INFORME Nro. MLC-UAI-INF-012-2021

AUDITORIA DE CARÁCTER ESPECIAL SOBRE EL CUMPLIMIENTO DE BUENAS PRÁCTICAS DE GOBIERNO DE TI QUE GARANTICEN EL ALINEAMIENTO ESTRATÉGICO DE LAS TECNOLOGÍAS DE INFORMACIÓN CON LOS OBJETIVOS DE LA MUNICIPALIDAD DE LA CRUZ, PARA PERMITIR ASEGURAR, DE MANERA RAZONABLE, EL BUEN DESEMPEÑO DE LOS PROCESOS SUSTANTIVOS Y LA CONTINUIDAD DE LOS SERVICIOS.

1. INTRODUCCION.

1.1 Origen del estudio.

Los criterios de auditoría son niveles razonables y alcanzables de desempeño en comparación con los cuales pueden evaluarse la economía, la eficiencia y la eficacia de las actividades. Reflejan un modelo normativo (es decir, deseable) con respecto a la materia que es objeto de revisión.

Por ello, es necesario la realización de un seguimiento periódico y ordenado de los diferentes sistemas financiero-contables y presupuestarios, así como de los procedimientos operativos y administrativos propios del Departamento de Tecnologías de Información y Comunicación municipal.

Por lo anterior, se hizo necesario la realización de un estudio que abarcara la evaluación de los controles internos, administración de recursos informáticos, planificación operativa y estratégica, gestión de riesgos, control y ejecución de proyectos de TIC de los períodos comprendidos entre el 1 de julio del 2015 al 31 de diciembre del 2020, lo anterior con el objetivo de determinar su eficiencia y eficacia.

Por ello, se incluyó en el Plan de Trabajo para el año 2021 la “Auditoria de carácter especial sobre el cumplimiento de buenas prácticas de Gobierno de TI que garanticen el alineamiento estratégico de las tecnologías de información con los objetivos de la Municipalidad de La Cruz, para permitir asegurar, de manera razonable, el buen desempeño de los procesos sustantivos y la continuidad de los servicios”.

Esta Unidad de Control y Fiscalización presenta los resultados obtenidos mediante la entrega formal de este informe.

1.2 Responsabilidad de la Administración.

La veracidad y exactitud de los datos contenidos en la información suministrada para este análisis, en relación al cumplimiento de buenas prácticas de Gobierno de TI que garanticen el alineamiento estratégico de las tecnologías de información con los objetivos de la Municipalidad de La Cruz, para permitir asegurar, de manera razonable, el buen desempeño de los procesos sustantivos y la continuidad de los servicios, es de total responsabilidad de la administración municipal de acuerdo con el artículo 10 y 16 de la Ley General de Control Interno.

1.3. Criterios del estudio.

a) Ley General de Control Interno, ley 8292.

b) Código Municipal Ley No. 7794 de la Rep. De Costa Rica y sus actualizaciones.

c) Normas Generales de Control Interno para el sector público, emitidas por la CGR.

d) Normas de Auditoria para el sector público, emitidas por la CGR.

e) Resolución "N-2-2007-CO-DFOE/ Normas Técnicas para la Gestión y el Control de Tecnologías de Información".

f) COBIT 4.1

1.4. Objetivo general del estudio.

Verificar el cumplimiento de buenas prácticas de Gobierno de TI que garanticen el alineamiento estratégico de las tecnologías de información con los objetivos de la Municipalidad de La Cruz, para permitir asegurar, de manera razonable, el buen desempeño de los procesos sustantivos y la continuidad de los servicios.

1.5. Naturaleza y alcance del estudio.

El estudio comprendió lo siguiente:

a) La evaluación de los controles internos, administración de recursos informáticos, planificación operativa y estratégica, gestión de riesgos y control y ejecución de proyectos de TIC del 1 de julio 2015 a diciembre 2020, así como, determinar su eficiencia y eficacia.

b) La verificación del Plan Estratégico de Tecnologías de Información si se está cumpliendo con lineamientos y si el mismo se encuentra en concordancia con el Plan Estratégico Institucional específicamente en los objetivos relacionados con TI.

c) Evaluación del estado de infraestructura de TI e integridad de bases de datos en los sistemas de información existentes en los siguientes aspectos:

1. Análisis de compatibilidad de la plataforma informática instalada de acuerdo con los requerimientos de infraestructura tecnológica, tanto en aspectos de sistemas operativos, software yhardware que están operando en la Municipalidad de La Cruz.

2. Evaluar la instauración o desarrollo de proyectos orientados a la aplicación de plataformas de pagoen línea y conectividades relacionadas para el pago y cumplimiento de las obligaciones económicasasociadas a servicios, tributos cánones y precios públicos municipales.

3. Evaluación de la integridad de base de datos del sistema informático administrativo en cuanto a lossiguientes procesos de información:

   - ✓ Carga de Datos al Sistema Informático Administrativo en todos sus módulos funcionales para todos los Departamentos de la "Municipalidad de La Cruz".
   - ✓ Intereses.
   - ✓ Modificación de parámetros de cobro por actualización de precios aplicables a todas las tablas de cobros aplicables por servicios municipales.
   - ✓ Evaluación de roles de acceso y privilegios por usuario autorizados para realizar cobros y gestiones relacionadas con ingresos de la "Municipalidad de La Cruz".
   - ✓ Evaluación de todos los resultados generados por los reportes computacionales generados por el sistema computacional instalado en la Municipalidad de La Cruz, relacionados con ingresos para determinar la confiabilidad e integridad de la información suministrada a loscontribuyentes.

d) Evaluar la seguridad informática aplicada a la protección y uso de los datos e informaciónmunicipal.

e) Evaluar el cumplimiento y ejecución de las recomendaciones y advertencias emitidas por laAuditoria Interna.

La auditoría se efectuó de conformidad con el "Manual de Normas Generales de Auditoría para el Sector Público", promulgado mediante la Resolución del Despacho de la Contralora General, No. R-CO-064-2014, publicada en La Gaceta N.° 184 del 25 de setiembre de 2014.

1.6. Limitaciones para llevar a cabo el objeto de estudio.

Algunos documentos, registros y otros soportes solicitados al Departamento de Tecnologías de Información y Comunicación, no fueron recibidos de forma oportuna y completa.

1.7 Comunicación preliminar de los resultados del estudio.

La comunicación preliminar de los principales resultados, conclusiones y recomendaciones producto del análisis, se efectuó mediante conferencia el día 02 de diciembre de 2021, con la presencia de la Sra. Socorro Díaz Chaves-Presidente del Concejo Municipal-, Licda. Rosa Obregón Álvarez-Directora Administrativa- como representante del Alcalde Municipal y el Ing. Eladio Bonilla Morales-Encargado del Departamento de TIC-.

Asimismo, al comunicar el informe preliminar del estudio, no se realizaron observaciones y hubo conformidad con las conclusiones y recomendaciones del estudio.

1.8. Generalidades acerca del tema objeto de estudio.

El gobierno corporativo y la gestión de las tecnologías de información le permite a una organización el cumplimiento de sus objetivos institucionales y la adecuada toma de decisiones, mediante el aseguramiento razonable de la confiabilidad, integridad y disponibilidad de la información que respalda sus funciones sustantivas, de ahí que los sistemas de información al tener áreas comunes de control y procedimientos relacionados pueden afectar el ambiente del procesamiento de la información. Por consiguiente, estos controles son de interés dentro del proceso de la auditoría, debido a que contribuyen a la confiabilidad que se puede depositar en los sistemas que procesan transacciones importantes y que podrían atenuar riesgos específicos identificados, tanto en el ámbito de controles generales del computador como en los controles de aplicación que procesan información significativa para la generación de los estados financieros, por lo que se aplicaron algunos procedimientos en el Área de Tecnología de Información.

La evaluación la realizamos basados en el manual de "Normas Técnicas para la Gestión y el Control de lasTecnologías 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 antesala de la cuarta revolución industrial inteligente.

Las técnicas utilizadas para realizar el estudio consistieron en sesiones de entrevistas, análisis de documentos, observación directa y la aplicación de los programas de auditoría desarrollados, por medio delcumplimiento de las normativas y leyes gubernamentales en conjunto con marcos de trabajo internacionales. Se solicitaron a los funcionarios entrevistados las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

Cabe indicar, que la auditoría se ejecutó en cumplimiento de las actividades de planificación contenidas en el Plan Anual de Trabajo de la Auditoría Interna para el ejercicio 2021.

1.9. Metodología aplicada.

La estrategia planteada para el desarrollo del presente estudio consideró la aplicación por parte de la Auditoría Interna, de una seria de guías que incorporan los criterios de evaluación y la recopilación de los documentos de respaldo.

El propósito de esa guía es determinar las principales áreas críticas y debilidades en la gestión llevada a cabo por el Departamento de Tecnologías de Información y Comunicación de la Municipalidad de La Cruz con base en la normativa vigente atinente a sus procesos.

Los procedimientos de auditoría ejecutados consideraron el análisis de la información suministrada en entrevistas y consultas realizadas a los funcionarios de la Municipalidad de La Cruz.

La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público (NGASP), promulgadas mediante la resolución del Despacho de la Contralora General, Nro. R-DC-64- 2014, el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente establecido.

1.10. Definiciones.

Los principales conceptos utilizados en la auditoría realizada se detallan a continuación:

Tabla No.1.

Conceptos utilizados en la auditoría.

Concepto	Definición
Funcionalidad	El sistema de información satisface los requerimientos funcionales establecidos por las partes interesadas, las cuales reflejan las necesidades y expectativas de laorganización.
Plan de contingencia informático	Plan que permite al departamento de tecnologías de información, responder a incidentes e interrupciones de servicios para la operación continua de los procesos críticos para el negocio y de los servicios de tecnologías de información.
Procesos críticos	Son aquellos procesos que permiten que un negocio siga en funcionamiento.
Suficiencia	El sistema de información satisface los requerimientos de negocio establecidos por las partes interesadas, las cuales reflejan las necesidades y expectativas de la organización.

Fuente: Contraloría General de la República.

1.11. Siglas.

A continuación, se indica el detalle de las siglas utilizadas en este informe:

Tabla Nro. 2.

Detalle de siglas usadas en el informe.

SIGLA	SIGNIFICADO
CGR	Contraloría General de la República
NTGCTI	Normas Técnicas para la Gestión y Control de las Tecnologías de Información
LCA	Ley de Contratación Administrativa
RLCA	Reglamento a la Ley de Contratación Administrativa
LCI	Ley No. 8292 Ley de Control Interno
RABS	Reglamento de Adquisición de Bienes y Servicios
SCI	Sistema de Control Interno
SEVRI	Sistema Específico de Valoración del Riesgo Institucional
TIC	Tecnologías de Información y Comunicación
PETIC	Plan Estratégico de Tecnología de Información y Comunicaciones

Fuente propia.

2. RESULTADOS DEL ESTUDIO.

Evaluar el cumplimiento y ejecución de las recomendaciones emitidas por la Auditoria Interna entreel segundo semestre del año 2015 y diciembre del año 2020.

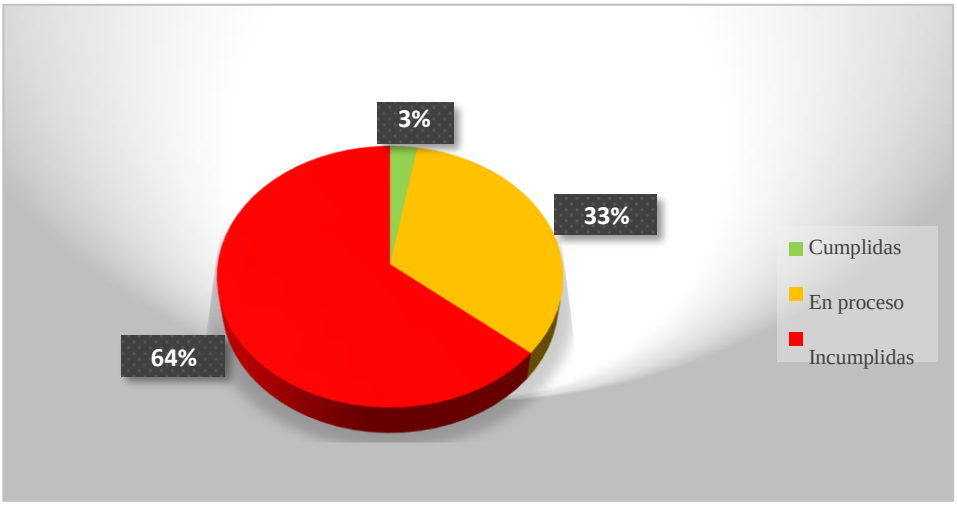
2.1. Cumplimiento de las recomendaciones de informes anteriores de la Unidad de Auditoria Interna.

De acuerdo con el análisis realizado, sobre el seguimiento de las recomendaciones emitidas por la Unidad de la Auditoría Interna de la Municipalidad de La Cruz, mediante el documento UAI-TIC-011-2016, se logró determinar, que de las de las 36 recomendaciones emitidas en ese informe, únicamente se encuentran cumplidas un 3%, el 33% se encuentran en proceso o parcialmente cumplidas y el 64% incumplidas cuatro años después de su emisión.

En el siguiente gráfico, de observa con detalle lo antes mencionado sobre el estado de las recomendaciones emitidas por la Unidad de la Auditoría Interna de la Municipalidad de La Cruz, mediante el documento UAI-TIC- 011-2016:

Gráfico No. 1.

Grado de cumplimiento de las recomendaciones emitidas en el documento UAI-TIC- 011-2016.



Fuente: Elaboración propia a partir de los papeles de trabajo.

En el anexo nro.1, se presenta la información comparativa de las estadísticas del estado de las recomendaciones emitidas en informe de control interno del año 2016.

Es importante mencionar que, para determinar el estado de las recomendaciones emitidas debe de entenderse lo siguiente:

- Incumplidas: corresponde a la implementación o cambio que no ha sido llevado a cabo,
- En Proceso o Parcialmente cumplidas: si la recomendación cuenta con algún grado de avance en su implementación, pero no ha sido totalmente implementada,
- Cumplida: la recomendación ha sido totalmente implementada y cuenta con evidencia que soportadicha implementación.

La mayoría de las recomendaciones en proceso corresponde al cambio al sistema DECSIS, no obstante, la mejora en temas sensibles tales como: accesos físicos, mejoras en la seguridad física, implementación de planes de continuidad, entre otras, continúan sin una atención oportuna.

Aunado a ello, los procesos de planificación estratégica, gestión de proyectos, implementación de un marco de gestión de tecnología, no han sido implementados, lo cual, coloca a la Municipalidad en un claro riesgo de obtener servicios de tecnología inoportunos, ineficientes y a un alto costo.

La no atención de las recomendaciones es una clara violación a los criterios de control que deben ser observados como parte de la gestión institucional de las TIC, por parte del jerarca y los titulares subordinados, como responsables de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292, la cual, establece en lo que nos ocupa lo siguiente, el Artículo 12 Inciso c):

> ¨…c) Analizar e implantar, de inmediato las observaciones, recomendaciones y disposiciones formuladas por la auditoría Interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan. ¨

Por otra parte, en artículo No. 17 inciso d) serán deberes del jerarca y los titulares subordinados los siguientes:

> ¨…d) Que sean implantados los resultados de las evaluaciones periódicas que realiza la Auditoría Interna.”

De la misma manera, las Normas de Control Interno para el Sector Público, establecen en su norma 6.1 sobre seguimiento establece que, como parte del Sistema de Control interno, el jerarca y los titulares subordinados, deben diseñar, adoptar, evaluar y perfeccionar actividades permanentes y periódicas para asegurar que las medidas producto de los hallazgos de auditoría, se atiendan de manera efectiva y con prontitud.

Adicionalmente contraviene lo establecido en el NTGCTI, en su numeral 5.2 “Seguimiento y evaluación del control interno en TI” al no establecer y mantener el sistema de control interno asociado a la gestión de TIC, evaluando su efectividad y cumplimiento de las medidas correctivas implementadas.

Evaluar los proyectos de TICS que se han realizado entre el segundo semestre del año 2015 y diciembre del año 2020; proyectos que tuvieron el fin de transformar o mejorar los procesos mecánicos en automatizados, contemplando como parámetros los principios de eficacia y eficiencia.

2.2. Evaluación de las políticas y procedimientos.

En la actualidad no se han implementado políticas ni se cuenta con instrumentos de gestión a nivel de procesos y procedimientos que incorpore una metodología para la gestión de proyectos, que permita tal y como lo establecen las NTGCTI en su numeral 1.5 Gestión de Proyectos "La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos", una adecuada gestión de proyectos.

Por lo que fuera de los requerimientos básicos realizados en las contrataciones, no se cuenta con un control real para gestionar los proyectos internos y externos, únicamente hay un cumplimiento de lo establecido en la Ley de Contratación Administrativa, sin la debida inclusión de las definiciones de requerimientos de términos de calidad y aceptación de los productos recibidos.

Algunos aspectos que se deben destacar:

1. El encargado de toda adquisición tecnológica es el Departamento de TIC, sin embargo, el responsable del proceso de análisis de las ofertas y recomendaciones para los procesos de adquisición es el Departamento de Proveeduría.

2. El análisis de contratación como criterio técnico para el departamento de Proveeduría está definido en función de precio, calidad, experiencia, desarrollo tecnológico, estándares y capacitación. No obstante, en el criterio técnico y en la recomendación final de las adquisiciones tecnológicas es importante la intervención del encargado de TIC.

El proceso de contratación administrativa sigue el siguiente flujo:

a. Se identifica alguna necesidad por parte del Departamento de TIC.

b. Se realiza un análisis de la factibilidad de la solicitud de manera interna en el Departamento de TIC, de ser aprobada la solicitud se traslada al departamento de proveeduría.

c. Proveeduría se encarga de realizar la creación de los documentos, la publicación de la solicitud a los interesados; es normal que se invite a una serie de proveedores a participar en una licitación abreviada.

d. Posterior a la aplicación por parte de los participantes en la licitación se realiza el estudio de cumplimiento de las propuestas por parte del equipo de TIC, donde se determina si el participante cumple o no los requerimientos establecidos.

e. La Proveeduría procede a realizar la adjudicación y la alcaldía realiza la aprobación final y adjudicación formal al proveedor.

f. Los pagos son realizados según las condiciones establecidas en el pliego cartelario, previa autorización del Departamento de TIC y la gestión ante la Alcaldía.

El proceso establece la responsabilidad de TIC, para la definición de los bienes y servicios a recibir, no obstante, las NTGCTI, en su numeral 3.4 "Contratación de terceros para la implementación y mantenimiento de software e infraestructura", inciso "d" requiere del establecimiento de un procedimientoo guía para la definición de los "términos de referencia", que incluya entre otras especificaciones, requisitos o condiciones requeridas o aplicables. Dicho "procedimiento o guía" no ha sido definido, con lo cual, no existe un adecuado control sobre los bienes y servicios adquiridos por la Unidad de Tecnología y no hay certeza sobre la calidad, el cumplimiento de los criterios, términos y aceptación de lo contratado.

2.3. Sobre las contrataciones realizadas.

Durante el periodo de estudio, se realizó un análisis sobre una muestra de 17 procedimientos de contrataciones, de las cuales, 16 eran contrataciones directas y 1 licitación abreviada. En la revisión se identificó los siguientes hallazgos:

- ✓ En la totalidad de los casos el Departamento de Tecnología de la Información y Comunicaciones es identificado como solicitante de las contrataciones, sin señalar la oficina final receptora.

- ✓ Las compras no se encuentran contempladas en el Programa de Adquisiciones o Plan de Compras Anual, que responda a una necesidad justificada.

- ✓ No se observó en la decisión inicial, que se hiciera referencia a los estudios legales y técnicos en los que se acredita que, en el caso concreto, se está ante un supuesto de prescindencia de los procedimientos ordinarios.

- ✓ En la totalidad de los casos la unidad interesada preparó y remitió a la Proveeduría, una solicitud de Bienes o Servicios, en la que se indicaron las características y condiciones de los bienes o servicios por contratar, no obstante no hay un procedimiento o guía para la definición de los "términos de referencia" que incluyan las especificaciones y requisitos o condiciones requeridos o

aplicables, así como, para la evaluación de ofertas que considere aspectos técnicos adicionales al costo, experiencia y tiempo de entrega.

La falta de definición de un marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica produce que las adquisiciones respondan a necesidades no controladas o que satisfagan las necesidades futuras de TIC, contrario a las NTGCTI en el numeral 3.1 "Consideraciones generales de la implementación de TI".

2.4. Gestión de proyectos.

La Municipalidad no ha establecido una metodología para la gestión de proyectos ni se cuenta con un comité de TIC que apoye la toma de decisiones y defina las estrategias para garantizar el control de calidad de los servicios recibidos.

Debido a esto, no hay una determinación de los causantes de los fallos o una identificación clara de responsabilidades en los servicios que son brindados por terceros a la entidad.

Esta situación es un incumplimiento a lo que indican las NTGCTI en su numeral 1.5 Gestión de Proyectos:

> "La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos".

Como consecuencia, no hay un control adecuado de la gestión de proyectos ya sean internos o externos, lo que a su vez ocasiona que la administración vea limitado él logró de sus objetivos, la satisfacción de los requerimientos y se cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.

2.5. Licenciamientos.

En la Municipalidad de La Cruz, se cuenta con el "Reglamento para el uso de las tecnologías de Información. Dicho reglamento fue publicado en La Gaceta del 12 de Julio del 2021.

Ese reglamento indica en el artículo nro. 4 incisos A, C, E, F y S los deberes y atribuciones del departamento de TI. También, establece como una de sus funciones la gestión de aplicativos.

A pesar de ello, no se logró, obtener evidencia de un inventario detallado de las licencias, sus ubicaciones y a quienes están asignadas.

Asimismo, no se logró observar un inventario manual o automatizado detallado de equipos de cómputo, donde se especifique el nombre del funcionario, las características del equipo en términos de hardware.

Estas debilidades, son el reflejo de incumplimiento de las NTGCTI en su numeral 4.2 Administración y operación de la plataforma tecnológica en su inciso d "Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas".

Lo expuesto, afecta el control que debe ejercer el departamento de TIC sobre los aplicativos existentes y sus usos en la Municipalidad de la Cruz.

Evaluar la gestión respecto a los criterios emitidos sobre la protección de los equipos de cómputo en los lugares en que se ubican, incluyendo la seguridad física y ambiental, así como, la comodidad para las personas usuarias finales.

2.6. Implementación de un marco de seguridad de la información.

En el "Reglamento para el uso de los recursos tecnológicos de información y comunicación", no se contemplan puntos críticos de la seguridad informática, en donde se cubran puntos tales como: el acceso físico al centro de datos, métodos de protección interno de sistemas tales como antivirus, respaldos y uso de los equipos de cómputo.

Aunado a lo anterior, no se realizan revisiones periódicas en donde se determine el nivel de cumplimiento de las medidas de seguridad en términos de hardware y software.

Tampoco, se realizan evaluaciones periódicas en donde se actualice y monitoree el marco de seguridad ni se cuenta con documentación en donde se determinen los responsables a cargo de la implementación del marco de seguridad de la información, lo que evidencia la inexistencia de un marco de seguridad de la información.

Lo anterior, contraviene lo establecido en las NTGCTI en su numeral 1.4 "Gestión de la Seguridad de la Información" que permita garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

2.7. Compromiso del personal con la seguridad de la información.

En la Municipalidad de La Cruz, se carece de normativa que defina las acciones de seguridad y capacidades que poseen los usuarios de la entidad.

Tampoco se cuentan con acuerdos de confidencialidad ni con medios para vigilar el cumplimiento de las responsabilidades.

El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TIC, tal y como lo establece la NTGCTI en su numeral 1.4.2 "Compromiso del personal con la seguridad de la información" que establece "El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI".

Debido a lo anterior, existe una probabilidad de riesgo sobre el uso inadecuado de los recursos de TIC.

2.8. Seguridad física y ambiental del cuarto de cómputo o servidores.

Se observaron algunas debilidades en el cuarto de cómputo o sala de servidores:

a) Únicamente cuenta con una puerta de doble llavín tradicional.

b) El llavín principal se encuentra dañado, por lo que la puerta se mantiene abierta, esto permite que el ingreso no se encuentre controlado y sea propenso a accesos indebidos

c) No se ha implementado un control o bitácora, que permita identificar los accesos al centro de datos.

d) El centro de datos carece de sensores de incendios, extintores y sensores de inundación.

e) No existen cámaras que permitan identificar a las personas cuando entran al cuarto de cómputo o servidores y la hora en que se acceso.

El "Reglamento para el uso de los recursos tecnológicos de información y comunicación para la Municipalidad de la Cruz", no especifica la restricción de acceso al centro de datos salvo las excepciones autorizadas por el departamento de TIC.

Lo expuesto son debilidades en la aplicación de lo que se establece la NTGCTI en su numeral 1.4.3 “Seguridad física y ambiental” que indica los siguiente “La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos”.

La falta de controles para el ambiente físico expone al centro de datos y su contenido a niveles de riesgos altos de perdida de información.

2.9. Control de acceso al sistema DECSIS y a carpetas compartidas.

Para el acceso al sistema DECSIS; se cuenta con roles de acceso claramente establecidos, que permite el manejo de las opciones del sistema. Las bases de datos son de acceso restringido al personal de TIC.

La solicitud de acceso a la información es realizada por el encargado del área ya sea por medio de correo electrónico o de manera escrita con la boleta de ingreso o cambio de permisos que se les proveen a usuarios determinados.

El sistema DECSIS cuenta con bitácoras de acceso, no obstante, a nivel de base de datos que es lo más sensible, no hay control de accesos manuales y limitados al personal de TIC.

El no establecimiento de medidas de control de accesos a nivel de base de datos contradice lo establecido en la NTGCTI en su numeral 1.4.5 “Control de Accesos” que establece la protección de la información de accesos no autorizados, por medio del establecimiento de un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación. Lo cual puede poner en riesgo la seguridad e integridad de la información.

2.10. Parámetros de contraseña.

En relación con este tema, el estudio permitió evidenciar algunas debilidades importantes, las cuales, se detallan a continuación:

a) Los parámetros de contraseñas no cumplen con los requerimientos de seguridad.

b) No se observó norma que establezca los parámetros necesarios para el establecimiento de claves de seguridad adecuadas.

c) No hay un control de bloqueo debido a la cantidad de fallos en el registro de las claves de acceso.

d) El reglamento vigente, no contempla aspectos relacionados al uso de contraseñas y/o bloqueos de seguridad, por lo que, los usuarios permanecen con las mismas contraseñas todo el tiempo que trabajan o están en la Municipalidad.

Esas debilidades, evidencian la falta de cumplimiento de las NTGCTI en su numeral 1.4.5 "Control de Acceso" en su numeral f:

> "…Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares".

Esto genera un riesgo ante la previsibilidad de los mecanismos de acceso, debido a la falta de actualización periódica y asignación de responsabilidades inadecuada a los usuarios municipales.

Evaluar la gestión en cuanto a planificación operativa, control interno y gestión de riesgos generales y los asociados a las operaciones y comunicaciones.

2.11. Gestión de riesgos.

Sobre la gestión de riesgos, se determinó que, se carece de un proceso para la identificación y gestión de riesgos de tecnologías de información, con lo cual, se expone a la materialización de vulnerabilidades de su plataforma debido a la falta de controles y monitoreo de los riesgos.

La no identificación de riesgo tecnológico contradice lo establecido en las NTGCTI en su numeral 1.3 "Gestión de riesgos" que establece que la organización debe responder adecuadamente a las amenazas quepuedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistemaespecífico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.

Adicionalmente, la inadecuada gestión de riesgos coloca la municipalidad en contraposición a lo establecido por la CGR en el oficio D-3-2005-CO-DFOE "Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)".

Todo esto, ocasiona que no se puede responder adecuadamente a las amenazas que puedan afectar la gestión de las TIC, si los mismos no han sido identificados y valorados,

con lo cual, se expone a que sus operaciones se vean afectadas de forma material y no tener una respuesta oportuna para minimizar el riesgo.

2.12. Planificación de las tecnologías de información y comunicación.

El Gobierno Corporativo Municipal, no ha definido un Plan Estratégico en Tecnologías de Información y Comunicación a mediano y largo plazo, que pueda orientar los esfuerzos relacionados con la función de apoyo de las TIC hacia el resto de los procesos sustantivos de la organización, con lo cual, no se puede identificar si sus objetivos se encuentran alineados al cumplimiento de los objetivos institucionales.

Más bien, se trabaja a nivel de Plan Operativo Anual, donde se establecen los objetivos, misión y visión junto al Plan de Desarrollo Municipal, no obstante, dicho plan no establece los requerimientos futuros y un horizonte a largo plazo que dirija la función de TI a satisfacer las necesidades de la organización.

Esta carencia, impide que se puedan medir, identificar y evaluar el logro del departamento de TIC; así como, su capacidad para responder de forma anticipada a las necesidades futuras de la Municipalidad y alineadas al Plan Estratégico Municipal y, además, limita el aporte que las TIC brindan al cumplimiento de los objetivos estratégicos institucionales, la maximización de los beneficios, el uso responsable de los recursos, la administración de los riesgos y la entrega de valor.

Lo expuesto es por inobservancia a las NTGCTI en su numeral, 1.1 “Marco estratégico de TI” y 2.1 “Planificación de las tecnologías de información” que permitan que TI apoye el cumplimiento de la misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

2.13. Infraestructura tecnológica.

La implementación del sistema DECSIS, implicó un cambio en algunos elementos de la plataforma tecnológica, no obstante, se identifica un rezago en la determinación clara de cuál o cuáles, son las nuevas tecnologías aplicables al departamento de TIC y cuál es el rumbo que debe tomar TIC para satisfacer las necesidades de la organización.

Además, existe un inadecuado control de los procesos realizados por el área de Bodegas que están ubicados fuera de las instalaciones municipales y no vinculados al sistema DECSIS.

El Departamento de TIC, en cierta medida es gestionado de forma reactiva y no proactiva a las necesidades de la organización, lo cual, impide aunado a limitaciones presupuestarias, dar una respuesta efectiva ante nuevas necesidades de infraestructura.

La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como, de la tendencia de las TIC para que, conforme a ello, optimice el uso de su infraestructura tecnológica, documente y respalde sus procesos, manteniendo el equilibrio que debe existir entre sus requerimientos, la dinámica y la evolución de las TIC.

La dinámica actual de TIC, impide que la organización cumpla con lo establecido en las NTGCTI en su numeral 2.3 de "Infraestructura Tecnológica".

2.14. Cumplimiento de obligaciones relacionadas con la gestión de TI.

La documentación de políticas y procedimientos relacionados con TIC, al momento de la auditoria, no se encuentran debidamente aprobadas por la Administración Superior, por lo que, solamente se puede tomar como un documento referencia de uso interno del área de TIC.

Por su parte, el Reglamento para el uso de los recursos tecnológicos de información y comunicación para la Municipalidad de la Cruz, es de reciente aprobación. Sin embargo, este presenta limitaciones en cuanto a materia de seguridad y gestión de TIC.

La administración superior, debe identificar y velar por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TIC con el propósito de evitar posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza.

La carencia de políticas, herramientas o instrumentos de gestión y lineamientos, contradice lo establecido en las NTGCTI en su numeral 1. 7 "Cumplimiento de obligaciones relacionadas con la gestión de TI" que indica:

> "La organización debe identificar y velar por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TI con el propósito de evitar posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza."

También, el numeral 5.1 "Seguimiento de los procesos de TI" que establece:

> "La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los

mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso."

Analizar las evidencias y respaldos de gestión asociadas a la seguridad de la información municipal y al compromiso del personal con la seguridad de la información contemplando como mínimo las políticas de uso, política de confidencialidad y privacidad, propiedad intelectual y derechos o licencias de uso.

2.15. Proceso de respaldo asociado a la seguridad de la información.

La institución no ha establecido un sistema de gestión que les permita establecer, implementar, operar, monitorear y revisar, así como, mantener y mejorar la seguridad de la información.

El proceso actual de respaldos de servidores, se realiza de manera diaria, de forma automática. Adicional, se realiza un respaldo semanal los sábados a las 5:00 a.m. Estos respaldos, se almacenan en dispositivos de almacenamiento externo (discos duros), ubicados en la propia Municipalidad.

Sin embargo, no se observó evidencia de que se realicen diariamente respaldos de forma rutinaria, de los equipos de cada usuario, salvo que medie una petición del usuario. Esto, podría exponer a la municipalidad a un riesgo de pérdida y recuperación de la información, incluso al riesgo inminente de mantener los respaldos de los discos duros externos dentro de la propia municipalidad, hace que la institución esté expuesta a perder sus copias de seguridad.

El no resguardo de la información de forma adecuada coloca a la municipalidad ante un riesgo de pérdida de información, que viola lo establecido en el numeral 4.2 "Administración y operación de la plataforma tecnológica" de las NTGCTI que indica en su inciso "h" lo siguiente "Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración".

2.16. Continuidad de los servicios de TI.

No se evidencia un proceso de gestión basado en una normativa de continuidad de negocios de los servicios de TIC.

Asimismo, no se ha definido un plan de continuidad de las operaciones en apoyo a la estrategia institucional por parte del departamento de TIC.

No obstante, se tienen claras las acciones en caso de desastre, pero es necesario que, se documenten y pongan en práctica las acciones preventivas y correctivas necesarias, que

permitan incluso evitar la dependencia hacia el personal de TIC, salvaguarda de la vida y de la información administrada por la Municipalidad.

Aunado a ello, no se tienen claras las acciones donde se indique la criticidad de la información de los sistemas en casos de desastres o riesgos.

El no tener definido un proceso de continuidad del negocio, coloca a la municipalidad ante un riesgo de negocio en marcha, que viola lo establecido en el numeral 1.4.7 "Continuidad de los servicios de TI" del NTGCTI que indica lo siguiente "La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TIC según su criticidad."

Analizar la gestión relativa al seguimiento de las contrataciones administrativas de tecnologías de información y comunicaciones, incluyendo la administración de la plataforma tecnológica y de los recursos financieros asignados.

2.17. Administración de servicios prestados por terceros.

La entidad no cuenta con ningún tipo de procedimiento o control de uso interno que, determine la adecuación de los servicios brindados por terceros, salvo lo establecido en la Ley y Reglamento de Contratación Administrativa.

El Departamento de TIC, no realiza una evaluación del servicio brindado por terceros, ya sea, en la gestión e implementación de sistemas o en la adquisición de equipo de cómputo.

Tampoco, hay una gestión de proyectos ni de proveedores que permita evaluar el desempeño de los mismos y lograr establecer las medidas necesarias para la recepción de servicios o productos a tiempo, con la calidad adecuada y a un costo razonable.

Asimismo, no se cuenta con herramientas de control que permitan monitorear su implementación, para prever el alcance y las limitaciones en la atención y cumplimiento de los requerimientos que permitan en el futuro poder satisfacer todas las necesidades del negocio, lo cual genera un incumplimiento a lo establecido en el numeral 3.4 "Contratación de terceros para la implementación y mantenimiento de software e infraestructura" de las NTGCTI.

2.18. Definición y administración de acuerdos de servicio entre el proveedor y la municipalidad para atender los eventos críticos durante el desarrollo y el período de garantía.

Al no existir un proceso para la gestión de Servicios de Tecnología, ni una definición formal y aprobada de un catálogo de servicios, impide desarrollar los acuerdos de nivel de servicio

Así pues, al no contar con acuerdos de niveles de servicio e indicadores de desempeño, limita la capacidad de realizar un monitoreo sobre la calidad del servicio que se entrega, lo que impide evaluar si la municipalidad está recibiendo el servicio requerido para la consecución de los objetivos institucionales.

Por lo que no se puede asegurar el cumplimiento de tres pilares fundamentales:

a) Entrega del servicio a tiempo, que cumplan con las agendas contractuales establecidas.

b) Que se entregue el servicio con calidad, que cumpla con las expectativas de los usuarios finales ylos requisitos acordados.

c) Que se entregue el servicio sin costos adicionales, que se ajuste al presupuesto definido para ello.

Esto afecta los niveles o acuerdos de servicio que definen características y cualidades de los servicios ofrecidos por el proveedor, tales como: tiempo de respuesta, horarios de atención, criticidad de los servicios,al no estar dichos elementos establecidos de forma clara y bien documentada, se coloca a la Municipalidadante un riesgo de atención que puede afectar su operatividad normal, afectando el servicio brindado a los usuarios municipales.

Lo expuesto, genera un incumplimiento a lo establecido en el numeral 3.4 “Contratación de terceros para la implementación y mantenimiento de software e infraestructura” y el numeral 4.1 “Definición y administración de acuerdos de servicio” de las NTGCTI.

Evaluar la depuración de las bases de datos y la integración de la red municipal, así como, el mantenimiento y la continuidad de servicio de los sistemas informáticos.

2.19. Administración y operación de la plataforma tecnológica.

El “Reglamento para el Uso de las Tecnologías de Información de la Municipalidad de la Cruz” – en el Capítulo IV - Del Software en los artículos del 11° al 14° se definen las restricciones que deben cumplirse por parte del usuario y el cumplimiento en términos de derechos de autor de los productos licenciados.

No obstante, no se cuenta con una definición puntual de las tareas y responsabilidades requeridas para poder mantener el óptimo funcionamiento de la plataforma tecnológica.

El mismo reglamento, indica que no se puede instalar software no licenciado, pero al no haber un inventario actualizado, documentado y referenciado de que personal los tiene asignado, se imposibilita la verificación razonable de esta situación.

Asimismo, al no contar con un procedimiento formalmente establecido que permita la administración de la configuración de los equipos que conforman la plataforma tecnológica, según los estándares internacionales y mejores prácticas de la industria tecnológica, hace que las bitácoras de registro de eventos no se encuentren configuradas correctamente, por lo que no se puede obtener información que permita verificar fallas o problemas en los servicios. Las bitácoras al ser cíclicas, cada 3 horas, la información va cayendo encima y al no ser histórico el respaldo en el disco duro y que dure mínimo un mes, se cuenta solo con la información de respaldo de las últimas 3 horas.

Lo anterior, genera un incumplimiento de las NTGCTI en su numeral 4.2 Administración y operación de la plataforma tecnológica en su inciso "d" "Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas" y del numeral 4.3 Administración de los datos" de las NTGCTI.

2.20. Administración de datos.

En las bitácoras de los sistemas operativos de los servidores, están desactivados los registros de actividades en la herramienta SQL Server.

Con esta debilidad, no se puede asegurar que los datos que son procesados en los sistemas, corresponden a transacciones válidasy debidamente autorizadas, que son procesados en forma completa, exacta, oportuna, transmitidos, almacenados y desechados en forma íntegra y segura. Adicionalmente, dificulta establecer las responsabilidades de las acciones llevadas a cabo en los sistemas de información.

Lo expuesto, es una inobservancia a lo que establecen los numerales 4.2 "Administración y operación de la plataforma tecnológica", 4.3 Administración de los datos" y 1.4.7 "Continuidad de los servicios de TI" de las NTGCTI.

2.21. Proceso de manejo de incidentes.

El manejo y atención de incidentes se realiza mediante correo electrónico. De manera interna, el departamento de TIC, maneja una herramienta que le permite llevar un registro del servicio que brinda a los usuarios, con el cual, se pueden realizar consultas a tiquetes anteriores, lo que permite minimizar costo y recurrencia, pero no cuenta con un esquema de clasificación y priorización de los incidentes.

No obstante, no hay un monitoreo o análisis de tendencias que permita identificar problemas y brindar una solución de forma proactiva a los incidentes recurrentes, debido a la ausencia de la documentación formal de un proceso de gestión de incidentes debidamente aprobado y formalizado, que permitan medir si los incidentes o problemas se analizan y resuelven de manera oportuna.

Es por ello, que no se cumple con lo que se establece las NTGCTI en su numeral 4.5 "Manejo de incidentes" que específica lo siguiente "La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TIC. La ausencia de un esquema de clasificación y priorización de los incidentes puede afectar darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario".

Evaluar los controles de acceso a los sistemas en general y el acceso de los servidores municipales a los distintos servicios que ofrece la red de Internet, así como, los archivos que los servidores municipales almacenan en el equipo de cómputo propiedad de la Municipalidad.

2.22. Seguridad en implementación y mantenimiento de software e infraestructura tecnológica.

El "Reglamento para el uso de los recursos tecnológicos de información y comunicación para la Municipalidad de la Cruz", establece requerimientos de seguridad enfocados al hardware e infraestructura mediante el uso de alimentación ininterrumpida de energía en todos los equipos y respaldos de la información.

No obstante, no se ha definido un "Plan de Mantenimiento Preventivo a Equipos de Información", por lo cual, no existe un control de cambios que respalde cada modificación o actualización de la infraestructura tecnológica y permita identificar obsolescencia tecnológica de los equipos.

La falta de mantenimiento de software e infraestructura tecnológica pueden ser causantes de daños o pérdida de información relevante o crítica para la entidad.

El inadecuado control del proceso de mantenimiento preventivo, genera un incumplimiento de las NTGCTI en su numeral 1.4 “Gestión de la Seguridad de la Información” que permita garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizadas, daño o pérdida u otros factores disfuncionales. Además, del numeral 4.2 “Administración y operación de la plataforma tecnológica” que indica “La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas”.

2.23. Segregación de funciones.

Las funciones y responsabilidades del Gestor de TIC se encuentran documentados en el perfil del puesto, el cual contempla la configuración y sus responsabilidades. Estas funciones y responsabilidades son diferente a las establecidas para el Técnico de Gestión de TI, encargado principalmente del soporte técnico.

Sin embargo, la falta de bitácoras de acceso, no permite identificar si la segregación de funciones del departamento de TIC, se está cumpliendo, el hecho que sean dos personas en TIC, hace que a pesar de tener claramente definidas las responsabilidades, no se pueda brindar la correcta operación de negocio a nivel de TIC.

El no poder identificar de manera exacta el origen y autorización de transacciones tal y como lo establecen los numerales 4.2 “Administración y operación de la plataforma tecnológica”, 4.3 Administración de los datos” y 1.4 “Gestión de la Seguridad de la Información” de las NTGCTI, puede poner en riesgo la gestión de la plataforma tecnológica.

Evaluar las asesorías emitidas por el departamento de Tecnologías de la Información tendientes a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.

2.24. Atención de requerimientos de los usuarios de TIC.

Como se mencionó en apartados anteriores, el manejo y atención de incidentes, se realiza mediante correo electrónico, no obstante, no se brinda un seguimiento adecuado a sus necesidades, cambios en el sistema, nuevas funcionalidades, ya que, no hay proceso definido para la gestión de cambios en los sistemas de información, que permita identificar, gestionar y cerrar las necesidades de los usuarios, por lo cual, no se pueden priorizar las necesidades de los proyectos de TIC.

Aunado a lo anterior, existe ausencia de una mesa de servicios que permita definir el perfil de usuario y estandarizar el acceso y autorización para los trámites más comunes y que permita priorizar las solicitudes.

Estas debilidades, impiden el cumplimiento de las NTGCTI en su numerales:

> 3.1 "Consideraciones generales de la implementación de TI" establece que se debe garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas y contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.
>
> 4.5 "Manejo de incidentes" que específica 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".

2.25. Seguimiento de los procesos de TIC.

El "Reglamento para el uso de los recursos tecnológicos de información y comunicación para la Municipalidad de la Cruz", es el documento guía que define los responsables y las responsabilidades del personal de la entidad.

No obstante, no se cuenta con una definición puntual de responsabilidades del personal para el seguimiento de los procesos de TIC.

No se ha definido un esquema, política y procedimiento que guie u oriente al departamento de TIC, de forma proactiva, en los seguimientos de los procesos de TIC.

Todo esto, hace que la municipalidad incumpla con las NTGCTI en su numeral 1.1 "Marco estratégico de TI" y 2.1 "Planificación de las tecnologías de información" que permitan que TI apoye el cumplimiento de la misión, visión y objetivos estratégicos institucionales mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes. Es necesario adaptar el reglamento a las particularidades propias de la municipalidad para que apoye los procesos de tecnologías alineados a la planificación institucional.

La inadecuada gestión de proyectos, la ausencia de una planificación estratégica a largo plazo impide una evaluación adecuada de la gestión de TIC, su apoyo o respuesta a los

procesos que debe desarrollar TIC de forma proactiva tal y como lo establece la NTGCTI en su numeral 1.5 Gestión de Proyectos "La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos".

2.26. Evaluación general sobre la madurez del sistema de control interno del departamento de TIC.

El Control Interno, es la estructura donde deben descansar las actividades y operaciones de la Municipalidad y como instrumento de eficiencia, la administración debe regirse por el conjunto de políticas y procedimientos establecidos formalmente en un sistema de control interno robusto, que proporcione una seguridad razonable en el logro de los objetivos y metas institucionales de las diferentes áreas de gestión.

La Ley General de Control Interno, en sus artículos 7, 8, 10 y 12, dicta lo concerniente a la obligatoriedad de disponer de un SCI. Emite el concepto de SCI, la responsabilidad y por último establece los deberes del jerarca y de los titulares subordinados en el SCI. De igual forma en esta Ley en los artículos 13, 14 15, 16 y 17, conceptualiza y enmarca cada uno de los componentes del SCI.

Asimismo, los artículos 9 y 22 incisos b) establecen la facultad y competencias de la Auditoría Interna para la fiscalización del SCI.

De acuerdo, con la herramienta aplicada, se logró determinar que, en el departamento de TIC, alcanzó un puntaje del 22%, situándose en la condición de un sistema "Incipiente", lo que significa que "existe evidencia de que la unidad o departamento ha emprendido esfuerzos aislados para el establecimiento del sistema de control interno; sin embargo, aún no se ha reconocido su importancia. El enfoque general en relación con el control interno es desorganizado.

A continuación, el detalle sobre el análisis de la evaluación efectuada:

Tabla No.3.

Resultados de la evaluación del índice de madurez del SCI.

Criterio	Valoración
ÍNDICE DE MADUREZ DEL SCI	**22**
Ambiente de Control	20
Valoración del Riesgo	20
Actividades de Control	16
Sistemas de Información	27
Seguimiento del SCI	25

Fuente: Aplicación de Herramienta de Evaluación del SCI.

A nivel de avance, se evidencia que el sistema de control interno del departamento es un reflejo del sistema de control interno institucional y se ubica por debajo de los estándares aceptables (mayor al 70%).

En virtud de lo anterior, se requiere que el Departamento de Tecnologías de Información y Comunicación, valore el ambiente de control del departamento, con respecto al compromiso interno y externo, la ética, la motivación del personal y la estructura que impera para el cumplimiento de los objetivos de la entidad, la implementación de un sistema específico de valoración del riesgo institucional (SEVRI), que permita su identificación y la mitigación de los mismos, actividades de control para determinar políticas, procedimientos, técnicas, prácticas y mecanismos que permiten mitigar los riesgos, incluyen aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones y generación de documentación, un sistema de información que ayude al conjunto de actividades realizadas con el fin de controlar, almacenar, y recuperar de modo adecuado la información producida o recibida por el departamento y el seguimiento del sistema de control interno que comprende las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno a lo largo del tiempo.

3. CONCLUSIONES.

Es importante recalcar que, el cumplimiento con las Normas Técnicas para el Control y Gestión de Tecnologías de Información, no es solo responsabilidad del Departamento de TIC, sino más bien, es responsabilidad de la Administración General y el Departamento de TIC dentro de sus funciones deberá apoyar la implementación y mantenimiento de las mismas.

Al carecer la institución de un Plan Estratégico de las Tecnologías de Información y Comunicación, pueden las acciones operativas de TIC, no estar respondiendo a los requerimientos y metas estratégicas definidas por la municipalidad, ya que, no existe un alineamiento entre un Plan Estratégico de TIC y un Plan Estratégico Municipal.

Al no existir un sistema o marco de gestión de la seguridad de la información global que contemple tanto el hardware como el software y en vista que la información que se utiliza en el desarrollo de las actividades de la Municipalidad, es un activo valioso que debe ser protegido desde el momento de su creación, durante su uso y hasta el momento de su destrucción, sin importar el formato en que se encuentre, es que la información debe ser clasificada apropiadamente para reflejar su importancia y confidencialidad para la Municipalidad y asimismo su resguardo.

La ausencia de un marco de trabajo definido para la evaluación de riesgos del departamento de TIC, puede limitar los resultados apropiados en la ejecución de sus actividades, al no contar con una gestión de riesgo de TIC, no se logran identificar todos aquellos eventos, sean amenazas o vulnerabilidades, con impacto potencial sobre las metas o las operaciones de la institución, aspectos de negocio, normativa regulatoria, legal, tecnológica, recursos humanos y operativos.

La presencia de estos riesgos en las actividades ejecutadas por el departamento de TIC, llevan a que una de las medidas a considerar, sea la implementación y seguimiento de un proceso de gestión de riesgos, que permita identificar, valorar y tratar los riesgos con el fin de disminuir el impacto que pueda ocasionar la materialización de los mismos y que con ello no se vea afectado el nivel de servicios ni el cumplimiento de los objetivos institucionales.

En términos generales y de acuerdo con los resultados obtenidos, se determinó que las deficiencias relacionadas con el gobierno de las tecnologías de información de la Municipalidad de La Cruz, limitan el aporte que éstas puedan brindar al cumplimiento de los objetivos estratégicos institucionales, la maximización de los recursos y beneficios, la administración de riesgos y la entrega de valor al Gobierno Corporativo.

Así mismo, la gestión de los sistemas de información no ha permitido, a pesar de los recursos invertidos en contrataciones, contar con un sistema integrado y suficiente que

apoye todos los procesos críticos, aunado a una exposición al riesgo de seguridad de la información, así como dependencia con sus proveedores.

La infraestructura de TIC, presenta debilidades que no permiten garantizar la integridad de la información, aunado a un esquema de seguridad de la información deficiente, lo cual podría generar pérdidas de datos y una incorrecta identificación de los responsables.

La Resolución "N-2-2007-CO-DFOE/ Normas Técnicas para la Gestión y el Control de Tecnologías de Información", fue derogada por la CGR, dando oportunidad a las organizaciones supervisadas el establecimiento de un marco de gestión de tecnología a partir del año 2022, lo cual deja a la Municipalidad de La Cruz en un encrucijada, ya que se requiere la inversión de recursos, tiempo y dinero para una correcta definición de dicho marco normativo, dando inicio a un compromiso del Concejo Municipal y de la Alcaldía para un cumplimiento adecuado de cara a la CGR.

El nuevo marco de gestión de tecnología establece un ciclo de implementación sugerido de tres etapas de priorización, con una duración de implementación en forma consecutiva de un año, seis meses y seis meses respectivamente, para un plazo máximo total de dos años, lo cual obliga a la Municipalidad de La Cruz y al máximo jerarca institucional, como responsable del establecimiento del Gobierno corporativo que apoye y supervise la adecuada implementación de Marco de Gestión de TIC y su gestión, por parte de la instancia competente en materia de TIC.

4. RECOMENDACIONES.

De conformidad con los resultados expuestos, se indican las siguientes recomendaciones, de acuerdo con los artículos 12 y 22 de la Ley General de Control Interno Nº 8292.

Además, es importante recordar que la misma ley de marras establece:

"Artículo 36.- Informes dirigidos a los titulares subordinados.

Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:

a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.

b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.

Artículo 37.- Informes dirigidos al jerarca.

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

Artículo 38.- Planteamiento de conflictos ante la Contraloría General de la República.

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

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

Artículo 39.- Causales de responsabilidad administrativa.

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

4.1. Al Concejo Municipal.

4.1.1. Apoyar a la administración activa en la forma y condiciones que le corresponden conforme a su competencia en las acciones que proponga para el cumplimiento de las recomendaciones giradas por esta Auditoría Interna, con el objetivo de potenciar las oportunidades de mejora en la gestión administrativa municipal, la toma de decisiones, tomando las medidas necesarias para subsanar las inconsistencias señaladas en este informe y garantizar transparencia en la gestión. Ver apartado 2.1 y 2.26.

4.1.2. Analizar, revisar y aprobar las políticas, procedimientos y normativas para el área de TIC remitidas por la Alcaldía al Concejo Municipal. Ver apartado 2.1, 2.2 y 2.26.

4.1.3. Establecer en conjunto con la Alcaldía un marco de gestión de tecnología de información de acuerdo con lo establecido por la CGR, a más tardar a enero 2022. Ver apartado 2.1.

4.2. Al Alcalde.

4.2.1. Establecer un modelo de gestión de tecnologías de información basada en riesgos. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.1, 2.6 y 2.11.

4.2.2. Definir en conjunto con el Gestor de TIC, la planificación estratégica de TIC con un horizonte de 4 años. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.12.

4.2.3. Implementar de manera integral un Plan de Continuidad de Negocio el cual contemple el correcto marco constitutivo con el que se rigen las funciones del área de TIC, sus objetivos y los responsables que participan. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir

del recibido de este informe. Ver apartado 2.16.

4.2.4. Delimitar estrategias para determinar el cumplimiento de los productos o servicios que se brindan a la entidad por parte de proveedores. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.1.

4.2.5. Establecer junto con el Concejo Municipal un marco de gestión de tecnología de información de acuerdo con lo establecido por la CGR. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.1.

4.2.6. Implementar las medidas de seguridad presentes en el documento de Directrices Generales en Tecnologías de Información y Comunicación para la Municipalidad de la Cruz. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.6 y 2.7.

4.2.7. Analizar la creación de un comité de TIC que sea conformado por funcionarios con capacidad y toma de decisiones para la correcta y apropiada aprobación y definición de objetivos del departamento de TIC. Crear el comité de TI. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.2, 2.3, 2.6, 2.7, 2.11, 2.16.

4.3. Al Encargado del Departamento de TIC.

4.3.1. Establecer un control de las recomendaciones para su atención oportuna e informar a la Auditoria Interna de forma trimestral de las medidas implementadas. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.1.

4.3.2. Establecer una serie de criterios técnicos para ser usados en la contratación de bienes y servicios que permita orientar a la Proveeduría Municipal en la definición de la calidad de los productos y servicios, experiencia, cumplimiento de estándares, confidencialidad de la información, acuerdos de niveles de servicio. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.2, 2.3.

4.3.3. Establecer un mecanismo de valoración del SCI, que permita identificar, evaluar, monitorear y actualizar los controles de TIC Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del

recibido de este informe. Ver apartado 2.26.

4.3.4. Alinear los procesos de trabajo a marcos de gestión actualizados, a más tardar 30 julio 2022:

a. Control Objectives for Information and Related Technology (COBIT) version 2019

b. ISO 27001 Information Security Management System (ISMS)

c. ISO 22301 Business Continuity Management.

Ver apartado 2.4, 2.6 y 2.14.

4.3.5. Definir una metodología de gestión de proyectos que oriente la adecuación de la construcción de proyectos, que defina responsables y calidad esperada de los proyectos. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.4.

4.3.6. Revisar y modificar Reglamento para el uso de las tecnologías de información para ajustarlo a las necesidades propias de la Municipalidad en temas de seguridad, con la definición correcta de responsabilidades. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.4 y 2.5.

4.3.7. Establecer un inventario detallado de equipos y licencias identificando responsables, y características de los equipos. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.5, 2.13 y 2.22.

4.3.8. Establecer un Sistema de Gestión de la Seguridad de la Información que definan aspectos de seguridad que deben ser conocidos e implementados en la Municipalidad. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.6 y 2.7.

4.3.9. Establecer el cumplimiento de contraseñas con respecto a las mejores prácticas de la seguridad, tanto a nivel de red como de sistemas. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.6 y 2.10.

Tabla Nro. 4.

Características de las contraseñas.

No.	Política	Valor
i.	Tamaño. Contraseña	**8 caract.**
ii.	Vencimiento	**30-90 Días**
iii	Históricos	**6 o más**
iv	Complejidad	**Activa**
v.	Bloqueo	3 intentos

Fuente: Propia.

4.3.10. Alinear el centro de datos a las mejores prácticas y estándares internacionales tales como TIA-942-2 e ISO/IEC 27002 y COBIT 2019 para la correcta gestión de la seguridad física y ambiental. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.6 y 2.8.

4.3.11. Configurar de manera apropiada las bitácoras de registro de eventos en las herramientas, sistemas operativos y bases de datos en donde se pueda determinar cualquier incidente. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.6, 2.9 y 2.19.

4.3.12. Definir matrices de acceso de todos los funcionarios a los sistemas y servicios brindados por TIC a los Departamentos y solicitar a los jefes respectivos la aprobación de éstas, para garantizar que los accesos estén debidamente asignados. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.6, 2.9, 2.20 y 2.23.

4.3.13. Realizar un análisis y definición del riesgo tecnológico de manera interna que contemple el impacto y la criticidad de los servicios que brinda TIC a lo largo de la entidad, que incluya la identificación de controles y el riesgo residual. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.11.

4.3.14. Definir un plan estratégico de TIC, que defina los objetivos, misión, visión, proyectos, recursos técnicos, humanos y financieros, que incluya un análisis

FODA de TIC para que guíe el quehacer de TIC en los próximos cuatro años. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.12.

4.3.15. Generar una CMDB (Base de Datos de Configuración), que lleve el correcto control de los activos de TIC, esto contempla hardware, software e infraestructura de servicios. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.13, 2.14, 2.22.

4.3.16. Implementar un sistema de mecanismo de alerta temprana contra catástrofes tales como sensores de incendios, inundaciones, sensores de humedad relativa y termómetros (separados de los que poseen los equipos de A/C). Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.8, 2.14.

4.3.17. Realizar la implementación de un procedimiento de revisión de las bitácoras de auditoria en donde se pueda ver toda la actividad y errores en bases de datos y sistemas operativos. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.9, 2.14, 2.19, 2.20.

4.3.18. Desarrollar un sistema de contingencias de TIC, que garantice la continuidad de los servicios críticos gestionados de TIC, a más tardar el 30 de marzo de 2022. Ver apartado 2.16.

4.3.19. Documentar en la contratación quien va a ser el encargado del proyecto de compra o del aplicativo si el cartel lo requiere sea el usuario o dueño del proceso. Ya que la unidad de TIC solo debería encargarse de requerimientos tecnológicos. Elaborar un procedimiento que delimite la responsabilidad de los actores participantes en los proyectos de TIC Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.17 y 2.18.

4.3.20. Establecer un mecanismo de aceptación de los servicios prestados por terceros de parte de los encargados funcionales de los servicios. Elaborar un procedimiento con los requerimientos de aceptación de servicios contratados. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.17.

4.3.21. Realizar análisis mensuales de los incidentes para determinar problemas o incidencias recurrentes y que puedan ser resueltos de forma oportuna. Elaborar un procedimiento para análisis. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido

de este informe. Ver apartado 2.21.

4.3.22. Establecer un mecanismo para la identificación de requerimientos de usuarios, que permita identificar entre otros: objetivo, detalle de requerimientos, elementos afectados, mejora esperada, tiempo estimado, costo estimado, priorización y autorizaciones. Para dar por atendida esta recomendación se establece un plazo de 60 días naturales a partir del recibido de este informe. Ver apartado 2.24.

Estudio elaborado por,

YEHUDIN GERARDO SANCHO ELIZONDO (FIRMA)
Firmado digitalmente por YEHUDIN GERARDO SANCHO ELIZONDO (FIRMA)
Fecha: 2021.12.02 15:40:58 -06'00'

Lic. Yehudin G. Sancho Elizondo.
Gestor Jurídico de Auditoria Interna.

MARIA LUISA OPORTA CENTENO (FIRMA)
Firmado digitalmente por MARIA LUISA OPORTA CENTENO (FIRMA)
Fecha: 2021.12.02 15:31:02 -06'00'

Licda. María Luisa Oporta Centeno.
Auditora de Apoyo.

GLEDYS HARLEY DELGADO CARDENAS (FIRMA)
Firmado digitalmente por GLEDYS HARLEY DELGADO CARDENAS (FIRMA)
Fecha: 2021.12.02 15:45:43 -06'00'

Lic. Gledys H. Delgado Cárdenas.
Auditor Interno.

c. MLC-UAI-EXP-05-2021.

ANEXO NRO 1.

Tabla Nro. 5.

Detalle de Estado de Ejecución de las Recomendaciones.
Informe UAI-TIC- 011-2016.

#	Item	Recomendación	Comentario	Resultado
1	**Marco estratégico de TI**	• Poner en vigencia con aprobación del Consejo Municipal y Alcaldía todo documento de políticas, procedimientos y normativas, para lo cual es recomendable volver a enviar para aprobación los documentos. • Se debe implementar de manera integral un Plan de Continuidad de Negocio el cual contemple el correcto marco constitutivo con el que se rigen las funciones del área de TI, sus objetivos y los responsables que participan. Ver Anexo #1 • El correcto alineamiento a los marcos de trabajo nacionales e internacionales tales como: ✓ Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la CGR. ✓ Normas Generales de Auditoria en el Sector Publico (R-DC-64-2014). ✓ Control Objectives for Information and Related Technology (COBIT) version 5. ✓ ISO 27001 Information Security Management System (ISMS).	Se realizó únicamente el Reglamento para el uso de los recursos tecnológicos de información y comunicación de la municipalidad de la Cruz. Por los demás documentos no se encuentran en borradores. Se esperó por el plazo de 1 año o más la aprobación y publicación del mismo. Sin embargo se pudo trabajar en varios documentos para ir alineando la documentación o llevando un control de versiones	**Parcialmente Cumplida**

#	Item	Recomendación	Comentario	Resultado
		✓ ISO 22301 Business Continuity Management. Esto para el correcto y apropiado funcionamiento de TI en los servicios que brinda a negocio.		
2	**Gestión de la calidad**	• Establecer un listado actualizado de servicios proporcionados por TI a la entidad. • Establecer SLA o acuerdos de nivel de servicio para poder establecer el cumplimiento en los servicios que TI brinda a negocio.	• El listado de servicios actualizado está presente, sin embargo, debería explicarse y cuales son disposiciones para no tener un marco amplio sobre el cual, no se tenga un rango de trabajo o cargas establecidas por el departamento. • No hay SLA o acuerdos de nivel de servicio para dichos servicios.	**Parcialmente Cumplida**
3	**Gestión de riesgos**	Realizar un análisis y gestión del riesgo de manera interna y alinearlo al SEVRI en el momento que finalice la implementación del mismo, el mismo debe contemplar el impacto y la criticidad de los riesgos que posee TI a lo largo de la entidad y los servicios que brinda.	La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
4	**Implementación de un marco de seguridad de la información**	• Contar con una clasificación que contemple el nivel de riesgo que poseen los recursos de TI, no solamente la obsolescencia • Poseer procesos formales en donde se determine el monitoreo y actualización del marco de seguridad global contemplando hardware y software	El departamento de TI solo cuenta con un listado de activos, el encargado indica que no se ha podido trabajar ampliar el documento con detalles de usuarios, depreciación, patrimoniado, etc.	**Incumplida**
5	**Compromiso del personal con la seguridad de la información**	• Dado el caso realizar acuerdos de servicios con proveedores cuando sea requeridos a la hora de realizar las contrataciones administrativas, esto se puede dar como lineamientos a la hora de realizar labores entre la entidad y el proveedor del servicio. • Delimitar estrategias para determinar el cumplimiento de los productos o servicios que se brindan a la entidad por parte de proveedores	El departamento de TI solo cuenta con un proceso no documentado que envían las especificaciones a proveeduría y lanzan un cartel o buscan oferentes para la adquisición. No cuentan con acuerdos ni SLAS/OLAS´S.	**Incumplida**
6	**Seguridad física y ambiental**	• Se deben implementar las medidas de seguridad presentes en el documento de Directrices Generales en Tecnologías de Información y Comunicación para la Municipalidad de la Cruz • Se recomienda alinear el centro de datos a las mejores prácticas y estándares internacionales tales como TIA-942-2 e ISO/IEC 27002 y COBIT 5 para la correcta gestión de la seguridad física y ambiental.	EL departamento continúa con las mismas condiciones de la auditoria pasada. Se cuenta con una puerta de doble llavín tradicional, uno con manecilla y otro no posee, y el llavín principal se encuentra dañada por lo que la puerta se mantiene abierta, consecuencia de que el ingreso sea descontrolado y	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
			propenso a accesos indebidos, solamente el personal de TI tiene llave. No se cuenta con control de accesos biométricos, ni cámaras de seguridad 24/7, y no se cuenta con bitácora de accesos al centro de datos.	
7	**Control de acceso**	• Se recomienda un nuevo análisis o asesoramiento para la correcta implementación de un directorio activo se pueda administrar de una manera centralizada el acceso a datos y sistemas de la entidad. • Se debe determinar documentación que determine quién es el responsable de los equipos en TI, tal como se recomienda en el ISO 22301 y COBIT v5 • Se debe definir como se debe manejar el proceso de los usuarios en la institución y el correcto manejo del ciclo de vida de los mismos. • Se recomienda poseer toda política y servicio que las herramientas posean configuradas de manera idónea para un correcto seguimiento del proceso de auditoria • Estudios del cumplimiento de contraseñas con respecto a las mejores prácticas de la seguridad o Política Valor Tam. Contraseña 8 caract.	No cuenta con un procedimiento para el ciclo de vida completo de cuentas de usuarios. En términos de control de accesos para la impresión se utilizan los equipos RICOH. No obstante no se cuenta con procesos o pistas en donde Auditoria pueda darle seguimiento a TI, se requiere controles, herramientas y mecanismos en donde Auditoria sea capaz de velar por el cumplimiento de las normativas internas y externas además de el correcto funcionamiento con base a mejores prácticas y marcos de trabajo internacionales,	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
		Vencimiento 30-90 Días Históricos 6 o más Complejidad Activa Bloqueo 3 intentos	solamente se cuenta con la capacidad de dar seguimiento a herramientas con bitácoras de auditoria las cuales no en todos los casos se encuentran debidamente configuradas por lo que esto y la documentación realizada por TI son los únicos recursos disponibles para el departamento de Auditoria. No se cuenta con un estudio o análisis que contemple cuales son contraseñas vulnerables para los sistemas de información	
8	**Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica**	• Se recomienda llevar un control de toda modificación o mantenimiento que se realice en los equipos de la entidad tomando en cuenta equipos cliente, servidores e infraestructura de servicios.	EL departamento continúa con las mismas condiciones de la auditoria pasada. No se cuenta con un control y solo se tiene un esquema para identificar la antigüedad y calificar el estado del equipo u otros.	**Incumplida**
9	**Continuidad de los servicios de TI**	• Se recomienda realizar la implementación de un plan de continuidad de negocio alineándose a el ISO 22301, COBIT v5 y el correcto cumplimiento de la Normas técnicas para la gestión y el control de las Tecnologías	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con plan de continuidad lo que se	**Parcialmente Cumplida**

#	Item	Recomendación	Comentario	Resultado
		de Información (N-2-2007-CO-DFOE) de la CGR	actualiza es a un reglamento y normativa para el uso de las tecnologías de información de la municipalidad. Sin embargo analizando el documento debe cambiarse y adaptarse al ambiente de la entidad ya que no se ha tropicalizado a condiciones que puedan cumplirse.	
10	**Gestión de proyectos**	• Se debe definir una metodología que permita controlar los proyectos que TI desea llevar a cabo o tiene en proceso • Determinar estrategias de control de calidad de los servicios brindados de manera interna y externa en los proyectos de TI	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con plan de proyectos o dicha metodología. No tienen estrategias de control de calidad para los servicios brindados.	**Incumplida**
11	**Decisiones sobre asuntos estratégicos de TI**	• Analizar la creación de un comité de TI que sea conformado por personeros con capacidad toma de decisiones para la correcta y apropiada aprobación y definición de objetivos del departamento de TI. • Implementación de un plan estratégico que se llegue a complementar con las labores que está realizando el departamento de Planificación y Coordinación Municipal.	Un Plan Estratégico alineado al plan estratégico de la municipalidad no existe, sin embargo, el departamento indica que se acoplan a trabajar en ese mismo. El comité de TI no existe.	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
12	**Planificación de las tecnologías de información**	• Alinear los procesos de trabajo con: ✓ Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la CGR. ✓ Normas Generales de Auditoria en el Sector Publico (R-DC-64-2014). ✓ Control Objectives for Information and Related Technology (COBIT) version 5. ✓ ISO 27001 Information Security Management System (ISMS) ✓ ISO 22301 Business Continuity Management. En donde se pueda obtener el óptimo funcionamiento de TI y el correcto cumplimiento de los con la visión, misión, objetivos de la entidad.	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna documentación que alinee los procesos de TI con los organizacionales. Además, el Reglamento para el uso de los recursos tecnológicos de información y comunicación de la municipalidad de la Cruz. Se aprobó hasta el mes de julio del 2021. No cumple como vigente ni esta tropicalizado a la gestión de la Municipalidad de La cruz.	**Incumplida**
13	**Modelo de arquitectura de información**	• Se recomienda realizar un análisis de actualización de aplicativos que permita que la seguridad e integración que posee la infraestructura actual de entidad sea optimizada.	No se cuenta con el análisis de aplicativos, pero si se migro a una nueva herramienta, la cual mejoro la integración de la infraestructura de la municipalidad. Se tiene en constante asesoría y mantenimiento, sin embargo no se cuenta con política de gestión de cambios, solo con un	**Parcialmente Cumplida**

#	Item	Recomendación	Comentario	Resultado
			formulario de solicitud para dichos cambios.	
14	**Infraestructura tecnológica**	• Se recomienda realizar un análisis objetivo el cual permita determinar el rumbo a seguir por parte del departamento de TI	Se cuenta con optimización de servicios y aprovechamiento con tecnologías por parte del departamento. proactividad por parte del área de TI. Sin embargo deben desarrollar y trabajar más en la etapa documental de ellos mismos para respaldo de labores.	**Parcialmente Cumplida**
15	**Independencia y recurso humano de la Función de TI**	• Realizar una clara definición de puestos y responsabilidades para el personal de TI	Aunque ya es un área Independiente y sigue sobre cargada, se tiene una clara definición sobre los puestos y responsabilidades del personal de IT. Lo que permite trabajar y saber cómo gestar sus labores.	**Cumplida**
16	**Consideraciones generales de la implementación de TI**	• Implementar pautas de aceptación para los proyectos de TI	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna documentación que alinee los procesos de TI o proyectos	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
			institucionales o algún departamento. Además el Reglamento para el uso de los recursos tecnológicos de información no indica alguna pauta o articulo para dicho punto.	
17	**Implementación de software**	• Definir estrategias que permitan la evaluación de la satisfacción de los servicios de TI con el usuario final. • Generar documentación para el proceso de asignación de roles y permisos donde se contemple el proceso completo de trabajo. • Se recomienda la correcta implementación y aprobación de las políticas de TI. • Llevar un control histórico de instalaciones para todos los equipos a lo largo de la entidad.	Se mantienen las mismas condiciones de la auditoria pasada. A razón de fallas en documentos tales como políticas, procedimientos y asignación de roles no se cuenta con lineamientos los cuales brinden un verdadero control con respecto a las implementaciones. Adicionalmente no se toma en cuenta el punto de vista del usuario final con respecto al servicio que TI está brindando, y TI tampoco cuenta con un historial de implementaciones realizadas a cada usuario y equipo crítico.	**Incumplida**
18	**Contratación de terceros para la implementación y mantenimiento**	• Se recomienda definir lineamientos para los requerimientos mínimos que debe cumplir un proveedor a la hora de brindar un servicio	Se mantienen las mismas condiciones de la auditoria pasada.	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
	de software e infraestructura		A razón de fallas en documentos tales como políticas, procedimientos y asignación de roles no se cuenta con lineamientos los cuales brinden un verdadero control con respecto a las implementaciones. Adicionalmente no se toma en cuenta el punto de vista del usuario final con respecto al servicio que TI está brindando, y TI tampoco cuenta con un historial de implementaciones realizadas a cada usuario y equipo crítico.	
19	**Definición y administración de acuerdos de servicio**	• Se recomienda que proveeduría posea un sistema de evaluación de proveedores con lo que se pueda optimizar la calidad de servicios que se le brinden a la entidad	Se mantienen las mismas condiciones de la auditoria pasada. A razón de fallas en documentos tales como políticas, procedimientos y asignación de roles no se cuenta con lineamientos los cuales brinden un verdadero control con respecto a las implementaciones. Adicionalmente no se toma en cuenta el punto de vista del usuario final con respecto al servicio que TI está brindando, y	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
			TI tampoco cuenta con un historial de implementaciones realizadas a cada usuario y equipo crítico.	
20	**Administración y operación de la plataforma tecnológica**	• Configurar de manera apropiada las bitácoras de registro de eventos en las herramientas, sistemas operativos y bases de datos en donde se pueda determinar cualquier incidente • Generar una CMDB con lo que se lleve el correcto control de los activos de TI, esto contempla hardware, software e infraestructura de servicios.	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna documentación completa de los activos de TI ya que no están completamente patrimoniados y documentados que personal los tiene. Las bitácoras están activas pero no hay revisiones periódicas y a nivel de base de datos no están configuradas ya que no se tiene conocimiento más que por ayuda del proveedor.	**Incumplida**
21	**Administración de los datos**	• Configurar de manera apropiada las bitácoras de registro de eventos en las herramientas, sistemas operativos y bases de datos en donde se pueda determinar cualquier incidente.	Las herramientas y sistemas cuentan con la configuración adecuada solo falta a nivel de base de datos verificar su configuración ya que por conocimiento no saben cómo esta pre-configurada.	**Parcialmente Cumplida**
22	**Atención de requerimientos**	• Se recomienda un análisis para la implementación de una mesa de servicios	Se mantienen las mismas condiciones de la auditoria pasada.	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
	de los usuarios de TI	que optimice la operación de TI, y mejore la atención al usuario final.	No se cuenta con alguna documentación ni herramienta parecida a una mesa de servicio.	
23	**Manejo de incidentes**	• Se recomienda un análisis para la implementación de una mesa de servicios que optimice la operación de TI, y mejore la atención al usuario final.	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna documentación ni herramienta parecida a una mesa de servicio.	**Incumplida**
24	**Administración de servicios prestados por terceros**	• Definir una figura que evalué la calidad y cumplimiento de los servicios que dan los proveedores, esto en el área de TI. • Definir un plan de evaluación de servicios que dan los proveedores.	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna documentación que alinee los procesos de TI o proyectos institucionales o algún departamento. Además el Reglamento para el uso de los recursos tecnológicos de información no indica alguna pauta o articulo para dicho punto.	**Incumplida**
25	**Seguimiento de los procesos de TI**	• Realizar una clara definición de puestos y responsabilidades para el personal de TI	Se aprobó el Reglamento para el uso de los recursos tecnológicos de información, sin embargo, falta tropicalizar o adaptar dicho reglamento, sobre procedimientos, procesos y políticas	**Parcialmente Cumplida**

#	Item	Recomendación	Comentario	Resultado
			No se cuenta con documentación alguna ni en modo borrador.	
26	**Seguimiento y evaluación del control interno en TI**	• Definir un marco de políticas de control interno de modo que se complemente a las labores del departamento de Planificación Institucional • Crear un registro histórico con las medidas correctivas implementadas, en dicho registró también llevar el control de las excepciones que se lleguen a presentar.	Se trabajó y se aprobó el Reglamento para el uso de los recursos tecnológicos de información. Sin embargo falta tropicalizar o adaptar dicho reglamento, sobre procedimientos, procesos y políticas No se cuenta con documentación alguna ni en modo borrador.	**Incumplida**
27	**Plan de Continuidad de Negocio**	• Definir un Plan de Continuidad de Negocio que cumpla con el ISO 22301 Business Continuity Management	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna documentación la cual responda a procesos o herramientas para la gestión de riesgo.	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
28	**Seguridad Física**	• Se recomienda separar las oficinas de TI, y todo el equipo de mantenimiento y en desuso del centro de datos • Se recomienda la implementación de sistemas de acceso biométrico, y cámaras de seguridad 24/7, y una bitácora de accesos. • Se recomienda la implementación de mecanismo de alerta temprana contra catástrofes tales como sensores de incendios, inundaciones, sensores de humedad relativa y termómetros (separados de los que poseen los equipos de A/C) • Se recomienda dar mantenimiento a los equipos de UPS y A/C periódicamente y mantener los reportes del mantenimiento como un histórico. • Se recomienda el estudiar la posibilidad de adquirir e implementar una planta eléctrica. • Se recomienda un mejoramiento en el sistema eléctrico según lo analizado por el área de TI para el mejoramiento de la vida útil de UPS y equipos a lo largo de la entidad.	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna mejora en la parte de seguridad física o mantenimientos periódicos de los activos.	**Incumplida**
29	**Parámetros de Contraseña**	• Se recomienda la estandarización de contraseñas y alineamiento con las mejoras prácticas para TI: Política Valor Tam. Contraseña 8 caract. Vencimiento 30-90 Días Históricos 6 o más Complejidad Activa	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con alguna mejora en la configuración ya que el encargado alega por falta de capacitación y	**Incumplida**

#	Item	Recomendación	Comentario	Resultado
		Bloqueo 3 intentos	cultura en el personal para activar políticas en el active directory o aplicativos. Por lo que los usuarios permanecen con las mismas contraseñas en todo el tiempo que trabajan o están en la municipalidad.	
30	**Roles de Acceso a Datos**	• Se recomienda realizar un análisis de mejoramiento de las herramientas para poder optimizar el control ya existente para no tener perdida de información y accesos no permitidos a datos sensibles.	La Municipalidad adquirió un sistema integrado llamado DECSIS el cual desde su creación definieron Roles de accesos por perfil y departamento. Sin embargo, la documentación de la misma no es muy disponible por el encargado de TI por el tema que el proveedor les gestiona los cambios o algunas configuraciones. Falta realizar algunas consultas a la base de datos, pero parece indicar que tienen las configuraciones de fábrica de Oracle 2016.	**Parcialmente Cumplida**
31	**Respaldo de Información**	• Se recomienda implementar el uso de bitácoras para el traslado de los respaldos de información al sitio alterno	Este proceso se realiza diaria mente programado y por seguridad de la información de la entidad, sin embargo,	**Parcialmente Cumplida**

#	Item	Recomendación	Comentario	Resultado
			no hay documentación alguna más que verificar el historial.	
32	**Bitácoras de Auditoría**	• Es recomendable realizar la implementación y la correcta configuración de las bitácoras de auditoria en donde se puede ver toda actividad y errores en bases de datos y sistemas operativos • Se recomienda optimizar, actualizar o sustituir los aplicativos que están presentado riegos en términos de control de actividad.	Este proceso se realiza diariamente por aplicativos y por seguridad de la información de la entidad, sin embargo, no hay documentación alguna más que verificar el historial.	**Parcialmente Cumplida**
33	**Exfuncionarios**	• Se recomienda realizar un análisis de mejoramiento de las herramientas para poder optimizar el control ya existente para no tener perdida de información y accesos no permitidos a datos sensibles.	La Municipalidad adquirió un sistema integrado llamado DECSIS el cual desde su creación definieron Roles de accesos por perfil y departamento. Sin embargo, la documentación de la misma no es muy disponible por el encargado de TI por el tema que el proveedor les gestiona los cambios o algunas configuraciones. Falta realizar algunas consultas a la base de datos, pero parece indicar que tienen las configuraciones de fábrica de Oracle 2016. No tienen documentación formal	**Parcialmente Cumplida**

#	Item	Recomendación	Comentario	Resultado
			de cómo está compuesto los roles y departamentos en el aplicativo sería recomendable tener un manual de TI y un manual de Usuario para esto. Así como formularios para la gestión de ingreso ya que solo se cuentan con un formulario de gestión de cambios	
34	**Control de Marcas**	• Se recomienda la migración de toda responsabilidad de administración, y extracción de reportes de los equipos de marcas al departamento de Recursos Humanos.	Por temas de Covid, no se está realizando el marcaje, sin embargo sigue en responsabilidad de TI.	**Incumplida**
35	**Seguridad de la información**	• Se recomienda la correcta configuración de las bitácoras para registro de actividades. • Considerar la implementación de un sistema de control de seguimiento para el acceso a los servidores y acceso a la información.	Este proceso se realiza diariamente por aplicativos y por seguridad de la información de la entidad, sin embargo, no hay documentación alguna más que verificar el historial.	**Parcialmente Cumplida**
36	**Análisis de contrataciones administrativas**	• Se recomienda contar con controles de calidad a los servicios que se proveen a la entidad, esto sea para el departamento de TI y para proveeduría. • Implementar el comité de informática el cual apoye la toma de decisiones y los proyectos a cumplir por TI.	Se mantienen las mismas condiciones de la auditoria pasada. No se cuenta con el comité de TI no existe a lo que se espera. No existe un control sobre los servicios de proveedores.	**Incumplida**