Municipalidad de San Carlos
Departamento de Auditoría Interna
Calle Central – Avenida 2. Apdo. 13. 4400.
Ciudad Quesada, San Carlos, Alajuela, Costa Rica

02 de octubre de 2024

INFORME-MSCCM-AI-011-2024

MUNICIPALIDAD DE SAN CARLOS

AUDITORÍA INTERNA

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Octubre, 2024

02 de octubre de 2024

INFORME-MSCCM-AI-011-2024

TABLA DE CONTENIDO

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Índice de Ilustraciones

Índice de Tablas

02 de octubre de 2024

INFORME-MSCCM-AI-011-2024

RESUMEN EJECUTIVO

El presente informe evalúa la seguridad de la información y ciberseguridad del Departamento de Tecnologías de la Información y Comunicación (TIC) de la Municipalidad de San Carlos. Este estudio fue realizado como parte del Plan Anual de Trabajo PAI-2024-03, y coordinado por la Contraloría General de la República (CGR), con el objetivo de fiscalizar la gestión de seguridad de la información y ciberseguridad en la institución.

En lo referente a guía de avance en el mismo se presentan tanto el objetivo general que contempla el evaluar si los procesos de gestión de seguridad de la información y ciberseguridad están alineados con el marco jurídico y técnico pertinente y los objetivos específicos que en concreto abarcan detalles como la gestión de la seguridad, la gestión de datos y la gestión de los servicios de seguridad.

Para este estudio el alcance y la metodología contemplan que el mismo abarca el segundo semestre de 2023, con posibilidad de ampliación según la necesidad. Se evaluaron la seguridad de la información y ciberseguridad que el departamento de TIC aplica para verificar el cumplimiento normativo, identificar brechas y proponer mejoras institucionales. La metodología incluyó la revisión de políticas de seguridad, la infraestructura de ciberseguridad, los estándares de seguridad, la evaluación de la exposición a amenazas, y la efectividad de los sistemas de seguridad en la Municipalidad.

Es importante mencionar algunos resultados clave, entre los que figuran:

Políticas de Seguridad de la Información TIC: Aunque la Municipalidad ha establecido Normas de TIC, se encontró que no se han publicado ni comunicado adecuadamente a los empleados y partes externas relevantes. Este es un punto crítico, ya que la falta de comunicación sobre estas normas podría comprometer la seguridad y el cumplimiento normativo en el ámbito de las TIC.

Gestión de Contraseñas y Autenticación: Se identificó una deficiencia en la gestión de contraseñas, ya que no se están cumpliendo con las mejores prácticas, como el almacenamiento de un historial de contraseñas anteriores. Esto puede debilitar la seguridad de los sistemas municipales.

Autenticación Multifactor (en adelante MFA): No se ha implementado MFA en los usuarios, herramientas y entornos del dominio, lo que representa un riesgo significativo en términos de protección contra accesos no autorizados. La falta de MFA aumenta la vulnerabilidad de la infraestructura tecnológica de la Municipalidad.

En cuanto al cumplimiento de Normas Internacionales, se toma como referencia la aplicación de normas y estándares internacionales como ISO/IEC 27001:2023, NIST SP 800-53 Rev. 4, COBIT 5, CIS CSC, ISA 62443-2-1:2009 e ISA 62443-3-3:2013.

Sobre la elaboración e implementación de planes como el Plan de Respuesta y Plan de Recuperación ante Incidentes de Seguridad: Se detecta que no se cuenta con estos planes o programas por lo que es de recomendar la creación y ejecución de los respectivos planes, incluyendo pruebas periódicas para asegurar su efectividad. Este tipo de acciones son esenciales para mitigar riesgos de ciberataques y garantizar la continuidad operativa de las operaciones de la Municipalidad.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

02 de octubre de 2024

INFORME-MSCCM-AI-011-2024

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

I. INTRODUCCIÓN.

1.1. Origen del Estudio.

El presente estudio se origina de conformidad con lo dispuesto en el Plan Anual de Trabajo PAI-2024-03 para el período 2024 de la Auditoría Interna de esta Municipalidad. Estudio especial coordinado por la Contraloría General de la República (CGR), con miras a fiscalizar la gestión de seguridad de la información y ciberseguridad.

1.2. Objetivo general.

Determinar si los procesos de gestión de seguridad de la información y ciberseguridad de la Municipalidad de San Carlos están razonablemente alineados con el marco jurídico y técnico relacionado

1.2.1. Objetivos específicos.

- Gestionar la seguridad
- Gestionar los datos
- Gestionar los servicios de seguridad.

1.3. Alcance del estudio.

Este estudio de auditoría abarca el periodo del II Semestre de 2023, con la posibilidad de ampliarse según la pertinencia y necesidades identificadas durante la ejecución del mismo. El alcance inicial incluye la evaluación de seguridad de la información y ciberseguridad del departamento de TIC, con miras a verificar el cumplimiento normativo, identificar brechas de seguridad y proponer mejoras en la gestión de seguridad de la información y ciberseguridad.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

1.4. Metodología General Aplicada

El desarrollo de esta auditoría se llevó a cabo mediante análisis utilizando datos proporcionados por el jefe del departamento de TIC, así como por los colaboradores que él mismo designó, además se realizó solicitud de información o evidencia probatoria a otros departamentos sobre temas concernientes a este estudio. En el contexto de las técnicas de auditoría, se implementaron las siguientes:

Técnicas de auditoría que se implementan en el estudio de carácter especial sobre Seguridad de la Información y Ciberseguridad mediante la aplicación de las herramientas aportadas por la CGR.

a) Revisión de la política de seguridad y documentación relevante: Evaluar la política de seguridad actual para verificar que esté alineada con los objetivos de la institución y las regulaciones o estándares pertinentes.

b) Identificación de prioridades y riesgos potenciales: Determinar los posibles riesgos que podrían afectar la seguridad de la información.

c) Revisión de la infraestructura de ciberseguridad existente: Analizar la eficacia de las medidas de seguridad actuales.

d) Verificación de los estándares de seguridad: Comparar las prácticas actuales con los estándares de seguridad reconocidos para identificar áreas de mejora.

e) Cambios y responsabilidades del personal de seguridad: Identificar las áreas que necesitan mejorar las brechas en la seguridad.

f) Evaluación del nivel de exposición a amenazas y ciberataques: Determinar el grado de vulnerabilidad de la Municipalidad a diferentes tipos de amenazas y ataques cibernéticos.

g) Análisis de la eficiencia de los sistemas y programas instalados: Evaluar si los sistemas y programas actuales son eficientes y efectivos en la protección de la información.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

h) Valoración de la robustez de las contraseñas empleadas por el personal: Verificar si las contraseñas utilizadas por el personal son seguras y cumplen con las políticas de seguridad de la institución.

1.5. Limitaciones.

El presente informe de auditoría se desarrolló bajo ciertas limitaciones, es importante mencionar la anuencia de los funcionarios auditados a brindar la información, sin embargo, se presentaron limitaciones inherentes al alcance, y al aplicar la metodología mediante las herramientas facilitadas por la CGR esta generó retrasos en los tiempos y plazos de entrega de la información y documentación por parte de TIC.

Cabe mencionar también que entre las limitantes se identifica la falta de acceso a la información, para la auditoría, necesaria para llevar a cabo una evaluación exhaustiva de documentos, registros y datos relevantes.

De igual forma la falta de acceso al contenido de normas y estándares, como NIST SP 800-53 Rev. 4, ISA 62443(2009 y 2013), CIS CSC y COBIT 5, ISO/IEC 27001:2023, limitó el acceso inmediato para realizar comparaciones detalladas.

Por último, se considera la existencia de algunas vulnerabilidades que pueden no haber sido detectadas debido a limitaciones y especificidades en las herramientas de evaluación o a la falta de visibilidad en todos los entornos tecnológicos.

1.6. Cumplimiento de Normas Técnicas de Auditoría.

El estudio se realizó con observancias a las Normas para el Ejercicio de la Auditoría Interna en el Sector Público[1]; el Manual de Normas Generales de Auditoría para el Sector Público[2], Reglamento de la Institución y Funcionamiento de la Auditoría Interna[3], entre otras y donde resulten aplicables.

[1] La Gaceta Nº. 28 del 10/02/2010
[2] Resolución del Despacho de la Contralora General, N° R-CO-xx-20xx
[3] La Gaceta Nº. xxx del xx/xx/20xx

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

1.7. Normas técnicas a cumplir.

Los resultados y la implantación de las recomendaciones del presente informe, se regirá entre otros, por lo dispuesto en los artículos 36, 37, 38 y 39 de la Ley General de Control Interno, los cuales en la parte que interesa señalan literalmente lo siguiente:

Las recomendaciones que se plantean en los diferentes informes de Auditoría, los cuales transcribimos a continuación.

> *"Artículo 36. —Informes dirigidos a los titulares subordinados. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*
>
> *c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*
>
> *Artículo 37. —Informes dirigidos al jerarca. Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo*

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.

Artículo 38. —Planteamiento de conflictos ante la Contraloría General de la República. Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

Artículo 39. —Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios.

El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable. (...)

(...) Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente.

El jerarca, los titulares subordinados y los demás funcionarios públicos también incurrirán en responsabilidad administrativa y civil, cuando corresponda, por obstaculizar o retrasar el cumplimiento de las potestades del auditor y los demás funcionarios de la auditoría interna, establecidas en esta Ley.

Cuando se trate de actos u omisiones de órganos colegiados, la responsabilidad será atribuida a todos sus integrantes, salvo que conste, de manera expresa, el voto negativo"

1.8. Comunicación preliminar de resultados

La comunicación preliminar de los resultados producto de la auditoría elaborada en el presente informe, se llevó a cabo en las instalaciones de la Municipalidad de San Carlos, específicamente en la oficina de Auditoría Interna, el día 30 de agosto 2024 a las 02:30 p.m. mediante oficio de convocatoria MSCCM-AI-0164-2024, estando presentes los siguientes funcionarios de la Municipalidad de San Carlos: Ing. Juan Diego González Picado, alcalde, Msc. Henry Saul Brenes Sandoval, jefe de TIC, y la Licda. Sandra Pérez Araya, jefa de Contabilidad, y Lic. Jimmy Segura Rodriguez, jefe de Control Interno, de parte de Auditoría Interna el Lic. Fernando Chaves Peralta, Auditor Interno, Licda. Roxana Guzmán Mena, Supervisora de Calidad y Lic. José Marcial Vargas Arguedas como Asistente de Auditoría.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

II. RESULTADOS

Antecedentes

Es importante mencionar como antecedente relevante que desde el 2009 el departamento de TIC de esta Municipalidad se rige por las Normas de TI (MP-TIC-001-2011), Aprobado por el Concejo Municipal, en Sesión Ordinaria celebrada el 25 de abril de 2011, mediante Artículo N° 30, Acta N° 27, las cuales se derivan de Las “Normas Técnicas para la Gestión y Control de las Tecnologías de Información” (N-2-2007-CO-DFOE), resolución N° R-CO-26-2007, elaborado por la Contraloría General de la República; cabe destacar que estás normas fueron derogadas mediante resolución R-DC-17-2020[4].

Además, actualmente en vista de la constante evolución, aplica para TIC lo que establece el MICITT en materia de marco de gobierno, basado en los cambios que se presentan y aplican para el sector público.

2.1. Políticas de seguridad de la información TIC.

2.1.1. Sobre la definición, publicación y comunicación.

El hallazgo 2.1.1. se centra en la definición, publicación y comunicación de las Normas de TIC. Aunque la evidencia aportada reconoce la existencia de estas normas, no se demuestra su publicación y comunicación a los empleados y partes externas relevantes. Este hallazgo se basa en el criterio establecido por varias normativas relevantes al tema, que incluyen **CIS CSC 19**, los dominios de **COBIT 5: APO01.03, APO13.01, EDM01.01, EDM01.02**, **ISA 62443-2-1:2009 4.3.2.6**, **ISO/IEC 27001:2023, Control 5.1**, y los controles de todas las familias de control de seguridad de **NIST SP 800-53 Rev. 4-1**.

La causa de este hallazgo radica en que la resolución a lo consultado carece de evidencia de registro de publicación y comunicación de las normas de TI a los empleados y partes externas relevantes. Este hallazgo tiene varios efectos potenciales.

4 Resolución R-DC-17-20204, del 17 de marzo del 2020 emitida por la Contraloría General de la República la cual entro en vigencia a partir del 27 de marzo 2020.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

La falta de comunicación de las políticas de seguridad de la información de TIC tanto a los usuarios internos como a las entidades externas puede incrementar significativamente el riesgo de incidentes de seguridad, incumplimiento normativo, pérdida de datos, daños, así como la interrupción de la continuidad de los servicios que brinda la institución. Algunos de estos riesgos incluyen brechas de seguridad, violaciones de confidencialidad, ataques cibernéticos, afectación a la reputación y pérdidas financieras.

Es esencial que la institución mantenga programas de concientización y capacitación en seguridad para garantizar que todos los empleados comprendan y cumplan con las políticas de seguridad establecidas. Además, la comunicación adecuada de estas políticas a las entidades externas es crucial para mitigar los riesgos asociados.

El cumplimiento de las normativas de seguridad de la información refuerza la importancia de definir, publicar y comunicar adecuadamente las normas de TI. La falta de cumplimiento con estos estándares puede tener implicaciones significativas para la seguridad de la información de la institución. Por lo tanto, es crucial que se tomen medidas para abordar este hallazgo y garantizar la conformidad con todas las normativas mencionadas, protegiendo así la integridad de la institución y sus servicios.

2.1.2. Sobre revisión de las políticas.

Se ha observado la condición de ausencia de evidencia sobre los intervalos de revisión de las políticas. Este hallazgo se basa en los criterios establecidos por la ISO/IEC 27001:2023, Controles 5.1, 5.10, 7.10 y 7.11, el NIST SP 800-53 Rev. 4 AC-1, que se refiere a la Política y Procedimientos de Control de Acceso. Este control establece la necesidad de desarrollar, documentar y difundir políticas y procedimientos para la implementación efectiva de los controles de acceso seleccionados y sus mejoras y el COBIT 5: EDM01.02 que contempla acciones de dirección de la gobernanza de TI.

La causa identificada para esta condición es la falta de evidencia que demuestre la planificación de intervalos de revisión de la normativa pertinente. Esta situación puede tener efectos significativos.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

La falta de revisión periódica de las políticas de seguridad de la información puede llevar a su desactualización, lo que a su vez puede resultar en la implementación de medidas de seguridad inadecuadas. Además, las políticas desactualizadas pueden dejar de cumplir con los requisitos legales o normativos actuales, exponiendo a la Municipalidad a posibles sanciones o a la pérdida de confianza de clientes o usuarios, proveedores de bienes y servicios, contratistas, consultores u otras entidades públicas o privadas.

Además, en ausencia de revisiones regulares, las políticas pueden dejar de abordar de manera efectiva los riesgos emergentes o los cambios en las amenazas. Esto puede resultar en una gestión de la seguridad de la información que es medianamente eficaz, con posibles consecuencias graves en términos de ataques cibernéticos o informáticos.

Por último, las políticas desactualizadas pueden estar desalineadas con los objetivos estratégicos de la Municipalidad, afectando la eficiencia y la efectividad de los controles de seguridad. También puede haber confusión y falta de conciencia entre los empleados si la comunicación de las políticas actualizadas es poco efectiva, lo que puede conducir a malentendidos y errores en la implementación.

2.2. Seguridad de acceso, información de autenticación.

2.2.1. Sobre Gestión de la Identidad y Acceso de los Usuarios.

Durante el estudio y de acuerdo a las consultas realizadas y la respuesta dada mediante el oficio MSC-AM-TI-2024-0070, se identificó que la configuración del historial de contraseñas en Active Directory solo recuerda una contraseña anterior, así como tampoco se evidencia el uso de MFA, esto se percibe en la siguiente imagen:

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Ilustración 1

Política de contraseñas para los usuarios del dominio

2. Se implementa como políticas de grupo para todos los usuarios del dominio la siguiente política de contraseñas:

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	Habilitada
Auditoría de longitud mínima de contraseña	No está definido
Exigir historial de contraseñas	1 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	8 caracteres
Reducir los límites de longitud mínima de la contraseña	No está definido
Vigencia máxima de la contraseña	30 días
Vigencia mínima de la contraseña	0 días

Imagen 1 "políticas de grupo del Active Directory"

Nota: Tomado de oficio MSC-AM-TI-2024-70

Para la configuración del historial de contraseñas, los siguientes estándares y normativas establecen importantes pautas de buenas prácticas en la gestión de contraseñas, sin embargo, muchas de estas como se observa en la anterior imagen contravienen la siguiente normativa: **ISO/IEC 27001:20|23:** Controles 5.17 y 5.36, que abordan la gestión de contraseñas y controles de acceso.

CIS CSC: Controles 1, 5, 12, 15 y 16, que recomiendan la implementación de políticas robustas de gestión de contraseñas.

NIST SP 800-53 Rev. 4: Controles AC-2, IA-5, SI-4 y CM-6, que proporcionan directrices específicas para la gestión de identidades y accesos, integridad de la información, y configuración segura.

Política de Grupo de Active Directory: "Enforce password history" según la documentación de Windows 10 de Microsoft Learn.

De igual forma se deja en inobservancia lo que establece el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica en el documento **MICITT-DGD-DRII-AT-127-2022** y en la **Directriz N° 133-MP-MICITT:** Instrucciones adicionales del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones; Además, **Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE):** Capítulo I, Puntos de control 1.4.4 y 1.4.5, que abarcan temas de seguridad en las operaciones y comunicaciones, así como el control de acceso.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

También, **COBIT 5: DSS05.03, DSS05.04, DSS06.03**: enfatiza en estos dominios la gestión de seguridad de usuarios finales, la gestión de identidad de usuarios y acceso lógico, incluyendo la administración de roles, privilegios y niveles de autorización. También, cabe referirse a la norma **ISA 62443-3-3:2013**, en los Requisitos de Sistema SR 1.1, SR 1.2, SR 1.5 y SR 1.7, la cual abarca aspectos sobre Identificación y autenticación de usuarios, el control de acceso (Políticas y mecanismos para restringir el acceso a recursos según roles y permisos definidos), el Control de sesiones contemplando la gestión y control de sesiones de usuario, incluyendo la terminación de sesiones inactivas y también gestión de contraseñas que se enfoca en requisitos para la creación, almacenamiento y manejo seguro de contraseñas.

Basado en el oficio MSC-AM-TI-2024-0070 y en los cuestionarios suministrados por la CGR sobre seguridad de la información ISO/IEC 27001:2023 y de ciberseguridad apoyado en NIST CSF y otras normas de referencia, se determinó que la configuración actual del historial de contraseñas en Active Directory se ha configurado con un nivel de seguridad muy débil ya que permite recordar únicamente una contraseña anterior, además de la ausencia de implementación de (MFA).

Por tanto y como consecuencia de esta realidad, es importante mencionar que configurar el historial de contraseñas de Active Directory para recordar únicamente una contraseña anterior y la falta de implementar la MFA puede tener consecuencias negativas y significativas para la seguridad de la Municipalidad. La configuración actualmente establecida permite la reutilización frecuente de contraseñas, incrementando el riesgo de que contraseñas previamente comprometidas sean reutilizadas por los usuarios. En caso de que un atacante haya obtenido una contraseña anterior, podría intentar utilizarla nuevamente con mucho mayor éxito, incrementando este riesgo el que la configuración de cuentas actual no contempla MFA.

Además, esta configuración facilita la exposición a ataques de fuerza bruta y ataques de diccionario, ya que los atacantes pueden adivinar con mayor facilidad las contraseñas antiguas. La capacidad de recordar solo una contraseña anterior y la ausencia de MFA reduce la efectividad de las políticas de contraseñas para prevenir accesos no autorizados, debilitando así las demás barreras de seguridad implementadas.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

En el caso de que un atacante logre comprometer una contraseña, se incrementa el riesgo de acceso no autorizado a la red institucional (red de dominio) en la cual se administra información confidencial. Esto puede derivar en incidentes de seguridad significativos y problemas de cumplimiento con regulaciones y estándares de seguridad. Por lo tanto, la insuficiencia en el historial de contraseñas y la falta de MFA comprometen la seguridad integral de la infraestructura de TI, aumentando su vulnerabilidad frente a ataques y amenazas cibernéticas.

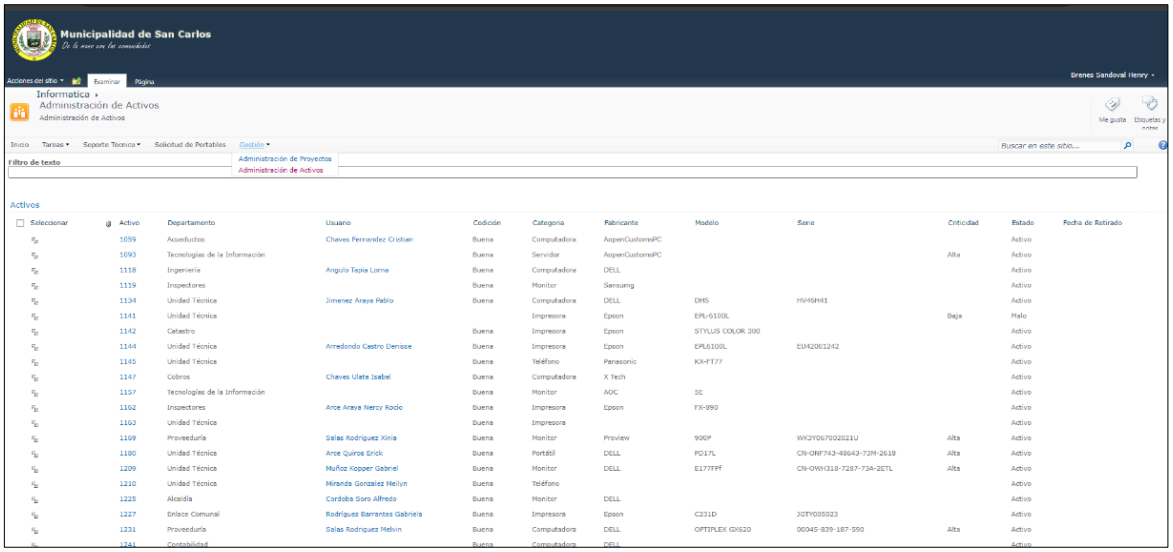
2.3. Uso aceptable de la información y otros activos asociados

2.3.1. Sobre Gestión de activos y Protección de la Información

El registro de activos tecnológicos en la Municipalidad es administrado en diferentes herramientas o sistemas, según lo evidenciado en los cuestionarios aplicados el departamento de TIC registra en SharePoint (ver ilustración 2), el departamento de Contabilidad lo hace en el sistema SAF, y por otra parte TIC también comunica que utiliza ManageEngine (ver *ilustración 3) para monitorear la cantidad de equipos en la red, sin detalles específicos de los activos, dejando en evidencia múltiples diferencias en los detalles de registro de dichos activos.*

Ilustración 2

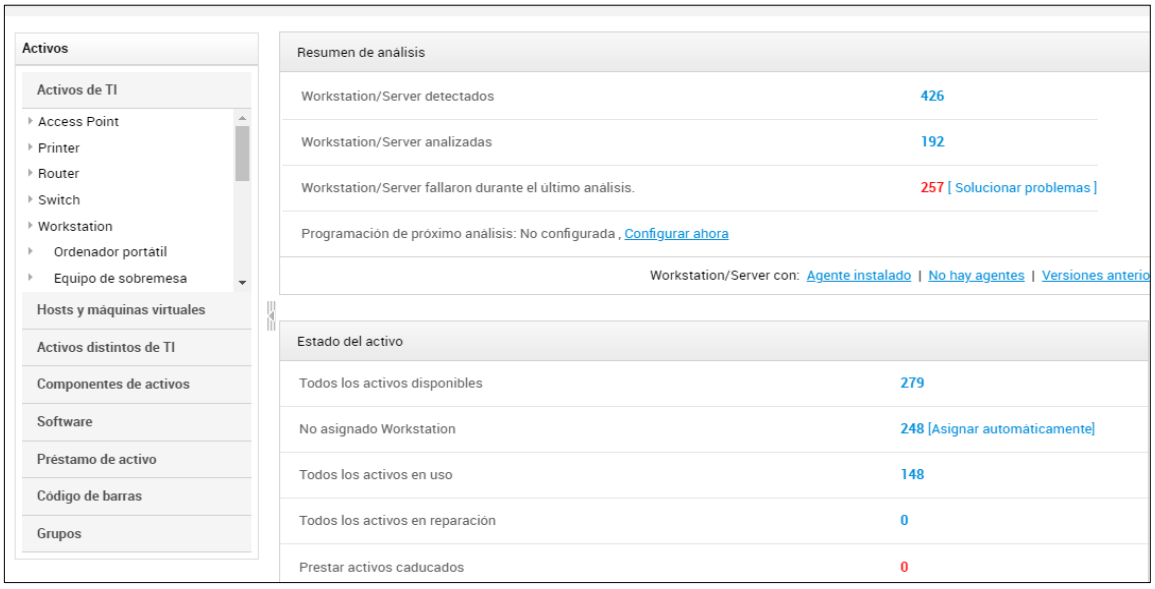
Control de activos en SharePoint



Nota: Tomado de evidencia aportada por TIC para cuestionario de Control - Seguridad de la Información

Ilustración 3

Control de activos en ManageEngine



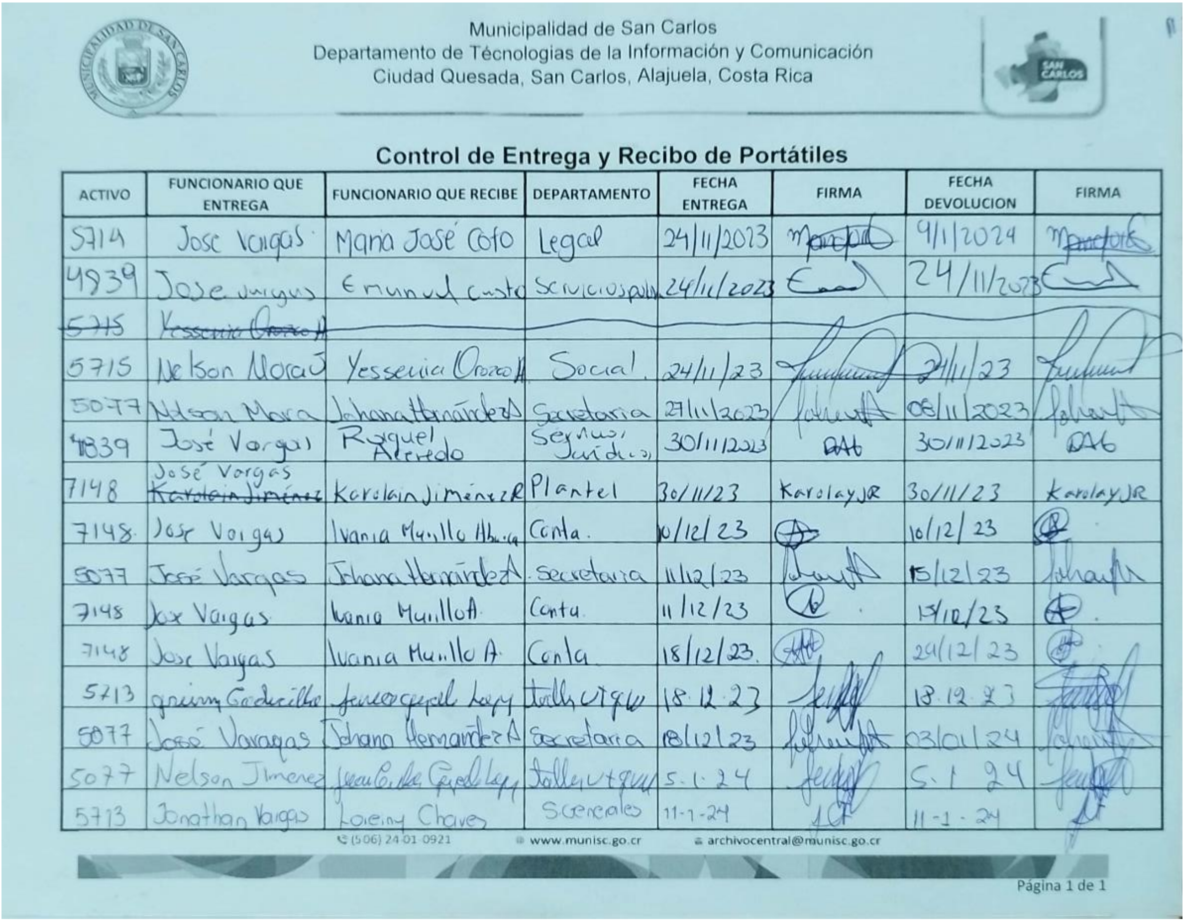
Nota: Tomado de evidencia aportada por TIC para Cuestionario Ciberseguridad basado en NIST CSF

Además de lo anterior, cabe referirse al préstamo de equipos y la entrega de suministros, los cuales se realizan de forma manual (ver ilustraciones 4 y 5), lo que expone una debilidad en el monitoreo o control por cuanto evidencia la falta de un sistema de registro y control centralizado.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Ilustración 4

Control préstamo de equipos



Municipalidad de San Carlos
Departamento de Técnologias de la Información y Comunicación
Ciudad Quesada, San Carlos, Alajuela, Costa Rica

Control de Entrega y Recibo de Portátiles

ACTIVO	FUNCIONARIO QUE ENTREGA	FUNCIONARIO QUE RECIBE	DEPARTAMENTO	FECHA ENTREGA	FIRMA	FECHA DEVOLUCION	FIRMA
5714	Jose Vargas	Maria José Coto	Legal	24/11/2023	[illegible]	9/1/2024	[illegible]
4939	Jose Vargas	Emanuel Castro	Servicios publ.	24/11/2023	[illegible]	24/11/2023	[illegible]
~~5715~~	~~Yessenia Orozco A~~						
5715	Nelson Mora J	Yessenia Orozco A	Social	24/11/23	[illegible]	24/11/23	[illegible]
5077	Nelson Mora	Johana Hernández A	Secretaria	27/11/2023	[illegible]	08/11/2023	[illegible]
4839	José Vargas	Raquel Alvarado	Servicios Jurídicos	30/11/2023	DAb	30/11/2023	DAb
7148	José Vargas ~~Karolain Jiménez~~	Karolain Jiménez R	Plantel	30/11/23	Karolay JR	30/11/23	Karolay JR
7148	Jose Vargas	Ivania Murillo Alvarado	Conta.	10/12/23	[illegible]	10/12/23	[illegible]
5077	José Vargas	Johana Hernández A	Secretaria	11/12/23	[illegible]	15/12/23	[illegible]
7148	Jose Vargas	Ivania Murillo A	Conta	11/12/23	[illegible]	15/12/23	[illegible]
7148	Jose Vargas	Ivania Murillo A	Conta	18/12/23	[illegible]	24/12/23	[illegible]
5713	[illegible]	[illegible]	taller UTGV	18.12.23	[illegible]	18.12.23	[illegible]
5077	José Varagas	Johana Hernandez A	Secretaria	18/12/23	[illegible]	03/01/24	[illegible]
5077	Nelson Jimenez	[illegible]	taller UTGV	5.1.24	[illegible]	5.1.24	[illegible]
5713	Jonathan Vargas	Loreiny Chaves	S. Generales	11-1-24	[illegible]	11-1-24	[illegible]

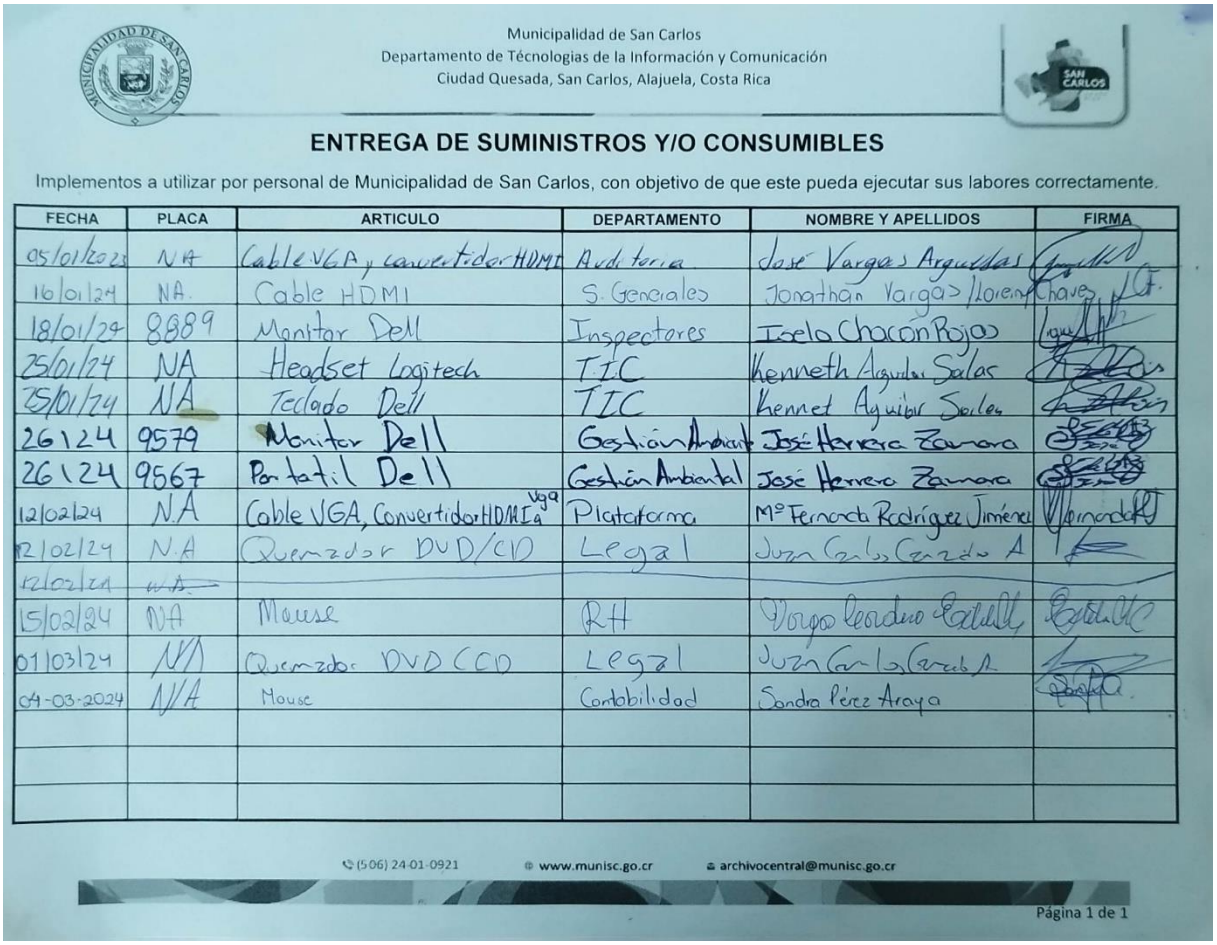
(506) 24 01 0921 www.munisc.go.cr archivocentral@munisc.go.cr

Página 1 de 1

Nota: Tomado de evidencia aportada por TIC para cuestionario de Control - Seguridad de la Información

Ilustración 5

Control entrega de suministros y consumibles



Municipalidad de San Carlos
Departamento de Técnologias de la Información y Comunicación
Ciudad Quesada, San Carlos, Alajuela, Costa Rica

ENTREGA DE SUMINISTROS Y/O CONSUMIBLES

Implementos a utilizar por personal de Municipalidad de San Carlos, con objetivo de que este pueda ejecutar sus labores correctamente.

FECHA	PLACA	ARTICULO	DEPARTAMENTO	NOMBRE Y APELLIDOS	FIRMA
05/01/2024	N/A	Cable VGA y convertidor HDMI	Auditoria	José Vargas Arguedas	
16/01/24	NA.	Cable HDMI	S. Generales	Jonathan Vargas Florencio Chaves	
18/01/24	8889	Monitor Dell	Inspectores	Isela Chacón Rojas	
25/01/24	NA	Headset Logitech	TIC	Kenneth Aguilar Salas	
25/01/24	NA	Teclado Dell	TIC	Kennet Aguilar Salas	
26/1/24	9579	Monitor Dell	Gestión Ambiental	José Herrera Zamora	
26/1/24	9567	Portatil Dell	Gestión Ambiental	José Herrera Zamora	
12/02/24	N.A	Cable VGA, Convertidor HDMI a Vga	Plataforma	Mª Fernanda Rodríguez Jiménez	
12/02/24	N.A	Quemador DVD/CD	Legal	Juan Carlos Cerdas A	
12/02/24	N.A.				
15/02/24	NA	Mouse	RH	Jorge Leandro Calvo	
01/03/24	N/A	Quemador DVD CD	Legal	Juan Carlos Cerdas A.	
04-03-2024	N/A	Mouse	Contabilidad	Sandra Pérez Araya	

(506) 24-01-0921 www.munisc.go.cr archivocentral@munisc.go.cr

Página 1 de 1

Nota: Tomado de evidencia aportada por TIC para cuestionario de Control - Seguridad de la Información

Lo anterior contraviene lo que establecen algunas normas en relación al adecuado y oportuno registro de activos para una eficiente administración en el uso y disposición de los mismos.

Vale indicar que la norma **ISO/IEC 27001:2023** establece en los Controles: 5.36-“Cumplimiento de Políticas, Reglas y Estándares de Seguridad de la Información”, 5.9-“Inventario de Información y Otros Activos Asociados”, 5.10 –“Uso Aceptable de la Información y Otros Activos Asociados”, 8.8-“Gestión de Vulnerabilidades Técnicas”; normas que establecen que las organizaciones requieren identificar y documentar los activos importantes para sus operaciones y los riesgos asociados, así como tomar medidas para dar seguridad y

protección a estos. Además, **CIS CSC** 1 y 4: Se enfoca en administrar activamente (inventario, seguimiento y corrección) todos los activos empresariales conectados a la infraestructura y en establecer y mantener la configuración segura de los activos y software empresariales. También cabe exponer lo que establece **COBIT 5** en algunos de sus apartados o dominios tales como APO12.01: que hace énfasis en la recolección de datos de manera eficiente y efectiva. Además, en sus apartados APO12.02, APO12.03 y APO12.04: Enfatizan lo relacionado con riesgos contemplando la importancia de analizar el riesgo de acuerdo con las políticas y procedimientos establecidos así como el mantener un perfil de estos riesgos y articular adecuadamente el riesgo para ayudar a identificar y abordar las posibles amenazas en las operaciones, por otra parte, DSS05.01 que contempla la protección contra malware y DSS05.05 Gestionar la seguridad física a los activos de TI, así también en sus apartados BAI09.02 que contempla el gestionar evaluaciones críticas identificando y analizando activos clave en términos de valor, relevancia y vulnerabilidad, como también el apartado BAI09.03 hace referencia a gestionar la evaluación del ciclo de vida supervisando el ciclo de vida de cada activo desde la adquisición hasta la disposición para evaluar su uso y rendimiento.

De forma similar el CAI09.01 se enfoca en el registro de activos mediante acciones como documentar todos los activos en un registro centralizado con detalles como descripción, ubicación y valor, mas no limitándose a solo lo mencionado en el apartado CAI09.02 que abarca la necesidad de administrar activos críticos, protegerlos y mantenerlos vitales con medidas de seguridad adicionales y mantenimiento regular, al igual el CAI09.03 que se enfoca en las acciones para administrar el ciclo de vida de los activos gestionando cada etapa del ciclo de vida de un activo, desde su adquisición hasta su disposición final.

En este enfoque de protección de los activos y la información también **NIST SP 800-53 Rev. 4:** en los controles CM-8 y PM-5 aborda la información de configuración de sistemas, la protección de la información y los recursos de gestión lo que abarca, mas no se limita a detalles como documentación de configuraciones, auditoría y revisión, así como detalles de control de acceso e integridad y confidencialidad de la información.

Las anteriores normas y criterios aquí expuestos dejan en evidencia la importancia vital de contar con una adecuada gestión (administración) de activos y su consecuente protección de la información, esto por cuanto las actuales Normas del departamento de Tecnologías de

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Información de la Municipalidad de San Carlos (MP-TIC-001-2011, 2011), se encuentra vigente y contempla escuetamente el abordaje referido al procedimiento o sistema con el que se dará la atención pertinente a la gestión de activos, principalmente en el registro, esto a pesar de que en dicho manual se cita en el capítulo 6 glosario

"6.1 ACTIVOS INFORMÁTICOS

Véase "6.39 Recursos informáticos".

6.39 RECURSOS INFORMÁTICOS

Véase "6.38 Recursos de TIC".

6.38 RECURSOS DE TIC

Aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de TIC de una organización" (pág. 37).

Además, sobre la protección de la información que cita dicho manual en el "CAPÍTULO 1, sección 1.6 SEGURIDAD EN LAS OPERACIONES Y COMUNICACIONES, punto 1.6.2 Protección de la Información", contempla un abordaje muy escueto en lo que se refiere a la adecuada protección (pág. 18).

Como resultado de lo anterior, algunos posibles efectos en lo detectado y la consecuente debilidad en la protección de la información podría conllevar a que se materialicen riesgos tales como:

- Pérdida de Control y Visibilidad sobre los Activos (Riesgo de Pérdida o Robo).
- Falla en el cumplimiento Normativo (Acciones sobre presuntos responsables).
- Mayor complejidad Operativa (Mantenimiento y soporte, Documentación incompleta).
- Impacto Financiero (Costos, inversión, soporte).
- Afectación a la protección de la Información (Seguridad, pérdida de datos).
- Toma de Decisiones (Planificación).

En virtud de lo anterior se pudo evidenciar en el presente estudio de auditoría la importancia que conlleva la oportuna y adecuada gestión de activos y protección de la información para así minimizar los potenciales riesgos señalados.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

2.3.2. Sobre Medios Extraíbles, Seguridad Física y Protección de la Información.

Es respuesta a la aplicación de los cuestionarios se indicó por parte del jefe de TIC, así como en lo resuelto por parte del administrador de redes, que se dispone de una política de seguridad a nivel de antivirus para el bloqueo de puertos USB, sin embargo, mediante pruebas de verificación realizadas para este estudio de auditoría se detecta que la política está siendo insuficiente, ineficiente o vulnerable en el uso de la mayoría de equipos en los que se realizó pruebas de conexión de dispositivos extraíbles (USB).

Sobre lo detectado anteriormente se evidencia la falta de cumplimiento a normas que establecen disposiciones para la adecuada administración de medios extraíbles y su uso en los equipos de la Municipalidad.

Para ello es importante tomar en cuenta lo que exponen las normas en los siguientes criterios:

- **ISO/IEC 27001:2023:** Controles 5.11, 5.12, 5.13, 7.1, 7.4, 7.5, 7.6, 7.7, 7.10, 7.12, 8.11, 8.12, 8.33, A.8.2.2, A.11.2.9, norma en la que se abarcan criterios que vienen a establecer parámetros para la debida protección de la información de los equipos en el uso de dispositivos extraíbles, mismas que deberían estar implementadas para el resguardo y protección de los activos e información que en ellos se gestiona.
- **COBIT 5:** APO13.01, DSS05.02, DSS05.06; de igual forma esta norma viene a definir controles y monitoreo responsable de dichos equipos en el uso de dispositivos de almacenamiento extraíbles, por consiguiente, la importancia de su cumplimiento.

Con contenido similar las siguientes normas nos dan elementos para la prevención en el uso de dispositivos de almacenamiento extraíbles, por lo cual es primordial tomarlas en cuenta para minimizar el uso no autorizado de dichos dispositivos.

- **CIS CSC:** Control 8: Malware Defenses. Este control se enfoca en limitar la capacidad de ejecución de software malicioso en sistemas de la institución mediante el uso de herramientas y procesos de defensa contra malware. Control 13. Data Protection. Abarca aspectos de protección de la información confidencial tanto en tránsito como en reposo
- **ISA 62443-3-3:2013:** SR 2.3. que trata sobre el "Uso de Autenticación Multifactor". Los sistemas deben requerir autenticación multifactor para acceder a las funciones críticas,

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

sistemas importantes o datos sensibles, lo que genera significativo impacto en la restricción para dispositivos extraíbles pues aporta mayor control sobre el acceso a datos, ayuda a la detección temprana de amenazas, reduce el riesgo de filtración de datos y apoya en el cumplimiento normativo.

- NIST SP 800-53 Rev. 4: MP-2, MP-3, MP-4, MP-5, MP-7. Los controles **MP (Media Protection) están diseñados para proteger la información sensible o crítica almacenada en medios físicos o digitales.

  MP-2: Protección de Medios de Información (Media Access): contempla establecer procedimientos y controles para restringir el acceso físico o digital a los medios que contienen información sensible.

  MP-3: Marcado de Medios (Media Marking): Este control requiere que los medios de información que contienen datos sensibles sean claramente etiquetados para indicar el nivel de protección necesario, en función de la clasificación de la información.

  MP-4: Transporte de Medios (Media Transport): Este control establece como requisito Implementar medidas de protección durante el transporte físico de medios (como cifrado, escoltas, envíos seguros) para evitar su pérdida o robo.

  MP-5: Almacenamiento de Medios (Media Storage): contempla Implementar controles para almacenar medios de manera segura (por ejemplo, en bóvedas, armarios seguros) cuando no están en uso para prevenir el acceso no autorizado.

  MP-7: Eliminación de Medios (Media Sanitization): Presenta como requisito el implementar procedimientos para la destrucción o desinfección segura de medios de almacenamiento (borrado seguro, trituración, desmagnetización) antes de su eliminación o reutilización.

A pesar de que el departamento de TIC responde a las preguntas de cuestionarios indicando textualmente: *“Sí, existe políticas aplicadas a los usuarios para el bloqueo de dispositivos de almacenamiento extraíbles”*; y que en el manual de Normas TI (MP-TIC-001-2011) establece en el inciso 1.6.3. Software Malicioso, en el inciso b) “*El uso de medios extraíbles personales de los funcionarios, que puedan ser un medio de entrada de software malicioso, deberán ser regulados por el Departamento de TIC; el cual en caso de valorar que el riesgo asociado al uso de estos dispositivos es muy alto; podrá restringir o eliminar completamente su uso dentro*

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

de la institución." Evidenciando de esta forma la irregularidad que se detecta en el uso de dispositivos extraíbles, consecuentemente se llevó a cabo pruebas al azar en equipos (computadoras) en diferentes departamentos para verificar si la política mencionada se está cumpliendo, sin embargo, como se muestra en la siguiente tabla resumen.

Tabla 1

Verificación de Política de Bloqueo de dispositivos USB

Fecha	Departamento	Equipo	Lectura	Escritura
16/07/2024	Plataforma de Servicios	MSCDPT-03	Se puede leer el contenido del USB	Se puede agregar contenido al USB
16/07/2024	Secretaría de Concejo	MSCDSC-02	Se puede leer el contenido del USB	Se puede agregar contenido al USB
16/07/2024	Auditoría Interna	MSCPAU-06	Se puede leer el contenido del USB	Se puede agregar contenido al USB
16/07/2024	Bienes Inmuebles	MSCPBI-05	Se puede leer el contenido del USB	Se puede agregar contenido al USB
16/07/2024	Proveeduría	MSCPPV-04	Se puede leer el contenido del USB	Se puede agregar contenido al USB
16/07/2024	Tesorería	MSCPTS-02	Se puede leer el contenido del USB	Se puede agregar contenido al USB
16/07/2024	Unidad técnica de Gestión Vial	MSCPUTGV-18	Se puede leer el contenido del USB	Se puede agregar contenido al USB

Nota: Elaboración de tabla con evidencia tomada en distintos puestos de trabajo de los departamentos.

Se detecta que, la política está fallando, por cuanto prácticamente en todos los equipos se pudo leer el contenido del dispositivo USB y se pudo agregar contenido al mismo, a excepción de los equipos o computadores del departamento de Catastro; por tanto, se detecta que el bloqueo de dispositivos USB probado no surte la restricción indicada para la política del Antivirus ESET (ver ilustración 6), ya que el bloqueo establecido solo se evidencia efectivo en los equipos del departamento de Catastro, no detallándose este particular en la política establecida.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Ilustración 6

Política de bloqueo USB aportado por TIC

Nota: Tomado de evidencia aportada por TIC para cuestionario de Control - Seguridad de la Información

Por ello si la política de bloqueo de dispositivos USB establecida en el antivirus de la red presenta deficiencia o falla en la efectividad, puede tener varios efectos negativos para la seguridad y el rendimiento de los sistemas, así mismo incrementa los riesgos asociados al uso de este tipo de dispositivos exponiendo a los equipos, datos e información a riesgos como: ataques por malware, fuga de datos, carga adicional a soporte técnico, interrupción del flujo laboral, por mencionar algunos.

Esta falla en la implementación de la política y su consecuente afectación a la seguridad también evidencia que el comité de seguridad carece de conocimiento de las irregularidades que se presentan ante el inadecuado uso de estos dispositivos potencializando de alguna manera los riesgos, mismos que no se evidencian en la valoración de riesgos consultados en el SEVRI de dicho departamento (revisión de riesgos contemplados en el SEVRI).

2.4. Actividades para medidas de atención ante incidentes de seguridad cibernética

2.4.1. Desarrollo, implementación y gestión de planes y procesos de respuesta ante incidentes de seguridad cibernética.

Producto de aplicación y análisis de los cuestionarios facilitados por la CGR, se desprende de las respuestas dadas por el departamento de TIC que: “no se cuenta con planes de respuesta ni procesos establecidos”, lo que configura incidentes de seguridad cibernética.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Se evidencia que se carece de los planes y procesos para dar respuesta ante incidentes y con ello el personal no se familiariza con sus roles y el orden de las operaciones, la compartición de información, la coordinación con las partes interesadas, la clasificación de incidentes, el manejo de vulnerabilidades y la incorporación de lecciones aprendidas, dichas actividades de control no son llevadas a cabo por un funcionario dedicado de forma regular a estas labores que garantice la atención inmediata, con acciones coordinadas y su respectiva documentación.

De lo anterior es importante señalar que la administración debe desarrollar, implementar y gestionar los planes y procesos necesarios considerando al menos los criterios que se exponen en las siguientes normas:

- **CIS CSC:** Controles 4 y 19, los cuales contemplan la administración de privilegios de usuario y la preparación y capacidad de respuesta ante incidentes de seguridad, abarcando aspectos como: Monitoreo y control, Revisión regular, Autenticación multifactor (MFA), Registro de auditoría, Plan de respuesta a incidentes, Capacitación, Monitoreo continuo, Lecciones aprendidas. Exponiendo como objetivo limitar y controlar el uso de cuentas con privilegios administrativos para prevenir el acceso no autorizado y asegurar que la institución esté preparada para responder eficazmente a incidentes de seguridad y minimizar el impacto de estos.
- **COBIT 5:** En los dominios que se exponen a continuación abarca la gestión de Riesgos y Seguridad mediante **EDM03.02** que contempla la gestión efectiva de los riesgos relacionados con TI, **APO12.03** el cual se centra en la protección de la información para asegurar su confidencialidad, integridad y disponibilidad y el **DSS05.07** que se enfoca en la implementación y gestión de servicios de seguridad. También, la Gestión de Servicios e Incidentes se contempla en los dominios **DSS02.02** el cual se enfoca en la gestión efectiva de incidentes y solicitudes de servicio, el **DSS03.04** con miras en resolver problemas y prevenir su recurrencia y el **DSS04.08** que se enfoca en asegurar que los servicios críticos de TIC puedan mantenerse o recuperarse en caso de una interrupción. Además, para la Gestión de TIC y Proyectos, el dominio **APO01.02** expone la importancia de establecer y mantener un marco

coherente y efectivo para la gestión de TIC y el dominio **BAI01.13** que hace énfasis en asegurar que los programas y proyectos se gestionen adecuadamente.

- En la norma **ISO/IEC 27001:2023** en Controles como la **6.3** aborda la planificación de la gestión de riesgos enfocándose en riesgos asociados con la seguridad de la información, incluyendo la evaluación de riesgos y la selección de controles adecuados, así mismo la sección **5.24** contempla el control de documentos y registros haciendo énfasis en la necesidad de controlar la creación, revisión, actualización y eliminación de documentos y registros relacionados con la gestión de la seguridad de la información. Además, la cláusula **7.4** que trata de la comunicación interna exige la planificación y realización de la comunicación interna para asegurar que todos los empleados y partes interesadas estén informados sobre los aspectos relevantes de la seguridad de la información.

- Las normas **NIST SP 800-53 Rev. 4:** en los controles CP-2, CP-7, CP-10, CP-12, CP-13, IR-4, IR-7, IR-8, IR-9 y PE-17, dan importante referencia sobre este hallazgo siendo que el control **CP-2** establece que las organizaciones deben **desarrollar, documentar y distribuir un plan de contingencia para su sistema de información**. El objetivo de este plan es proporcionar procedimientos para asegurar la continuidad de las operaciones esenciales de la misión y los servicios municipales en caso de una interrupción en los sistemas de información. El control **CP-7** hace énfasis en asegurar la disponibilidad y la resiliencia del sistema de información ante fallos o interrupciones, garantizando que las operaciones puedan continuar con el menor impacto posible en caso de contingencias, también en el control **CP-10** se refiere a la **Capacidad de Recuperación de la Información**. Este control establece que las organizaciones deben implementar procedimientos para restaurar los datos del sistema de información desde las copias de seguridad necesarias cuando se produce una interrupción o un fallo en el sistema. El **CP-12** expone que se debe garantizar que la información no se vea comprometida durante su transmisión, utilizando métodos de protección apropiados para mantener la confidencialidad e integridad de los datos, el CP-13 se refiere a la **Distribución Alternativa de la Información (Alternative Communication Paths)**. Establece que las organizaciones deben identificar y usar rutas alternativas de

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

comunicación para transmitir información en situaciones en las que los canales de comunicación primarios no están disponibles o han sido comprometidos. El **IR-4** se enfoca en el análisis sistemático de incidentes de seguridad para comprender su causa y efectos, mejorar las prácticas de respuesta y fortalecer la postura de seguridad de la institución en el futuro, El control **IR-7** se refiere a la **Respuesta a Incidentes de Seguridad de la Información (Incident Response Assistance)**. Este control establece que las organizaciones deben asegurarse de que exista asistencia disponible para ayudar a los usuarios en la preparación, respuesta y manejo de incidentes de seguridad de la información. El **IR-8** se enfoca en garantizar una comunicación efectiva y adecuada durante y después de un incidente de seguridad para asegurar que la respuesta al incidente sea coordinada y que todas las partes interesadas sean informadas según sea necesario. El control **IR-9** se refiere a la **Revisión de Incidentes (Incident Reporting)**. Este control establece que las organizaciones deben garantizar que se realice una revisión adecuada y la documentación de todos los incidentes de seguridad de la información para identificar lecciones aprendidas y mejorar las políticas y procedimientos relacionados con la respuesta a incidentes. Por último, también el control **PE-17** se refiere a la **Protección de la Infraestructura Física para el Acceso Remoto (Remote Access Protection)**. Este control establece que las organizaciones deben proteger el acceso remoto a sus sistemas de información, asegurando que las conexiones remotas se realicen de manera segura y controlada.

Ante la ausencia de un enfoque estructurado y formal para el desarrollo, implementación y actualización de planes de respuesta a incidentes de seguridad cibernética, podrían dejar a la institución vulnerable en la respuesta ante cualquier ataque cibernético que se presente. Conforme a lo manifestado en las respuestas dadas en el cuestionario, las cuales exponen textualmente: *“No se cuenta con planes de respuesta establecidos”, “No existe un proceso establecido”*, como se indicó anteriormente, lo que efectivamente evidencia que se carece de actividades de control que minimicen los riesgos ante ataques cibernéticos al no contar con planes, procesos y procedimientos que den respuesta inmediata ante posibles incidentes de seguridad cibernética, incrementando el riesgo de daños significativos a la institución,

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

incluyendo pérdida de datos, interrupciones operativas, afectación o daño a la reputación e inclusive posibles sanciones regulatorias.

2.4.2. El departamento de TIC presenta deficiencias en el desarrollo, ejecución y actualización de los planes de recuperación.

Con base en lo manifestado por el departamento de TIC en los cuestionarios aplicados, (01 - Herramienta GSI y 02 - Checklist NIST CSF 1.1 español), aún tienen pendiente establecer formalmente planes y estrategias de recuperación posterior a cualquier evento de afectación a la seguridad de la información.

En relación con este hallazgo existen normativas y estándares que abordan el tema y la consecuente importancia de contar con planes de recuperación acordes con las necesidades de seguridad de la Municipalidad, criterios de los que actualmente se carece en la normativa interna, al respecto se citan normas que dan fundamento para atender este tipo de debilidades detectadas:

- La norma **CIS CSC** Control **10** se enfoca en la recuperación de datos, instando a las organizaciones a implementar medidas para recuperar datos esenciales en caso de pérdida o daño.
- **COBIT 5** tiene varios dominios y subprocesos relevantes para el tema de los planes de recuperación, entre los cuales están:
    - **APO12.06** Este subproceso se centra en la respuesta a riesgos, asegurando que la institución tenga estrategias y planes para responder a los riesgos.
    - **BAI03.02** se refiere a la definición y mantenimiento de requisitos técnicos y soluciones, asegurando que las soluciones de TIC cumplan con los requisitos empresariales.
    - **BAI05.07**, este dominio se centra en la gestión del entorno de soluciones, incluyendo la planificación para la recuperación de desastres y la continuidad del negocio.

- **BAI07.08** que se enfoca en la revisión de los cambios implementados en la institución para evaluar su éxito.
- **DSS02.05** establece un marco para asegurar que los servicios proporcionados por la institución se alineen con las expectativas de los clientes.
- **DSS03.04** se centra en capturar y compartir las lecciones aprendidas durante el proceso de resolución del problema.
- **DSS04** se centra en gestionar la continuidad, con **DSS04.02** proporcionando directrices para mantener un plan de continuidad de negocio.
- **DSS04.03** asegurando que los planes de continuidad y recuperación sean efectivos y estén preparados para ser ejecutados cuando sea necesario.

- Así también la norma **ISA 62443-2-1:2009** en algunas de sus secciones abarca el tema de la recuperación posterior a los incidentes de seguridad en TIC, a continuación, se enumeran algunas de estas que inciden considerablemente en los Planes de recuperación:
  - La sección **4.3.2.5.3** de la norma ISA 62443-2-1:2009 proporciona directrices detalladas sobre cómo gestionar los cambios en los sistemas de control industrial para asegurar que se realicen de manera controlada y segura.
  - En la sección **4.3.2.5.7** se establece como objetivo proporcionar un marco estructurado para gestionar los parches de seguridad en los sistemas de control, asegurando que las vulnerabilidades sean abordadas de manera efectiva sin comprometer la estabilidad y seguridad del sistema. Esto es crucial para mantener la integridad, disponibilidad y confidencialidad de los sistemas de automatización y control.
  - La sección **4.3.4.5.1** aborda algunos aspectos sobre los incidentes y todo lo que estos conllevan, en el caso en particular de relación con planes de recuperación menciona como dato importante que es necesario implementar la **Revisión Posterior al Incidente**, especificando que después de resolver un

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

incidente, se realiza una revisión para evaluar la eficacia de la respuesta y para identificar mejoras en el proceso de gestión de incidentes.

- Como punto relevante de esta norma, la sección **4.3.4.5.11** establece pautas a seguir sobre la revisión post-incidente, el propósito de esta revisión es asegurar que la institución pueda aprender de los incidentes pasados y mejorar continuamente sus capacidades de respuesta y seguridad. Esto es esencial para fortalecer la resiliencia de los sistemas de control industrial frente a futuros incidentes, siendo esto clave en la elaboración y actualización de Planes de Recuperación.

- Además, la norma **ISA 62443-3-3:2013** contempla considerables aportes a los planes de recuperación de la institución, a continuación, se exponen secciones relativas a esto:

  - El propósito de la sección **SR 3.3** es establecer un marco sólido para el monitoreo de la seguridad en los sistemas de control industrial. Al implementar un monitoreo efectivo, las organizaciones pueden detectar y responder rápidamente a las amenazas de seguridad, minimizando el impacto de los incidentes de seguridad y protegiendo la integridad y disponibilidad de los sistemas y consecuentemente apoyando de esta forma a que los planes o procesos de recuperación ante incidentes resulten más prácticos y efectivos.

  - En la sección **SR 7.3** se contemplan aspectos de relevante importancia relacionados con la verificación de la función de seguridad: como lo son la revisión periódica, el realizar pruebas de seguridad, la documentación de resultados, la revisión y actualización, la definición de responsabilidad y la verificación de conformidad con otros estándares.

  - En la sección **SR 7.4** se enfatiza la importancia de un proceso continuo y sistemático para la gestión de vulnerabilidades, asegurando que los sistemas de control industrial sean resistentes a las amenazas cibernéticas y que puedan operar de manera segura y confiable lo que repercute en la aplicación

de planes o procesos de recuperación, siendo que lo ideal es requerir lo menos posible la aplicación de estos.

- La norma **ISO/IEC 27001:2023**, en algunos de sus apartados, contempla aspectos válidos a considerar en la elaboración de planes, procedimientos y proyectos de recuperación tras incidentes de seguridad de la información.
    - Entre los dominios y sus correspondientes controles o secciones se encuentra el apartado **5.24**, el cual hace hincapié en algunos detalles importantes para la elaboración de Planes de recuperación ante incidentes. El objetivo de este apartado es garantizar que las organizaciones tengan un enfoque sistemático y basado en riesgos para proteger sus activos de información.
    - El objetivo de la sección **7.4** es asegurar que los detalles sobre la seguridad de la información y el Sistema de Gestión de Seguridad de la Información (SGSI) se comuniquen de manera adecuada, oportuna y eficaz a todas las partes interesadas. Esto promueve la comprensión clara y unificada de las políticas, procedimientos y cambios que afectan la seguridad de la información dentro de la institución, siendo estas acciones fundamentales para el desarrollo de procedimientos de recuperación.
    - En cuanto al objetivo de la sección **7.5** es asegurar que la documentación del SGSI sea adecuada y esté controlada de manera eficaz para apoyar la implementación, operación y mejora continua del sistema, abarcando aspectos relacionados con documentación, contemplando la creación, actualización y el control de información documentada.
    - También cabe mencionar que la **sección 8** abarca la planificación y el control de la seguridad de la información, la evaluación y el tratamiento de riesgos, asegurando que se gestionen de manera efectiva los procesos que podrían afectar la seguridad de la información.
    - Por último, la norma **ISO/IEC 27001:2023** propiamente en la **cláusula 10** tiene relación directa con los planes de recuperación toda vez que asegura que la institución no solo mantenga un SGSI efectivo, sino que también lo mejore

continuamente, adaptándose a nuevos riesgos y oportunidades para garantizar la protección adecuada de la información.

- Así como las anteriores normativas o criterios de respaldo del presente hallazgo, las normas **NIST SP 800-53 Rev. 4** brindan importantes aportes, relacionados con la categoría de controles de Planificación de la Continuidad del Negocio (CP - Continuity Planning), entre los cuales priman:
    - La **sección 7.5** especifica requisitos para la creación, actualización y control de la documentación del SGSI.
    - El control **CP-4** da pautas para la **"Recuperación de la Continuidad del Negocio"** y cuyo objetivo es asegurar que la institución pueda restaurar rápidamente las operaciones críticas y minimizar el impacto de un incidente sobre la continuidad del negocio, protegiendo así la integridad y disponibilidad de la información y los sistemas esenciales.
    - El control **CP-7** se refiere a la **"Protección de la Información de Continuidad del Negocio"** cuyo objetivo es garantizar que la información vital para la planificación y gestión de la continuidad del negocio esté protegida adecuadamente, asegurando que la institución pueda continuar operando de manera efectiva incluso durante o después de un incidente.
    - En la NIST Special Publication 800-53 Revision 4, el control **CP-10** se refiere a **"Planificación y Pruebas de Continuidad de las Comunicaciones"**. Este tiene como objetivo hacer énfasis en garantizar que la institución pueda mantener y restaurar las capacidades de comunicación esenciales durante y después de un incidente que interrumpa las operaciones normales, minimizando el impacto en la capacidad de coordinar y gestionar la continuidad del negocio.
    - Así también el CP-11 tiene como objetivo garantizar que la institución esté adecuadamente preparada para restaurar sus operaciones críticas después de una interrupción, minimizando el impacto en la capacidad de continuar operando y protegiendo la información y los activos esenciales.

- Por ultimo las normas NIST SP 800-53 Rev. 4 expone importante impacto o dirección para este hallazgo en los controles **CP-12**: mismo que se enfoca en procedimientos de recuperación, **CP-13**: que se centra en la continuidad de las comunicaciones, **IR-3**: que trata sobre la notificación de incidentes, **IR-4**: cubre la capacidad para dar respuesta a incidentes, **IR-6**: aborda la planificación de la recuperación de incidentes, **IR-7**: este control se enfoca en ejercicios y pruebas de recuperación de incidentes, **IR-8**: que trata sobre la coordinación con las entidades externas, **IR-9**: que cubre la evaluación y mejora continua de la respuesta a incidentes.
- Abordar estos controles es de vital importancia en este hallazgo pues los mismos tienen una relación muy directa con los planes de recuperación ante incidentes de seguridad de la información o ciberseguridad.

Con base en lo comunicado por el departamento de TIC las actuales “Normas TI”, así como el departamento en concreto presenta carencia en la elaboración, implementación y actualización de planes, procedimientos o proyectos para la gestión de la recuperación ante incidentes de seguridad de la información.

Entre las posibles repercusiones que pueden materializarse se presenta el riesgo de la ausencia en la comunicación a las partes internas y externas interesadas, así como también a los equipos ejecutivos y de administración correspondientes y en falencia de la protección de los activos tangibles e intangibles con que cuenta e inclusive provee TIC. Además, cabe enumerar como otros posibles efectos, aunque no los únicos a los que está expuesta la institución, los siguientes:

- Ineficiencias en la restauración de servicios críticos.
- Posibilidad de mayor riesgo de pérdida de datos.
- Riesgo de tiempos de inactividad prolongados.
- Así como es muy importante mencionar la apremiante incapacidad para incorporar lecciones aprendidas de futuros incidentes en los respectivos planes.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

III. CONCLUSIONES.

Posterior a lo verificado, se determina que el Departamento de TIC presenta yerros tanto en lo operativo como en lo normativo, requiriendo llevar a cabo acciones de actualización o mejora de sus normas, políticas, así como también en algunas configuraciones enfocadas propiamente a garantizar la protección de la información y la ciberseguridad. Por tanto, es crucial para el Departamento de TIC establecer canales de comunicación claros y efectivos para asegurar que todas las partes, proveedores, clientes y usuarios en general estén al tanto de las políticas de seguridad de la información vigentes y que las mismas se cumplan, generando los debidos registros tanto en el proceso de elaboración, implementación y actualización como en las acciones de comunicación o socialización respectivas.

Además, es realmente importante y necesario que se elaboren e implementen nuevas políticas o un marco de gobierno, tomando en consideración que, en el entorno actual, donde las TIC evolucionan de manera acelerada, es esencial que la Municipalidad de San Carlos adopte un enfoque proactivo y dinámico en la gestión y gobernanza de estas tecnologías. Aunque los procesos de gestión de seguridad de la información y ciberseguridad cuentan con una norma establecida la cual cumple la función de guía generalizada, estas deberían ajustarse a las normas, estándares, marcos jurídicos y técnicos vigentes. Además, la auditoría ha revelado que las políticas y procedimientos existentes no se actualizan con la frecuencia necesaria para adaptarse a los vertiginosos cambios tecnológicos y a las constantes nuevas amenazas emergentes.

Para mantener una postura de seguridad robusta y resiliente frente a estos desafíos, es imperativo que se elabore, implemente y mantenga un marco de gobierno de TIC flexible y adaptable al entorno institucional. Para ello, se girarán recomendaciones que permitirán mejoras en la administración municipal a través de procesos acordes con los hallazgos señalados en el apartado de resultados, a fin de que se lleve a cabo una actualización continua de políticas, asegurando su alineación con las mejores prácticas y estándares internacionales, y permitiendo la incorporación rápida de nuevas tecnologías y la adaptación a los cambios regulatorios.

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

La adopción de un marco de gobierno de TIC dinámico no solo protegerá a la institución contra las amenazas actuales, sino que también la preparará para futuras evoluciones tecnológicas, mitigando riesgos y asegurando su competitividad y conformidad normativa. En resumen, la constante actualización de las políticas de TIC es una estrategia esencial para garantizar la seguridad, eficiencia y sostenibilidad de las operaciones tecnológicas en la Municipalidad de San Carlos.

Además, cabe mencionar que el Departamento de TIC ha estado trabajando desde 2022 en la adopción de las normas emitidas por el MICITT. A través del plan de implementación titulado "Diseño e implementación del Marco de Gobierno y Gestión de Tecnologías de Información", se han venido ejecutando cambios conforme a la hoja de ruta establecida. Este marco fue aprobado en el acta 18-2022, sesión ordinaria del 21 de marzo de 2022.

Esto evidencia que el departamento TIC trabaja con vistas a la modernización y el cumplimiento normativo. Sin embargo, es fundamental que se mantenga el ritmo de estas actualizaciones y que se realicen los ajustes necesarios para que el marco de gobierno aprobado siga alineándose con las mejores prácticas y se adapte a los constantes cambios tecnológicos y normativos.

IV. RECOMENDACIONES.

4.1. A la Alcaldía Municipal:

4.1.1. Girar instrucción en un plazo de un mes calendario a partir de haberse recibido este informe al jefe del departamento de TIC para que establezcan formalmente los canales de comunicación y publicación a los clientes internos y externos relevantes sobre las Normas de Tecnologías de Información y un plazo de seis meses calendario para que se lleve a cabo dicha actividad para lo cual deberán remitir mediante oficio a la Auditoría Interna el cumplimiento de esta recomendación. (ver punto 2.1.1. de resultados).

4.1.2. Girar instrucción en un plazo de un mes calendario a partir de haberse recibido este informe al jefe del departamento de TIC para que diseñe y comunique

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

programas de capacitación y concientización en seguridad de la información contemplando las políticas, normas y estándares de seguridad vigentes y sobre las cuales se rige las políticas Municipales establecidas, para ello cuenta con un plazo de dos meses a partir de haber recibido este informe para dar cumplimiento a esta recomendación, para lo cual deberán remitir mediante oficio a la Auditoría Interna el cumplimiento. (ver punto 2.1.1. de resultados).

4.1.3. Emitir instrucciones a la jefatura de TIC dentro de un plazo de 15 días para que, se incluyan en sus planes o procesos los plazos de revisión y actualización de políticas o normas de TIC, para lo cual cuentan con plazo de un mes a partir de recibido este informe y deberán comunicar a la auditoria mediante oficio de cumplimiento, (ver resultado 2.1.2.)

4.1.4. Girar instrucción en un plazo de quince días al departamento de TIC para que implanten conforme lo evidenciado en el hallazgo las mejoras en la gestión de contraseñas y autenticación (al menos las últimas 10 contraseñas anteriores), asegurando el cumplimiento de las normativas y estándares aplicables. Al respecto se concede un plazo de un mes para que se realicen las configuraciones y su debida implementación, para ello deberá remitir oficio de cumplimiento a la Auditoría Interna, una vez recibido este informe (ver resultado.2.2.1.)

4.1.5. Girar instrucción en plazo de un mes calendario a la jefatura del departamento de TIC para que presente propuesta para aplicar la configuración necesaria para hacer efectiva la Autenticación Multifactor (MFA), para todos los usuarios del dominio. Considerando los estándares internacionales (ISO/IEC 27001:2023, NIST SP 800-53, CIS CSC, COBIT 5) y las directrices nacionales vigentes, en busca de optimizar la protección integral de la infraestructura de TI, para esto cuentan con un plazo de seis meses a partir de recibido este informe y deberán remitir oficio de cumplimiento (ver resultado 2.2.1.).

4.1.6. Emitir indicación en plazo de un mes para que el departamento de TIC presente una propuesta de control *de activos de tecnologías que permita el control eficaz, eficiente, transparente y dinámico y que incluya el préstamo de activos y la* entrega

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

de suministros de TIC. Para lo cual cuentan con plazo de 3 meses a partir de recibir este informe, una vez realizada la gestión, remitir a esta auditoría oficio de cumplimiento y su correspondiente propuesta, (ver resultado 2.3.1.)

4.1.7. Girar instrucción en plazo de 15 días a la jefatura de TIC para que realice una revisión exhaustiva y actualice la política configurada en la herramienta correspondiente sobre bloqueo de dispositivos de almacenamiento extraíbles (USB), asegurando su correcta implementación y efectividad, divulgar la implementación a los usuarios y asegurando que los riesgos asociados al uso de dispositivos USB estén contemplados en el Sistema de Evaluación de Riesgos (SEVRI) de TIC, para esto se otorga un plazo de 30 días hábiles posterior al recibido de este informe. Además, deberán comunicar a esta auditoría mediante oficio el cumplimiento de esta recomendación (ver resultado 2.3.2.).

4.1.8. Girar instrucción en un plazo de quince días a la jefatura de TIC, conforme a lo evidenciado en el punto 2.4.1. de este informe, para que se desarrollen, implementen y gestionen los planes y procesos de respuesta ante incidentes de seguridad cibernética. A partir de la aprobación de la normativa interna sobre ciberseguridad, considerando que la administración cuenta con el Plan de trabajo 2024 para el Nuevo Marco de Gobierno de TIC y que TIC ha comunicado verbalmente tener previsto un avance relacionado con esta recomendación, se establece que el informe de dicho avance sea entregado mediante oficio a esta auditoría tres meses posterior a la entrega del informe del estudio, contemplando este comunicado para diciembre 2024, (ver resultado 2.4.1.)

4.1.9. Girar instrucción en plazo de un mes a la jefatura de TIC para que con base en el resultado 2.4.2, lleve a cabo las acciones de desarrollo formal de planes de recuperación, contemplando al menos etapas como ejecución y pruebas, actualización continua de los planes, asignación de responsabilidades y monitoreo. Para esto cuenta con plazo de dos meses una vez recibido este informe y deberá remitir mediante oficio a la Auditoría Interna el cumplimiento de esta recomendación, (ver resultado 2.4.2.).

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

V. ANEXOS

En este apartado se incluye el análisis de las observaciones recibidas de la Administración Activa en la Conferencia Final realizada a este informe el día 30 de agosto del 2024, y según lo estipulado en la Norma N° 205, específicamente en el punto 9 de las Normas Generales de Auditoría para el Sector Público (R-DC-064-2014), a continuación, el detalle del análisis realizado a dichas observaciones:

N° Punto	**Resultado 2.3.2.**		
Observación de la Administración	*Medios extraíbles, que la norma no dice debe sino "podrá" "puede", indica no es una política generalizada, que se han ido aplicando las normas de forma selectiva según la necesidad del cliente (departamento).*		
¿Se acoge?	*Si*	*No*	*Parcial*
		X	
Argumento de la AI	*Considerando la siguiente normativa se mantiene lo indicado en el resultado 2.3.2., ya que el control MP-7 de la NIST SP 800-53 Rev. 4, establece que la institución debe restringir o prohibir el uso de ciertos tipos de medios de información en sistemas o componentes definidos por la institución, utilizando salvaguardas de seguridad también definidas por la institución.* *El CIS establece en el Control 8: Protección contra Malware (Malware Defenses) sobre Control de Dispositivos Externos: Implementar controles para dispositivos externos (por ejemplo, unidades USB) para evitar la introducción de malware. y sobre Limitación de Privilegios: Limitar los privilegios de los usuarios para evitar la ejecución de software no autorizado que podría contener malware.* *En la norma ISA 62443-3-3:2013 el requisito SR 2.3: Gestión de Privilegios de Usuario (Account Management) contempla entre otros la Asignación de Privilegios: Los privilegios de acceso deben ser asignados de acuerdo con el principio de mínimo privilegio, lo que significa que los usuarios solo deben tener los derechos necesarios para realizar sus tareas específicas y nada más. Y también contempla la Revisión de Privilegios: Los privilegios de acceso*		

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

	deben revisarse regularmente para asegurarse de que siguen siendo apropiados para las responsabilidades actuales del usuario. Esto incluye la revocación o modificación de privilegios cuando un usuario cambia de rol o deja la institución. *En la norma COBIT 5, el proceso DSS05.02 Proteger contra el malware indica textualmente, "La institución debe implementar medidas para prevenir, detectar y remediar ataques de malware a través del establecimiento de controles de seguridad efectivos", La implementación de lo establecido en este proceso está directamente relacionado con el bloqueo de medios extraíbles, ya que esta acción previene el acceso no autorizado y la posible fuga de información sensible entre otros.* *El proceso DSS05.06 Monitorear la seguridad contiene la indicación "El monitoreo permite a la institución detectar anomalías y tomar medidas preventivas o correctivas para mitigar el impacto de posibles amenazas a la seguridad.", aplicando este en el tema de prevención a la importante necesidad de control sobre medios o dispositivos que representen riesgo para la seguridad de la información.* *Por tanto, la gestión de los riesgos asociados al uso de dispositivos o medios extraíbles no escapa a la prevención que un adecuado marco de gestión debe contener y por tanto en esto la necesidad institucional de restringir en su totalidad el uso de medios extraíbles.*
N° Punto	**Recomendación 4.1.2.**
Observación de la Administración	*Cambiar "desarrolle e implemente" por "diseñe y comunique" programas de capacitación y concientización*
¿Se acoge?	*Si* | *No* | *Parcial* | | ***X***
Argumento de la AI	*En relación con lo contemplado en esta recomendación la norma ISO/IEC 27001:2023 en el control 5.1 Políticas de seguridad de la información, indica textualmente "La política debe ser comunicada a todas las partes interesadas" y las normas NIST SP 800-53 Rev. 4 en el control AC-1, establece la necesidad*

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

	de desarrollar, documentar y difundir políticas y procedimientos para la implementación efectiva de los controles de acceso seleccionados y sus mejoras. *Se da como aceptada la modificación solicitada en el sentido de que se está trabajando conforme a la aprobación del nuevo marco de gobierno en las actividades de diseño y comunicación en sustitución de desarrollar e implementar, que viene a reforzar lo citado en los criterios acá indicados.*
N° Punto	**Recomendación 4.1.5.**
Observación de la Administración	*Sobre "Autentificación de multifactor (MFA)", modificar para que presente propuesta para aplicar (…)-, y cambiar el plazo de 15 días a 6 meses.*
¿Se acoge?	*Si* | *No* | *Parcial* **X**
Argumento de la AI	*En relación con lo contemplado en esta recomendación la norma ISO/IEC 27001:2023 en el control 5.1 Políticas de seguridad de la información, indica textualmente "La política debe ser comunicada a todas las partes interesadas" y las normas NIST SP 800-53 Rev. 4 en el control AC-1, establece la necesidad de desarrollar, documentar y difundir políticas y procedimientos para la implementación efectiva de los controles de acceso seleccionados y sus mejoras.* *Con base en lo verificado y en análisis de que la MFA implica entre otros una posible inversión significativa, así como la anuencia de TIC para implementar las mejoras indicadas se da como aceptada la modificación solicitada, en el sentido de que se presente una propuesta para aplicar MFA en plazo de 6 meses.*
N° Punto	**Recomendación 4.1.6.**
Observación de la Administración	*Sobre registro y control de activos, revisar la propuesta de recomendación en referencia a los resultados.*
¿Se acoge?	*Si* | *No* | *Parcial* **X**

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

Argumento de la AI	*Sobre este particular se expone a continuación algunos puntos, controles o dominios de normas y estándares, tales como:* *ISO/IEC 27001:2023 Control 5.9 Inventario de Información y Otros Activos Asociados* *Este control trata sobre el inventario de la información y otros activos asociados. Su objetivo es reconocer y gestionar adecuadamente los activos de información para garantizar su seguridad* *CIS CSC 1: Inventario y Control de Activos de Hardware* *Este control se enfoca en el inventario y control de los dispositivos de hardware que están conectados a la red de una institución. Uno de sus objetivos es: Mantener un inventario actualizado de todos los dispositivos hardware autorizados.* *COBIT 5 DSS05.05 Gestionar la seguridad física a los activos de TI* *Se enfoca en la gestión del acceso físico a los activos de información y tecnología (I&T). Este control es crucial para garantizar que solo las personas autorizadas tengan acceso a datos y sistemas tecnológicos sensibles, reduciendo así el riesgo de brechas de seguridad y ciberataques. Este control ayuda a proteger los activos críticos de la institución contra el robo, la manipulación y otras actividades maliciosas, mejorando así la postura general de seguridad de la institución.* *Esta recomendación busca mejorar:* 1. *Eficiencia y Agilidad: Un sistema digital permitirá una consulta más ágil y precisa de los registros, reduciendo el tiempo y esfuerzo necesarios para gestionar estos procesos.* 2. *Alertas y Notificaciones: La implementación de un sistema digital permitirá la configuración de alertas y notificaciones automáticas, mejorando la gestión y seguimiento de los préstamos y entregas.* 3. *Reducción de Errores: La digitalización minimizará los errores humanos asociados con el manejo de documentos en papel.*

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

	4. Sostenibilidad: La posible eliminación del uso de papel contribuirá a iniciativas de sostenibilidad y reducción de residuos. *5. Acceso seguro y controlado a la información: Permitiendo control de usuarios para registro de entregas y devoluciones entre otros.* *Lo anterior por cuanto actualmente las acciones de control de préstamo de activos y la entrega de suministros o consumibles de TIC se llevan a cabo en papel, además de que se detectó que los controles de activos con que cuentan actualmente no presentan registros actualizados o acordes a la realidad de los mismos.* *Por tanto, se modifica la recomendación para que el departamento de TIC en el plazo ya establecido presente una propuesta de control de activos de tecnologías que permita el control eficaz, eficiente, transparente y dinámico y que incluya el préstamo de activos y la entrega de suministros de TIC.*
N° Punto	**Recomendación 4.1.7.**
Observación de la Administración	*Corregir redacción; sobre (..) actualice la política configurada en la herramienta correspondiente sobre bloqueo de dispositivos.*
¿Se acoge?	*Si* | *No* | *Parcial* **X**
Argumento de la AI	*Se lleva a cabo modificación en la redacción para mejorar su interpretación y correcta aplicación en lo que a herramientas de administración de la seguridad se refiere,* *Lo anterior por cuanto en las herramientas aplicadas para este estudio TIC indica que se cuenta con la política aplicada en la herramienta antivirus y al momento de la presentación del informe el señor Henry Brenes argumenta que la política si existe, sin embargo, solo se está aplicando al departamento de Catastro, por lo tanto, no es funcional en el resto de equipos de la Municipalidad.* *Quedando el texto de la siguiente forma:* *"realice una revisión exhaustiva y actualice la política configurada en la herramienta correspondiente sobre bloqueo de dispositivos de*

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

	almacenamiento extraíbles (USB), asegurando su correcta implementación y efectividad, divulgar la implementación a los usuarios y asegurando que los riesgos asociados al uso de dispositivos USB estén contemplados en el Sistema de Evaluación de Riesgos (SEVRI) de TIC"		
N° Punto	**Recomendación 4.1.8.**		
Observación de la Administración	*Cambiar redacción .../ a partir de la aprobación de la normativa interna sobre ciberseguridad, se cambia de dos meses a tres meses.*		
¿Se acoge?	*Si*	*No*	*Parcial*
			X
Argumento de la AI	*Tomando en consideración que la administración cuenta con el Plan de trabajo 2024 para el Nuevo Marco de Gobierno de TIC y siendo que TIC nos comunica tener ya previsto la entrega del avance relacionado con esta recomendación se establece la entrega de oficio en el que informe a esta auditoría el avance en el cumplimiento de esta recomendación tres meses posteriores a la entrega del informe del estudio, contemplándose este comunicado para diciembre 2024.*		

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr

02 de octubre de 2024

INFORME-MSCCM-AI-011-2024

Atentamente

AUDITORÍA INTERNA

FERNANDO CHAVES PERALTA (FIRMA) 2024.10.02 14:11:44 -06'00'

Lic. Fernando Chaves Peralta

Auditor Interno

ROXANA GUZMAN MENA (FIRMA) Firmado digitalmente por ROXANA GUZMAN MENA (FIRMA) Fecha: 2024.10.02 14:16:07 -06'00'

Lic. Roxana Guzman Mena

Supervisora de Calidad

Firmado digitalmente por JOSE MARCIAL VARGAS ARGUEDAS (FIRMA) Fecha: 2024.10.02 14:14:43 -06'00'

Lic. José M. Vargas Arguedas

Asistente de auditoría

(506) 2401-0990 www.munisc.go.cr auditoria@munisc.go.cr