitado, a más tardar el 31 de marzo de 2023.

ii) Remitir informes donde se haga constar el avance respecto a la implementación del plan de remediación de las vulnerabilidades sobre seguridad de la información para el 31 de julio de 2023 y el 30 de noviembre de 2023.

4.15. Elaborar, aprobar e implementar mecanismos para monitorear e identificar posibles riesgos y vulnerabilidades relacionados con la seguridad de la información, que les permitan tomar decisiones oportunas para reducir el impacto de estos riesgos en los procesos del negocio, ese mecanismo debe considerar al menos las acciones, los responsables, la generación de informes y su periodicidad, de forma tal que se subsanen las debilidades comentadas en este informe (Ver párrafos del 2.55 al 2.65). Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor:

i) Un oficio en el cual se haga constar que se elaboraron los mecanismos solicitados a más tardar el 31 de julio de 2023.

ii) Un oficio donde se detalle el avance de su implementación a más tardar el 22 de diciembre de 2023.

4.16. Diseñar, aprobar, comunicar e implementar un programa de sensibilización en materia de seguridad de información que cubra a todo la Municipalidad. Al respecto, se deberá elaborar el material respectivo, ejecutar el programa de sensibilización y llevar a cabo actividades de reforzamiento en el tiempo para asegurar que el esfuerzo es sostenido. Además las actividades realizadas deberán documentarse adecuadamente (Ver párrafos del 2.55 a 2.65). Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General:

i) Un oficio donde se haga constar que se diseñó, aprobó, comunicó e inició el programa de sensibilización, a más tardar el 29 de setiembre de 2023.

ii) Un informe en el que se detalle el grado de avance en la implementación y los pendientes así como las actividades programadas para asegurar la sostenibilidad del programa de sensibilización, a más tardar el 22 de diciembre de 2023.

Firmado digitalmente por
VIVIAN GARBANZO NAVARRO
Fecha: 2023-02-23 12:14

Licda. Vivian Garbanzo Navarro
Gerente de Área

Firmado digitalmente por FRANCISCO JAVIER
HERNANDEZ HERRERA
Fecha: 2023-02-23 12:05

Lic. Francisco Hernández Herrera
Asistente Técnico

Firmado digitalmente por MARCELA RAMIREZ
ROJAS
Fecha: 2023-02-23 12:23

MATI. Marcela Ramírez Rojas
Coordinadora

Firmado digitalmente por GUIDO
ALBERTO ARQUIN LOBO
Fecha: 2023-02-23 12:15

Lic. Guido Arquín Lobo
Colaborador

Firmado digitalmente por KEVIN RODRIGUEZ
MUÑOZ
Fecha: 2023-02-23 12:17

Lic. Kevin Rodríguez Muñoz
Colaborador