MUNICIPALIDAD DE CARTAGO

Informe de Auditoría de Sistemas y Tecnología de Información

- ***Carta de Gerencia T.I. 1-2017***
- ***Informe Final.***

Cartago, 20 de junio de 2018

Señores
Municipalidad de Cartago
Área de Tecnologías de la Información
Departamento Financiero-Administrativo
Alcandía
Consejo Municipal

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del período 2017 a la Municipalidad de Cartago y con base en el examen efectuado, observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en el manual de "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" emitido por la Contraloría General de la República y los estándares establecidos según los Objetivos de Control para Información y Tecnología Relacionada – CobiT®, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-1-2017.

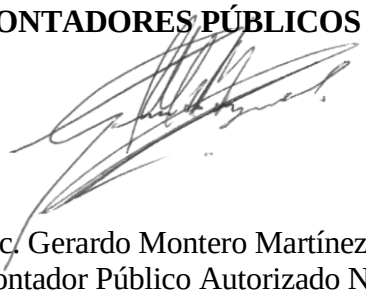
Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o colaboradores en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con las Tecnologías de Información.

Es importante señalar que la estructura de control interno establecida, incluyendo los procedimientos de control para la actividad sujeta a evaluación, son de entera responsabilidad de la administración de la Municipalidad de Cartago.

La auditoría no está diseñada para detectar todas las deficiencias en los procesos y objetivos de control evaluados, ya que no se lleva a cabo de forma continua durante el período de revisión; las evaluaciones realizadas consisten en un estudio sustentado en muestras y pruebas selectivas de la evidencia que respalda el cumplimiento de los procesos y objetivos de control evaluados, los cuales, producto de sus limitaciones inherentes, pueden presentar resultados fallidos debido a errores o debilidades propias del control interno que ocurran y no sean detectadas. Lo anterior deja manifiesto que los eventos subsecuentes a este informe están sujetos al riesgo de que los controles establecidos se tornen inadecuados, producto de cambios en las condiciones de la Municipalidad.

La auditoría realizada fue requerida por la administración de la Municipalidad de Cartago, producto de lo anterior, los resultados expresados en el presente informe son de carácter confidencial y deben ser utilizados exclusivamente por las personas autorizadas para tal fin.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS



Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad No. 0116 FIG7
Vence el 30 de setiembre del 2018.

"Exento del timbre de Ley 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8".

CONTENIDO

ORIGEN DEL ESTUDIO

Como parte de la evaluación de los estados financieros de la Municipalidad de Cartago, realizamos la evaluación de los controles generales de la gestión de tecnología de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en el manual de "Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información (N-2-2007-CO-DFOE)" emitidas por la Contraloría General de la República, los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés) y en general las mejores prácticas de la industria de tecnología de información.

ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

1. Seguimiento a recomendaciones anteriores.
2. Verificación del control interno en materia tecnológica con base en la normativa interna establecida.
3. Oportunidades de mejora identificadas en la evaluación.

El alcance de la auditoría realizada se fundamenta en lo establecido en las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" emitidas por la Contraloría General de la República y los estándares establecidos según los Objetivos de Control para Información y Tecnología Relacionada – CobiT®.

OBJETIVO DEL ESTUDIO

1. Establecer un entendimiento integral de la Municipalidad, así como de la plataforma tecnológica que soporta sus operaciones y documentación asociada.

2. Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, Procedimientos del auditor en respuesta a los riesgos evaluados, evaluamos la gestión de las tecnologías de información de la Municipalidad de Cartago.

PERIODO DE LA AUDITORÍA.

El estudio se realizó durante los meses de mayo y junio del año 2018 y corresponde a la auditoría del periodo del 2017.

LIMITACIONES DEL ESTUDIO.

Durante el proceso de auditoría externa efectuado no se presentaron limitaciones.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por el área de Tecnología de Información, aplicamos cuestionarios de control interno relacionados con la administración del área, seguridad física y lógica de los sistemas de información, continuidad de las operaciones, políticas en cuanto al uso adecuado del equipo de cómputo, internet y correo, planes de capacitación, bitácoras de los sistemas, plan operativo anual y sistemas de información que posee la Municipalidad.

Además, se formularon preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los funcionarios las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

RESUMEN EJECUTIVO

La Municipalidad de Cartago ha realizado un esfuerzo para cumplir con las normas técnicas emitidas por la Contraloría General de la República, desarrollando un conjunto de documentos e implementando acciones que sustentan sus operaciones en materia de Tecnología de Información, sin embargo, existen deficiencias de control y oportunidades de mejora. Producto de lo anterior y a partir de la aplicación del estudio realizado se identificaron los resultados que se muestran a continuación:

Matriz de Calificación

Esta matriz se utiliza para evaluar y calificar el entorno de Tecnologías de Información. Específicamente se trabaja sobre ocho áreas de evaluación, que en conjunto estructuran el entorno de TI.

Matriz de Calificación de Tecnología de Información
Institución: Municipalidad de Cartago **Tipo de Entidad: Municipalidad**
Período: 2017
Hecho por: CRC y JFN **Fecha: 20-06-2018**

Área de revisión	Objetivos	Calificación					
Gestión de las T.I.	**13 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1.	Procedimientos para la administración y formalización de los niveles de servicio acordados.	**X**					Se cuenta con el documento Informes niveles de servicio v2, el cual describe los acuerdos de niveles de servicio establecidos en la municipalidad.
2.	Plan de Capacitación para los funcionarios de TI y usuarios finales, del periodo 2017.		**X**				Se suministro el plan de capacitación, no obstante, se evidenció que no presenta la estructura adecuada. Ver hallazgo 01 del periodo 2015.
3.	Evaluar los procedimientos establecidos por el área de tecnologías de información para el manejo de incidentes.		**X**				Se revisó la herramienta actual Software de administración de incidentes de TI, con el procedimiento actual, el cual se cumple a cabalidad, sin embargo, en el Hallazgo 03 del presente informe se hace mención de cómo se deben gestionar incidentes, solicitudes y problemas según las mejores prácticas.
4.	Evaluar la metodología de Gestión de la Calidad formalmente aprobada.		**X**				El Área de Informática se apega al sistema de gestión de la calidad institucional, mediante el cual, han documentado y formalizado sus procesos. Sin embargo, esta metodología no garantiza la mejora continua de los productos y servicios de tecnologías de información. Sin embargo cabe mencionar que la calidad si se gestiona en algunos servicios, tal es el caso de gestión de incidentes, donde se establecieron informes, métricas y auditorías de calidad. Ver hallazgo 08 del periodo 2016.

Matriz de Calificación de Tecnología de Información
Institución: Municipalidad de Cartago **Tipo de Entidad: Municipalidad**
Período: 2017
Hecho por: CRC y JFN **Fecha: 20-06-2018**

Área de revisión	Objetivos	Calificación					
5.	Evaluar las actas del Comité de Tecnologías de Información del periodo 2017; así como el respectivo reglamento.		**X**				No se pudo verificar la realización de una sesión ya sea ordinaria o extraordinaria para el último trimestre del 2017.
6.	Evaluar el plan estratégico de tecnologías de la información actualizado.	**X**					Se suministro un avance para la creación del PETIC del periodo 2018-2020, además se cuenta con un informe de seguimiento para su cumplimiento en el periodo 2017.
7.	Evaluar el plan anual operativo del año 2017. Incluir Ejecución.	**X**					Se evidenció la ejecución total del plan.
8.	Evaluar el manual de puestos del personal TI.	**X**					Se suministró el manual de puestos actualizado para el Área de Informática.
9.	Evaluar la metodología empleada para la administración de proyectos.			**X**			Se suministro la metodología para la administración de proyectos, sin embargo, está en fases de revisiones y no se encuentra aprobada. Ver hallazgo 01 del periodo 2016.
10.	Gestiones para contar con bitácoras de control en los documentos de T.I. que indiquen al menos fechas de creación, aprobación, actualización del manual, versión, etc.	**X**					Según los documentos entregados para la auditoría correspondiente al periodo 2017, no se detectaron inconsistencias en este punto.
11.	Gestiones realizadas para contar con un Auditor de TI	**X**					Se comprobó que, a partir del 02 de abril de 2018, la Municipalidad de Cartago cuenta con el nombramiento de un auditor interno de TI, a manera de interino.
12.	Metodología de administración para las solicitudes de los usuarios y clientes		**X**				La Municipalidad cuenta con un procedimiento para la atención de solicitudes de clientes y usuarios. Este procedimiento se lleva a cabo, cada vez que los jefes de áreas y departamentos notifican cuando se requiere deshabilitar o eliminar cuentas de usuario. No obstante, se comenta que en ocasiones no se realizan estas notificaciones, pero el departamento de TI se encuentra pendiente de estas solicitudes.
13.	Repositorio Central para la gestión de la configuración	**X**					El repositorio central que se utiliza es la MuniRed.

Matriz de Calificación de Tecnología de Información
Institución: Municipalidad de Cartago **Tipo de Entidad: Municipalidad**
Período: 2017
Hecho por: CRC y JFN **Fecha: 20-06-2018**

Área de revisión	Objetivos	Calificación					
Total Área	**(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)**						**85.38**
Seguridad Lógica y acceso a datos	**6 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1	Evaluar la lista de funcionarios activos del active directory institucional	**X**					El active directory y la base de datos de usuarios activos, se encuentran sin inconsistencias (No existen exfuncionarios con accesos, ni usuarios genéricos sin su debida explicación y función).
2	Evaluar la política de seguridad de la información en donde se establezcan lineamientos referentes a: 1. Implementación de un marco de seguridad de la información 2. Compromiso del personal con la seguridad de la información 3. Seguridad física y ambiental 4. Seguridad en las operaciones y comunicaciones 5. Control de acceso 6. Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica		**X**				Se han implementado mejoras a las políticas de seguridad física y seguridad en los sistemas de información; sin embargo, aún hay aspectos de seguridad que no se encuentran totalmente centralizados en la política de seguridad de la información, por ejemplo, el control de acceso, la seguridad en la implementación y la seguridad de las operaciones y comunicaciones se encuentran en documentos separados a la política, y tampoco se encuentran referenciados dentro de esta. Ver Hallazgo 14 del periodo 2016.
3	Procedimientos documentados para la medición de la capacidad y desempeño de la plataforma tecnológica.		**X**				Se han generado dos documentos referentes al monitoreo y a la mejora del procedimiento de capacidad y desempeño, sin embargo, deben ser sometidos a revisión y aprobación por el sistema de gestión de calidad para su incorporación al procedimiento 7P04. A pesar de lo anterior no se está contemplando la realización de proyecciones de uso de la plataforma tecnológica. Ver Hallazgo 09 del periodo 2016.
4	Estudio de vulnerabilidad de la red	**X**					Se suministró evidencia de un estudio de vulnerabilidad de la red.

Matriz de Calificación de Tecnología de Información
Institución: Municipalidad de Cartago **Tipo de Entidad: Municipalidad**
Período: 2017
Hecho por: CRC y JFN **Fecha: 20-06-2018**

Área de revisión	Objetivos	Calificación					
5	Diagrama de la red	**X**					Se cuenta con el diagrama de la red.
6	Mecanismos de monitoreo de la red institucional.	**X**					Si se realizan monitoreo de la red institucional.
Total Área	**(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)**						**91.67**
Seguridad física: Servidores de datos y Estaciones de Trabajo.	**3 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1	Evaluar el inventario de software y hardware instalado por equipo e institucional.	**X**					La Municipalidad cuenta con una herramienta para administrar las licencias y los recursos conectados a la red.
2	Revisar la seguridad física presente en el cuarto de servidores.	**X**					El cuarto de servidores cuenta con los controles mínimos de seguridad física.
3	Plan formal para la actualización de hardware y software	**X**					Existe un procedimiento para revisar y sustituir equipo de cómputo. También se suministró un plan de renovación y adquisición de equipo.
Total Área	**(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)**						**100**
Sistemas de Información	**3 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1	Gestiones realizadas para contar con una herramienta para el control de las versiones de los programas fuentes.	**X**					Se cuentan con mecanismos para el control de versiones.
2	Manuales técnicos y de usuario de los diferentes sistemas en producción	**X**					Se cuenta con los respectivos manuales técnicos y de usuarios de los sistemas de información de la Municipalidad.
3	Integración y funcionamiento de los sistemas	**X**					La recomendación del hallazgo se ve subsanada con el sistema Wizdom. Además, se está implementando el CRM de Microsoft Dynamics.
Total Área	**(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)**						**100**

Matriz de Calificación de Tecnología de Información
Institución: Municipalidad de Cartago **Tipo de Entidad: Municipalidad**
Período: 2017
Hecho por: CRC y JFN **Fecha: 20-06-2018**

Área de revisión	Objetivos	Calificación					
Bases de Datos	**6 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1	Integridad de la información de base de datos de Cuentas por cobrar.		**X**				Se detectaron inconsistencias en la base de datos de Cuentas por cobrar. Ver Hallazgo 02 del presente informe. Este tema es competencia del Área Usuaria.
2	Respaldos ejecutados.	**X**					Se evidenció el cumplimiento de la ejecución de los respaldos.
3	Planes de pruebas establecidos para los respaldos de información.	**X**					Se cuenta con un plan de pruebas establecido para los respaldos de información.
4	Respaldo de las gestiones realizadas para la integración de las bases de datos del Sistema de Información Geográfica y Bienes Inmuebles.	**X**					Se cuenta con una interface en el sistema CRM de Microsoft Dynamics, la cual permite crear las solicitudes, para que sean revisadas, aprobadas y aplicadas en ambos sentidos.
5	Respaldo de las gestiones realizadas para implementar el histórico de intereses por cobrar a nivel de base de datos de las cuentas por cobrar.	**X**					Se cuenta con un histórico de los intereses en las cuentas por cobrar.
6	Bitácora de las cintas de respaldo envidas al sitio externo.	**X**					Los respaldos se envían automáticamente al sitio alterno, por medio de red.
Total Área	**(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)**						**95.83**
Continuidad de las Operaciones	**2 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1	Evaluar el plan de contingencia y continuidad actualizado que garantice la recuperación de la información en caso de desastres y la continuidad de las operaciones.	**X**					Se cuenta con un plan de contingencia y continuidad para los procesos tecnológicos.
2	Evidencia de la ejecución del plan de pruebas efectuado al plan de contingencia y	**X**					Se evidencia las pruebas realizadas al plan de contingencia y continuidad.

Matriz de Calificación de Tecnología de Información **Institución: Municipalidad de Cartago** **Tipo de Entidad: Municipalidad** **Período: 2017** **Hecho por: CRC y JFN** **Fecha: 20-06-2018**							
Área de revisión	**Objetivos**	**Calificación**					
	continuidad de las operaciones.						
Total Área	**(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)**					**100**	
Riesgos tecnológicos	**1 punto**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	**Justificación**
1	Metodología empleada para la administración del riesgo informático	**X**					La metodología de riesgos se encuentra implementada desde el 06 de junio de 2018.
	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)					**100**	
Seguimiento procesos de T.I.	**2 puntos**	**C 100**	**PA 75**	**PB 35**	**NC 0**	**NA**	
1	Informes de Auditoría Interna emitido en el 2017 y 2018, relacionados con TI.		**X**				No se evidenciaron informes en el periodo 2017. Sin embargo, se comprueba que se han realizado trabajos sobre seguimientos a recomendaciones de auditorías externas de periodos anteriores, seguimientos a políticas sobre el uso de correo electrónico e internet y sobre un software de compras que se encuentra en proceso de adquisición por parte de la municipalidad en el periodo 2018. Ver Hallazgo 03 del periodo 2016.
2	Informes de auditoría externa periodos anteriores		**X**				Todos los años la Institución realiza auditorías externas y como parte de estas se encuentra un seguimiento a los principales procesos tecnológicos de la Institución. A pesar de lo anterior, no se han atendido todas las recomendaciones generadas a partir de dichos estudios. Ver sección "Seguimiento Auditorías Anteriores."
	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) /(Valor Total de los puntos del área - el valor de los objetivos NA)					**75**	

C: Cumple, la entidad muestra un excelente desempeño con respecto al factor evaluado.
PA: Cumple Parcialmente Alto, la entidad muestra deficiencias, pero en general el desempeño con respecto al factor evaluado es bueno.
PB: Cumple Parcialmente Bajo, incumple significativamente con el factor evaluado.

NC: No Cumple, la entidad incumple con el factor evaluado.
NA: No Aplica, la evaluación de estos requerimientos.

Cuadro resumen por Área de Revisión

Área de revisión	Calificación
Gestión de las T.I.	85.38
Seguridad Lógica y acceso a datos	91.67
Seguridad física: Servidores de datos y Estaciones de Trabajo	100
Sistemas de Información	100
Bases de Datos	95.83
Continuidad de las Operaciones	100
Riesgos tecnológicos	100
Seguimiento procesos de T.I.	75

Cuadro comparativo periodo 2015, 2016 y 2017

Área de revisión	Objetivos	Calificación		
Gestión de las T.I.	**13 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Procedimientos para la administración y formalización de los niveles de servicio acordados.	35	35	100
2.	Plan de Capacitación para los funcionarios de TI y usuarios finales, del periodo 2017	75	100	75
3.	Evaluar los procedimientos establecidos por el área de tecnologías de información para el manejo de incidentes.	100	75	75
4.	Evaluar la metodología de Gestión de la Calidad formalmente aprobada.	100	75	75
5.	Evaluar las actas del Comité de Tecnologías de Información del periodo 2017 y 2018; así como el respectivo reglamento.	35	75	75
6.	Evaluar el plan estratégico de tecnologías de la información actualizado.	75	100	100
7.	Evaluar el plan anual operativo del año 2017. Incluir Ejecución.	100	100	100
8.	Evaluar el manual de puestos del personal TI.	100	100	100
9.	Evaluar la metodología empleada para la administración de proyectos.	35	35	35
10.	Gestiones para contar con bitácoras de control en los documentos de T.I. que indiquen al menos fechas de creación, aprobación, actualización del manual, versión, etc.	75	75	100
11.	Gestiones realizadas para contar con un Auditor de TI	35	0	100

Área de revisión	Objetivos	Calificación		
Gestión de las T.I.	**13 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
12.	Metodología de administración para las solicitudes de los usuarios y clientes	75	75	75
13.	Repositorio Central para la gestión de la configuración	100	100	100
Total área		**72.30**	**72.69**	**85.38**

Área de revisión	Objetivos	Calificación		
Seguridad Lógica y acceso a datos	**5 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Evaluar la lista de funcionarios activos del active directory institucional	100	75	100
2.	Evaluar la política de seguridad de la información en donde se establezcan lineamientos referentes a: 1. Implementación de un marco de seguridad de la información 2. Compromiso del personal con la seguridad de la información 3. Seguridad física y ambiental 4. Seguridad en las operaciones y comunicaciones 5. Control de acceso 6. Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica	75	75	75
3.	Procedimientos documentados para la medición de la capacidad y desempeño de la plataforma tecnológica.	75	75	75
4.	Estudio de vulnerabilidad de la red	100	100	100
5.	Diagrama de la red	100	100	100
6.	Mecanismos de monitoreo de la red institucional.	100	100	100
Total área		**91.67**	**87.50**	**91.67**

Área de revisión	Objetivos	Calificación		
Seguridad física: Servidores de datos y Estaciones de Trabajo.	**3 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Evaluar el inventario de software y hardware instalado por equipo e institucional.	100	100	100
2.	Revisamos la seguridad física presente en el cuarto de servidores.	75	100	100
3.	Plan formal para la actualización de hardware y software	75	100	100
Total área		**83.33**	**100**	**100**

Área de revisión	Objetivos	Calificación		
Sistemas de Información	**2 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Gestiones realizadas para contar con una herramienta para el control de las versiones de los programas fuentes.	100	100	100
2.	Manuales técnicos y de usuario de los diferentes sistemas en producción	100	100	100
3.	Integración y funcionamiento de los sistemas	75	75	100
Total área		**91.6**	**91.60**	**100**

Área de revisión	Objetivos	Calificación		
Bases de Datos	**6 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Integridad de la información de base de datos de Cuentas por cobrar	75	75	75
2.	Respaldos ejecutados	100	100	100
3.	Planes de pruebas establecidos para los respaldos de información.	100	75	100
4.	Respaldo de las gestiones realizadas para la integración de las bases de datos del Sistema de Información Geográfica y Bienes Inmuebles.	75	75	100
5.	Respaldo de las gestiones realizadas para implementar el histórico de intereses por cobrar a nivel de base de datos de las cuentas por cobrar	35	75	100

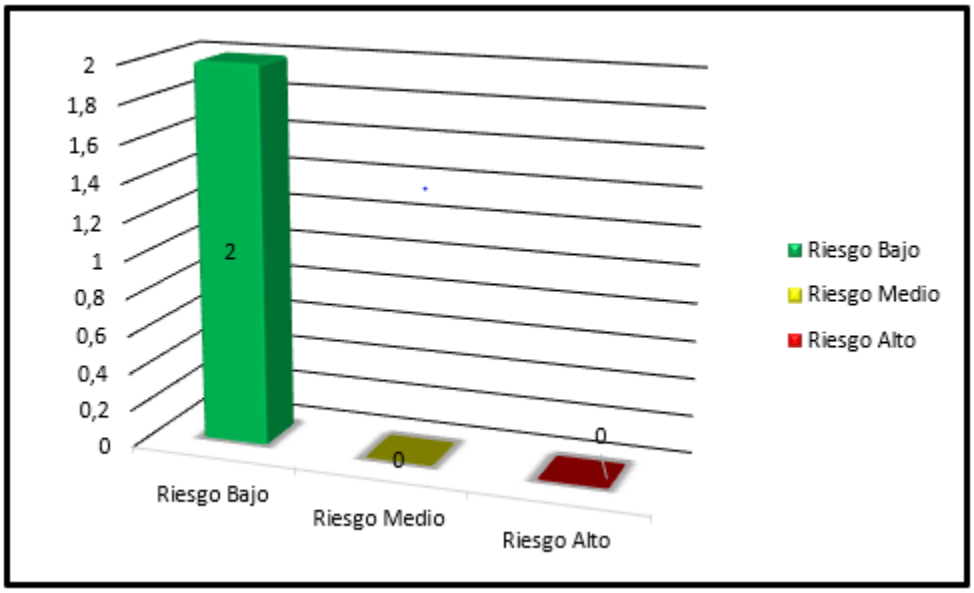
Área de revisión	Objetivos	Calificación		
Bases de Datos	**6 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
6.	Bitácora de las cintas de respaldo envidas al sitio externo	100	100	100
Total área		**80.83**	**83.83**	**95.83**

Continuidad de las Operaciones	**2 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Evaluar el plan de contingencia y continuidad actualizado que garantice la recuperación de la información en caso de desastres y la continuidad de las operaciones.	100	100	100
2.	Evidencia de la ejecución del plan de pruebas efectuado al plan de contingencia y continuidad de las operaciones.	100	100	100
Total área		**100**	**100**	**100**

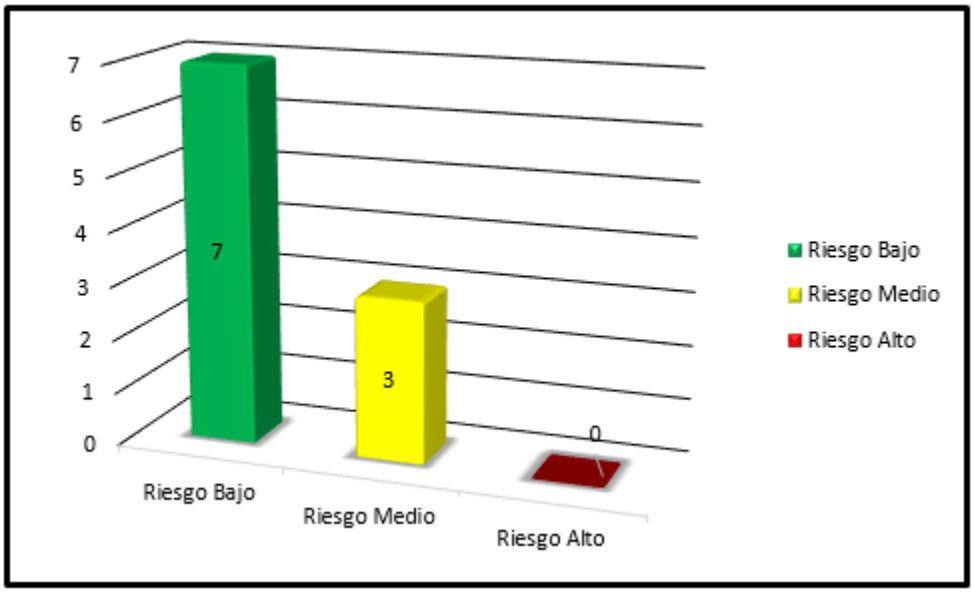
Área de revisión	Objetivos	Calificación		
Riesgos tecnológicos	**1 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Metodología empleada para la administración del riesgo informático	75	75	100
Total área		**75**	**75**	**100**

Área de revisión	Objetivos	Calificación		
Seguimiento procesos de T.I.	**2 puntos**	**Periodo 2015**	**Periodo 2016**	**Periodo 2017**
1.	Informes de Auditoría Interna emitidos en el 2017 y 2018, relacionados con TI.	0	0	75
2.	Informes de auditoría externa periodos anteriores	75	75	75
Total área		**37.5**	**37.50**	**75**

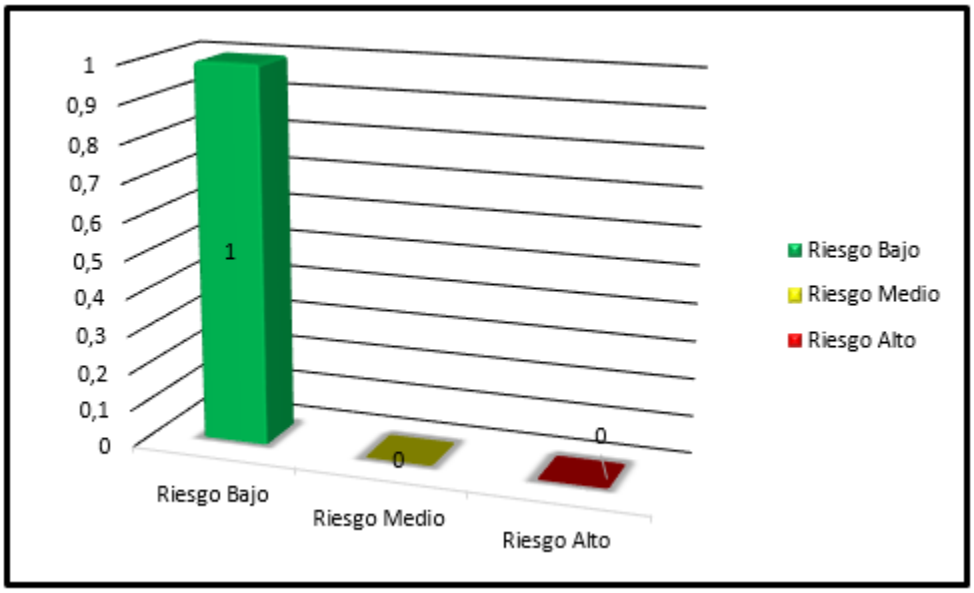
Por otra parte, se identificaron una serie de hallazgos, y asuntos a informar (que se encuentran en proceso o pendientes) que a continuación se agrupan por periodo y por nivel de riesgo:



Recomendaciones emitidas en el periodo 2017.



Recomendaciones emitidas en el periodo 2016.



Recomendaciones emitidas en el periodo 2015.

HALLAZGOS

HALLAZGO 01: POSIBLES INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LA BASE DE CUENTAS POR COBRAR. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión de la información de los registros almacenados en las bases de datos de cuentas por cobrar con corte al 31 de diciembre del año 2017, se determinó las siguientes inconsistencias:

- **Parquímetros**
  - Los registros almacenados en la base de datos de cuentas por cobrar por concepto de parquímetros a veces indica en el campo provincia el valor "3 "o a veces el valor "CARTAGO".
  - Los registros almacenados en la base de datos de cuentas por cobrar por concepto de parquímetros a veces indica en el campo cantón el valor "1 "o a veces el valor "CARTAGO".

- **Patentes**
  - La cuenta 400301 tiene como cédula asociada el número 0, la misma tiene 9 pagos pendientes por las siguientes actividades.
    - Supermercado licor
    - Timbre parque nac. Licores
    - Multa ley de licores
  - Existe un registro en la base de datos de cuentas por cobrar por concepto de patente comercial que no posee la actividad registrada.
  - Existen 370 registros asociados a patentes con monto 0. Dentro de las actividades de las patentes se encuentra.
    - 4 – Alquiler de maquinaría
    - 12 – Bus cantonal
    - 40 – Colegio Bilingüe
    - 16 – Consultorio Médico
    - 11 – Cooperativa
    - 20 – Escuela de enseñanza
    - 40 – Fabrica
    - 46 – Manufacturera
- **Servicios municipales**
  - Existen 16 registros con cédula igual a 0.
  - Existen 15 registros con trimestre igual a 0.
  - En la columna de trimestre se guardan valores desde el 0 hasta el 12.
  - Existe un registro con monto negativo, el monto es de -¢6104.
  - Existen 71 registros con monto igual a 0.

Al tener presente estas inconsistencias en las bases de datos de cuentas por cobrar, a la Municipalidad de Cartago se le podría dificultar el cobro de los servicios suministrados a los contribuyentes.

CRITERIO:

Según el proceso **4.3 "Administración de los datos"** presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, indica lo siguiente: "*La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura."*

RECOMENDACIONES:

Al Área Tributaria en conjunto con el Área de Informática:

1. Determinar las causas de las inconsistencias en las bases de datos de cuentas por cobrar.

2. Establecer en conjunto con el área de informática un plan de acción para la depuración de las inconsistencias identificadas, además de dar seguimiento y velar por la ejecución de dicho plan.
3. Establecer validaciones para asegurar la integridad y confiabilidad de los datos almacenados.

HALLAZGO 02: AUSENCIA DE UNA PROCEDIMIENTO PARA LA ADMINISTRACIÓN DE PROBLEMAS. RIESGO BAJO.

CONDICIÓN:

Se determinó que la Municipalidad de Cartago no cuenta con un procedimiento documentado para la administración de problemas por parte del Área de Informática. Lo que se suministró fue el procedimiento de atención de incidentes, esto debido a que a lo interno del área de informática se trata por igual un incidente que un problema.

Al no tener un procedimiento para la administración de problemas, no se puede dar un tratamiento a los incidentes recurrentes, averiguar causas, raíces de incidentes comunes, y minimizar el impacto de ciertos incidentes que no se pueden prevenir.

CRITERIO:

Según el proceso **4.5 "Manejo de incidentes"** presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitida por la Contraloría General de la República menciona lo siguiente: *"La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario".*

RECOMENDACIONES:

Al Área de Informática:

1. Diseñar e implementar un procedimiento para la administración de problemas informáticos, el mismo se puede incluir como una actualización del documento 7P04 Gestión de TI V.05 en el apartado 3.2.2 Atención de incidencias informáticas, de tal forma que se le pueda dar seguimiento a los incidentes recurrentes y poder encontrar una solución final a los mismos, evitando que afecten la disponibilidad de los servicios informáticos, especialmente los que son críticos para la municipalidad. Dentro del procedimiento se debe considerar como mínimo lo siguiente.
    a. Identificación de problemas mediante incidentes repetitivos o conocidos.
    b. Clasificación de problemas según categoría, impacto, urgencia y prioridad.
    c. Determinar la causa raíz del problema.
    d. Definir un plan de acción para la resolución de problemas.
    e. Definir el proceso de cierre del problema.

2. Se recomienda tomar en cuenta las buenas prácticas de ITIL V3 2011, para realizar el procedimiento de administración de problemas, el cual se ubica en la Fase de Operación, en el proceso de Gestión de Problemas, además tomar en cuenta Gestión de Solicitudes y Gestión de Incidentes, de tal modo que se considere las diferencias entre estos procedimientos.

COMENTARIO DE ADMINISTRACION:

Actualmente los problemas se gestionan con el formulario de SNC (Salidas no Conformes).

MATRIZ DE SEGUIMIENTO A CARTAS A GERENCIA ANTERIORES

MATRIZ DE SEGUIMEINTO A CG ANTERIORES CON RECOMENDACIONES DIRIGIDAS A TI

CG 1-2016	
HALLAZGO 01: AUSENCIA DE UNA METODOLOGÍA DE GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN RIESGO MEDIO.	
RECOMENDACIÓN	***Al Área de Informática:*** 1. Desarrollar una metodología para la gestión de proyectos de tecnologías de información que abarque el ciclo de vida del proyecto (inicio, planeación, ejecución, control y cierre), y que contemple como mínimo aspectos como: a. Análisis de factibilidad, viabilidad o bien análisis de las posibles alternativas para el desarrollo de un proyecto. b. Alcance del proyecto. c. Roles y responsabilidades d. Costos y recursos requeridos (incluyendo recurso humano). e. Riesgos. f. Cronograma. g. Gestión de la calidad. h. Monitoreo y mecanismos de control.
COMENTARIOS DE LA ADMINISTRACIÓN	El documento METODOLOGÍA UTILIZADA PARA LA ADMINISTRACIÓN DE PROYECTOS se encuentra en la etapa de aprobación, ver hallazgo 01
ESTADO	**EN PROCESO** Se considera este hallazgo "En Proceso", ya que se informa que actualmente la metodología de proyectos se encuentra en una fase de revisiones y aprobación para su implementación.
HALLAZGO 08: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE LA CALIDAD DE LOS SERVICIOS DE T.I. RIESGO MEDIO.	
RECOMENDACIÓN	***Al Área de Informática:***

	1. Gestionar la definición, aprobación y divulgación de un procedimiento para gestionar la Calidad, con el fin de detallar cómo se llevará a cabo todo el proceso de mejora continua de los servicios y productos que ofrece el Área de Informática. El proceso de gestión de calidad de TI se puede enfocar en los siguientes puntos: a. Se debe definir un proceso de planeación el cual de contemplar las siguientes actividades: i. Definir los servicios y productos de TI que se van medir. ii. Definir las métricas e indicadores que van a dar apoyo al proceso de medición. iii. Elaborar encuestas de satisfacción a los usuarios de la Municipalidad para medir la percepción en la calidad de los servicios. iv. Definir un cronograma y programa de trabajo que indique los pasos a seguir para realizar las mediciones. b. Ejecutar el programa de trabajo y documentar los resultados y mejoras obtenidos. c. Verificar y dar seguimiento al proceso de ejecución y resultados de las mediciones, para ello se debe considerar lo siguiente: i. Verificar e identificar desviaciones entre los resultados obtenidos contra las métricas e indicadores definidos inicialmente. ii. Verificar las encuestas de satisfacción de los usuarios y determinar cuáles son los puntos que más requieren atención, según la percepción de estos. d. Desarrollar una estrategia de mejora contemplando lo siguiente: i. Definir y ejecutar planes de acción correctivo para las debilidades identificadas. ii. Documentar los resultados obtenidos y presentarlos ante el Comité de TI para su respectivo conocimiento. 2. Garantizar que el procedimiento se alinee a los procesos del Sistema de Gestión de Calidad definidos por la Municipalidad. 3. Presentar el procedimiento ante el Comité de TI para su respectiva aprobación.
COMENTARIOS DE LA ADMINISTRACIÓN	Rosita / Maykel / Eduardo/Daniel
ESTADO	**PENDIENTE** No se brindó ningún documento que respalde algún progreso sobre este hallazgo. Sin embargo cabe mencionar que la calidad si se gestiona en algunos servicios y productos de TI, tal es el caso de gestión de incidentes, donde se han establecido informes, métricas y realizado auditorias de calidad. No obstante, no se cuenta con el procedimiento para la gestión de calidad de los servicios de TI.

HALLAZGO 09: AUSENCIA DE UN PLAN FORMAL PARA LA GESTIÓN DE LA CAPACIDAD Y DESEMPEÑO DE LA PLATAFORMA TECNOLÓGICA DE LA MUNICIPALIDAD DE CARTAGO. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Informática:*** 1. Generar un modelo de monitoreo como parte del procedimiento existente para la plataforma tecnológica considerando al menos los siguientes aspectos: a. Periodicidad del monitoreo. b. Indicadores de rendimiento. c. Herramienta utilizada para el monitoreo (parámetros de configuración). d. Umbrales de monitoreo (gestión de alertas). e. Reportes periódicos (mensuales o según la periodicidad que se defina) de los siguientes aspectos: i. Reportes de disponibilidad. ii. Reportes de capacidad. iii. Reportes de excepciones (situaciones esporádicas que pueden levantar una alerta sobre capacidad o disponibilidad). 2. Generar un plan de capacidad y desempeño incluyendo un análisis del comportamiento en el consumo de recursos. En el mismo se debe realizar una proyección de los recursos para determinar cuál va a ser el consumo futuro por parte de la Municipalidad y así generar una estrategia para sustentar los recursos que se van a requerir a futuro. Además, se debe incluir un plan de trabajo incluyendo los aspectos a realizar durante el periodo, entre ellos: a. Componentes que se deben actualizar en el proceso de monitoreo (nuevo equipo, retiro de ítems de configuración). b. Implementación de nuevas herramientas o nuevas configuraciones. c. Identificación de parámetros a monitorear. d. Gestión de acuerdos de nivel de servicio o acuerdos de nivel operativo (en caso de que existan). e. Entre otros aspectos.
COMENTARIOS DE LA ADMINISTRACIÓN	Se generan los documentos respectivos como instructivos con los elementos sugeridos, pero deben ser sometidos a revisión por el sistema de gestión de calidad para su incorporación al procedimiento 7P04.
ESTADO	**EN PROCESO** El hallazgo se considera en proceso, ya que se informa que se generan dos documentos, pero deben ser sometidos a revisión y aprobación por el sistema de gestión de calidad para su incorporación al procedimiento 7P04.

HALLAZGO 10: EXISTENCIA DE USUARIOS GENÉRICOS Y UNA CUENTA DE USUARIO DE UN EXFUNCIONARIO HABILITADA. RIESGO BAJO.	
RECOMENDACIÓN	***A las áreas usuarias de la Municipalidad*** 1. Notificar con antelación a TI cuando un funcionario ya no labora para la Municipalidad o si por alguna circunstancia esta fuera de la institución por un periodo de tiempo prolongado. ***Al Área de Informática:*** 1. En base al listado proporcionado por las distintas áreas usuarias de la Municipalidad deshabilitar las cuentas de usuario de funcionarios que cesan sus labores para la Institución según lo establecido por el procedimiento de gestión de usuarios 2. Valorar la existencia de usuarios genéricos y deshabilitar aquellos que no son requeridos en la operativa de TI. Además, documentar la debida justificación de este tipo de cuentas de usuarios. 3. Realizar revisiones periódicas sobre los directorios de usuarios para mantener al mínimo el uso de usuarios genéricos y validar que no se cuente con cuentas de exfuncionarios activas. En caso de presentarse la imperiosa necesidad de mantener a un usuario genérico se debe documentar su justificación y responsable.
COMENTARIOS DE LA ADMINISTRACIÓN	Gilberto / Daniel
ESTADO	**CORREGIDO** Se corrige el hallazgo, ya que se revisó la base de datos de usuarios, y no se encontró evidencia de la existencia de cuentas de exfuncionarios activas. Está prueba se realizó en conjunto con la lista de cesantes de la municipalidad en el periodo 2017-2018, para corroborar si alguna persona que ya no labora en la municipalidad se encontraba dentro de la base de datos de usuarios. Además, como producto de la revisión, no se encontraron usuarios genéricos que no posean su respectiva justificación y encargado de manejar estas cuentas.
HALLAZGO 11: AUSENCIA DE UNA HERRAMIENTA ESPECIALIZADA PARA LA GESTIÓN DE INCIDENTES DE TI. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Informática:*** 1. Elaborar un cronograma de implementación del System Center Service Manager, para llevar un control del avance y cumplimiento del proyecto de una mesa de servicio para los usuarios de la Municipalidad. 2. Efectuar un análisis de la herramienta System Center Service Manager con el fin de verificar que se pueden implementar las actividades mínimas dentro de la gestión de incidentes tales como: a. Registrar desde un único punto de contacto, los incidentes de los usuarios.

	b. Identificar y clasificar el incidente de acuerdo con parámetros de impacto y urgencia. c. Realizar una pre-evaluación del incidente para determinar si el mismo se puede atender en un primer nivel o debe ser escalado a un nivel más especializado. d. Verificar si existen soluciones registradas en la base de datos de conocimiento acerca de la resolución de casos similares. e. Resolver el incidente, registrar nuevas soluciones y asegurarse de que el servicio opera de la manera esperada. f. Notificar al usuario acerca de la solución del mismo y esperar su visto bueno. g. Cerrar el incidente y mantener actualizado su estado. h. Generar reportes periódicamente para verificar incidencias no resueltas, verificar el estado de los indicadores del servicio y determinar las mejoras correspondientes en la gestión del servicio. 3. Una vez implementada la solución indicada, capacitar a los usuarios del sistema para que los mismos reporten los incidentes a través de dicha solución. 4. Verificar de manera periódica, el estado de los casos registrados para asegurar que los mismos se hayan resuelto de manera oportuna. Del mismo modo, definir métricas e indicadores para medir la satisfacción del servicio como parte del proceso de calidad del Área de Informática.
COMENTARIOS DE LA ADMINISTRACIÓN	Ver documento en carpeta de hallazgo # 11 **AUSENCIA DE UNA HERRAMIENTA**
ESTADO	**CORREGIDO** Por medio de la evidencia suministrada y la revisión presencial, se pudo corroborar las actualizaciones necesarias en la herramienta interna, llamada Software de administración de incidentes de TI, para cumplir con el procedimiento de atención de incidencias.
HALLAZGO 12: AUSENCIA DE BITÁCORAS PARA EL MÓDULO DE ACTIVOS FIJOS Y FALTA DE REVISIÓN DE LAS BITÁCORAS PARA EL SISTEMA WIZDOM. RIESGO BAJO.	
RECOMENDACIÓN	***A las áreas usuarias en conjunto con el Área de Informática:*** 1. Efectuar una valoración de los sistemas de información actuales que no poseen pistas de auditoría con el fin de determinar la factibilidad de implementar dicho control en ellos. 2. Para aquellos módulos que no poseen pistas de auditoría, implementar las bitácoras respectivas considerando al menos: a. Identidad del usuario del sistema. b. Recursos solicitados.

	c. Acciones privilegiadas solicitadas. d. Identificador de la terminal. e. Hora de inicio y finalización. f. Número de intentos de conexión. 3. Definir formalmente los responsables de revisar las pistas de auditoría de los sistemas de información de la Municipalidad. Además, se debe definir la periodicidad de las mismas 4. Revisar y dar seguimiento a las pistas de auditoría de cada uno de los distintos sistemas de información de la Municipalidad. Para ello se debe: a. Elaborar un cronograma para planificar de forma periódica la revisión de pistas de auditoría. b. Generar informes de los resultados de la revisión para comunicarlos a las respectivas direcciones. c. Generar planes de acción de los casos que presenten inconsistencias en las pistas de auditoría.
COMENTARIOS DE LA ADMINISTRACIÓN	Se elabora un listado de las aplicaciones para identificar si tiene o no bitácora de auditoria. Debido al cambio de aplicaciones a plataformas modernas, se debe evaluar la factibilidad de bitácoras en aplicaciones antiguas. Actualmente la revisión de pistas de auditoria se da por demanda cuando las áreas usuarias lo solicitan y el responsable es quien se designe por medio del sistema de gestión de incidencias. En este momento, no hay seguimiento de las pistas de auditoria porque el recurso humano es limitado en el área de TIC, para atender labores como esta.
ESTADO	**EN PROCESO** Este hallazgo se considera en proceso, ya que se comunica que en la actualidad no hay seguimiento de las pistas de auditoria porque el recurso humano es limitado en el área de TIC, para atender labores como esta. Además, como parte al seguimiento del hallazgo se elabora un listado "Bitácoras auditoria", para identificar si tiene o no bitácora de auditoria, además se evalua la factibilidad de generar bitácoras en aplicaciones antiguas, ya que los sistemas más modernos son más factibles a realizar las revisiones en sus bitácoras. No obstante, aún no se definen periodos de revisiones ni planes de acción para subsanar las inconsistencias que se puedan encontrar en las pistas de auditoria.
HALLAZGO 13: NO SE EVIDENCIÓ EJECUCIÓN DE PRUEBAS A LOS RESPALDOS DE INFORMACIÓN. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Informática:*** 1. Elaborar un plan de restauraciones para la ejecución de pruebas de respaldos de las bases de datos de la Municipalidad. El plan debe considerar al menos los responsables, fecha, cronograma y bitácora. Para definir la periodicidad en la que se van a probar los respaldos, se debe considerar como mínimo la criticidad de la información en el respaldo y, además la cantidad de personal del área.

	2. Realizar y documentar detalladamente pruebas periódicas de los respaldos de la información de las bases de datos de la Municipalidad, de acuerdo con el plan de pruebas elaborado según la recomendación anterior.
COMENTARIOS DE LA ADMINISTRACIÓN	Infraestructura / David
ESTADO	**CORREGIDO** El 11/05/2018 se actualizó el documento "Pruebas para los respaldos de la información", donde se indica las pruebas tanto para respaldos internos, como externos, además fue brindado el formulario 7F81 con la validación de los respaldos, para la validación de los respaldos externos se registra en el formulario de validación de respaldos en sitio externo. Se cuenta con una bitácora para los respaldos internos y otra para los externos donde se incluyen los elementos necesarios para su registro y seguimiento.
HALLAZGO 14: NO SE CUENTA CON UN DOCUMENTO INTEGRAL QUE CENTRALICE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. RIESGO BAJO.	
RECOMENDACIÓN	***Al Comité de Tecnologías de Información y Comunicaciones en coordinación con el Área de Informática:*** 1. Valorar la consolidación de los lineamientos de seguridad de la información con el fin de evitar la duplicidad de lineamientos y tener un mejor control del versionamiento de documentos. 2. Definir lineamientos en complemento con la política de seguridad de la información para los siguientes aspectos: a. Gestión de activos de TI: Definir políticas para la clasificación de activos según su criticidad y nivel de seguridad requerido. Además, se debe incluir lineamientos para el uso de dispositivos removibles (por ejemplo, llaves USB, HDD portables, etc.). b. Lineamientos de seguridad para el mantenimiento de sistemas e implementación de software. c. Lineamientos para la gestión de aquellos incidentes que comprometan la seguridad de la información. 3. Integrar el proceso de seguridad de la información con el proceso de continuidad de TI, en el cual se identifique cuales aspectos mínimos se deben considerar durante la ejecución del plan de continuidad. 4. Efectuar las gestiones para que la política de seguridad de información se revise y apruebe por parte de la instancia correspondiente, considerando el visto bueno de las áreas usuarias. 5. Capacitar a las áreas usuarias en la implementación de medidas de seguridad de la información y dar seguimientos a los casos que poseen un mayor riesgo. ***Al Área de Informática en coordinación con la Auditoría Interna*** 6. Realizar seguimientos periódicos al cumplimiento de la política de seguridad de la información y documentar los resultados de la revisión.

COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** El hallazgo se considera en proceso, ya que en el documento "Políticas acceso municipalidad V2" se define una serie de lineamientos bien estipulados sobre el control de accesos en toda la Municipalidad, pero en la Política de Seguridad de la información no se encuentran mencionados, ni menciona este documento. Lo mismo pasa con otros documentos como "Control de acceso"," seguridad en la implementación" y "Seguridad operaciones y comunicaciones". Por lo que se considera que aún existe una descentralización de la información referente a la política de Seguridad, no obstante, también se evidencia que se han realizado avances, producto de las revisiones y modificaciones según las recomendaciones del informe de auditoría del periodo 2016.
Carta a Gerencia 2015	
HALLAZGO 02: AUSENCIA DE UNA METODOLOGÍA PARA LA ADMINISTRACIÓN DE PROBLEMAS. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Informática:*** 1. Definir, divulgar e implementar una metodología o procedimiento para la administración de problemas informáticos, o caso contrario, actualizar el documento 7P04 "Gestión de TI V.2 en el apartado 2.5 sobre Atención de incidencias informáticas, de manera tal que se identifiquen aquellos incidentes que se materializan de manera repetitiva y que afecta la disponibilidad de los servicios informáticos, en especial a aquellos que son críticos. El procedimiento debe considerar al menos lo siguiente: a. Identificación de problemas mediante incidentes repetitivos o conocidos. b. Clasificación de problemas según categoría, impacto, urgencia y prioridad. c. Determinar la causa raíz del problema. d. Definir un plan de acción para la resolución de problemas. e. Definir el proceso de cierre del problema.
COMENTARIOS DE LA ADMINISTRACIÓN	Se actualizó el documento 7P04 Procedimiento de TIC, en el apartado 3.2.2 Atención de incidentes informáticos, además se desarrolló un sistema para la gestión de incidentes con el que se administran los problemas desde la apertura hasta la finalización del mismo.
ESTADO	**NO APLICA** Se procede a actualizar el hallazgo al periodo actual por antigüedad.

Carta a Gerencia 2014	
HALLAZGO 05: NO EXISTE LA APLICACIÓN DE UNA METODOLOGÍA DE RIESGOS DE T.I. EN LA MUNICIPALIDAD DE CARTAGO. RIESGO MEDIO.	
RECOMENDACIÓN	Desarrollar y aplicar una metodología de riesgos de T.I., esta metodología debe desarrollarse con base en la metodología institucional de riesgos. Para tal proceso se debe de tomar en consideración lo siguiente: 1. Definir prioridades para todas las aplicaciones, sistemas y sitios que están en línea con los objetivos del negocio. Incluyen esas prioridades en el plan de continuidad. Cuando se definan las prioridades, considerar: a. Riesgo del negocio y riesgo operativo de TI. b. Interdependencias. c. El marco de trabajo de la clasificación de datos. d. SLAs y OLAs e. Costos. 2. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad para periodos críticos de operación.
COMENTARIOS DE LA ADMINISTRACIÓN	La metodología utilizada para la gestión del riesgo en el área de TIC está basada en COBIT e ISO 31001, orientado en al sistema de gestión de calidad de la Municipalidad bajo el estándar ISO 9001-2015. El plan para la gestión de riesgo se encuentra en la etapa de desarrollo y se tiene planificado que entre en producción en el segundo semestre del año 2018.
ESTADO	**CORREGIDO** El hallazgo se considera Corregido, ya que se identificó que existe un "PLAN PARA LA GESTION DE LOS RIESGOS DEL AREA DE TIC" (Metodología de Riesgos), debidamente actualizada y desarrollada para los 5 dominios del área de TIC (gestión, operación, infraestructura, plataforma y recurso humano). Además, se comprueba que la metodología de riesgo se empezó a implementar a partir del 06 de junio del 2018.
Carta a Gerencia 2009	
HALLAZGO 1: BITÁCORAS DE CONTROL RIESGO MEDIO.	
RECOMENDACIÓN	Revisar y documentar las actualizaciones, fecha de creación o aprobación de las políticas y procedimientos con que se cuenta, logrando en forma efectiva y oportuna hacer uso apropiado de la documentación que se encuentre actualizada.
COMENTARIOS DE LA ADMINISTRACIÓN	Todos los documentos oficiales que utiliza el área de TIC se encuentran en el sistema de gestión de calidad bajo la norma ISO 9001-2015, con el estándar que incluye el control de versiones.

ESTADO	**CORREGIDO** Se hizo una revisión en cada uno de los documentos entregados para los requerimientos iniciales, se determinó que, si cuentan con control de versiones y cambios, cabe destacar que hay varios documentos que no están aprobados, esto debido a que están en proceso de implementación y aprobación.
HALLAZGO 9: ADMINISTRACIÓN DE ACUERDOS DE SERVICIO. RIESGO MEDIO.	
RECOMENDACIÓN	1. Definir los acuerdos de niveles de servicio necesarios para la operatividad de los servicios. 2. Confeccionar los procedimientos para la administración y formalización de los niveles de servicio acordados.
COMENTARIOS DE LA ADMINISTRACIÓN	1-Se ha trabajado en establecer los niveles de servicios de las TIC, se aporta documento de "Informe Niveles de Servicio V2" 2- En el procedimiento 7P04, apartado Atención de incidencias informáticas (3.2.2), se indica la forma en la que se atenderán los incidentes y el tiempo de atención que se brindará, esto se tiene parametrizado en el sistema de Gestión de Incidentes. Ver hallazgo número 9 en carta a la gerencia 2009
ESTADO	**CORREGIDO** En el documento Informes niveles de servicio V2 se estable el catálogo de servicios de TI, compuesto de 24 servicios, además de su respectivo SLA para cada servicio.

MATRIZ DE SEGUIMEINTO A CG ANTERIORES CON RECOMENDACIONES DIRIGIDAS A DISTINTAS ÁREAS USUARIAS DE LA MUNICIPALIDAD DE CARTAGO

CG 1-2016	
HALLAZGO 02: CUMPLIMIENTO PARCIAL DEL REGLAMENTO INTERNO DE GESTIÓN DE LA COMISIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (CTIC). RIESGO BAJO.	
RECOMENDACIÓN	***A la Alcaldía*** 1. Girar instrucciones a la Comisión de Tecnologías de Información y Comunicaciones, para que sesione periódicamente según lo establecido en su reglamento.
COMENTARIOS DE LA ADMINISTRACIÓN	

ESTADO	**EN PROCESO** Se determinó que, en los meses de octubre, noviembre y diciembre, no se realizó ninguna sesión, ya sea ordinaria o extraordinaria por parte de la CTIC.
HALLAZGO 03: AUSENCIA DE INFORMES DE AUDITORÍA INTERNA REFERENTES A LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA MUNICIPALIDAD. RIESGO MEDIO.	
RECOMENDACIÓN	***Al Consejo Municipal*** ***1.*** Girar instrucciones a la Auditoría Interna para que realice estudios asesorías y/o advertencias relacionadas con el control interno de TI. ***A la Auditoría Interna*** 2. Efectuar estudios de auditoría interna referentes a TI. En caso de ser requerido recurso humano adicional al que existe actualmente, efectuar las gestiones necesarias, considerando las siguientes opciones: a. Contratar un auditor interno de tecnologías de información. b. Contratar periódicamente servicios profesionales externos de auditoría que apoyen a la Auditoría Interna en los estudios referentes a TI definidos dentro del plan de auditoría, incluso, podría pedirse asesoría a un externo desde la concepción del plan anual de auditoría.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** Este hallazgo se considera "En Proceso", ya que por medio del documento "Gestiones de Auditoria interna de TI" se determina que a partir del nombramiento de un auditor interno de TI (02 de abril de 2018), se pretende subsanar los problemas existentes referentes a la falta de informes de auditoría de TI. Lo cual determina que la Municipalidad de Cartago se encuentra trabajando en este hallazgo.
HALLAZGO 04: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LA BASE DE DATOS DE ACTIVOS. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área Financiera*** 1. Establecer un plan de acción para subsanar las inconsistencias identificadas, considerando lo siguiente: a. Determinar las causas de las inconsistencias en las bases de datos de activos. b. Realizar un levantamiento o verificación de activos de tal manera que se puedan identificar los datos reales. c. Realizar una depuración de las inconsistencias actuales.

COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** Se corrige el hallazgo, ya que no se encontraron inconsistencias en la base de datos de activos, por lo que se considera que las inconsistencias halladas en periodos anteriores ya fueron subsanadas.
HALLAZGO 05: POSIBLES INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LA BASE DE DATOS DE CUENTAS POR COBRAR. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área Tributaria*** 1. Determinar las causas de las inconsistencias en las bases de datos de cuentas por cobrar. 2. Establecer un plan de acción para la depuración de las inconsistencias identificadas, además de dar seguimiento y velar por la ejecución de dicho plan.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**NO APLICA** Las inconsistencias en la base de datos de cuentas por cobrar de parquímetros ya fueron subsanadas según el reporte brindado, sin embargo, hay otras inconsistencias que deben ser actualizadas al periodo actual, por lo cual se procede a crear un nuevo hallazgo.
HALLAZGO 06: INCONSISTENCIAS EN LA INFORMACIÓN ALMACENADA EN LA BASE DE DATOS DEL RUC. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área Tributaria:*** 1. Levantar un listado de los contribuyentes que poseen alguna inconsistencia en su información, principalmente en su número de cédula, de manera tal que en el próximo trámite que realicen se haga la gestión para actualizar la respectiva información.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** Ya se corrigieron dos casos que presentaban la irregularidad, además se están realizando comunicados para que las personas que presenten esta irregularidad procedan a actualizar los datos.
HALLAZGO 07: AUSENCIA DE UN MODELO INTEGRAL DE ARQUITECTURA DE INFORMACIÓN. RIESGO BAJO.	

RECOMENDACIÓN	***A la Comisión de Tecnologías de Información en coordinación con el Área de Informática:*** 1. Efectuar las gestiones para que las distintas áreas de la Municipalidad coordinen entre ellas y definan un modelo de arquitectura de la información el cual refleje la relación y comunicación de datos entre los procesos de la Municipalidad. Para ello se debe considerar los siguientes componentes: a. Procesos de negocio. b. Gestión de la información. c. Procesos y servicios de TI. d. Sistemas de información e. Personal involucrado en la manipulación de datos. f. Datos municipales. 2. Revisar el modelo de arquitectura de información al menos una vez al año, con el fin de mantenerlo actualizado de acuerdo con cambios en la infraestructura, personal o procesos de la Municipalidad. 3. Efectuar las gestiones para que el modelo de arquitectura de información cuente con la aprobación formal y sea comunicado a los interesados. 4. Valorar el uso de marcos de referencia como guía para crear un modelo de arquitectura de información robusto. Dichos marcos pueden ser: a. TOGAF (The Open Group Architecture Framework): es un marco de referencia utilizado como estándar global para la arquitectura empresarial. Dicho estándar permite asegurar que todas las unidades organizaciones manejen un mismo lenguaje de comunicación, ya que proporciona el diseño, planificación, implementación y gobierno de la información a nivel organizacional. b. COBIT 5 (Control Objectives for Information and related Technology): Marco de referencia que consolida COBIT 4.1 con otros marcos como Val IT y Risk IT, para la formulación de buenas prácticas y la toma de decisiones concernientes a T.I. en soporte de los objetivos organizacionales.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** Actualmente no se cuenta con un modelo integral de arquitectura de información. Solo se cuenta con un documento referente a un estudio para el Proyecto Implantación del SIAF en el Área Administrativa Financiera de la Municipalidad de Cartago. Además, los estudios relacionados son de sistemas específicos (WIZDOM y CORE) en el modelo de aplicaciones, y tecnología. No obstante, este modelo está considerado como anexo (Anexo 2 Modelo Integración SIAF (21-10-15)) y no es considerado como un modelo de arquitectura de información.

HALLAZGO 10: EXISTENCIA DE USUARIOS GENÉRICOS Y UNA CUENTA DE USUARIO DE UN EXFUNCIONARIO HABILITADA. RIESGO BAJO.	
RECOMENDACIÓN	***A las áreas usuarias de la Municipalidad*** 2. Notificar con antelación a TI cuando un funcionario ya no labora para la Municipalidad o si por alguna circunstancia esta fuera de la institución por un periodo de tiempo prolongado. ***Al Área de Informática:*** 4. En base al listado proporcionado por las distintas áreas usuarias de la Municipalidad deshabilitar las cuentas de usuario de funcionarios que cesan sus labores para la Institución según lo establecido por el procedimiento de gestión de usuarios 5. Valorar la existencia de usuarios genéricos y deshabilitar aquellos que no son requeridos en la operativa de TI. Además, documentar la debida justificación de este tipo de cuentas de usuarios. 6. Realizar revisiones periódicas sobre los directorios de usuarios para mantener al mínimo el uso de usuarios genéricos y validar que no se cuente con cuentas de exfuncionarios activas. En caso de presentarse la imperiosa necesidad de mantener a un usuario genérico se debe documentar su justificación y responsable.
COMENTARIOS DE LA ADMINISTRACIÓN	Incorporar en el Procedimiento de Recursos Humanos que, ante la separación de un funcionario por Jubilación, despido, o un permiso sin goce de salario superior a los tres meses, se deberá notificar al Área de Informática. PROCESO 7P02 GESTION DE TALENTO HUMANO
ESTADO	**CORREGIDO** Se corrige el hallazgo, ya que no se encuentra evidencia de la existencia de cuentas de exfuncionarios activas, ni de usuarios genéricos sin su respectiva justificación.
HALLAZGO 14: NO SE CUENTA CON UN DOCUMENTO INTEGRAL QUE CENTRALICE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. RIESGO BAJO.	
RECOMENDACIÓN	***Al Comité de Tecnologías de Información y Comunicaciones en coordinación con el Área de Informática:*** 6. Valorar la consolidación de los lineamientos de seguridad de la información con el fin de evitar la duplicidad de lineamientos y tener un mejor control del versionamiento de documentos. 7. Definir lineamientos en complemento con la política de seguridad de la información para los siguientes aspectos: a. Gestión de activos de TI: Definir políticas para la clasificación de activos según su criticidad y nivel de seguridad requerido. Además, se debe incluir lineamientos para el uso de dispositivos removibles (por ejemplo, llaves USB, HDD portables, etc.).

	b. Lineamientos de seguridad para el mantenimiento de sistemas e implementación de software. c. Lineamientos para la gestión de aquellos incidentes que comprometan la seguridad de la información. 8. Integrar el proceso de seguridad de la información con el proceso de continuidad de TI, en el cual se identifique cuales aspectos mínimos se deben considerar durante la ejecución del plan de continuidad. 9. Efectuar las gestiones para que la política de seguridad de información se revise y apruebe por parte de la instancia correspondiente, considerando el visto bueno de las áreas usuarias. 10. Capacitar a las áreas usuarias en la implementación de medidas de seguridad de la información y dar seguimientos a los casos que poseen un mayor riesgo. ***Al Área de Informática en coordinación con la Auditoría Interna*** 7. Realizar seguimientos periódicos al cumplimiento de la política de seguridad de la información y documentar los resultados de la revisión.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** El hallazgo se considera en proceso, ya que en el documento "Políticas acceso municipalidad V2" definen una serie de lineamientos bien estipulados sobre el control de accesos en toda la Municipalidad, pero en la Política de Seguridad de la información no se encuentran mencionados, ni menciona este documento. Lo mismo pasa con otros documentos como" Control de acceso"," seguridad en la implementación" y "Seguridad operaciones y comunicaciones". Por lo que se considera que aún existe una descentralización de la información referente a la política de Seguridad, no obstante, también se evidencia que se han realizado avances, producto de las revisiones y modificaciones según las recomendaciones del informe de auditoría del periodo 2016.
CG 2015	
HALLAZGO 01: AUSENCIA DE UN PLAN DE CAPACITACIÓN FORMAL PARA LOS FUNCIONARIOS DEL ÁREA DE INFORMÁTICA. RIESGO BAJO.	
RECOMENDACIÓN	***Al Área de Recursos Humanos en coordinación con el Área de Informática*** 1. Crear un plan formal de capacitación para el personal del Área de Informática, el mismo debe contemplar al menos los siguientes aspectos: a. Alineación estratégica b. Objetivos del plan de capacitación. c. Temas o áreas de conocimiento que se desean abordar.

	d. Priorización de los temas o áreas de conocimiento que se desea abordar. e. Cantidad de personal y personal al que va dirigido la capacitación. f. Fechas de ejecución de las capacitaciones. g. Costos asociados (capacitación, material, entre otros).
COMENTARIOS DE LA ADMINISTRACIÓN	Con la formulación del PAO de cada año, a los Encargados de Área y Jefes de Departamento se les remite una carpeta para que plasmen las necesidades de capacitación y que ésta sean insumos para la Unidad de Capacitación a fin de realizar el Plan de Capacitación Institucional. Esta Unidad no ha recibido solicitud de requerimiento alguno por parte de TI.
ESTADO	**EN PROCESO** Este hallazgo se considera "En proceso", ya que por medio de las evidencias suministradas se logra comprobar que para el periodo 2018 se cuenta con un documento llamado "6F16 Detección de necesidades de capacitación 2018" donde se describen las necesidades de capacitación de los colaboradores de TI, para el siguiente periodo. Además, se logra comprobar por medio del plan de capacitación suministrado, que se han efectuado tres capacitaciones en lo que lleva del periodo 2018, que concuerdan con lo que señala el documento de necesidades antes mencionado. No obstante, este plan de capacitación sigue la misma estructura (nombre funcionario, nombre capacitación, horas y su respectivo costo) del periodo 2017, lo cual se considera inadecuada ya que no contempla aspectos relevantes como fechas a realizar las capacitaciones, alineación estratégica, organización a capacitar y materiales a utilizar.
HALLAZGO 04: INCUMPLIMIENTO DEL PROCEDIMIENTO "DESHABILITAR O ELIMINAR CUENTAS DE USUARIO". RIESGO MEDIO.	
RECOMENDACIÓN	***A la Alcandía*** 1. Girar instrucciones para que los encargados de departamentos o de áreas cumplan a cabalidad con el procedimiento de deshabilitar o eliminar cuentas de usuarios según se establece, y comuniquen oportunamente al encargado de TI cuando algún funcionario a cargo abandona la Institución.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** Se corrige el hallazgo, ya que según el procedimiento "Deshabilitar o eliminar cuentas de usuario" encontrado en el documento "7P04, Gestión de TI", los jefes de las áreas usuarias deben notificar a TIC para deshabilitar a un funcionario (cesante), lo cual, según TIC en el documento "usuarios genéricos" menciona que mensualmente están realizando revisiones sobe las bases de datos para evitar inconsistencias con los colaboradores cesantes y sobre

	usuarios genéricos que las áreas usuarias reportan con esta condición. Por lo que se concluye, que el procedimiento se está cumpliendo a cabalidad.
CG 2013	
HALLAZGO 03: EL SISTEMA DE RECURSOS HUMANOS Y CONTABILIDAD NO SE ENCUENTRAN INTEGRADOS. RIESGO MEDIO.	
RECOMENDACIÓN	Integrar el sistema contable con el de recursos humanos, para evitar re-digitación y error en la información.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** Por medio de la evidencia entregada, se validó que el sistema de contabilidad ya está integrado con el sistema de recursos humanos. También se adjuntó una licitación directa para integrar el sistema de Recursos Humanos con el Core (Microsoft Dynamics), para terminar de integrarlo con el nuevo sistema.
CG 2011	
HALLAZGO 1: NO EXISTE UN HISTÓRICO DE INTERESES POR COBRAR GUARDADO A NIVEL DE BASE DE DATOS PARA LAS CUENTAS POR COBRAR. RIESGO ALTO.	
RECOMENDACIÓN	Implementar una solución técnicamente factible para poder mantener un histórico de los intereses por cobrar por concepto de pendientes de cobro de cada contribuyente por cada servicio, la solución debe generar los históricos de interés al ejecutarse un proceso programado diario de cálculo de pendientes de cobro.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** Por medio de la especificación funcional EF 15 Área Tributaria-Control de Interés se verificó que la debilidad mencionada ha sido subsanada, además se vio su cumplimiento en las bases de datos de cuentas por cobrar.
CG 2010	
OPORTUNIDAD DE MEJORA 9: LA BASE DE DATOS DEL SISTEMA DE INFORMACIÓN GEOGRÁFICA (SIG O GIS) Y DE BIENES INMUEBLES NO ESTÁN INTEGRADAS RIESGO ALTO	
RECOMENDACIÓN	Valorar la posibilidad de integrar la base de datos del SIG con el sistema de Bienes Inmuebles, después de analizar la factibilidad tanto económica, operativa y tecnológica con el objetivo de tener información adecuada y pertinente en ambos sistemas.

COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** Se verificó por medio de la especificación EF 10 Área Tributaria – Indicaciones de Actualizaciones Core Tributario con GIS, que se cuenta con una funcionalidad dentro de Microsoft Dynamics para crear solicitudes de un sistema a otro y viceversa, para que sean revisadas, aprobadas y ejecutas por el personal ya sea de GIS o del Core Tributario.
CG 2009	
HALLAZGO 6: INTEGRACIÓN DE LOS SISTEMAS. RIESGO ALTO.	
RECOMENDACIÓN	Dar seguimiento y solicitar reportes de avance sobre la implementación de la aplicación para el área financiera en que se pueda garantizar que los datos financieros sean parte de una cadena de valor y no un simple documento para el intercambio de información, con un lenguaje común, único y uniforme desde el punto de vista contable y confiable desde el punto de vista informático.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**CORREGIDO** La recomendación del hallazgo se ve subsanada con el sistema Wizdom, el cual integra el flujo de los datos ingresados y gestionados a nivel financiero – contable, por medio de las entrevistas a sistemas, se pudo corroborar que las áreas se integran entre sí por medio de Microsoft Dynamics, tal es el ejemplo de: • Plataforma y Servicios. • Urbanismo. • Comercial. El Core Microsoft Dynamics está en proceso de producción, por lo cual en este momento se están realizando pruebas, modificaciones y actualizaciones de requerimientos por parte de las áreas usuarias.

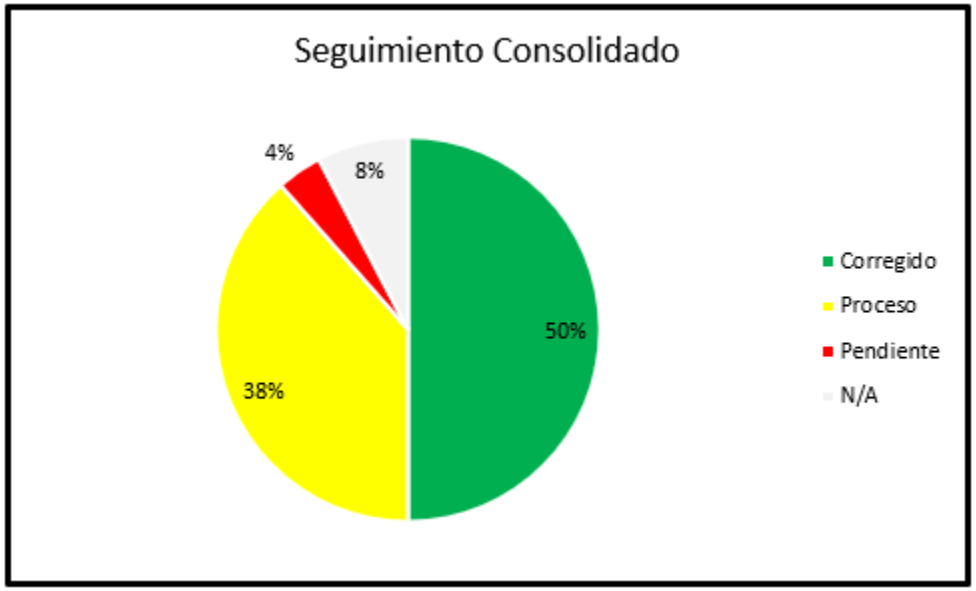
RESUMEN

Consolidado

A continuación, se resume de forma consolidada el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores de manera gráfica:

CONSOLIDADO					
Año/Estado	**CORREGIDO**	**PROCESO**	**PENDIENTE**	**NO APLICA**	**Total**
2016	5	9	1	1	**16**
2015	1	1	0	1	**3**
2014	1	0	0	0	**1**
2013	1	0	0	0	**1**
2011	1	0	0	0	**1**
2010	1	0	0	0	**1**
2009	3	0	0	0	**3**
TOTAL	**13**	**10**	**1**	**2**	**26**

Gráficamente, la tabla anterior se visualiza de la siguiente manera:

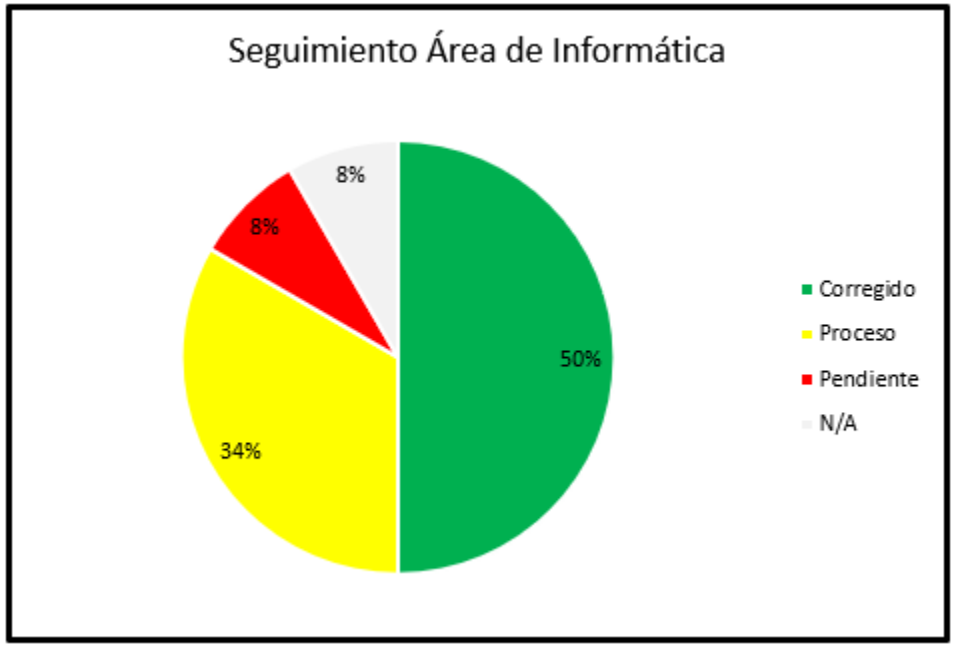


Área de Informática

En las siguiente tabla se muestra el detalle del cumplimiento de las recomendaciones responsabilidad del Área de Informática:

RECOMENDACIONES DIRIGIDAS AL ÁREA DE INFORMÁTICA					
Año/Estado	**CORREGIDO**	**PROCESO**	**PENDIENTE**	**NO APLICA**	**Total**
2016	3	4	1	0	**8**
2015	0	0	0	1	**1**
2014	1	0	0	0	**1**
2009	2	0	0	0	**2**
TOTAL	**6**	**4**	**1**	**1**	**12**

Gráficamente, la tabla anterior se visualiza de la siguiente manera:

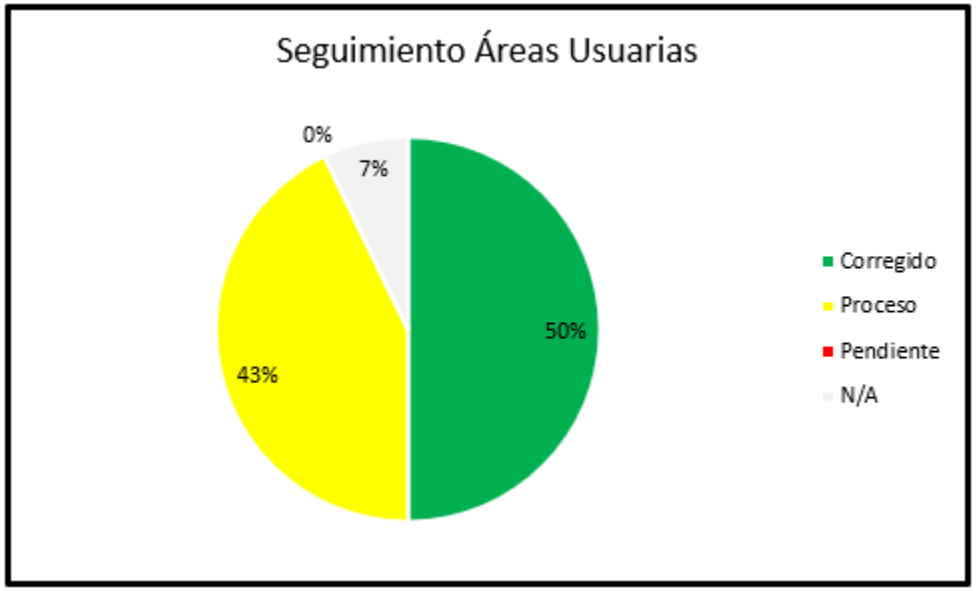


Áreas usuarias

En las siguiente tabla se muestra el detalle del cumplimiento de las recomendaciones responsabilidad de Áreas Usuarias:

RECOMENDACIONES DIRIGIDAS A ÁREAS USUARIAS					
Año/Estado	**CORREGIDO**	**PROCESO**	**PENDIENTE**	**NO APLICA**	**Total**
2016	2	5	0	1	**8**
2015	1	1	0	0	**2**
2013	1	0	0	0	**1**
2011	1	0	0	0	**1**
2010	1	0	0	0	**1**
2009	1	0	0	0	**1**
TOTAL	**7**	**6**	**0**	**1**	**14**

Gráficamente, la tabla anterior se visualiza de la siguiente manera:


Seguimiento Áreas Usuarias
0%
7%
50%
43%
Corregido
Proceso
Pendiente
N/A

ANEXOS

ANEXO I EVALUACIÓN FUNCIONAL DE ALGUNOS SISTEMAS DE INFORMACIÓN IMPLANTADOS EN LA MUNICIPALIDAD DE CARTAGO.

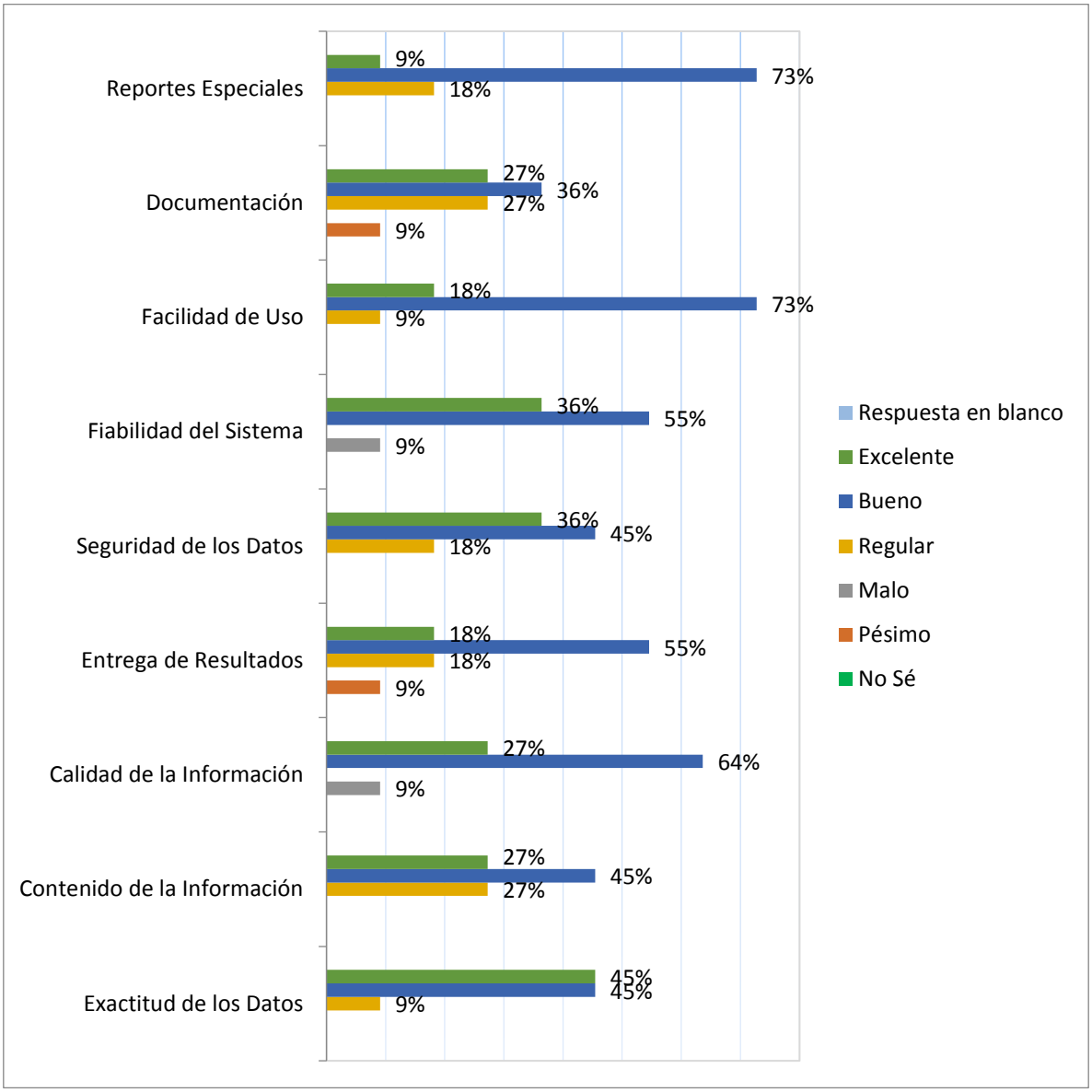
En este apartado se muestra el resultado de la evaluación realizada respecto a la calidad funcional de los sistemas de información implantados en la Municipalidad de Cartago según la percepción de los usuarios finales.

Los módulos revisados en el proceso de evaluación de la calidad funcional se muestran en la tabla siguiente:

Sistema por Valorar
Emisión Bienes Inmuebles
CORE Tributario
GIS
Plataforma de Servicios
Permisos de Construcción CRM
WIZDOM
Parquímetros
Cobros
Cobro Administrativo
Patentes
Exoneraciones Inmueble Único

Resultados obtenidos de la evaluación a la Municipalidad de Cartago

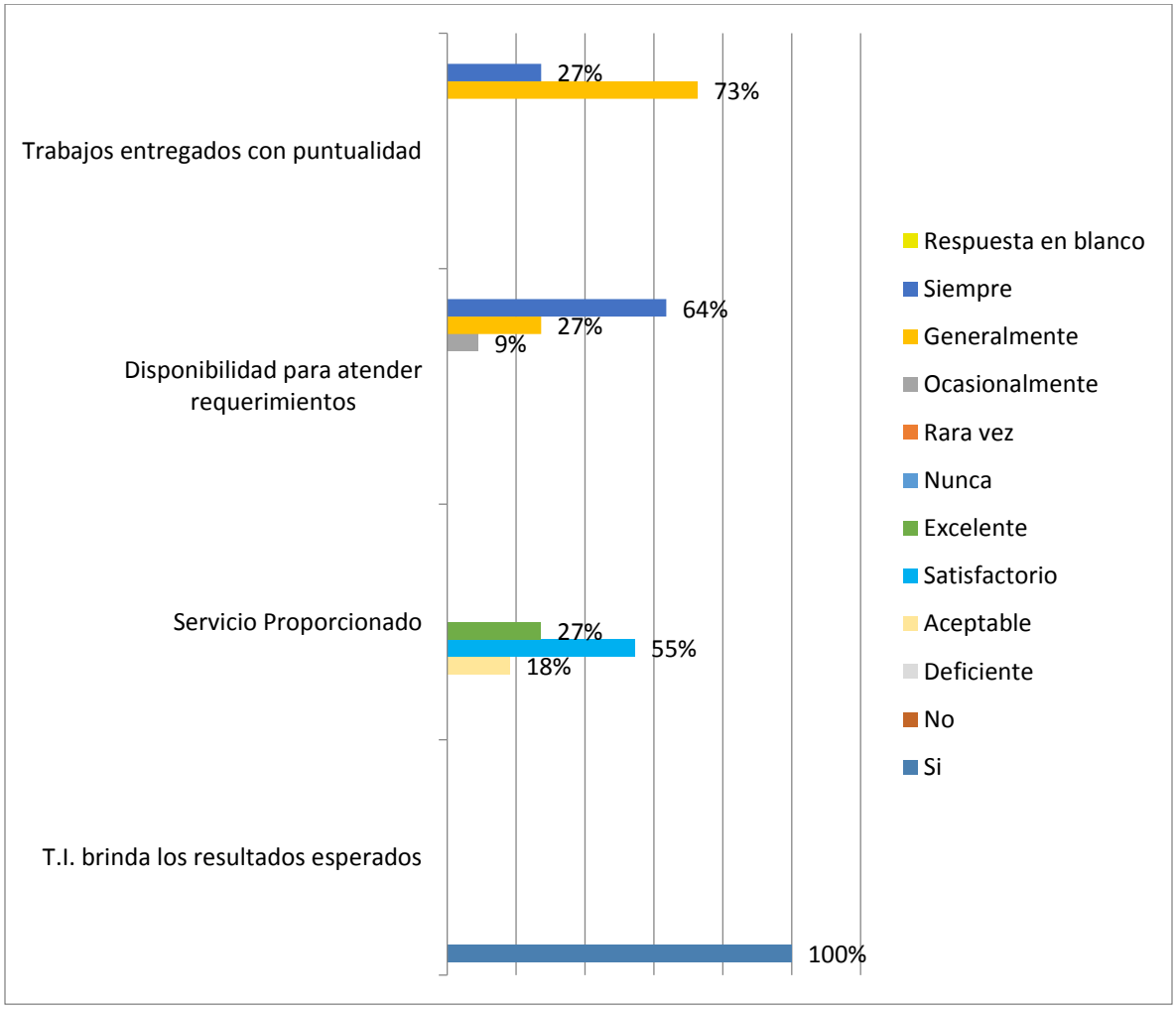
El detalle de la evaluación de la calidad funcional según usuarios de los sistemas de la Municipalidad de Cartago detallados en el cuadro anterior, se muestran en el gráfico siguiente:



Según los resultados obtenidos, los cuales se observan en el gráfico anterior, la percepción de la calidad de los sistemas se encuentra entre los valores "bueno" y "excelente", los cuales son los dos valores más altos en la calificación, sin embargo, para la categoría de contenido de la información, documentación, seguridad de los datos, entrega de resultados y reportes especiales, la opinión varía mucho respecto a otras categorías, siendo esta calificada como "regular" en algunas ocasiones. Además, es importante mencionar que, en los aspectos de

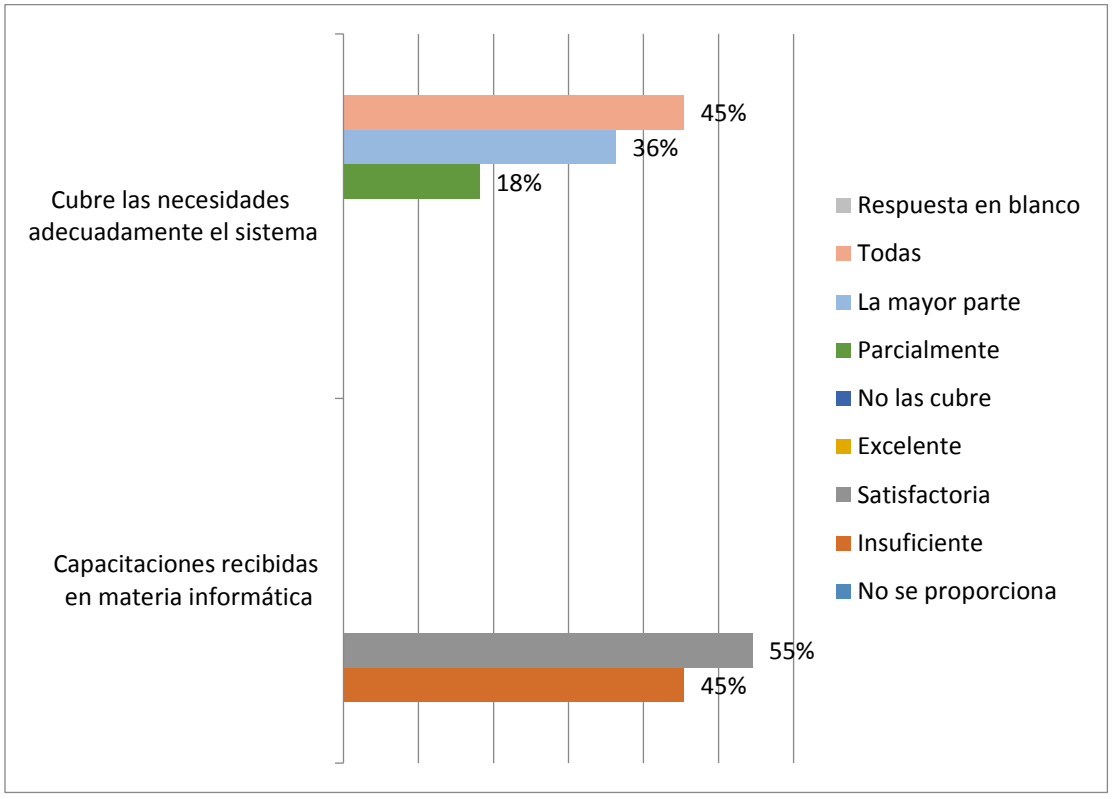
fiabilidad del sistema, calidad de la información, documentación y entrega de resultados, existe una pequeña población que refleja una disconformidad con los resultados obtenidos actualmente.

La percepción de los usuarios finales respecto al servicio brindado por parte del Área de Informática de la Municipalidad de Cartago, se muestran en el gráfico siguiente:



El gráfico anterior, corresponde principalmente a la satisfacción que poseen los usuarios respecto al servicio que brinda TI, en función a los sistemas de información utilizados. En el mismo se ve reflejado que la mayoría de las opiniones de los usuarios reflejan están conformes con el servicio de TI. No obstante, hubo opiniones que reflejaron cierto nivel de disconformidad con la gestión de las tecnologías de información.

Percepción de los usuarios finales respecto a si los sistemas de información de la Municipalidad de Cartago cubren la mayor parte de las necesidades actuales:



El gráfico anterior corresponde a la comodidad que sienten los usuarios frente al uso del sistema de información evaluado. Se puede evidenciar que el 55% de los usuarios indicaron estar conformes con las capacitaciones recibidas, no obstante, el 45% de los usuarios de los sistemas, indicaron que no están satisfechas con el entrenamiento recibido, lo cual puede reflejar una notable falta de capacitación ante el uso de los sistemas. Además, como parte del análisis del grafico anterior, hubo una mayoría (45%) en la que expresó que el sistema cubre todas sus necesidades laborales, así como, el 36% de las personas, afirman que los sistemas cubren la mayoría de sus necesidades, lo cual puede evidenciar que aún hay aspectos a los cuales se les puede prestar la debida atención para que la Municipalidad pueda ofrecer un mejor servicio.

Comentarios o mejoras por parte de los usuarios referentes a la valoración de los sistemas de información:

- Mejorar la comunicación y la capacitación para los usuarios de los sistemas.

- Un sistema de alarmas en el cual indique alguna situación especial de algún contribuyente. Por ejemplo, notificaciones al realizar una Prescripción, Casos listos para Cobro Judicial, Cortas, Inspecciones, Compensaciones, entre otras.

- Solicitudes de trámites a través del sistema, por ejemplo, traslados y demás.

- Los sistemas nuevos presentan gran cantidad de pasos para realizar una función que en los sistemas anteriores se realizaban en dos pasos, se debe buscar mejorar los tiempos con los sistemas nuevos, y no disminuir el tiempo de respuesta como se ha hecho.

- Se requieren separaciones de vistas de escritorio en el sistema, ya que actualmente el sistema es muy incómodo y no permite observar pantallas más que la del sistema.

- Implementar sistemas con una metodología de proyectos, involucrando a los usuarios finales, ya que actualmente se presentan problemas en la aceptación de los nuevos sistemas, ya que no se consideran riesgos de cambios y aceptación por los usuarios.

- Considerar disminuir las facturas físicas, ya que son muy grandes y consumen gran cantidad de papel.

RECOMENDACIÓN

Propiciar una reunión entre el Área de Informática con los usuarios de las áreas involucradas, con el fin de llevar a cabo las mejoras que correspondan, levantando los requerimientos necesarios para cubrir las necesidades o debilidades que, de una u otra forma, afectan los servicios que brinda la Municipalidad de Cartago.

Considerar elaborar material para generar capacitaciones sobre los nuevos sistemas que se están implementando dentro de la Municipalidad de Cartago, ya que los usuarios sienten que existen debilidades en las capacitaciones sobre el uso de los sistemas.

ANEXO II Análisis de Riesgos T.I.

Área de Informática

Periodo 2017

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio ☑	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo ☑	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

A. SEGURIDAD FÍSICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones Administración	Tipo de riesgo
		SÍ	NO			
A.1	Proceso de autorización de ingreso		✓	Se le debe presentar al director de TI la justificación requerida, para analizarla y proceder con la aprobación y configuración del acceso.		B
A.2	Personal interno y externo debidamente identificado (gafete)		✓	Se utiliza un gafete.		B
A.3	Revisión de equipos de ingreso y salida		✓	Se traslada a un sitio de la Municipalidad para el manejo de desecho de equipo y se coordina con las demás áreas para hacer la respectiva salida. El equipo ingresa al almacén para que se le asigne la respectiva placa, posteriormente pasa a TI el cual lo incluye en inventario. Si se trata de un equipo delicado, el mismo lo gestiona TI directamente, y este envía la información a él área de control de activos.		B
A.4	Bitácoras de acceso al edificio y centro de cómputo		✓	Se cuenta con una bitácora digital (registros en pantalla) para el acceso al departamento de TI y una bitácora electrónica para el acceso al cuarto de servidores.		B
A.5	Acceso restringido a personal de informática definido		✓	Solo los colaboradores encargados de infraestructura y la jefatura del área de TI, pueden ingresar.		B
A.6	Una sola vía de acceso		✓	Solo existe una vía de acceso al departamento de TI y cuarto de servidores.		B
A.7	Externos son acompañados por internos		✓	Solo acompañados de un funcionario, se puede ingresar al departamento de TI.		B
A.8	Puerta de acceso segura		✓	La puerta es de vidrio, sin embargo, la misma está monitoreada por una cámara de seguridad.		B

A.9	Acceso con tarjeta electrónica al centro de datos		✓	Los funcionarios solo pueden ingresar al departamento por medio de la tarjeta electrónica.		B
A.10	Alarmas de detección de intrusos	✗		No se cuenta con alarmas de detección de intrusos.		B
A.11	Monitoreo de la entrada por cámara de seguridad		✓	Se cuenta con una cámara de seguridad, la cual está instalada en el interior del cuarto de servidores.		B
A.12	Ubicación en un sitio seguro (lugares colindantes)		✓	El cuarto de servidores se encuentra en un lugar seguro, dentro del departamento de Informática, en el segundo piso de la Municipalidad de Cartago.		B
A.13	Lugar completamente cerrado		✓	Sí se encuentra en un lugar completamente cerrado.		B
A.14	Paredes de concreto	✗		Una parte de una de las paredes es de gypsum. No obstante, la misma colinda con la oficina de TI.		B
A.15	Cielo raso sellado		✓	El cielo raso está completamente cerrado.		B
A.16	Equipos ubicados en rack		✓	Los equipos si se encuentran ubicados en racks.		B
A.17	Los racks están asegurados		✓	Los racks se encuentran correctamente asegurados.		B
A.18	Cableado de datos independiente del eléctrico		✓	El cableado de datos se encuentra totalmente independiente del cableado eléctrico.		B
A.19	Cableado entubado y canaleteado		✓	Se comprueba que el cableado se encuentra entubado y canaleteado.		B
A.20	Cableado debidamente rotulado		✓	Sí se cuenta con cableado rotulado.		B
A.21	Hay un sitio alterno		✓	Sí existe un sitio alterno.		B

B. INSTALACIÓN ELÉCTRICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
B.1	Hay pararrayos		✓	Sí se cuenta con pararrayos.		B
B.2	Circuito eléctrico independiente		✓	Sí se cuenta con un circuito eléctrico independiente.		B
B.3	Interruptor de emergencia en la sala de cómputo (palanca)		✓	Sí se cuenta con interruptores de corriente que controlan el flujo eléctrico en el cuarto de servidores.		B
B.4	Cableado eléctrico debidamente entubado o cubierta contra incendios		✓	Sí se posee cableado entubado y debidamente protegido.		B
B.5	Conexión de los equipos a UPS		✓	Sí se cuenta con una conexión de todos los equipos a la UPS.		B
B.6	UPS ubicada en un sitio seguro		✓	La UPS se encuentra dentro del cuarto de servidores.		B
B.7	Pruebas periódicas de la UPS (bitácora)	✗		Se realizan ocasionalmente, ya que no hay un periodo establecido para las revisiones.	En ocasiones los de mantenimiento, en sus revisiones de cada dos meses, realizan las pruebas sobre las UPS.	B
B.8	UPS en contrato de mantenimiento preventivo y correctivo		✓	Sí se encuentra en mantenimiento por parte de un proveedor de servicio.	Cada dos meses, la someten a revisión.	B
B.9	Conexión a Planta eléctrica		✓	Sí existe una conexión con la planta eléctrica.		B
B.10	Planta eléctrica ubicada en un sitio seguro		✓	La planta eléctrica si se encuentra en un lugar seguro, dentro de las instalaciones de la Municipalidad.		B
B.11	Pruebas periódicas de la planta eléctrica		✓	Sí se realizan pruebas a la planta eléctrica.		B
B.12	Planta eléctrica en contrato de mantenimiento preventivo y correctivo		✓	Se le da mantenimiento bimensual por parte de un proveedor de servicios.		B

B.13	Luces de emergencia en el centro de cómputo o cercanías		✓	Sí se cuenta con luces de emergencia dentro del cuarto de Servidores y área de informática.		B
B.14	Pruebas periódicas de sistema de iluminación de emergencias		✓	Sí se realizan pruebas de iluminación de emergencias.		B

C. INSTALACIÓN AIRE ACONDICIONADO

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
C.1	Equipo de aire acondicionado independiente para el centro de datos		✓	Se posee 3 aires acondicionados, dedicados al centro de datos.		B
C.2	Equipo de respaldo para el aire acondicionado		✓	Si se posee equipo de respaldo, en caso de que algún aire acondicionado falle.		B
C.3	Contrato de mantenimiento preventivo y correctivo		✓	Cada dos meses se realiza el mantenimiento preventivo sobre los equipos de aire acondicionado.		B
C.4	Control y monitoreo de humedad y temperatura		✓	Existe una herramienta (Watchdog) que permite el control y monitoreo de humedad y temperatura.	Se encuentra dentro del cuarto de servidores.	B

D. DESASTRES NATURALES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones Administración	Tipo de riesgo
		SÍ	NO			
D.1	Brigada de emergencias		✓	Sí se cuenta con una brigada de emergencia.		B
D.2	Capacitación del personal		✓	Sí se realizan capacitaciones al personal sobre emergencias.		B
D.3	Rutas de evacuación y salidas de emergencia		✓	Sí se tienen definidas las salidas de emergencia a nivel municipal.		B

D.4	Señalización		✓	Cada lugar de la Municipalidad de Cartago cuenta con su respectiva rotulación, y ayuda en caso de evacuación.		B
D.5	Simulaciones periódicas	✗		No se realizan simulaciones por parte de la brigada de emergencia.	El área de TIC no tiene injerencia en este tema.	B
D.6	Fácil acceso por Unidades de Bomberos		✓	Sí es de fácil acceso para las Unidades de Bomberos.		B
D.7	Sistemas de detección de humo/calor/fuego		✓	Existen dos detectores de humo.		B
D.8	Sistemas automáticos y manuales de alarma		✓	Sí se cuenta con un sistema que genera automáticamente alarmas sobre acciones previamente configuradas.		B
D.9	Extinguidores cercanos portátiles (revisados al día)	✗		Los extinguidores están a más de 5 metros de distancia del cuarto de servidores.	Los extinguidores si se encuentran al día.	B
D.12	Uso de aspersores	✗		No se cuenta con aspersores o un sistema supresor de incendios.	Solo cuentan con alarmas de incendio.	B
D.11	Pisos falsos		✓	No se cuenta con piso falso.	Sí se cuenta con techo falso.	B
D.12	Desnivel en el piso		✓	Si se cuenta con un desnivel en el piso, para que, en el caso de una inundación, pueda filtrar el agua rápidamente.		B

E. FALLAS HARDWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
E.1	Redundancia de servidores críticos		✓	Se tiene un clúster con 5 nodos, con servidores virtualizados, en caso de la pérdida de un nodo, la carga se balancea en los demás nodos.		B
E.2	Mantenimiento preventivo		✓	Los servidores que gestionan los servicios críticos se encuentran bajo un contrato de mantenimiento, los demás son a lo interno.		B

E.3	Mantenimiento correctivo		✓	Los servidores que gestionan los servicios críticos se encuentran bajo un contrato de mantenimiento, los demás son a lo interno.		B

F. FALLAS SOFTWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
F.1	Política de uso de recursos (prioridades en procesos)		✓	Sí se cuenta con políticas para la red (se tienen grupos con diferentes perfiles de acceso), correo electrónico, telefonía (llamadas internas, externas nacionales o internacionales). Las cuentas de los usuarios no tienen privilegios de administrador en las máquinas.		B
F.2	Control de cambios		✓	Se cuenta con un documento de políticas de TI el cual tiene lineamientos para la gestión de cambios, las solicitudes se realizan a través de correo electrónico. Para los cambios en los sistemas, se debe llenar un formulario.		B

G. FALLAS EN COMUNICACIONES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
G.1	Redundancia de equipos y enlaces		✓	Se cuenta con dos enlaces de proveedores distintos: ICE y JASEC, y se tiene redundancia en el equipo de firewall.		B
G.2	Mantenimiento preventivo		✓	Sí se realiza por medio de un contrato con un proveedor de servicio (DESCA).		B
G.3	Mantenimiento correctivo		✓	Sí se realiza por medio de un contrato con un proveedor de servicio (DESCA).		B

H. RESPALDOS Y RECUPERACIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
H.1	Política de respaldos		✓	Se cuenta con procedimientos para la realización de respaldos de información.		B
H.2	Procedimientos para respaldo y recuperación		✓	Se cuenta con procedimientos para la realización de respaldos de información.		B
H.3	Almacenamiento de información		✓	Se almacena una copia de información en el cuarto de servidores y otra se envía al sitio alterno.		B
H.4	Traslado de respaldos		✓	Se envían vía VPN al sitio alterno.		B
H.5	Configuración de programas para respaldo		✓	Se realiza una configuración previa, antes de realizar los respaldos.		B

I. ATAQUES POR VIRUS

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
I.1	Política de antivirus		✓	Se cuenta con la política y con el sistema (Windows Defender).		B
I.2	Programa antivirus		✓	Windows Defender		B
I.3	Actualización del antivirus		✓	Se tienen las actualizaciones automáticas.		B
I.4	Administración de incidentes y problemas	✗		No existe una división entre incidentes y problemas, no obstante, si se lleva un adecuado seguimiento a cada incidente, pero no ha problemas.		M

J. INTRUSIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
J.1	Política de acceso lógico		✓	Se tiene un procedimiento documentado para la solicitud de accesos.		B
J.2	Control de acceso a aplicaciones		✓	Las jefaturas realizan la solicitud de acceso a TIC.		B
J.3	Monitoreo de usuarios y accesos	✗		Se realiza ocasionalmente la revisión, generalmente bajo demanda.		M

K. ADMINISTRACIÓN DE OPERACIONES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
K.1	Capacitación personal técnico		✓	Cada año se verifica que necesidades se tienen para determinar que capacitaciones son requeridas.		B
K.2	Segregación de funciones		✓	Sí se segregan las funciones (infraestructura, soporte, desarrollo de software, jefatura y secretaria administrativa).		B

L. RIESGOS DE LA GESTIÓN DE TI

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.1	¿Se tienen definido un plan estratégico para TI alineado con el de la organización?		✓	Sí se posee y se encuentra alineado.		B
L.2	¿El Plan estratégico ha sido divulgado a los niveles que corresponde?		✓	Sí, están publicados tanto en la intranet como en la página Web institucional y cuando se entregó se presentó a la CTI y Consejo.		B
L.3	¿Se tienen definidas las políticas y procedimientos para TI?	✗		No se cuenta con un procedimiento de calidad de TI.		B
L.4	¿Se tiene definido el apetito de riesgos para TI? (Nivel de riesgo que la Institución quiere aceptar)		✓	Se cuenta con un nivel de riesgo aceptable por la institución.		B
L.5	¿Los riesgos que la organización se encuentra dispuesta a aceptar se encuentran aprobados formalmente por la Administración y el Comité de Riesgos?	✗		Actualmente se cuenta con lineamientos institucionales para la gestión de riesgos; sin embargo, no se hace evidencia de la aceptación de los riesgos por la Administración y el Comité de Riesgos.		B
L.6	¿El mapa de riesgos es revisado y actualizado periódicamente?		✓	Se cuenta con un mapa de riegos en el plan para la gestión de riesgos del área de TIC.	El plan se está implementando por lo que no se puede determinar las revisiones y actualizaciones periódicas.	B
L.7	¿La evaluación de riesgos considera elementos cualitativos y cuantitativos?		✓	El plan para la gestión de riesgos del área de TIC cuenta con una sección donde estipula la evaluación de riesgos de manera cualitativa y cuantitativa.		B
L.8	¿Los riesgos de TI son revisados con los usuarios del sistema?	✗		Se han realizado talleres de SEVRI donde se revisan riesgos. Adicionalmente cuando se solicitan mejoras a los sistemas, se evalúan riesgos de implementación. Sin embargo, no se cuenta con una metodología definida.		B
L.9	¿Se han implementado anti virus y firewalls?		✓	Sí se tiene implementado ambos elementos, inclusive se tiene redundancia de firewall.		B

L.10	¿Se han establecido los protocolos para la realización de copias de seguridad?		✓	Se cuenta con procedimientos para la realización de respaldos de información.		B
L.11	¿La seguridad de la información es un tema de seguimiento para la alta gerencia como para el Comité de Auditoría?		✓	Se realiza tanto en el Sistema de Gestión de Calidad, así como el seguimiento de los hallazgos de Auditoria Externa. Uno de los requerimientos solicitados por la administración es la seguridad para el acceso a los sistemas de información.		B
L.12	¿Las políticas y procedimientos relacionados con TI son revisados y actualizados periódicamente, considerando los cambios en la industria y la regulación externa?		✓	Se identificaron documentos con control de versiones, lo cual, se determina que se han realizado cambios periódicamente.		B
L.13	¿Se tiene definido el perfil para cada cargo de TI y los colaboradores vinculados cumplen con el mismo?		✓	Se cuenta con un documento el cual describe los perfiles de los funcionarios de TI.		B
L.14	¿Se tienen definidas y divulgadas las funciones y responsabilidades de cada colaborador del área?		✓	Sí se encuentran divulgadas las funciones y responsabilidades de cada colaborador.		B
L.15	¿Las responsabilidades de cada nivel y colaborador, parten del principio de segregación de funciones?		✓	Sí se cuenta con una segregación de funciones.		B
L.16	¿La creación de usuarios y la asignación de los permisos y/o perfil en los aplicativos es solicitada y aprobada formalmente por cada líder de área?		✓	Las jefaturas son las que solicitan los permisos al Área de Informática.		B
L.17	¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de las mismas?		✓	Cuando se implementan los sistemas, se dan capacitaciones sobre los mismos. Además, se tienen las cuentas de los usuarios con permisos restringidos.		B
L.18	¿Las herramientas de TI permiten tener la trazabilidad de las operaciones realizadas así como de los usuarios (logs)?		✓	Sí se registran las acciones realizadas por los usuarios en locks.		B
L.19	¿Se monitorea el estado de los equipos (Hardware)?		✓	Sí se cuenta con un documento donde se registran los equipos de hardware.		B

L.20	¿La seguridad física de las instalaciones donde operan los equipos y personas de TI, es evaluada y revisada periódicamente, cumplimiento con los protocolos establecidos?		✓	Se revisan durante el proceso de auditoría externa.		B
L.21	¿La organización desarrolla un plan de formación integral tanto para los miembros de TI como para los usuarios de la herramienta, orientado al uso, seguridad y ética en la utilización de las mismas?		✓	Sí se posee un plan de capacitación el cual se debe de mejorar.		B
L.22	¿Se han establecido indicadores de gestión que permitan medir el desempeño de las herramientas y de los colaboradores del área?		✓	Sí, se han establecido indicadores de gestión a nivel interno del área de TIC con lo que se puede medir el desempeño y tiempos de respuesta de los colaboradores.		B
L.23	¿Se han implementado planes de acción correctivos, para aquellos casos en que los indicadores presentar resultados inferiores a los esperados?		✓	Se utiliza una herramienta para medir la gestión de salidas no conformes con lo que se implementan acciones correctivas para los indicadores que presentan resultados no esperados.		B
L.24	¿Se han adquirido pólizas de seguro para eventos de riesgos en el área de TI?		✓	Sí, se cuenta con póliza de seguro para los activos de TI críticos, estos los gestiona el área Financiera.		B
L.25	¿Cada proyecto de TI tienen definidos y documentos los riesgos tanto de su desarrollo como de la puesta en marcha, así como tiene la proyección de recursos financieros a invertir?	✗		No se cuenta con una metodología de gestión de riesgos de TI para proyectos.		M
L.26	¿Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de TI y dicho seguimiento es documentado?		✓	Se mantiene un constante seguimiento a los contratos, se da seguimiento al cronograma donde se indican las fechas aproximadas para brindar el mantenimiento, además se valoran los tiempos de respuesta brindados.		B
L.27	¿Todos los cambios desarrollados en las aplicaciones y/o software son documentados y custodiados?		✓	Sí se realiza una documentación de software o cambios recomendados.		B

L.28	¿Se ha establecido el plan de continuidad para los procesos de TI?		✓	Sí se cuenta con un plan de continuidad para los procesos de TI.		B
L.29	¿Se solicita el apoyo de consultores externos para los proyectos estratégicos?		✓	Sí se solicita apoyo de externos cuando es requerido.		B

M. SISTEMAS DE INFORMACIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones Administración	Tipo de riesgo
		SÍ	NO			
M.1	Los accesos son autorizados por un nivel superior.		✓	Los accesos son solicitados por las jefaturas de las áreas.		B
M.2	Los accesos otorgados son revisados periódicamente.		✓	Las revisiones se realizan cada mes.		B
M.3	La asignación de los accesos parte de la segregación de funciones.		✓	Si se hace una asignación de accesos, a partir de la segregación de funciones.		B
M.4	Cada usuario tiene asignada una clave de composición alfa numérica y de mínimo 8 caracteres		✓	Sí, ya que cada usuario tiene asignada una clave de mínimo 8 caracteres y de composición alfanumérica.		B
M.5	Se pueden rastrear las operaciones realizadas por los usuarios por medio de los logs		✓	Sí se pueden rastrear operaciones por medio de logs.		B
M.6	Se cuenta con una política de copias de seguridad y de restauración.		✓	Se cuenta con un procedimiento para la realización de respaldos de información.		B
M.7	La información sensible se encuentra protegida de modificaciones no autorizadas.		✓	Sí se protege la información sensible en el área de Informática.		B
M.8	Se cumplen con los niveles de seguridad físicos para los servidores.		✓	Sí se cumplen con los niveles de seguridad físicos para los servidores.		B
M.9	Asignación de usuarios y claves personalizada		✓	Los usuarios siguen un estándar, y las claves si pueden ser personalizadas a cumplimiento de las reglas existentes.		B
M.10	Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.		✓	Sí se segregan estas funciones, existen diferentes niveles de accesos.		B

M.11	Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.		✓	Se notifican a las áreas usuarias cuando se implementa un cambio.		B
M.12	Las modificaciones en las bases de datos son realizadas por un área independiente a la que utiliza la información.		✓	Los cambios a las bases de datos solo pueden ser modificadas por el área de TIC. Encargado de BD		B
M.13	Los cambios en la base de datos permiten tener la trazabilidad de quien los realiza por medio de los logs.		✓	Sí se cuentan con logs en las bases de datos.		B
M.14	Se tiene un número reducido de administradores.		✓	Sí, se tiene un número reducido de usuarios administradores, según las necesidades de la Institución se crean roles y se asignan a los usuarios.		B
M.15	Se cuenta con un diccionario de datos para la base de datos, identificando las relaciones internas que tiene y los accesos de consulta o modificación.		✓	Sí se cuenta con un diccionario de datos.		B
M.16	Definición y documentación de la Política de Cambios		✓	Se cuenta con el procedimiento 7P04, el cual documenta el procedimiento de cambios.		B
M.17	Segregación de funciones entre el desarrollador, aprobador y responsable de administrar en producción		✓	Sí se realizan segregaciones de funciones, ya que cada colaborador verifica las solicitudes de nuevas funcionalidades, las revisan con el jefe a cargo, se desarrollan y se colocan en producción.		B
M.18	Aprobación del usuario final de los cambios.		✓	Se realizan revisiones con los usuarios finales para verificar sus aprobaciones.		B
M.19	Asignación usuarios y permisos, previo requerimiento y aprobación del Director y/o Responsable del área que utiliza la aplicación.		✓	Las jefaturas de las áreas usuarios son las que solicitan los permisos de los sistemas.		B
M.20	Reportes periódicos de los cambios que se consideran críticos en las aplicaciones, para validar su autorización por parte del nivel aprobador de los cambios.		✓	Sí se generan reportes a partir de los cambios realizados, para verificar el cumplimiento de las funciones en las áreas usuarias.		B

M.21	Validación periódica de los cambios en permisos y asignación de usuarios por parte del nivel autorizador.	✗		La revisión de permisos se realiza bajo demanda.		M
M.22	Bloqueo de usuarios retirados, previa comunicación de Gestión Humana.		✓	Existe un procedimiento para deshabilitar cuentas de usuario, que se realiza a partir de proactividad del área de TIC y por notificaciones previas.		B
M.23	Revisión periódica de la compatibilidad de los accesos otorgados de acuerdo con el reporte de funciones de Gestión Humana y el principio de segregación de funciones.	✗		La revisión de permisos se realiza bajo demanda.		M
M.24	Bloqueo de usuarios en vacaciones	✗		Se cuenta con un procedimiento, sin embargo, el área de TIC cumple con desactivar los usuarios, pero en ocasiones las áreas usuarias no notifican o envían información sobre el bloqueo a colaboradores.		M
M.25	Identificación de los usuarios que realizan las transacciones, por medio de los Logs.		✓	Sí se cumple con esta condición.		B
M.26	Certificaciones externas sobre la calidad del servicio prestado.		✓	Se realizan auditorías externas anualmente.		B
M.27	Suscripción de un acuerdo sobre privacidad con el proveedor.		✓	Sí se cuenta con acuerdos sobre privacidad con los proveedores.		B
M.28	Plan de contingencia para migrar a otro servidor		✓	Sí se cuenta con un plan de contingencias.		B
M.29	Plan de capacitaciones en seguridad, para los usuarios con accesos más vulnerables.		✓	Se han realizado capacitaciones a los usuarios con la implementación de los sistemas de información.		B
M.30	Cifrar las bases de datos más sensibles, junto con controles de monitoreo.	✗		Actualmente no se cifran las Bases de Datos.		M
M.31	Limitar el acceso a los datos y/o solicitar mayores autenticaciones, de acuerdo al dispositivo y al lugar desde donde se ingresa.		✓	Se puede acceder a la información desde fuera de la Institución, utilizando un canal seguro como lo es una VPN la cual es proveída por el equipo de seguridad perimetral Fortigate 800D		B

M.32	Instalar en los dispositivos móviles parches que permitan aislar los datos de la compañía de los personales.		✓	Se puede acceder a la información desde dispositivos móviles utilizando varias medidas de seguridad tales como la autenticación e identificación del usuario la cual es validada por la aplicación que provee los datos, además no se expone directamente la base de datos, sino que se presenta por medio de algún web service o espejo de la base de datos.		B
M.33	Se realizan pruebas periódicas sobre la recuperación de datos.		✓	Se han realizado recuperaciones de información, por medio de proveedores.	Se realizan bajo solicitud.	B

--Última Línea--