MUNICIPALIDAD DE CURRIDABAT

Un servicio profesional comprometido
con la objetividad y el servicio al cliente

INFORME AM-001-2018

EVALUACION DEL SISTEMA DE BIENES INMUEBLES

Realizado por:
Luis Fernando Solís Hernández

Supervisado por:
Gonzalo Chacón Chacón

Enero 2018

INDICE

RESUMEN EJECUTIVO

¿Qué se examinó?

Los módulos del Sistema de Cobro Municipal (*en adelante identificado como SCM*) correspondientes a los procesos de Bienes Inmuebles de la Dirección de Sistemas de Información Territorial.

Los mecanismos para el resguardo de la seguridad y disponibilidad de la información, y la seguridad de los activos de tecnología relacionados con el SCM y los procesos de bienes inmuebles.

¿Por qué es importante?

El SCM procesa información perteneciente, entre otros, a la recaudación de impuestos de bienes inmuebles que si no se cuenta con los mecanismos que aseguren un correcto flujo de la información, así como la integridad de los datos en bases de datos, servidores y cualquier otro medio de almacenamiento, elevan los niveles de riesgo de robo y pérdida de información, modificación no autorizada de los datos e incluso la comisión de posibles delitos contra el erario municipal.

¿Qué se encontró?

Mecanismos de control débiles e incluso inexistentes en algunas áreas de examen; información de nombres de usuario, contraseñas, perfiles y roles de usuarios internos de la Municipalidad de Curridabat, expuesta para que personas no autorizadas puedan hacer uso de ella; información personal de contribuyentes, propiedades y datos financieros expuestos a personas no autorizadas; un sistema informático que no genera un registro claro de las transacciones realizadas (*pistas de auditoría*) e información imprecisa que imposibilita el cumplimiento de algunos de los objetivos del control interno.

¿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 AI para el período 2017, el cual es del conocimiento del Concejo Municipal y comunicado a la CGR.

1.2 Objetivo

Determinar la confiabilidad y suficiencia de la información, así como la idoneidad de los mecanismos y controles contemplados para su seguridad.

1.2.1 Específicos

- Verificar la suficiencia de los mecanismos de control que garanticen la confiabilidad y oportunidad de la información.
- Realizar pruebas para determinar la suficiencia e idoneidad de los controles implementados por parte del Departamento de Informática.
- Corroborar la existencia e implementación de políticas que procuren la confiabilidad y oportunidad de la información.
- Revisar los controles que garanticen la seguridad de los equipos que albergan bases de datos, códigos fuentes y ejecutables en producción.

1.3 Alcance

El estudio abarca la revisión de controles de seguridad de la información y de activos de tecnología relacionados con el SCM específicamente lo atinente a Bienes Inmuebles y la información que ahí se genera.

La información que se analiza corresponde al período comprendido entre el 01 de enero de 2016 y el 31 de enero de 2017.

No son objeto del estudio las actividades que lleva a cabo la administración en términos del cumplimiento de la Ley N°7509, así como los controles o tareas propias de la Dirección de Sistemas de Información Territorial.

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 efectividad del SCM específicamente los módulos de Bienes Inmuebles que estén alineados con lo establecido en la normativa legal, técnica y administrativa aplicable.

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 al alcance

No se presentaron limitaciones durante el desarrollo del presente estudio.

1.7 Comunicación de Resultados

El pasado 24 de enero de 2018, la Auditoría Interna, mediante una reunión denominada “conferencia final” dio a conocer al Ing. Federico Sánchez Díaz, Coordinador del Departamento de Informática, al Ing. Douglas Alvarado Ramírez, Director de Sistemas de Información Territorial y al Lic. Emerson Meneses Méndez, Jefe Tributario , funcionarios de la Administración, los resultados a los cuales se llegó en el desarrollo del estudio, así como las conclusiones y las recomendaciones que a criterio de esta Auditoría deberían girarse.

Adicionalmente, no se contó con la participación del Lic. Huberth Méndez Hernández, Gerente Territorial, a quien se le extendió invitación por medio del oficio AIMC-009-2018 para que asistiera a la conferencia final para conocer el informe.

Tomando en consideración que los funcionarios antes mencionados que asistieron a la reunión avalaron lo expuesto, se sometió 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 expusieron el presente informe el Lic. Luis Fernando Solís Hernández, Profesional Analista de Auditoría y el Lic. Gonzalo Chacón Chacón, Auditor Interno.

2. RESULTADOS

	Condición	Causas / Efectos	Criterios	Recomendaciones
▪ **PLAN DE CONTINGENCIA Y RECUPERACIÓN**				
2.1	Carencia de un Plan de Contingencia y de un Plan de Recuperación[1].	Causas: No se logró evidenciar la existencia de un análisis de riesgos tecnológicos ni un Sistema de Evaluación de Riesgo, los cuales son requeridos para generar los planes de contingencia y recuperación. Efectos: La institución se expone a riesgos como los que se indican a continuación: Pérdida parcial o total de la información; daño o pérdida parcial o total de los activos de tecnología; suspensión parcial o total de los servicios municipales; afectaciones directas e indirectas en las finanzas institucionales; daños importantes en la infraestructura tecnológica de la institución, así como posibles daños de la estructura física.	▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), Normas 5.7.4 y 5.9. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), Normas 1.3 y 1.4.	A la Gerencia Territorial: Girar las instrucciones al Departamento de Informática para que en conjunto con las demás áreas usuarias de la Municipalidad de Curridabat realicen lo siguiente: **2.1.1** – En un plazo no mayor al 28/09/2018, elaborar y aprobar un plan de contingencias y recuperación de desastres que considere al menos lo siguiente: a) Identificar los servicios críticos y priorizar el orden de restauración según esa criticidad. b) Identificar la infraestructura crítica, la cual se le dará prioridad según el punto anterior. c) Monitoreo y reporte de la disponibilidad de los recursos críticos. d) Procesamiento de información alternativo. e) Alineamiento con los principios de respaldo y recuperación de datos. f) Roles y responsabilidades de los encargados de ejecutar el plan. g) Procesos de comunicación/distribución durante la ejecución del plan. h) Planeación de las pruebas respectivas del plan de contingencia y continuidad.

[1] *Esto se desprende de un informe realizado por la firma Carvajal en el período 2016, comunicado a la Administración mediante la Carta de Gerencia TI-I-2016, en la misma que se indica el compromiso de la Administración por cumplir con las recomendaciones emitidas en el informe señalado durante el segundo semestre del 2017, no obstante, el Coordinador del Departamento de Informática aseguró que "Se está trabajando en este Plan y se finalizará su desarrollo para este año -2017-, previendo su implementación para el 2018."*

	Condición	Causas / Efectos	Criterios	Recomendaciones
				i) Mantenimiento y actualización del plan de contingencias y continuidad j) Entrenamiento/capacitación de las partes involucradas respecto a los procesos y sus roles y responsabilidades. k) Revisión post-reanudación para mejorar el plan de acuerdo con los resultados obtenidos. Para dar por atendida esta recomendación se deberá aportar una copia certificada del plan debidamente aprobado al que hace referencia el punto 2.1.1.
▪	**NORMALIZACIÓN DE LOS DATOS**			
2.2	El SCM no registra en base de datos todos los datos que se ingresan por medio de la aplicación.	Causas: Ausencia de un control de calidad de los sistemas de información desarrollados por la institución, debidamente estructurado y documentado que permita registrar un adecuado control de cambios y un adecuado análisis de posibles fallas u omisiones de las aplicaciones; carencia de un marco para desarrollo e implementación de sistemas informáticos. Efectos: Información municipal poco confiable; datos imprecisos e incorrectos; Eventuales errores a nivel de procesos internos de diversas áreas usuarias que requieren de esta información.	▪ Ley General de Control Interno (*Ley N°8292*), artículo 15, inciso V. y artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), Norma 5.1, 5.2, 5.3, 5.4, 5.6, 5.7 (*5.7.4*), 5.8, 5.9 y 6.4. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), Norma 1.2, 1.4 (*1.4.4*), 2.2 y 4.3. ▪ Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (*Ley N°8968*), artículos 6 y 10.	A la Gerencia Territorial: Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.2.1** – En un plazo no mayor al 28/05/2018, establecer y poner en práctica un procedimiento para el aseguramiento de la calidad de los programas informáticos desarrollados por la Municipalidad de Curridabat, en el cual se integren políticas y parámetros que permitan estandarizar la información que se ingresa a las bases de datos institucionales, así como políticas de revisión y mantenimiento de las aplicaciones y los datos que por estas se procesan. Para dar por atendida esta recomendación se deberá aportar una certificación que indique la disposición, documentación y

	Condición	Causas / Efectos	Criterios	Recomendaciones
				puesta en marcha del procedimiento al que hace referencia el punto 2.2.1. **2.2.2** – En un plazo no mayor al 28/05/2018, hacer una revisión detallada de la funcionalidad y controles de los campos de los formularios que integran los módulos de bienes inmuebles del SCM, y en caso de ser requerido realizar los ajustes y mejoras correspondientes. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de la revisión solicitada, así como los ajustes o mejoras que se realicen, según lo señalado en el punto 2.2.2.
2.3	Ausencia de mecanismos a nivel de aplicación que garanticen la normalización de los datos registrados en bases de datos. **Esta situación también se dio a conocer a la Administración mediante informe de auditoría externa según consta en carta de gerencia CG-1-2016 del Despacho Carvajal & Colegiados con fecha del 23/05/2017.*	Causas: Ausencia de control de calidad de los sistemas desarrollados por la institución; carencia de un marco para desarrollo e implementación de sistemas informáticos que contemplen la integración de mecanismos de control que coadyuven a asegurar que los valores que ingresan los usuarios, por medio de la aplicación, cumplan con las características mínimas necesarias para que la información sea confiable. Efectos: Registro de información incompleta, incongruente y que no cumple con el objetivo de mantener información de	▪ Ley General de Control Interno (*Ley N°8292*), artículo 15, inciso V. y artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), Norma 5.1, 5.2, 5.3, 5.4, 5.6, 5.7 (*5.7.4*), 5.8, 5.9 y 6.4. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), Norma 1.2, 1.4 (*1.4.4*), 2.2 y 4.3.	A la Gerencia Territorial: Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.3.1** – En un plazo no mayor al 31/05/2018, realizar los ajustes y correcciones en todos los formularios de los módulos de bienes inmuebles del SCM con el fin de implementar mecanismos de control que impidan que los usuarios del sistema ingresen datos incompletos, con valores no válidos[2] o dejen en blanco los espacios de datos que podrían ser considerados como

[2] *Valores que podrían ser considerados como no válidos: Caracteres especiales en campos en donde solo se deberían de admitir números, espacios en blanco en donde no deberían de existir (por ejemplo: número de identificación, número de teléfono, etc), entre otros.*

	Condición	Causas / Efectos	Criterios	Recomendaciones
		calidad que sirva a los propósitos de la institución; ingreso de datos no válidos e incompletos que consumen gran espacio en la base datos; ingreso de información repetida que podría generar trabajos extraordinarios de depuración por parte de las áreas usuarias; ingreso de información incompleta que no genera valor a las funciones de las áreas usuarias y a la institución en general. Adicionalmente, se determinó que la ausencia de los mecanismos a los que hace la referencia la condición encontrada ha incidido en que el 58.6% de los campos de la tabla "Contribuyentes" en la base de datos, de una muestra de 25% de los registros de esa entidad, se encuentran vacíos, contienen datos incompletos, valores confusos, que podrían considerarse no válidos o que no se encuentran actualizados. Derivado de lo anterior, la información es inexacta y poco confiable pues su integridad no está asegurada, lo que podría incidir en la ejecución de otros procesos de las áreas usuarias de los datos como por ejemplo la localización de bienes inmuebles y contribuyentes para notificaciones u otras gestiones, la recuperación del pendiente de cobro, entre otros.	▪ Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (*Ley N° 8968*), artículos 6 y 10.	básicos[3] y necesarios para la gestión municipal. Para dar por atendida esta recomendación se deberá aportar una certificación que indique la realización de los ajustes y mejoras solicitadas según lo señalado en el punto 2.3.1. **2.3.2 –** En un plazo no mayor al 01/05/2018, identificar y depurar todos los datos de pruebas, datos duplicados, entidades de pruebas en la base de datos, entre otros aspectos que la administración considere necesario para la normalización de la información, para lo cual debe tomar las previsiones y contingencias necesarias con el fin de garantizar la integridad de los datos. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.3.2. Girar las instrucciones a la Dirección de Sistemas de Información Territorial y demás áreas usuarias de la información institucional, para que realicen lo siguiente: **2.3.3 –** En un plazo no mayor al 31/03/2018 se disponga de un plan que permita la recolección y actualización de información de los contribuyentes en bases de datos.

[3] *Datos que podrían ser considerados como básicos para la gestión municipal en el contexto de este estudio: Número de identificación, nombre de contribuyente, número de teléfono, dirección física del contribuyente, etc.*

	Condición	Causas / Efectos	Criterios	Recomendaciones
				Para dar por atendida esta recomendación se deberá aportar una certificación que especifique el plan que la administración ejecutará según lo indicado en la recomendación 2.3.3.
2.4	Tablas de datos en la base de datos no tienen configuradas las reglas de validación en campos cuyos valores son necesarios para diversos procesos de la gestión municipal.	Causas: No se ha implementado un marco estandarizado para el diseño de base datos y cada uno de sus elementos; No se ha implementado un adecuado plan para el monitoreo y mantenimiento de la base de datos. Efectos: Registro de información incompleta, incongruente y que no cumple con el objetivo de mantener información de calidad que sirva a los propósitos de la institución; Ingreso de datos no válidos e incompletos que consumen espacio en la base datos; Ingreso de información repetida o confusa que podría generar trabajos extraordinarios de depuración por parte de las áreas usuarias; Ingreso de datos no válidos e incompletos que no generan valor a las funciones de las áreas usuarias y a la institución en general.	▪ Ley General de Control Interno (*Ley N°8292*), artículo 15, inciso V. y artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), Norma 5.1, 5.2, 5.4, 5.6 (*5.6.1 y 5.6.2*), 5.7 (*5.7.4*), 5.8, 5.9 y 6.4. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), Norma 1.2, 1.4 (*1.4.4*), 2.2 y 4.3. ▪ Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (*Ley N°8968*), artículos 6 y 10.	A la Gerencia Territorial: Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.4.1** En un plazo no mayor al 30/07/2018, se disponga de un Marco para el Diseño y Monitoreo de las Bases de Datos de la Institución que contemple al menos lo siguiente: a) Documentación y actualización de diccionarios de datos detallando tipos de campos, tipos de llaves, relaciones, etc. b) Documentación de diagramas Entidad-Relación (*E-R*). c) Parametrización de campos de bases de datos según la naturaleza de la información que corresponde a los mismos. d) Plan para el testeo en ambiente de desarrollo, el cual debe integrar procedimientos de respaldo, contingencia y recuperación. e) Definición e implementación de roles y responsabilidades para el diseño, implementación y monitoreo de las bases de datos. Para dar por atendida esta recomendación se deberá aportar una copia certificada del

	Condición	Causas / Efectos	Criterios	Recomendaciones
				documento al que hace referencia el punto 2.4.1., indicando además un cronograma documentado que detalle los pasos para la implementación de dicho marco. **2.4.2** – En un plazo no mayor a los treinta días hábiles posteriores al cumplimiento de la recomendación 2.4.1, desarrollar e implementar un plan para realizar los ajustes necesarios a nivel de aplicación que aseguren el cumplimiento del marco al que hace referencia la recomendación 2.4.1, de manera que la información que vaya a ingresar a partir de la implementación de dicho marco reúna las características adecuadas propias de su naturaleza, para esto se deben contemplar las contingencias, pruebas y planes de recuperación respectivas. Para dar por atendida esta recomendación se deberá aportar una copia certificada del plan desarrollado e implementado según lo señalado en el punto 2.4.2.
▪	**SEGURIDAD DE ACTIVOS Y DATOS (*SEGURIDAD FÍSICA Y LOGICA*)**			
2.5	Las ventanas del cuarto de servidores (*Una de las cuales se ubica cerca del techo del estacionamiento del edificio que a su vez se comunica con la vía pública*), no cuenta con dispositivos de seguridad que impidan el ingreso de	Causas: Carencia de un marco oficializado para la gestión de riesgos de tecnologías de información que integre el análisis de riesgos como el expuesto; La Administración no ha detectado y valorado el potencial riesgo expuesto. Efectos: Actos de vandalismo que pongan en riesgo la integridad de los activos, los funcionarios e instalaciones; Robo o	▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), Norma 5.7.4. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), Norma 1.4 (1.4.3).	A la Alcaldía, Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.5.1** – En un plazo no mayor al 31/03/2018, reforzar la protección perimetral del cuarto de servidores de la institución contemplando para ello la incorporación de mecanismos de prevención (*principalmente en las ventanas*)

	Condición	Causas / Efectos	Criterios	Recomendaciones
	terceros desde el exterior del edificio municipal, lo que potencia el riesgo de robo o daños a los servidores que alojan los sistemas de información municipales, bases de datos y otros activos (*como equipos de telecomunicaciones, respaldo, monitoreo, entre otros*).*. **Esta situación fue notificada a la Administración mediante oficios AIMC-080-2017 y AIMC-094-2017, del cual se recibió respuesta el 03/08/2017 mediante oficio AMC-1091-07-2017.* **Esta situación también se dio a conocer a la Administración mediante informe de auditoría externa según consta en carta de gerencia CG-1-2016 del Despacho Carvajal & Colegiados con fecha del 23/05/2017.*	destrucción de activos de tecnología que a su vez podrían potenciar la paralización parcial o total de las operaciones de la institución; Robo o destrucción de información que a su vez podrían potencia la paralización parcial o total de las operaciones de la institución.		que ayuden a mitigar los riesgos de ingreso no autorizado, robo y/o daños en los activos de tecnología. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.5.1. **2.5.2** – En un plazo no mayor al 31/03/2018, reforzar la seguridad interna del cuarto de servidores de la institución contemplando para ello la incorporación de dispositivos para detección, monitoreo y alerta de ingresos no autorizados. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.5.2.
2.6	Las cajas para breakers (*centros de carga*) que regulan el suministro eléctrico del cuarto de servidores se ubican en una zona dentro del edificio la cual es de libre acceso para cualquier funcionario municipal. Esto facilitaría una	Causas: Carencia de un marco oficializado para gestión de riesgos de tecnologías de información que integre el análisis de riesgos como el expuesto; La Administración no ha detectado y valorado el potencial riesgo expuesto. Efectos: Riesgo de manipulación indebida de dispositivos que regulan el suministro eléctrico, lo que podría atentar contra la	▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), Norma 1.4 (*1.4.3 y 1.4.7*).	A la Alcaldía, Girar las instrucciones al Departamento de Informática para que en conjunto con la Gerencia Territorial realicen lo siguiente: **2.6.1** – En un plazo no mayor al 31/03/2018, disponer de mecanismos que protejan las cajas de breaker (*centros de carga*) y cualquier otro dispositivo de regulación del

	Condición	Causas / Efectos	Criterios	Recomendaciones
	inadecuada manipulación de los sistemas de control eléctrico del cuarto de servidores.*. **Esta situación fue notificada a la Administración mediante oficio AIMC-094-2017, del cual se recibió respuesta el 03/08/2017 mediante oficio AMC-1091-07-2017.* **Esta situación también se dio a conocer a la Administración mediante informe de auditoría externa según consta en carta de gerencia CG-1-2016 del Despacho Carvajal & Colegiados con fecha del 23/05/2017.*	integridad de las personas e instalaciones de la municipalidad; Riesgo de manipulación indebida de dispositivos que regulan el suministro eléctrico del cuarto de servidores de la institución, lo que potencia el daño de activos de tecnología y aumenta el riesgo de pérdida de información e interrupción parcial o total de los servicios municipales.		suministro eléctrico del cuarto de servidores, contra la manipulación inadecuada de los mismos. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.6.1.
2.7	Carencia de mecanismos que exijan a los usuarios del SCM realizar el cambio de contraseña de forma periódica.	Causas: No se pone en práctica una política que obligue a los usuarios a gestionar cambios de contraseñas de forma periódica; Ausencia de un marco de seguridad informática que contemple entre otras cosas, la gestión de contraseñas de usuarios. Efectos: Si los usuarios no llevan a cabo cambios de contraseñas periódicas, estas podrían ser vulnerables a que terceras personas logren obtenerlas e incurrir en delitos como usurpación de identidad con el fin de llevar a cabo operaciones y transacciones no autorizadas; La eventual fuga de contraseñas pondría en riesgo los datos institucionales y aumenta el riesgo de que se llevan a cabo transacciones no	▪ Ley General de Control Interno (*Ley N°8292*), artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), normas 5.7 (*5.7.4*) y 5.8. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), normas 1.4 (*1.4.1, 1.4.2, 1.4.4, 1.4.5 y 1.4.6*).	A la Gerencia Territorial: Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.7.1** – En un plazo no mayor al 26/03/2018, definir, documentar, oficializar, implementar y comunicar a los usuarios de una Política de Gestión de Contraseñas de usuarios que al menos señale lo siguiente: a) Que obligue a los usuarios a realizar un cambio de contraseñas cada período de tiempo. b) Que indique las características que deben reunir las contraseñas de los usuarios (*longitudes y tipos de caracteres aceptados*) y que obligue a los usuarios a utilizarlas.

	Condición	Causas / Efectos	Criterios	Recomendaciones
		autorizadas que podrían afectar entre otras cosas a las finanzas, operaciones, servicios e imagen de la institución.		Para dar por atendida esta recomendación se deberá aportar una copia certificada del documento al que hace referencia el punto 2.7.1.
2.8	No se evidencia la existencia de un proceso formal y seguro para el cambio y comunicación de contraseñas temporales a los usuarios.	Causas: No se pone en práctica una política que defina cuáles son los mecanismos correctos para que los usuarios realicen los cambios de contraseñas de forma segura y oportuna; No se ha implementado un marco de seguridad informática que contemple entre otras cosas, la debida gestión de contraseñas de usuarios; El SCM no cuenta con un mecanismo integrado para el cambio de contraseña de usuario. Efectos: Alto riesgo de fuga de contraseñas lo que potenciaría que terceras personas puedan ingresar a los sistemas municipales con credenciales de otros funcionarios; Riesgo de transacciones no autorizadas; Riesgo de modificaciones de información no autorizados; Riesgo de extracción y pérdida de información; Riesgo de paralización parcial y total de las operaciones y servicios municipales; Riesgo de comisión de delitos que involucren las finanzas institucionales.	▪ Ley General de Control Interno (*Ley N°8292*), artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), normas 5.7 (*5.7.4*) y 5.8. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), normas 1.4 (*1.4.1, 1.4.2, 1.4.4, 1.4.5 y 1.4.6*).	A la Gerencia Territorial, Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.8.1** – En un plazo no mayor al 30/04/2018, dotar al Sistema de Cobro Municipal de un mecanismo seguro por el cual los usuarios puedan realizar el cambio de su contraseña en el momento que lo requieran. Esto debe ser ejecutado en concordancia con la Política para la Gestión de Contraseñas a la que se refiere la recomendación 2.7.1. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.8.1.
2.9	Base de datos vulnerable ante posibles intrusiones de personas que con un conocimiento técnico básico podría acceder	Causas: Utilización de un gestor de base de datos que carece de controles suficientes para la seguridad de los datos; Gestor de base de datos que almacena todos los datos de la misma base de datos,	▪ Ley General de Control Interno (*Ley N°8292*), artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-*	A la Gerencia Territorial, Girar las instrucciones al Departamento de Informática para que realice lo siguiente:

	Condición	Causas / Efectos	Criterios	Recomendaciones
	hasta la ubicación de esos datos por medio de la red institucional. **Esta situación también se había dado a conocer a la Administración mediante los informes de auditoría interna AM-009-2011 "Revisión Control Interno en TI" y AM-002-2016 "Evaluación del Sistema de Facturación y Cobro".*	en solo archivo el cual es fácilmente corrompible desde diferentes sistemas operativos; Base de datos desprotegida y sin mecanismos activos de autenticación; A nivel de servidor no se cuenta con mecanismos de control y protección suficientes que restrinjan el acceso de usuarios no autorizados hasta la ruta en donde se aloja la base de datos. Efectos: Alto riesgo de alteración, robo y pérdida de información; Alto riesgo de robo de contraseñas de usuarios y comisión de delitos de usurpación de identidades; Riesgo de interrupción de servicios y operaciones; Riesgo de afectación financiera en la recaudación de impuestos; Riesgo de afectación de la imagen institucional; Riesgo de afectación en la prestación de los servicios institucionales, entre otros.	*2009-CO-DFOE*), normas 5.2, 5.3, 5.7 (*5.7.1 y 5.7.4*), 5.8 y 5.9. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), normas 1.4 (*1.4.1, 1.4.2, 1.4.4, 1.4.5, 1.4.6 y 1.4.7*).	**2.9.1** – En un plazo no mayor al 31/03/2018, dotar de los mecanismos de autenticación al gestor de bases de datos del SCM, para que únicamente usuarios autorizados tengan acceso a los datos ahí alojados. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.9.1. **2.9.2** – En un plazo no mayor al 01/08/2018, implementar una solución de base de datos que brinde herramientas de seguridad, monitoreo, control de usuarios, pistas de auditoría y registro de transacciones, que además permita la transaccionalidad y almacenamiento de volúmenes de información acorde con los requerimientos institucionales, y que cuente con una licencia que permita satisfacer las necesidades de la municipalidad observando y cumpliendo para ello las disposiciones legales referentes a este tema. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.9.2. **Esta recomendación (2.9.2), también se había dado a conocer a la Administración mediante el informe de auditoría interna AM-009-2011 "Revisión Control Interno en TI".*
2.10	Contraseñas de usuarios del SCM vulnerables, fácilmente accesibles por	Causas: Carencia de un procedimiento oficializado para gestión de usuarios; Utilización de un gestor de base de datos	▪ Ley General de Control Interno (*Ley N°8292*), artículo 16.	A la Gerencia Territorial:

	Condición	Causas / Efectos	Criterios	Recomendaciones
	medio de la red institucional y fácilmente descifrables. **Esta situación también se había dado a conocer a la Administración mediante el informe de auditoría interna AM-002-2016 "Evaluación del Sistema de Facturación y Cobro".*	débil que no integra controles suficientes que garanticen la seguridad de los datos; Los mecanismos de protección de la base de datos a nivel del servidor no son suficientes. <u>Efectos</u>: Extracción, modificación y eliminación no autorizada de datos de la institución; Alto riesgo de comisión de delito de suplantación de identidad de usuarios; Debido a que muchos usuarios suelen utilizar las mismas contraseñas para otros sistemas, correos electrónicos, redes sociales, entre otros, se eleva el riesgo de suplantación de identidad que a su vez podría potenciar otros riesgos como fraudes a nombre de la Municipalidad de Curridabat al tener la posibilidad de acceder a otras cuentas de correo electrónico de la institución, entre otros.	▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), normas 5.2, 5.3, 5.7 (*5.7.1 y 5.7.4*), 5.8 y 5.9. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), normas 1.4 (*1.4.1, 1.4.2, 1.4.4, 1.4.5, 1.4.6 y 1.4.7*).	Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.10.1** – En un plazo no mayor al 31/05/2018, implementar mecanismos de protección de contraseñas en bases de datos actual del SCM, que garanticen la protección de contraseñas, perfiles y demás datos de los usuarios de los sistemas municipales, a la vez que impidan la extracción de contraseñas por ningún medio o aplicación. Para dar por atendida esta recomendación se deberá aportar una certificación que indique el cumplimiento de lo indicado en la recomendación 2.10.1, así como las mejoras implementadas. **Esta recomendación (2.10.1), también se había dado a conocer a la Administración mediante el informe de auditoría interna AM-002-2016 "Evaluación del Sistema de Facturación y Cobro"*
2.11	La ruta de acceso a la base de datos es fácilmente detectable e identificable. ** Esta situación también se había dado a conocer a la Administración mediante el informe de auditoría interna AM-002-2016 "Evaluación del Sistema de Facturación y Cobro".*	<u>Causas</u>: La arquitectura del SCM (*Cliente - Servidor*), requiere que los ficheros (*ejecutables, bases de datos, entre otros*) se localicen en carpetas compartidas por medio de la red; Acorde con el diseño del Sistema de Cobro Municipal, para este poder localizar y acceder a la base de datos debe obtener la ruta de ficheros instalados en el entorno local; El SCM no cuenta con un procedimiento de encriptación y desencriptación de cadenas de texto alojadas en los archivos que contienen la ruta de la base de datos; Los	▪ Ley General de Control Interno (*Ley N°8292*), artículo 16. ▪ Normas de Control Interno para el Sector Público (*N-2-2009-CO-DFOE*), normas 5.2, 5.3, 5.7 (*5.7.1 y 5.7.4*), 5.8 y 5.9. ▪ Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (*N-2-2007-CO-DFOE*), normas 1.4 (*1.4.1,*	A la Gerencia Territorial: Girar las instrucciones al Departamento de Informática para que realice lo siguiente: **2.11.1** – En un plazo no mayor al 31/03/2018, realizar las correcciones y ajustes necesarios a nivel del SCM con el fin de proteger los archivos locales que alojan las rutas de servidores y bases de datos. Para dar por atendida esta recomendación se deberá aportar una certificación que

	Condición	Causas / Efectos	Criterios	Recomendaciones
		nombres de los archivos del SCM a nivel local, hacen que la información o parámetros alojados en ellos sean fácilmente descifrables e identificable. Efectos: Cualquier persona que tenga acceso a un equipo de cómputo municipal y si el mismo cuenta (*o en su defecto contó en algún momento y no ha sido formateado*) con la instalación del SCM, puede obtener con facilidad la ruta de acceso a la carpeta de red que contiene todos los archivos de la base de datos municipal así como los archivos del SCM, lo que aumenta el riesgo de extracción de contraseñas, robo de información, pérdida de información, alteración de información, comisión de fraudes, entre otros.	*1.4.2, 1.4.4, 1.4.5, 1.4.6 y 1.4.7*).	indique el cumplimiento de lo indicado en la recomendación 2.11.1. **Esta recomendación (2.11.1), también se había dado a conocer a la Administración mediante el informe de auditoría interna AM-009-2011 "Revisión Control Interno en TI" y AM-002-2016 "Evaluación del Sistema de Facturación y Cobro".*

3. CONCLUSIONES

Los módulos de los procesos de Bienes Inmuebles del Sistema de Cobro Municipal, así como la base de datos relacionada a este, cuentan con mecanismos que se presumen vulnerables y no permiten una adecuada mitigación de los riesgos de robo, pérdida y modificación no autorizada de información.

La institución es susceptible a mejoras en materia de seguridad de la información, que permitan disponer de controles más eficaces.

LUIS FERNANDO SOLIS HERNANDEZ (AUTENTICACION)

Firmado digitalmente por LUIS FERNANDO SOLIS HERNANDEZ (AUTENTICACION)
Razón: Soy el autor de este documento
Ubicación:
Fecha: 2018-01-26 15:19:50

Luis Fernando Solís Hernández
Auditor Analista

GONZALO ANTONIO CHACON CHACON (FIRMA)

Firmado digitalmente por GONZALO ANTONIO CHACON CHACON (FIRMA)
Razón: Estoy aprobando este documento con mi firma legalmente vinculante
Ubicación:
Fecha: 2018-01-26 15:50:40

Gonzalo Chacón Chacón
Auditor Interno