Municipalidad de Curridabat
Auditoría Interna

Curridabat
CIUDAD DULCE

Informe MC-AI-INF-001-2020

EVALUACIÓN DE LA PLATAFORMA DE INTERNET Y CORREO ELECTRONICO

Realizado por
Luis Fernando Solís Hernández

Supervisado por
Gonzalo Chacón Chacón

Febrero 2020

INDICE

RESUMEN EJECUTIVO 2

1. INTRODUCCIÓN 4

1.1 Origen 4

1.2 Objetivo 4

1.2.1 Específicos 4

1.3 Alcance 4

1.4 Responsabilidad de la Administración y la Auditoría 5

1.5 Regulaciones de Control Interno 5

1.6 Limitaciones 5

1.7 Comunicación de Resultados 5

2. RESULTADOS 7

ÁREA DE EXAMEN 1: SERVICIO DE INTERNET 7

ÁREA DE EXAMEN 2: SERVICIO DE CORREO ELECTRONICO 19

3. CONCLUSIONES 25

RESUMEN EJECUTIVO

¿Qué se examinó?

Entre otras cosas, se valoraron mecanismos de control para el otorgamiento y declinación de accesos de los usuarios a servicios de internet y correo electrónico institucionales, los controles relacionados al registro y atención de incidentes vinculados a esos servicios, así como la administración de las herramientas de control y monitoreo utilizadas por el Departamento de Informática para velar por el correcto uso de los recursos de internet y correo por parte de los usuarios.

Se analizaron reportes de tráfico de internet generados por medio de las herramientas de monitoreo utilizadas por la institución.

Así mismo, se realizaron sondeos para evaluar el grado de satisfacción de los usuarios con dichos servicios, así como la satisfacción de los funcionarios con los procesos de divulgación de políticas y procedimientos, también de la gestión de actualización y capacitación que se brinda de cara a los funcionarios municipales en el uso de los servicios antes citados.

La existencia y puesta en práctica de procedimientos o directrices que regulen a nivel institucional la utilización de los servicios de internet y el correo electrónico municipal.

¿Por qué es importante?

Los servicios de internet y correo electrónico institucional son herramientas adquiridas y utilizadas por la Municipalidad de Curridabat con recursos del erario público a fin de apoyar todas las gestiones internas que requieren de servicios de conectividad para sus operaciones, como son aquellos procesos relacionados con gestiones que requieren acceso a plataformas financieras y de otras instituciones.

Como parte del control interno institucional, se debe velar por el buen uso de los recursos públicos, el resguardo de los activos, la seguridad de la información y por ende garantizar la seguridad y continuidad en las comunicaciones, siendo así vigilante de aquellos factores que potencien riesgos relacionados con las tecnologías de información.

Por lo anterior, resulta de suma importancia la fiscalización de estos recursos y de los procesos administrativos inherentes.

¿Qué se encontró?

Entre algunas de las condiciones halladas durante las revisiones realizadas, se encontraron procesos débiles de capacitación y divulgación de políticas, así como controles vulnerados relacionados con la detección de usos de servicios de internet y correo electrónico no adecuados, y que además riñen contra las mismas directrices internas de la institución.

Se observó un importante número de dispositivos móviles y equipos de cómputo particulares conectados a redes inalámbricas de la red del edificio principal y otras localidades de la municipalidad haciendo uso del ancho de banda de red, lo que podría incidir en situaciones relacionadas con la lentitud de la red o incluso suspensiones de los servicios.

Se evidenciaron usuarios correspondientes a funcionarios municipales y asesores utilizando los servicios de internet para acceder a sitios de entretenimientos, redes sociales, entre otros.

A pesar de lo anterior, se evidenció que la institución cuenta con algunas herramientas de tecnologías que siendo correctamente administradas podrían mitigar la mayoría de los riesgos relacionados con las condiciones encontradas y que serán presentadas mediante el presente informe.

¿Qué sigue?

Se emiten recomendaciones a las personas encargadas del área o proceso, con el fin de que las situaciones encontradas sean subsanadas.

1. INTRODUCCIÓN

El estudio se realiza conforme a lo establecido en el artículo N° 22 de la Ley General de Control Interno.

1.1 Origen

Este estudio es de carácter tecnológico y obedece al cumplimiento del Plan Anual de trabajo de la Auditoría Interna para el período 2019, el cual es del conocimiento del Concejo Municipal y comunicado a la CGR.

1.2 Objetivo

Determinar la aplicación de políticas y normativa existentes en el buen uso de los recursos de comunicación Institucional.

1.2.1 Específicos

1) Determinar la instauración de mecanismos que controlen el buen uso y administración del servicio de internet y correo electrónico institucional.
2) Determinar la existencia de mecanismos básicos de control que mitiguen riesgos inherentes a la transferencia de datos por medio de internet y correo electrónico.
3) Determinar la implementación de mecanismos que permitan llevar a cabo monitoreos y mediciones periódicas del tráfico de internet y correo electrónico institucional que ayuden a la toma de decisiones.
4) Valorar la existencia de planes de contingencia que garanticen la continuidad del servicio de internet en áreas primordiales.

1.3 Alcance

El alcance del presente estudio se limitó al examen de la calidad de los servicios de internet y correo electrónico de la Municipalidad de Curridabat, así como la valoración de los mecanismos implementados para el monitoreo y control del tráfico de datos por medio de la red institucional hacia internet. La revisión de

documentación correspondiente a reportes de tráfico generado durante porciones de tiempo del período 2019.

Se revisaron procedimientos y directrices internas relacionadas con el otorgamiento y declinación de accesos a distintos recursos de internet, así como la gestión de cuentas de correo electrónico, entre otros aspectos relacionados.

1.4 Responsabilidad de la Administración y la Auditoría

La veracidad y exactitud de la información en la que se basó esta Auditoria para llegar a los resultados obtenidos en el presente informe, es responsabilidad de la Administración Activa.

La responsabilidad de esta Auditoría consiste en emitir una opinión sobre la administración y control de los servicios de internet y correo electrónico de la institución, el uso que los usuarios dan a estos servicios, así como su alineación con las normativas legales, técnicas y administrativas aplicables.

1.5 Regulaciones de Control Interno

Las recomendaciones que se derivan del estudio deben ser atendidas conforme a las regulaciones de la Ley General de Control Interno Nº 8292, artículos 10,12, 36, 38 y 39.

1.6 Limitaciones

Durante el procedimiento de examen de administración de enrutadores inalámbricos, se solicitó en varias ocasiones que se suministrada a esta auditoría, copia de los contratos de los servicios de internet prestados por los proveedores a la institución, así como que se facilitara un recurso humano del Departamento de Informática con acceso a las consolas administrativas de los equipos de difusión de señal inalámbrica de internet de todos los sitios de dominio institucional en donde usuarios y funcionarios de la Municipalidad de Curridabat cuentan con accesos a internet institucional, sin embargo, no se aportó información concisa de lo solicitado y tampoco se asignó ningún funcionario para realizar las labores señaladas.

1.7 Comunicación de Resultados

El 04 de febrero de 2020 la Auditoría Interna, mediante una reunión denominada "*conferencia final*", dio a conocer a la Doctora Alicia Borja Rodríguez, Alcaldesa Municipal y al Ingeniero Federico Sánchez Díaz, Jefe del Departamento de Informática, los resultados a los cuales se

llegó durante el desarrollo del estudio, así como las conclusiones y las recomendaciones que a criterio de esta Auditoría deberían girarse.

Tomando en consideración que los funcionarios antes mencionados avalaron lo expuesto, se sometieron a consenso los plazos de cumplimiento de las referidas recomendaciones.

Se confeccionó además un documento denominado “Acta de Validación” en el cual se detallan los principales aspectos del estudio y los plazos de cumplimiento de las recomendaciones acordados.

Por parte de la Auditoría expuso el presente informe el Lic. Luis Fernando Solís Hernández, Profesional Analista de Auditoría.

2. RESULTADOS

ÁREA DE EXAMEN 1: SERVICIO DE INTERNET

Regulaciones internas

Se llevó a cabo una verificación general sobre la existencia e implementación de regulaciones internas en la institución para el monitoreo y control, relevantes al uso y administración de los servicios de internet de la municipalidad.

Una vez revisada toda la información obtenida se logró determinar que sí se cuenta con directrices, reglamentos y procedimientos por parte de la administración en cuanto al uso aceptado del servicio de internet institucional, sin embargo, se encontraron debilidades asociadas con la divulgación de esa información a los usuarios institucionales, situación que fue corroborada mediante encuesta realizada a una población del 25% de los usuarios institucionales y que se plasma en la condición del hallazgo #2.1 de este informe.

Durante este procedimiento no se encontraron condiciones que determinaran la comunicación de un hallazgo.

Calidad del servicio de internet

Para verificar la percepción de la calidad del servicio de internet de la institución para la ejecución de las labores de los funcionarios de la municipalidad se realizaron evaluación mediante sondeos en muestras de poblaciones de usuarios, así mismo se llevaron a cabo análisis de reportes de firewall para determinar el uso del servicio, así como posibles incidencias en la calidad de los servicios, entre otros.

De este procedimiento se derivaron los siguientes hallazgos:

	Condición	Causas / Efectos	Criterios	Recomendaciones
2.1	Desde el año 2012 no se llevan a cabo procesos de divulgación de información relacionada con normas y políticas de seguridad de información, así como del uso que se debe dar a recursos como internet y correo electrónico institucional.	Causas: Lo anterior se debe a una posible debilidad en la gestión de inducción, actualización y capacitación de los colaboradores de la institución en torno al uso de estas tecnologías y canales de comunicación oficiales, así	Según lo indicado por: –La Ley General de Control Interno (8292), artículos 15, incisos a) y b). –Las Normas Técnicas para la Gestión y el	A la Alcaldía Municipal: **2.1.1** Girar instrucciones a quien corresponda para que se desarrolle, documente, apruebe y promueva un programa anual de capacitación y actualización mediante charlas o talleres, dirigido a funcionarios actuales y

	Así mismo, el 79% de los funcionarios (de la muestra del 25% de funcionarios municipales que son usuarios de los servicios de correo e internet municipal) manifestaron no recordar haber recibido inducción, charlas o capacitación en relación al uso del servicio de internet y correo electrónico institucional, sus beneficios, controles, políticas y riesgos. Por otra parte, el 69% de esa misma muestra manifestó no tener conocimiento de la normativa institucional en materia del uso de los servicios mencionados.	como debilidad en los mecanismos de divulgación de información como los preceptos institucionales que regulan el uso de los recursos, así como las obligaciones de los funcionarios. <u>Efectos</u>: Los usuarios de los servicios de internet y correo electrónico municipal, podrían incurrir en usos inapropiados de los servicios creando brechas de seguridad que pondrían en riesgo la información institucional, los activos de tecnologías y comunicaciones, así como la imagen institucional. Esta condición provoca que la mayoría de los usuarios de estos servicios no adopten las mejores prácticas en el uso de los servicios oficiales de comunicación con herramientas de trabajo y por el contrario, se aumenta la probabilidad de incurrir en prácticas no adecuadas que potenciarían riesgos que exponen la información institucional, las comunicaciones y demás	Control de las Tecnologías de Información (N-2-2007-CO-DFOE), norma 1.4.2, inciso a.	nuevos funcionarios de todas las áreas de la municipalidad y que hacen uso de los servicios de internet y correo electrónico institucional, para que en materia del uso de estos servicios como herramientas de trabajo, se informe acerca de las políticas, reglamentos y sus actualizaciones, así como acerca de las amenazas entorno a estos servicios, sus riesgos, los controles con que cuenta la institución y sanciones ante eventuales incumplimientos. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como adjuntar una copia del documento desarrollado y aprobado por el ente correspondiente, debe indicarse además el puesto y nombre del funcionario responsable de la puesta en marcha de este programa.

		activos a riesgos que atentarían contra los objetivos de seguridad y del control interno institucional.		
2.2	Más del 76% de los funcionarios (de la muestra del 25% de funcionarios municipales que son usuarios del servicio de internet municipal), manifestaron experimentar interrupciones del servicio de internet institucional al menos una vez al mes. Áreas que por la naturaleza de sus funciones requieren hacer uso del servicio de internet constantemente para realizar consultas en bases de datos de otras instituciones, efectuar transferencias bancarias, pagos, consultas y registros de proveedores, gestión de facturas electrónicas, pagos de nóminas, etc.	<u>Causas:</u> Las causas se deben a factores externos propios de la prestación del servicio por parte del proveedor. <u>Efectos:</u> Al no tener acceso oportuno a información de bases de datos externas, cuentas bancarias, expedientes judiciales, registros de proveedores, sistemas de hacienda, entre otros, se podría incurrir en la paralización temporal de operaciones y procesos administrativos institucionales que podrían potenciar otros riesgos asociados con asuntos legales, bancarios, tributarios, riesgos de imagen institucional, entre otros.	Según lo indicado por: – Las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), norma 5.7, sub-norma 5.7.4. – Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), norma 1.4.4, inciso a.	<u>Al Departamento de Informática:</u> **2.2.1** Elaborar, aprobar y documentar un plan de contingencia que permita mitigar el riesgo de interrupción del servicio de internet a áreas críticas de la Municipalidad de Curridabat. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, mismo al que se debe adjuntar copia del plan de contingencia documentado.
2.3	Según lo indicaron los propios funcionarios, y además se evidenció en reportes de tráfico de internet de Palo Alto, se encontró que usuarios	<u>Causas:</u> Posible debilidad en los procesos de monitoreo y control del tráfico de la red institucional.	Según lo indicado por: – Las Normas Técnicas para la Gestión y el Control de las	<u>Al Departamento de Informática:</u> **2.3.1** Identificar todos aquellos servicios y aplicaciones que no tengan relación con las funciones

	de los servicios de internet de la municipalidad utilizan servicios y aplicaciones, dentro de las cuales se destacan servicios de streaming, redes sociales, almacenamiento en línea, entre otros, cuyos usos desvirtúan lo dispuesto por la "Directriz para el Uso del Servicio de Correo Electrónico y Acceso a Internet, Versión 1.2" con fecha del 29/02/2011, que regula el uso del servicio de internet en la Municipalidad de Curridabat.	<u>Efectos:</u> Esto abre brechas de seguridad que podrían desencadenar en alteración, robo y pérdidas importantes de información, afectación sobre activos de tecnologías, paralización de operaciones e incluso afectación de la imagen institucional, además de otros riesgos asociados con fraudes, ataques cibernéticos, divulgación de contenido infectado con malware, divulgación de pornografía, incumplimiento de las disposiciones que regulan el uso de los servicios de internet, entre otro.	Tecnologías de Información (N-2-2007-CO-DFOE), norma 1.4.2, inciso b, norma 1.4.4, inciso c. - Directriz en el Uso del Servicio de Correo electrónico y Acceso a Internet, versión 1.2, punto 3.1.2.	inherentes de la institución, y que además generan tráfico en la red de internet institucional con el fin de proceder a inhabilitarlos todos, al menos que exista una necesidad documentada, justificada y autorizada por parte de cada jefatura. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación. **2.3.2** Desarrollar, documentar y poner en práctica un procedimiento de monitoreo del tráfico de la red institucional, en el que se especifique además el funcionario responsable de su ejecución, la periodicidad con que se ejecutaran las revisiones, los procesos para el otorgamiento y restricción de accesos a sitios web, entre otros. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo

				de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, adjuntado además una copia del procedimiento documentado.

Uso del servicio

Durante el procedimiento se generaron reportes de tráfico de internet obtenidos mediante el firewall Palo Alto y la consola de administración de enrutadores Meraki.

Mediante esta revisión se analizó el uso que los funcionarios, asesores y otras personas hacen del servicio de internet institucional.

Además, se verificaron accesos que se han otorgado a diferentes personas como excepciones para permitir la navegación en sitios web de transmisión de videos, redes sociales, entre otros; así como políticas o directrices que regulen esa gestión.

De lo anterior, se logró obtener información que llevó a esta auditoría al planteamiento del siguiente hallazgo:

2.4	Durante la revisión de tráfico de internet se detectaron conjuntos de usuarios a quienes se les asignó a nivel de firewall, la regla "Libre Tránsito" y otros a quienes se les otorgó acceso para navegación en sitios web de transmisión de videos (como Youtube por ejemplo), y que no evidencian contar con una autorización o justificación para contar con esos accesos de manera permanente, así mismo, tampoco se encontró	Causas: No se dispone de una política para el otorgamiento y declinación de accesos "especiales" a servicios de internet así como para la asignación de reglas que permitan un "libre tránsito" de los usuarios que navegan en sitios web. Así mismo, a nivel de firewall y enrutadores, no se encuentran debidamente configuradas las reglas o políticas que restrinjan accesos	Según lo indicado por: – Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), sub normas 1.4.4 inciso c, 1.4.5, incisos a, d y e, y la 4.2, inciso a. – Directriz para el Uso del Servicio de Correo Electrónico y Acceso a	A la Alcaldía Municipal: **2.4.1** Desarrollar, documentar y poner en práctica, un procedimiento que regule y controle el otorgamiento de todos los accesos a servicios específicos de internet, desde el otorgamiento de accesos estándares a servicios básicos de internet hasta accesos de "libre tránsito" o especiales para sitios web específicos o restringidos. El procedimiento debe establecer, entre otros, cuáles son los medios y canales

	alguna norma o directriz que regule la autorización y otorgamiento de reglas a esos usuarios que les permita acceder a esos sitios web o contar con la regla antes mencionada. Adicionalmente, se observaron usuarios utilizando la red institucional para acceder a servicios de entretenimiento como por ejemplo Netflix, cuyos tiempos de actividad superan en algunos casos dos horas de conexión que a su vez generan un alto consumo del ancho de banda de la red institucional.	a sitios web de entretenimiento, redes sociales, entre otros. <u>Efectos</u>: Esto se traduce en una significativa brecha de seguridad para las plataformas y activos institucionales, debido a que los usuarios tienen acceso ilimitado a diferentes sitios web de distintas categorías según la clasificación de Palo Alto, de manera que se abren la posibilidad de transferencia de archivos que podrían estar infectados con malware, que a su vez podría vulnerar la plataforma de comunicaciones de la institución, activos de tecnologías y la integridad de la información institucional. Adicionalmente, esta condición abre la posibilidad de que usuarios de los servicios de internet institucional, hagan un uso indebido de los recursos accediendo a servicios y sitios web que riñen contra el control interno institucional, y que a su vez podrían incurrir en desatención de sus labores, además podrían ocasionar suspensiones temporales de	Internet (MC-PSIN-0004), "Usos Aceptables", "Usos Inaceptables" inciso c., "Administración de la Red", inciso a, d, e, g y h, "Prohibiciones", inciso g.	oficiales para la solicitud de esos accesos, así como contar con la respectiva justificación y autorización por parte de las jefaturas inmediatas. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, en el que, además, se adjunte copia del documento recomendado. <u>Al Departamento de Informática:</u> **2.4.2** Proceder con la inhabilitación de los servicios y aplicaciones a nivel de la red de internet institucional, que no se ajusten a lo establecido en la Directriz para el Uso del Servicio de Correo Electrónico y Acceso a Internet (MC-PSIN-0004) y notificar a cada uno de los usuarios afectados para que se proceda según lo establecido en el procedimiento para el otorgamiento y control de accesos a servicios de internet indicado en la recomendación anterior.

		servicios esenciales para distintos procesos de la institución y potenciar incidentes que harían lentas las comunicaciones basadas en servicios de internet.		Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de tres meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, en el que, además, se adjunte una lista de los usuarios que fueron afectados, así como sus respectivas notificaciones.

Control de incidencias

Durante la revisión, se obtuvo acceso a la herramienta "Aranda" para el registro y control de incidencias relacionadas con la suspensión de servicios de internet.

De lo anterior, se verificó la existencia de instrumentos de registros y medición de las incidencias, sin embargo, se determinó el siguiente hallazgo:

2.5	Áreas y procesos críticos de la institución son vulnerables a suspensiones temporales (*que incluso han significado períodos mayores a 5 horas*) de las comunicaciones indispensables para la ejecución de labores que son clave para la institución.	<u>Causas:</u> Las causas que provocan esta condición obedecen en gran parte en factores externos propios de la prestación del servicio del proveedor hacia la institución. <u>Efectos:</u>	Según lo indicado por: –Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), norma 1.4.7.	<u>Al Departamento de Informática:</u> **2.5.1** Elaborar, aprobar y documentar un plan de contingencia que permita garantizar la disponibilidad de los servicios de internet y correo electrónico de las áreas críticas de la institución que requieren de la

		Derivado de esto, cada vez que se produce la suspensión del servicio de internet, las comunicaciones de áreas claves de la municipalidad se ven afectas pues algunos de sus procesos dependen de estos servicios para llevarse a cabo, como son las gestiones de facturas electrónicas, transferencias bancarias, consultas a bases de datos externas de propiedades, pagos de nóminas y proveedores, entre otros. Esto significa un riesgo de afectación y paralización de servicios municipales en sus ámbitos operacionales y administrativos, lo que atenta contra el principio de disponibilidad de la información y el control interno.		conectividad con bases de datos externas y entidades financieras. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de tres meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como adjuntar una copia del documento al que se refiere esta recomendación.

Administración de enrutadores

Para la revisión programada en este procedimiento, se realizó un análisis comparativo entre los equipos de cómputo y dispositivos móviles registrados como activos municipales, y la lista de equipos o dispositivos conectados a las redes inalámbricas de la municipalidad, para de esta manera determinar la existencia de equipos no autorizados que hacen uso de los recursos de red institucional.

Así mismo, se revisó la existencia de procedimientos para la gestión de accesos a dichas redes inalámbricas y mecanismos de control implementados por la administración para efectos de administrar los servicios inalámbricos de la red institucional.

Durante el procedimiento de examen de administración de enrutadores inalámbricos, se solicitó en varias ocasiones que se suministrada a esta auditoría, copia de los contratos de los servicios de internet prestados por los proveedores a la institución, así como que se facilitara un recurso humano del Departamento de Informática con acceso a las consolas administrativas de los equipos de difusión de señal inalámbrica de internet de todos los sitios de dominio institucional en donde usuarios y funcionarios de la Municipalidad de Curridabat cuentan con accesos a internet institucional, sin embargo, no se aportó información concisa de lo solicitado y tampoco se asignó ningún funcionario para realizar las labores señaladas.

En este procedimiento surgieron los siguientes hallazgos:

2.6	No se cuentan con controles sobre los niveles de servicios de internet que se prestan a la municipalidad, su disponibilidad, soporte y calidad, entre otros aspectos atinentes a su continuidad.	Causas: No se cuenta con los contratos físicos o los acuerdos de servicios de de internet. Efectos: Desconocimiento de los términos contractuales por la prestación de servicios de internet, obligaciones de las partes, así como las cláusulas que detallen acciones sancionatorias en caso de eventuales incumplimientos.	Según lo indicado por: –Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), norma 4.1.	Al Departamento de Informática: **2.6.1** Solicitar a los proveedores copia de los acuerdos de servicios o los contratos de los servicios de internet con que cuenta la institución y desarrollar e implementar los mecanismos de control que permitan monitorear de forma periódica el cumplimiento de los acuerdos o cláusulas establecidas. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de un mes calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como adjuntar una copia de cada uno de los contratos a los que se refiere esta

				recomendación y los controles adoptados según lo recomendado.
2.7	Dentro de la lista de usuarios administradores de la herramienta Meraki se encontró activo a un exfuncionario del Departamento de Informática que dejó de laborar para la institución hace varios meses.	Causa: No se llevó a cabo una debida gestión de usuarios que permitiera realizar la debida desactivación del exfuncionario. Efectos: Esto potencia riesgos asociados a la seguridad de las comunicaciones institucionales y la información al existir la posibilidad de que otras personas (o incluso el mismo exfuncionario) tengan accesos administrativos a las herramientas institucionales utilizando el usuario de esa persona para llevar a cabo acciones que pondrían en riesgo la infraestructura.	Según lo indicado por: - Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), sub norma 1.4.5, incisos d y f.	Al Departamento de Informática: **2.7.1** Inhabilitar de la herramienta Meraki todos los accesos administrativos de usuarios correspondientes a exfuncionarios de la institución y adoptar las medidas correspondientes para que situaciones similares no se vuelvan a repetir. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de siete días hábiles, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación.
2.8	Se encontró que dispositivos móviles (tabletas y teléfonos móviles) que al parecer no son oficiales o activos municipales, registran conexiones a distintos SSID de redes principales de la Municipalidad de Curridabat, dentro de las cuales se logran visualizar los siguientes	Causas: No se pone en práctica un control para el otorgamiento de accesos a las redes inalámbricas instituciones en el cual solo se concedan accesos a equipos y dispositivos oficiales o a aquellos que cuenten con una autorización y justificación debidamente documentada.	Según lo indicado por: - Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), normas 1.4.4, incisos a y c,	Al Departamento de Informática: **2.8.1** Analizar cada caso para proceder, según corresponda, a excluir o bloquear de los SSID de redes principales de la institución de todas las oficinas municipales, a todos aquellos equipos y dispositivos móviles que no son propiedad de la Municipalidad de

	puntos de acceso: AlcaldíaH, Edificio Principal - Cuarto Piso, MC-La Cometa-A2, CDH-El Hogar-A1, MC-La Cometa-A3, CDH-El Tiribi-A1, CDH-El Hogar-A3, MC-La Cometa-A1, CDH-El Tiribi-A3, Edificio Principal - Segundo Piso, Edificio Principal - Primer Piso y MC-La Piscina. Adicionalmente, verificando las políticas de seguridad y mecanismos de control aplicados a estos equipos, se determinó que todos estos puntos de acceso a las redes principales se encuentran abiertos a que los usuarios de los dispositivos conectados accedan directamente a la LAN municipal o principal de la oficina donde se ubique.	<u>Efectos:</u> Esta condición evidencia una importante brecha de seguridad de la información y las telecomunicaciones que falta al control interno y mejores prácticas en temas de ciberseguridad al exponer la red institucional a infecciones de malware, ciberataques, robos de información, entre otros.	1.4.5, incisos a, d, e, y f.	Curridabat, con excepción de aquellos que cuenten con una debida autorización y justificación documentada, y tomar las medidas preventivas necesarias para que las contraseñas de accesos a esos SSID sean única y exclusivamente del conocimiento del administrador de las redes y jefatura del Departamento de Informática, así como implementar las acciones preventivas necesarias para evitar que equipos y dispositivos no oficiales, que no cuenten con autorización y justificación documentada, se vuelvan a conectar a esas SSID. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, en el que además se adjunte una lista de todos los equipos y dispositivos que fueron excluidos o bloqueados de las SSID de redes principales, así como una descripción de los controles adoptados según lo recomendado.

Otorgamiento y declinación de accesos

Se llevó a cabo una revisión general sobre la existencia de procedimientos o directrices que regulen el otorgamiento y declinación de accesos de usuarios a las redes inalámbricas de la institución, así como filtros o políticas que limiten dichos accesos a sitios web permitidos, aplicaciones y servicios como herramientas de trabajo.

Durante este análisis se detectó lo siguiente:

2.9	El otorgamiento de acceso a las redes wifi de la Municipalidad de Curridabat para usuarios funcionarios, asesores e invitados, se da de manera subjetiva y carente de controles.	Causas: No se cuenta con ninguna norma, directriz o procedimiento que regule el otorgamiento y restricción de accesos de usuarios o dispositivos a las distintas redes wifi de la institución. Efectos: Esta situación provoca que se otorguen accesos a diferentes usuarios sin que se midan los privilegios y restricciones a los que estos deberían tener, así como los tiempos para la revocación de permisos temporales. Esto potencia riesgos asociados al uso no correcto de los servicios oficiales de	Según lo indicado por: –Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), norma 1.4.5, incisos a, d, e y f.	A la Alcaldía Municipal: **2.9.1** Desarrollar, documentar y poner en práctica un procedimiento detallado que defina los perfiles de usuarios, equipos y dispositivos que contarán con acceso a las redes wifi de la institución, que a su vez contemple los niveles de acceso y restricción en la red. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de lo recomendado, así como adjuntar una copia del documento al que se refiere esta recomendación.

		comunicaciones, lo que además pondría en riesgo la infraestructura tecnológica, riesgos de imagen, divulgación sin control de las claves de acceso a los servicios de internet, entre otros.		<u>Al Departamento de Informática:</u> **2.9.2** Definir, documentar y poner en práctica una política para la parametrización y activación de los filtros correspondientes en cada uno de los enrutadores y puntos de acceso a las SSID de las redes principales de trabajo y de invitados, de manera que se aseguren los accesos a esas redes solo a los equipos y dispositivos que sean activos municipales o que cuenten con una justificación válida, autorizada y documentada. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de lo recomendado, así como adjuntar una copia del documento al que se refiere esta recomendación.

ÁREA DE EXAMEN 2: SERVICIO DE CORREO ELECTRONICO

Regulaciones internas

Se llevó a cabo una revisión para verificar la existencia e implementación de regulaciones internas en la institución para el monitoreo y control, relevantes al uso y administración de los servicios de correo electrónico municipal.

Una vez realizado el análisis de la información obtenida se logró determinar que la institución sí se cuenta con directrices, reglamentos y procedimientos por parte de la administración en cuanto al uso del correo electrónico municipal, sin embargo, se halló una condición que se indica a continuación:

2.10	Se han detectado cadenas masivas de correo electrónico no deseado (también conocido como correo "spam" o correo basura) generadas y divulgadas desde cuentas oficiales de correo de la Municipalidad de Curridabat, mismas que son utilizadas por funcionarios que omiten adoptar medidas básicas para prevenir este tipo de cadenas masivas de correo.	Causa: Esta situación se debe especialmente a la ausencia de lineamientos predefinidos que pauten el actuar de los funcionarios ante el envío o recepción de correos masivos. Así mismo, según se desprende en el sondeo realizado y analizado durante el procedimiento B.01.02 de este estudio, la falta de capacitación en el uso de las herramientas de correo electrónico institucional podría ser un factor que incide en esta condición. Efectos: El correo electrónico no deseado es también considerado un factor de riesgos de información para las	Según lo indicado por: – Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), subnorma 1.4.2, incisos a y b, subnorma 1.4.4, inciso c. – Directriz para el Uso del Servicio de Correo Electrónico y Acceso a Internet (Versión 1.2), número 3.4 "Uso del Correo Electrónico", inciso b y f.	Al Departamento de Informática: **2.10.1** Instruir a todos los usuarios del correo electrónico municipal para que adopten las medidas correspondientes con el fin de evitar la generación y divulgación de cadenas masivas de correos electrónicos no deseados interna y externamente de la Municipalidad de Curridabat. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como adjuntar una copia del comunicado emitido a todos los usuarios del servicio de correo electrónico municipal.

		organizaciones y personas particulares, estos suelen ser fuentes de ataques mediante distribución de "malware" y fuentes de información para extracción de datos mediante técnicas de ingeniería social como "phishing". El no adoptar medidas preventivas y correctivas ante escenarios de recepción y distribución masiva de correos electrónicos potencian riesgos de seguridad de la información y de las comunicaciones. Adicionalmente, la vulnerabilidad en el establecimiento de controles que prevengan el correo "spam", potencia que los usuarios falten a las disposiciones institucionales relacionadas con el uso correcto y aceptable del correo electrónico institucional.		**2.10.2** Llevar a cabo las diligencias necesarias ante la entidad correspondiente para que se modifique de la directriz "Directriz para el Uso del Servicio de Correo Electrónico y Acceso a Internet" de manera que se incluya las pautas y controles que coadyuven en la mitigación de la generación y divulgación masiva de correos electrónicos no deseados. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de dos meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como adjuntar una copia de la directriz actualizada con los controles adoptados en atención de la presente recomendación.

Uso del servicio

Para este procedimiento se llevó a cabo una revisión general para determinar la implementación de instrumentos de tecnología que permitan el monitoreo, control y medición del uso que los usuarios hacen del correo electrónico institucional.

Derivado de los análisis realizados, se determinó el siguiente hallazgo:

2.11	La consola de administración del servicio de correo electrónico (G Suite Basic) con que cuenta la institución, no contempla mecanismos de trazabilidad o pistas de auditoría que permitan determinar de forma detallada y dar seguimiento al uso que los funcionarios municipales hacen de dicho servicio. Lo anterior por cuanto la consola señalada solo cuenta con mecanismos básicos de monitoreo que únicamente permiten obtener resultados macros del tráfico de correo electrónico, sin embargo, no permiten dar seguimiento a casos específicos.	<u>Causas:</u> La licencia de la herramienta G Suite Basic corresponde a un paquete de servicio que solo aporta mecanismos básicos de monitoreo y administración. <u>Efectos:</u> Derivado de esto, no es posible medir con exactitud y de forma detallada el tráfico de correo electrónico, así como determinar los usos que los usuarios dan a las cuentas de correo. Lo anterior crea una brecha de control al no permitir medir y analizar la información antes citada, lo que se traduce en una debilidad de control interno. Adicionalmente, esta situación podría limitar algunas de las responsabilidades encomendadas al Departamento de Informática según la Directriz para el uso	Según lo indicado por: –Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), subnorma 1.4.5, inciso j.	<u>Al Departamento de Informática:</u> **2.11.1** Llevar a cabo las gestiones correspondientes a fin de dotar a la institución de un servicio de correo electrónico cuya herramienta administrativa permita implementar mecanismos de control y auditoría con la capacidad de monitorear el tráfico de correo electrónico institucional, así como establecer una trazabilidad detallada de al menos, el origen y destino de los mensajes de correo electrónico, dentro del marco legal costarricense. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de tres meses calendario, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación.

		del servicio de correo electrónico y acceso a internet (versión 1.2) en su punto 3.2, incisos a, d, e y f.		

Control de incidencias

Durante la revisión de la información sujeta de análisis para este procedimiento, se observó la utilización de una herramienta de gestión de dominio de correo electrónico que integra algunos mecanismos de alertas que brindan un soporte a la administración para conocer eventuales actividades sospechosas, incidentes, tráfico irregular de correo electrónico, entre otros.

De lo anterior, se logra determinar que la institución sí cuenta con un control y registro de incidencias relacionadas con el servicio de correo electrónico oficial de la institución.

Control de acceso al servicio

Como parte de este procedimiento, se llevó un análisis sobre la existencia y puesta en práctica de procedimientos documentados para el otorgamiento y declinación de accesos a los servicios de correo electrónico institucional y la respectiva gestión de usuarios.

Adicionalmente, se llevó a cabo una revisión de accesos a las cuentas de correo electrónico de exfuncionarios, derivado de lo cual se encontró la siguiente condición:

2.12	Se han encontrado cuentas de correo electrónico activas pertenecientes a exfuncionarios municipales que dejaron de laborar para la institución hace más de seis meses e incluso se registran accesos a dichas cuentas durante el mes de enero de 2020 en algunos de los casos. (Ver evidencia en el	<u>Causas:</u> Omisión o debilidad en el control del cumplimiento de lo establecido en el procedimiento "Mantenimiento de Cuentas de Exfuncionarios". <u>Efectos:</u> La existencia de cuentas activas de correo electrónico oficiales de la Municipalidad de	Según lo indicado por: –Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), sub normas 1.4.4, incisos a, b y 1.4.5, inciso a.	<u>Al Departamento de Informática:</u> **2.12.1** Proceder con la inactivación inmediata de todas las cuentas de correo de electrónico oficial correspondientes a exfuncionarios municipales y adoptar las medidas necesarias para que la situación no se vuelva a presentar.

	procedimiento B.02.04 – Tareas realizadas / Fecha: 28/01/2020 puntos 7, 8, 9 y10).	Curridabat que le fueron asignadas a exfuncionarios mientras estos formaban parte de la institución, supone un grave riesgo de seguridad de la información que además potencia otros riesgos asociados con eventuales fraudes, riesgos de imagen, entre otros. Mientras esas cuentas de correo electrónico sigan activas, existe la posibilidad de que la misma persona a quien le fue asignada esa cuenta haga uso indebido de la misma, a su vez, terceras personas podrían tener acceso a las credenciales de dichas cuentas y hacer usos indebidos de estas.		Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de tres días hábiles, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como incluir una descripción de las medidas adoptadas para mitigar el riesgo de que esta situación vuelva a ocurrir. <u>Al Departamento de Recursos Humanos:</u> **2.12.2** Instaurar un mecanismo que permita informar de forma oportuna al Departamento de Informática cada vez que algún colaborador deja de formar parte de la Municipalidad de Curridabat. Para dar por atendida esta recomendación, se debe remitir por medio de correo electrónico a esta auditoría, en un plazo máximo de cinco días hábiles, un oficio (firmado digitalmente) donde se comunique el cumplimiento de esta recomendación, así como incluir una descripción del mecanismo que será adoptado para cumplir con lo recomendado.

3. CONCLUSIONES

Los servicios de internet y correo electrónico institucional deben ser controlados como las herramientas de trabajo que son, los cuales son instrumentos fundamentales para la gestión de comunicación de información que a su vez resulta ser un activo organizacional y, por ende, deben ser controlados y mitigados los riesgos asociados a estas comunicaciones.

Por lo anterior, la institución debe mejorar y fortalecer la gestión de accesos a dichos servicios utilizando para ellos las herramientas de tecnologías con que se cuentan actualmente, configurando para esto políticas que coadyuven en la restricción de accesos a servicios, aplicaciones y sitios web no autorizados, así como controlando el uso del correo electrónico solo para asuntos que competen a las funciones y operaciones institucionales.

Adicionalmente, la capacitación de los usuarios junto a un proceso de actualización y concientización son fundamentales para que los funcionarios comprendan la importancia de la implementación de las mejores prácticas en el control y uso de los servicios de internet y correo electrónico.

Aunado a lo anterior, es indispensable contar con procesos y directrices debidamente documentados que además contemplen los instrumentos para el registro y monitoreo de los servicios sujetos de este estudio.

LUIS FERNANDO SOLIS HERNANDEZ (FIRMA)
Firmado digitalmente por LUIS FERNANDO SOLIS HERNANDEZ (FIRMA)
Fecha: 2020.02.05 09:29:45 -06'00'

Luis F. Solís Hernández
Profesional Analista de Auditoría

GONZALO ANTONIO CHACON CHACON (FIRMA)
Firmado digitalmente por GONZALO ANTONIO CHACON CHACON (FIRMA)
Fecha: 2020.02.05 09:21:27 -06'00'

Gonzalo Chacón Chacón
Auditor Interno