



MUNICIPALIDAD DE BELÉN  
AUDITORÍA INTERNA

INFORME  
INF-AI-08-2019

AUDITORIA OPERATIVA  
DE PROCESOS Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

OCTUBRE DE 2019

## Contenido

I.	INTRODUCCIÓN.....	5
II.	COMUNICACIÓN DE RESULTADOS .....	8
III.	RESULTADO OBTENIDO .....	9
3.1	Alineamiento de la Tecnología de Información con la Planeación Estratégica.....	9
3.1.1	Plan Estratégico Actual de Tecnología de Información.....	9
3.2	Implementación de los Cambios en SIGMB en el Ambiente Productivo .....	12
3.2.1	Registro Evaluación y Trazabilidad de Cambios en SIGMB. ....	13
3.2.2	Implementación de los cambios del SIGMB en el Ambiente Productivo.....	15
3.3	Gestión de Servicios, Incidentes y Problemas .....	16
3.3.1	Monitoreo Trazabilidad de las Peticiones de Servicio e Incidentes .....	17
3.3.2	Registro Integral de Peticiones de Servicio e Incidentes .....	18
3.3.3	Gestión de los Problemas .....	20
3.4	Gestión de Usuarios .....	21
3.4.1	Gestión de Claves del Sistema SIGMB. ....	21
3.4.2	Uso de Mecanismos de Autobloqueo de Equipos .....	22
3.4.3	Gestiones de Personal y Gestión de Usuarios .....	23
IV.	CONCLUSIONES.....	24
V.	RECOMENDACIONES.....	26
	A LA ADMINISTRACIÓN.....	26

## RESUMEN EJECUTIVO

*Este informe es el resultado de un estudio de auditoría programado en el Plan de Auditoría del año 2018, orientado para verificar que la función de la Unidad de Informática garantice, de manera razonable, la entrega de servicios de Tecnologías de Información concordantes con los niveles requeridos para la consecución de los objetivos institucionales mediante una Auditoría de los procesos claves de dicha Unidad, tales como alineamiento estratégico control de cambios, gestión de usuarios, gestión de servicios, incidentes y problemas, lo anterior a través de la observación del marco regulatorio vigente y las mejores prácticas aplicables al Sector Público desde la perspectiva de los temas por analizar.*

*Esta auditoría abarcó las acciones realizadas por la Administración en cuanto a la existencia de un sistema de controles que le permita a la Municipalidad de Belén:*

- *Tener la planeación de tecnología de información alineada a la estrategia empresarial.*
- *Una gestión de cambios en programas e infraestructura que mantenga la integridad y seguridad de la información.*
- *Una gestión de servicios, incidentes y problemas que permita el debido registro, seguimiento y cierre de los casos reportados.*
- *Una gestión de usuarios que logre resguardar la información de accesos y modificaciones no autorizadas.*

*Con el desarrollo del trabajo de auditoría, esta unidad de fiscalización determinó a través del análisis realizado, eventuales vulnerabilidades que enfrenta la Municipalidad en la entrega de servicios de Tecnologías de Información. Para ello, se efectuó una valoración integral de:*

- *Documentación con los lineamientos formales de la definición y aplicación de los controles vinculados a los aspectos a evaluar.*
- *De las prácticas con las cuales se están implementado los controles que deben existir para gestionar los aspectos a evaluar.*
- *Los controles existentes para el acceso al centro principal de procesamiento de datos de la Municipalidad.*
- *Ejecución de pruebas para validar la implementación de políticas de acceso y uso a recursos al sistema informático principal.*

**Municipalidad de Belén**  
**Auditoría Interna**  
**INF-AI-07-2019**

---

*En este orden de ideas, se encontró que la Municipalidad con relación a los servicios de Tecnología de Información de la Unidad Informática presenta una serie de debilidades de control que giran en torno a los siguientes puntos:*

- a. La carece de un documento formal de planeación estratégica de Tecnología de Información.*
- b. Las actividades con las que actualmente se están gestionando los cambios en el aplicativo Sistema de Gestión Municipal Belén (SIGMB), no permiten tener un sistema de control que garantice el debido registro, priorización, seguimiento, pruebas e implementación de cada ajuste realizado en el sistema.*
- c. El acceso del proveedor del Sistema de Gestión Municipal Belén (SIGMB) de manera directa a realizar instalaciones en el ambiente productivo de este, puede violentar la integridad de la información y comprometer la continuidad de las operaciones de la Municipalidad.*
- d. Las prácticas ejecutadas para gestionar los cambios asociados al Sistema de Gestión Municipal Belén (SIGMB), impiden mantener un debido control sobre el monitoreo y niveles de cumplimiento en la atención de cada uno de los casos reportados para este sistema.*
- e. Existen incidentes y peticiones de servicio que no son registrados en la plataforma destinada para este fin, lo que impide clasificarlos y tener registrada la trazabilidad de cada caso de forma centralizada.*
- f. Ausencia de un control que permita monitorear y gestionar proactivamente el cumplimiento de los tiempos de solución de los incidentes y gestión de servicios registrados mediante la plataforma de mesa de servicio.*
- g. La gestión actual de los problemas impide solucionar de forma oportuna una situación desde su raíz, en vez de aplicar medidas paliativas.*
- h. Debilidades en la aplicación de controles asociados con:*
  - a. La activación, vigencia y renovación de las claves de acceso del Sistema de Gestión Municipal Belén (SIGMB).*
  - b. Aplicación de auto-bloqueo en las máquinas de los usuarios por tiempo de inactividad.*
- i. Con respecto a la gestión de usuarios y sus respectivos accesos y perfiles, se identificó que las acciones de personal, como vacaciones, cambios de puestos, licencia de maternidad, entre otras; no son comunicadas de forma oportuna a la Unidad de Informática, por lo que existe el riesgo de que:*
  - a. Haya usuarios no autorizados con accesos.*
  - b. Haya accesos a los aplicativos que no se encuentren acorde con las funciones de los usuarios.*
- j. La Unidad de informática ha implementado mecanismos de seguridad para minimizar el acceso al centro de procesamiento principal, sin embargo, la ubicación de este centro y las*

*condiciones ambientales de resguardo con que cuenta, lo exponen a potenciales incidentes que pueden provocar interrupciones en las operaciones de los procesos de la Municipalidad.*

*Bajo este contexto, en el tanto la Administración desarrolle acciones de mejora en los puntos enumerados anteriormente, ello repercutirá positivamente en las distintas fases de los procesos que fueron objeto de estudio.*

*Dadas las debilidades identificadas se giran una serie de disposiciones a la Administración, con el fin de que ésta, diseñe e implemente a la brevedad posible, mecanismos de control que logren mitigar los riesgos e impactos asociados a cada una de las debilidades de control interno enumeradas.*

*Además, es importante recalcar que lo indicado en el informe de la Auditoría será objeto de seguimiento en fechas posteriores según lo establecido en la norma 2.11 de las Normas para el Ejercicio de la Auditoría Interna en el Sector Público.*

ORIGINAL FRAMING

**Municipalidad de Belén**  
**Auditoría Interna**  
**INF-AI-07-2019**

---

I. INTRODUCCIÓN

1.1 Origen del estudio.

El presente estudio se efectuó con fundamento en las competencias conferidas a las auditorías internas en el artículo 22 de la Ley General de Control Interno y en cumplimiento del Plan Anual de Trabajo del año 2018 de esta Auditoría Interna.

1.2 Hipotesis.

Las actividades de alineamiento estratégico y de gestión de control de cambios, usuarios, servicios, incidentes y problemas, de tecnologías de información son gestionadas de manera eficaz en la Municipalidad de Belén.

1.3 Objetivo general del estudio.

Evaluar el desempeño en la ejecución de las actividades de alineamiento estratégico y de gestión de control de cambios, usuarios, servicios, incidentes y problemas, de tecnologías de información, dentro de un debido marco normativo y de controles aplicable.

Objetivos Específicos:

- Validar que la planeación de tecnología de información se encuentra alineada a la planeación estratégica vigente de la Municipalidad de Belén.
- Revisar que la gestión de cambios en los programas e infraestructura de tecnología de la Información se realiza de acuerdo con las mejores prácticas utilizadas por la institución.
- Constatar que la gestión de servicios, incidentes y problemas se ejecuta de manera formal, respetando los niveles de servicios y manteniendo el debido registro y comunicación de toda la trazabilidad de cada caso.
- Comprobar que la gestión de usuarios se ejecute de manera formal y que en dicha gestión se cuente con los controles físicos y lógicos necesarios que limiten los accesos no autorizados a la información de la Municipalidad de Belén.

1.4 Alcance.

El estudio de auditoría comprende la validación de los controles existentes para la debida gestión de:

- Planeación estratégica de la Unidad de Informática.
- Cambios en programas e infraestructura respecto a la integridad y seguridad de la

**Municipalidad de Belén**  
**Auditoría Interna**  
**INF-AI-07-2019**

---

información.

- Registro, seguimiento y cierre de servicios, incidentes y problemas.
- Perfiles de accesos de usuarios a los recursos informáticos.

La evaluación de estos controles tuvo como fecha de corte el 5 de junio de 2019.

#### 1.5 Criterios Utilizados en la Revisión.

El marco utilizado para el desarrollo del presente estudio de auditoría es el siguiente:

- Ley General de Control Interno, No.8292 y su reglamento.
- Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitidas por la Contraloría General de la República.
- Las Normas Generales de Auditoría para el Sector Público, R-DC-64-2014.
- Normas de control interno para el Sector Público (N-2-2009-CO-DFOE)
- Marco Normativo Interno de la Municipalidad de Belén.
- Reglamento para el Uso de las Tecnologías de Información de la Municipalidad de Belén
- Ley de Contratación Administrativa N° 7494.
- Marco para la gestión gobierno y las tecnologías de información (TI), COBIT 5.

La aplicación de este marco se realiza según los objetivos y alcance definido para el presente estudio.

#### 1.6 Metodología Aplicada.

Las técnicas de auditoría realizadas para lograr los objetivos definidos en el presente estudio fueron las siguientes:

- Revisión documental

Se solicitaron documentos mediante los cuales se gestione:

- La planeación de la tecnología de información.
- El registro y supervisión sobre los cambios en las aplicaciones.
- El registro y trazabilidad de los servicios, incidentes y problemas.
- Registro, modificación y control de acceso de usuarios a los sistemas

La revisión sobre la documentación solicitada se centró en los siguientes aspectos:

- Existencia de la documentación.
  - La formalización de los documentos.
  - La redacción de elementos que permitan gestionar el elemento evaluado.
- Revisión de la ejecución de la práctica

Por la naturaleza del estudio, la principal responsable de la gestión de los controles asociados a las prácticas de planeación estratégica de tecnología de información, gestión de cambios, gestión de accesos, gestión de servicios, incidentes y problemas, es la Unidad de Informática; por lo que se realizó una sesión de trabajo con la responsable de esta unidad, para validar la ejecución de los siguientes aspectos:

- Mecanismos para realizar y administrar la planeación estratégica de tecnología de información.
  - Implementación de los controles definidos para la gestión de cambios.
  - Implementación de los controles definidos para la gestión de servicios, incidentes y problemas.
  - Implementación de los controles definidos para la gestión de accesos a usuarios.
- Ejecución de pruebas de acceso al Sistema de Gestión Municipal Belén (SIGMB)

Utilizando un usuario funcional del Sistema de Gestión Municipal Belén (SIGMB), se realizan pruebas de acceso para evaluar:

- Accesos no autorizados.
  - Prácticas de renovación de claves de acceso.
- Ejecución de pruebas de inspección

Las pruebas de inspección se centraron en:

- Revisión de las instalaciones de centro principal de procesamiento de datos (data center) para validar la existencia de vulnerabilidades asociadas a accesos no autorizados.
- Recorrido por estaciones de trabajo para validar la aplicación de controles de auto-bloqueo de equipos, por periodo de inactividad.

#### 1.7 Declaración de Cumplimiento de Normas

De conformidad con lo establecido en la Norma 1.3.3 de las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, se declara que las actividades del presente estudio se realizaron de conformidad con lo establecido en el Manual de Normas Generales de Auditoría para el Sector Público, entre otra normativa legal y técnica atinente a la materia.

#### 1.8 Responsabilidad de la Administración.

La administración es responsable de establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento, esto de conformidad con el artículo 10 de la Ley de Control Interno.

*“Artículo 10 - Responsabilidad por el sistema de control interno.  
Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.”*

#### 1.9 Limitaciones.

No se presentaron situaciones que impidieran o limitaran el desarrollo de las actividades planificadas para obtener los objetivos definidos en el trabajo de esta auditoría.

## II. COMUNICACIÓN DE RESULTADOS

En cumplimiento con lo establecido en el apartado 205. Comunicación de resultados de las Normas Generales de Auditoría para el Sector Público, los artículos 35, 36, 37 de la Ley General de Control Interno y el punto 4.5 del Procedimiento para la Tramitación de Informes de la Auditoría Interna de la Municipalidad de Belén, se comentaron los hallazgos contenidos en este informe, en la oficina de esta auditoría, lo cual consta en la minuta de auditoría XXXX de octubre del año en curso, en presencia de los siguientes funcionarios de la Municipalidad: Horacio Alvarado Bogantes, Alcalde, y Alina Sanchez Gonzalez, Coordinadora de Informática, quienes aceptaron el resultado de dicho informe.

### III. RESULTADO OBTENIDO

Mediante el estudio realizado se determinó lo siguiente:

#### III.1 Alineamiento de la Tecnología de Información con la Planeación Estratégica.

El Marco de gestión de tecnología de información como COBIT 5, indica que la estrategia diseñada para gestionar la tecnología de información debe planificarse, formalizarse, monitorearse y ajustarse a la estrategia empresarial. Para que estas acciones se puedan llevar a cabo es necesario establecer un documento formal que detalle cómo la tecnología de información colaborará en el logro de los objetivos definidos por el negocio.

El Plan Estratégico de Tecnología de Información (conocido normalmente como PETIC) debe contener al menos los siguientes componentes claves:

- Definición de metas que indiquen cómo TI contribuirá a los objetivos estratégicos, así como los costos y riesgos relacionados.
- Definición de métricas para medir el logro de las metas establecidas.
- Definición del presupuesto de inversión.
- Estrategia de adquisiciones.

El detalle del PETIC, debe permitir diseñar planes tácticos mediante los cuales se logre definir el plan de proyectos con los cuales se dará cumplimiento a la estrategia establecida.

Debe existir una constante retroalimentación entre el rumbo de la estrategia del negocio con la ejecución del PETIC, de forma tal que se logre identificar de forma oportuna cualquier ajuste que sea necesario implementarse en pro de lograr los objetivos empresariales definidos.

Como producto del estudio de auditoría se identificaron los siguientes hallazgos, vinculados con la planeación estratégica de TI:

##### III.1.1 Plan Estratégico Actual de Tecnología de Información.

En la actualidad la Municipalidad de Belén cuenta con un plan estratégico para el periodo 2013-2017, el cual ya cumplió su ciclo vida. La propuesta del nuevo plan estratégico tiene un periodo que abarca del 2018 al 2038; sin embargo, este plan no se ha formalizado.

Con respecto a este tema, es relevante reseñar que el 7 de noviembre del 2017, en la Sesión Ordinaria 66-2017, en el artículo 8, se conoció el Oficio AMB-MC-204-2017 de la Alcaldía por medio del cual remite el oficio PI-15-2017, suscrito por el Coordinador de Planificación donde presenta el Plan Estratégico Municipal 2018-2038.

Posteriormente, en Sesión Ordinaria 15-2019 realizada el 12 de marzo de ese mismo año, en el artículo 24 se acordó lo siguiente:

*“SE ACUERDA POR UNANIMIDAD: (...) SEGUNDO: Solicitar a los Directores de la Municipalidad de Belén, sus análisis y propuestas sobre el Plan Estratégico 2018-2038. TERCERO: Se invitan a participar en reunión de trabajo y Sesión Extraordinaria a convenir.”*

Por otra parte, la Coordinadora de la Unidad de Informática comenta que se encuentra en la elaboración de un documento de plan estratégico alineado al plan estratégico institucional 2018 al 2038. Sobre este particular, la Coordinadora del Comité de Tecnologías de Información, señala que en reunión de dicho Comité celebrada el 7 de agosto del 2019 la Coordinadora de Informática realizó una exposición de una propuesta de Plan Estratégico, sin embargo este no se aprobó, ya que se sugirió efectuar mejoras.

Dado que el plan estratégico que la Unidad Informática está elaborando se apoya en el plan institucional que no ha sido formalizado (aprobado por el Concejo Municipal), no es factible, para la fecha de este informe satisfacerse sobre niveles de alineamiento entre estas planificaciones. Por lo tanto, el análisis se centró en el alineamiento existente entre la planeación estratégica de tecnología de información y el plan estratégico 2013-2017.

Según la evidencia analizada, la Unidad de Informática ha desarrollado las siguientes acciones relacionadas con la planeación estratégica 2013-2017:

- Relaciona los proyectos, programas y planes de tecnología de información con los objetivos estratégicos definidos; según se muestra en el siguiente cuadro:

Cuadro No1

Relación Planes, programas y proyectos con objetivos estratégicos

Objetivo	Planes, programas y proyectos
3.1.2.3 Eficiencia en la tramitología administrativa	<p>4.1.1.3 Implementar un sistema de control interno y valoración del riesgo de las TIC (se realizó una propuesta de mejora ante el Comité Gerencial de TI, sobre la implementación de las Normas Técnicas para el control y la gestión de las tecnológicas de Información de la Municipalidad. Donde el alcance incluye a toda la organización en la implementación de las Normas Técnicas a la luz de los diferentes sistemas de gestión involucrados, va a requerir un esfuerzo de varias fases, mediante iteraciones que permitirán ir madurando y adoptando los diferentes sistemas de gestión empleando un enfoque de desarrollo por procesos, según la normativa N-2-2007-CO-DFOF, el cual involucra los siguientes sistemas:</p> <ul style="list-style-type: none"> <li>o Sistema de Gestión de Servicios.</li> <li>o Sistema de Gestión de Calidad.</li> <li>o Sistema de Gestión de Riesgos.</li> <li>o Sistema de Gestión de Seguridad.</li> <li>o Sistema de Gestión de Cumplimiento.</li> <li>o Sistema de Gestión de Planeación Estratégica.</li> <li>o Sistema de Gestión del Recurso Humano.</li> <li>o Sistema de Gestión de Continuidad.</li> <li>o Sistema de Gestión de Proyectos.</li> </ul>
	<p>4.1.1.4 Sistematizar la información municipal, a través de la tecnología en busca de una mejor toma de decisiones. (sistemas de ofimática, Sistemas ingresos, servicios línea).</p>
	<p>4.1.3.2 Implementar el proyecto Gobierno Electrónico, como mecanismo que permita acceder a la información y trámites administrativos de manera permanente y oportuna. (Servicios en línea, expediente electrónico, firma digital, tramites en línea, factura electrónica).</p>

Fuente: Unidad de Informática

- Gestiona el cumplimiento de la ejecución de los proyectos de TI.
- Registra la percepción que tienen los usuarios sobre las tareas desarrolladas por la Unidad de Informática.
- Gestiona la asignación y control presupuestario asignado a la TIC.

Sin embargo, no se encontró un documento formal de planeación estratégica de Tecnología de Información en el cual se esté gestionando como mínimo lo siguiente:

- Definición de objetivos estratégicos de Tecnología de Información y el soporte que los mismos brindan a los objetivos estratégicos del negocio.
- Definición de la estrategia de Tecnología de Información para alcanzar sus objetivos.
- Métricas que permitan analizar cómo la Tecnología de Información colabora en el logro de la estrategia del negocio.
- Determinación de los recursos de Tecnología de Información que se necesitan para desarrollar la estrategia definida.
- Monitorear el uso de los recursos de Tecnología de Información en la obtención de la estrategia planeada.
- Gestión de riesgos asociados a la estrategia de Tecnología de Información definida.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo I Normas de Aplicación General, definen lo siguiente:

*“1.1 Marco estratégico de TI. El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.”*

No tener un plan estratégico de tecnología de información en el cual se formalice y monitoree el aporte que la tecnología de información tiene dentro de la planeación estratégica institucional, limita la comprensión de los interesados en las oportunidades y limitaciones que tiene la tecnología de información para poder lograr las metas propuestas; por lo que se podría estar diseñando estrategias no reales de cumplir con los recursos actuales de tecnología; o bien se podría tener una inversión en tecnología que no va alineada a la misión planteada.

### **III. 2 Implementación de los Cambios en SIGMB en el Ambiente Productivo.**

En tecnología de información, la gestión de cambio involucra la implementación de software y hardware, producto de una solicitud de ajuste; dicha solicitud puede generarse por parte de las unidades usuarias o puede ser impulsada por factores de cambios en la tecnología. Una efectiva gestión de cambios se debe realizar de forma controlada, desarrollando normas y procedimientos que estandaricen esta actividad. Los controles claves que se deben considerar para la gestión de cambios son:

- Registro formal de petición de cambio: cada solicitud de cambio debe tener un proceso formal de autorización y debe existir un mecanismo oficial en el cual se registren las peticiones

autorizadas; este mecanismo debe contar con facilidades que permitan dar trazabilidad a cada petición, desde su registro hasta su cierre.

- Evaluación y priorización de cambios: las peticiones registradas deben ser analizadas y priorizadas utilizando métodos que se encuentren alineados a la estrategia del negocio.
- Administración de cambios de emergencia: debe existir un protocolo que indique como se identificarán y tramitarán los cambios de emergencia. Todo cambio de emergencia debe contar con un proceso de documentación que permita evidenciar los ajustes realizados.
- El debido cuidado en la implementación de los cambios: la implementación de los cambios se debe realizar en un ambiente controlado, resguardando la integridad de la información.

Cada cambio que involucre una entrega de componentes debe ser gestionado según las prácticas formales establecidas para el control de activos.

Como producto del estudio de auditoría se identificaron los siguientes hallazgos, vinculados con el control de cambios:

#### III.2.1 Registro, Evaluación y Trazabilidad de Cambios en SIGMB.

En el documento AMB-CC-003-2019, con fecha del 26 de marzo de 2019, la administración autoriza a los funcionarios para que las mejoras relacionadas con el Sistema de Gestión Municipal Belén (SIGMB); sean comunicadas y gestionadas mediante correo electrónico a la empresa DECSA con copia a la Unidad de Informática. Esta decisión:

- Posibilita al proveedor para tomar control sobre cada mejora.
- Establece el correo electrónico como el medio de comunicación oficial entre la Municipalidad de Belén y el proveedor.
- Establece una vía de comunicación directa entre el proveedor y los usuarios.

Lo descrito anteriormente crea una debilidad en los controles asociados a administración del cambio, ya que no permite gestionar de forma adecuada:

- El análisis del cambio.
- Impactos del cambio.
- Implementación del cambio.
- Documentación y monitoreo del cambio.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo III Implementación de tecnologías de información, indica:

*“3.2 Implementación de software. La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:*

- a. Observar lo que resulte aplicable de la norma 3.1 anterior.*
- b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.*
- c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.*
- d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.*
- e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.*
- f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.” (subrayado y negrita no es del original).*

Que la Municipalidad de Belén no cuente con un mecanismo formal centralizado en el cual se logre registrar, analizar y dar seguimiento de manera eficiente a cada una de las solicitudes de cambio del Sistema de Gestión Municipal Belén (SIGMB), limita a la Unidad de Informática en la ejecución de las siguientes acciones:

- Determinar la magnitud del ajuste a realizar, y las implicaciones técnicas que dicho ajuste podría tener en el ambiente productivo.
- Controlar oportunamente los tiempos de respuesta dados por el proveedor en la solución de cada solicitud.
- Tener una postura formal sobre el proceso de pruebas que debería seguirse para implementar el ajuste.

Además, expone a la Municipalidad de Belén a dependencias innecesarias del proveedor externo, y al riesgo de mantener un sistema informático en constante cambio sin control sobre las fuentes, la documentación y la operación de este.

Por otra parte, es importante señalar que la Municipalidad cuenta con un licenciamiento del software Aranda para la gestión de la mesa de ayuda por medio de la cual se registra, analiza y da seguimiento a las solicitudes de los usuarios.

Adicionalmente, la Municipalidad posee un contrato de servicio de apoyo para la atención de diferentes reportes que ingresan en la mesa de ayuda con la empresa el ORBE, el cual tiene como finalidad:

- Atención de incidentes reportados por la mesa de servicios.
- Revisión, readecuación y documentación de los procesos ITIL.
- Revisión del catálogo de servicios actual de la Municipalidad.
- Instalación de todos los módulos necesarios de la solución para gestionar la mesa de servicio.

Como se puede observar la Municipalidad dispone de una herramienta que centraliza cualquier solicitud de los funcionarios, por lo que con la situación descrita en el presente punto la misma se puede deducir que esta siendo subutilizada, es decir, los recursos no están siendo aprovechados de la manera más eficiente.

### III.2.2 Implementación de los cambios del SIGMB en el Ambiente Productivo.

Actualmente la Unidad de Informática se le imposibilita realizar los pases a producción; producto de mejoras o correcciones en el aplicativo que el proveedor del Sistema de Gestión Municipal Belén (SIGMB) haya desarrollado. Los pases a producción son instalados por el mismo proveedor, quien tiene la potestad de decidir si el cambio a aplicar será instalado de manera directa en el ambiente productivo o de forma previa se instalará en un ambiente de pruebas para ser validado antes de su instalación. Para acceder al ambiente de la Municipalidad de Belén, el proveedor solicita permiso de ingreso a la Unidad de Informática, la cual se lo brinda de manera temporal.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo I Normas de Aplicación General, definen lo siguiente:

*“1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica. La organización debe mantener la integridad de los*

*procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.*

*Para ello debe:*

- a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.*
- b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.*
- c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.*
- d. Controlar el acceso a los programas fuente y a los datos de prueba.” (subrayado y negrita no es del original).*

Las tareas de desarrollo y producción tienen que estar separadas, de forma tal que los programadores nunca ingresen al ambiente productivo; esto con la finalidad de garantizar la integridad del ambiente en donde se está administrando la información productiva de la empresa. El hecho de que el proveedor del Sistema de Gestión Municipal Belén (SIGMB), ingrese a los ambientes de pruebas y productivo de la institución, violenta de forma directa lo descrito anteriormente y expone a la Municipalidad de Belén a los siguientes riesgos:

- Pérdida de control en las modificaciones que se están instalando, en la actualidad solamente el proveedor tiene pleno dominio de las funcionalidades que se instalan cada vez que se solicita acceso.
- Como consecuencia del punto anterior, la Municipalidad de Belén no tiene mecanismos que le permitan garantizar las funcionalidades reales que se instalan en cada acceso.
- Alteraciones, pérdidas o corrupción de datos por no haber efectuado un adecuado proceso de pruebas que detectara inconsistencias de manera oportuna.
- Afectación del servicio brindado, producto de cualquier cambio en el ambiente productivo efectuada de forma no controlada.

### III.3 Gestión de Servicios, Incidentes y Problemas.

Toda necesidad relacionada con tecnología de información que los usuarios tengan debe ser gestionada de manera formal, según sea su naturaleza. Rutinariamente los usuarios pueden solicitar atención por alguno de los siguientes elementos:

- Servicio: un servicio es una solicitud sobre la operación de algún componente de tecnología de información; un ejemplo de servicio es la solicitud para la creación o modificación de usuarios.

- Incidente: un incidente es un evento sobre algún recurso de tecnología de información, que provoca afectación en la continuidad de la operación.
- Problema: cuando un incidente o solicitud de cambio por errores se convierte en algo repetitivo, que no solo afecta a un usuario en particular; se podría estar ante la gestión de un problema.

La debida atención de los servicios e incidentes involucra la ejecución de las siguientes tareas:

- Definición de esquemas para realizar una clasificación y priorización de casos.
- Registro formal de casos en donde se pueda documentar toda la trazabilidad del proceso, desde su ingreso hasta su solución.
- Analizar la tendencia de los incidentes.

A su vez, la debida gestión de los problemas conlleva el desarrollo de las siguientes acciones:

- Identificar, clasificar y priorizar los problemas.
- Valorar las causas que están provocando la manifestación de los problemas.
- Contar con una base de errores conocidos en donde se registre el análisis causa-raíz efectuado y la solución del caso, esta base debe mantenerse actualizada. Esta base de conocimiento permitirá tener a mano una solución para problemas que muestren el mismo análisis causa-raíz.
- Realizar análisis de tendencias (en especial de gestión de cambios y reportes de incidentes) que permita gestionar problemas de manera preventiva.

Como producto del estudio de auditoría se identificaron los siguientes hallazgos:

### III.3.1 Monitoreo Trazabilidad de las Peticiones de Servicio e Incidentes.

Dentro de la gestión de los incidentes y peticiones de servicio no se obtuvo evidencia que permita determinar, la existencia de una gestión proactiva en el monitoreo de la trazabilidad de los casos, a través de la cual se identifiquen las causas de incumplimiento de plazos y se logre documentar y subsanar las mismas.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo IV Prestación de servicios y mantenimiento, definen lo siguiente:

*“4.5 Manejo de incidentes. 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.” (subrayado y negrita no es del original).*

No contar con un monitoreo proactivo en la trazabilidad de solución de los casos registrados; limita la gestión y el control de la Municipalidad para poder determinar oportunamente:

- Si los tiempos definidos a nivel contractual se están cumpliendo.
- Validar los incumplimientos y tomar decisiones sobre los mismos, de acuerdo con los niveles de servicio establecidos.
- Contar con la información suficiente y necesaria para poder evaluar la efectividad del proveedor.

### III.3.2 Registro Integral de Peticiones de Servicio e Incidentes.

En la evidencia remitida por la Unidad Informática, relacionada con el registro y control de peticiones de servicio e incidentes, se denota dos situaciones que muestran que no todos los incidentes y/o peticiones de servicio cuentan con un único mecanismo de registro que permita analizar de forma centralizada y ágil toda la trazabilidad de cada uno de los casos:

#### a) Primer hecho: Aplicativo SIGM:

En el documento AMB-CC-003-2019, con fecha del 26 de marzo de 2019, la administración autoriza a los funcionarios para que los incidentes y/o peticiones de servicio relacionadas con el Sistema de Gestión Municipal Belén (SIGMB); sean comunicadas y gestionadas mediante correo electrónico a la empresa DECSA con copia a la Unidad de Informática. Esta decisión:

- Posibilita al proveedor para tomar control sobre cada caso.
- Establece el correo electrónico como el medio de comunicación oficial entre la Municipalidad de Belén y el proveedor.
- Establece una vía de comunicación directa entre el proveedor y los usuarios.

Lo descrito anteriormente crea una debilidad en el sistema de control, al no permitir desarrollar controles constantes vinculados con:

- Dar trazabilidad a los casos.
- Gestionar tiempos de respuesta.
- Administrar eventuales conflictos en la solución de casos.

b) Segundo hecho: Sistema Web

Para el caso del sistema WEB, la Unidad de Informática aporta evidencia que muestra la existencia de 143 mensajes de correo electrónicos mediante los cuales se han gestionado casos asociados a este sistema. La naturaleza de estos casos se resume en el siguiente cuadro:

Cuadro No2

Tipos de casos registrados del sistema WEB registrados mediante correo electrónico

Tipo de casos <sup>1</sup>	Cantidad
Alcance de la Solución	2
Solicitudes técnicas de Recursos	7
Ajustes, cambios, y problemas	85
Solicitud que hace referencia a mismos casos	35
No se relaciona a gestión de servicios o incidentes	14
<b>TOTAL</b>	<b>143</b>

Fuente: elaboración propia, basada en evidencia proporcionada por la Unidad de Informática

Los hechos detallados en los párrafos muestran que la totalidad de casos asociados al sistema WEB, no se está gestionando de manera centralizada a través de la herramienta tecnológica con la cual cuenta la Unidad de Informática; esto dificulta poder analizar la trazabilidad de cada caso de una forma eficiente y eficaz.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo IV Prestación de servicios y mantenimiento, definen lo siguiente:

*“4.5 Manejo de incidentes. 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.” (subrayado y negrita no es del original).*

<sup>1</sup> El detalle de cada tipo en el cual se agruparon los correos electrónicos analizados es el siguiente:

**Alcance de la Solución:** Se refiere a correos en los cuales se gestiona con el proveedor cronogramas o planificaciones de ajustes.

**Solicitudes técnicas de Recursos:** Casos vinculados con requerimientos técnicos gestionados con el proveedor.

**Ajustes, cambios, y problemas:** Casos vinculados con solución de requerimientos, cambios o problemas presentes en la solución.

**Solicitud que hace referencia a mismos casos:** correos que hacen mención a casos presentados en el punto anterior.

**No se relaciona a gestión de servicios o incidentes:** correos vinculados a gestiones de coordinación con el proveedor.

No tener todos registros gestionados por los usuarios sobre peticiones de servicio e incidentes centralizados en una única herramienta impide:

- Establecer prioridades de atención, según la criticidad de cada caso reportado.
- Dar trazabilidad a los casos, lo que imposibilita tener control del nivel de avance y gestionar de forma oportuna cualquier desviación en los tiempos definidos de atención y solución.
- Realizar análisis de tendencias sobre incidentes recurrentes.
- Identificar de forma ágil y oportuna el estado de un caso; analizando lo actuado en cada uno de esos estados.
- Analizar el comportamiento de un proveedor en un lapso determinado.
- Identificar de forma oportuna incumplimientos.

### III.3.3 Gestión de los Problemas.

Respecto a la gestión de problemas, no se tiene evidencia que demuestre que se está realizando una práctica formal, que permita valorar y documentar el problema raíz e ir creando una base de conocimientos.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo IV Prestación de servicios y mantenimiento, definen lo siguiente:

*“4.5 Manejo de incidentes. 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.” (subrayado y negrita no es del original).*

La falta de un análisis formal de problemas asociados con la tecnología de información puede provocar pérdida de efectividad y oportunidad en la gestión, dado que los recursos se enfocan en minimizar situaciones puntuales recurrentes, en vez de analizar las causas y atacar la raíz del evento.

Es importante informar que, con respecto a la gestión de incidentes y problemas, el Concejo Municipal mediante sesión ordinaria No. 39-2019 del 2 de julio del presente año conoció y aprobó entre otra normativa, la Política de Seguridad Física y Ambiental, la cual norma entre varios aspectos la gestión de incidentes de seguridad.

#### III.4 Gestión de Usuarios.

Para gestionar la atención de necesidades de los usuarios se debe contar con un marco para administrar la seguridad de información el cual debe estar formalizado, implementado, divulgado y debe ser sometido a revisiones periódicas para identificar necesidades de actualización. Los elementos claves que deben estar presentes en este marco son:

- Clasificación de los recursos según su criticidad y evaluación de riesgos.
- Culturización en la seguridad de información hacia los usuarios, haciendo hincapié, en las responsabilidades que tienen en este tema.
- Definición de medidas de control a nivel físico y ambiental que deben existir para el resguardo de la información.
- Establecimiento de mecanismos de autenticación a nivel de ingreso a la red institucional, así como a los recursos dentro de la misma.
- Definición de esquemas con niveles de responsabilidades para proceder a la solicitud, modificación y eliminación de accesos.
- Coordinación de acciones entre unidades para que se habiliten o bloqueen accesos a los usuarios sin actividad dentro del ambiente productivo.
- Esquemas de acceso seguro para terceras partes.
- Monitoreo de accesos al ambiente.

Como producto del estudio realizado se identificaron los siguientes hallazgos:

##### III.4.1 Gestión de Claves del Sistema SIGMB.

La contraseña de ingreso al Sistema de Gestión Municipal Belén (SIGMB) por parte de cada usuario no cuenta con políticas de cambio de primer ingreso, renovación y vigencia; lo que denota la falta de un control formal y estandarizado para el uso de claves de acceso que sea de aplicación obligatoria para todos los recursos de Tecnología de Información en los cuales se necesite autenticar a un usuario.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo I Normas de aplicación general, definen lo siguiente:

*“1.4.5 Control de acceso. La organización debe proteger la información de accesos no autorizados.*

*Para dicho propósito debe:*

....

*f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. 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...”*  
*(subrayado y negrita no es del original).*

El carecer de reglas formales y estandarizadas para la creación, definición, vencimiento y renovación de la contraseña en el Sistema de Gestión Municipal Belén (SIGMB), torna vulnerable la información que se gestiona en este aplicativo; ya que la contraseña podría ser fácilmente violentada, por lo que existe la posibilidad de que usuarios sin la debida autorización tengan acceso a la información. Por ello es necesaria una adecuada gestión de las claves, para contribuir a disminuir los riesgos que la institución soporta, y a minimizar los daños en los activos de información, en caso de que los riesgos lleguen a materializarse.

#### III.4.2 Uso de Mecanismos de Autobloqueo de Equipos.

Ante la ausencia de una práctica formal implementada de manera general por parte de la Unidad de Informática, mediante la cual se activen mecanismos de auto-bloqueo en los equipos de los usuarios, cuando éstos tengan con un periodo de inactividad, se incumple con lo establecido en el siguiente marco normativo;

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo I Normas de aplicación general, definen lo siguiente:

*“1.4.5 Control de acceso. La organización debe proteger la información de accesos no autorizados.*

*Para dicho propósito debe:*

...

*i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.*

*..." (subrayado y negrita no es del original).*

La falta de mecanismos de auto-bloqueo en los equipos de cómputo expone a la Municipalidad a que se pueda extraer o alterar información almacenada, mediante accesos no autorizados.

#### III.4.3 Gestiones de Personal y Gestión de Usuarios.

En relación con la existencia de un procedimiento o política formal mediante la cual las unidades usuarias respectivas, le informen a la Unidad de Informática, sobre acciones de personal (renuncias, despidos, incapacidades, licencias, movimientos internos, vacaciones, entre otros) que estén vinculadas con la gestión de los usuarios, no se obtuvo evidencia de este.

Las Normas Técnicas para la Gestión y el control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en el Capítulo I Normas de aplicación general, definen lo siguiente:

*"1.4.5 Control de acceso. La organización debe proteger la información de accesos no autorizados.*

*Para dicho propósito debe:*

...

*f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. 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..." (subrayado y negrita no es del original).*

La falta de gestión entre las unidades responsables de las acciones de personal y la Unidad de Informática hacen que exista la posibilidad de:

- Tener usuarios no activos con asignación de contraseñas a los diferentes recursos de tecnología de información de la Municipalidad de Belén.
- Que los usuarios tengan permisos no acordes con las funciones que desempeñan actualmente, debido a movimientos de puestos dentro de la Municipalidad.

Cualquiera de estas dos situaciones expone a la información a sufrir violaciones en su integridad y confidencialidad.

Es de relevancia acotar que, con respecto a la gestión de los usuarios de los sistemas de la Municipalidad, el Concejo Municipal mediante sesión ordinaria No. 39-2019 del 2 de julio del presente año conoció y aprobó entre otra normativa, la Política de Seguridad de la Información y la Política de Control de Accesos, las cuales regulan la administración de las claves de accesos y los movimientos de personal.

#### IV. CONCLUSIONES

De acuerdo con los aspectos descritos anteriormente, es posible concluir lo siguiente:

1. Con base en los resultados obtenidos, se concluye que ante la carencia de un marco estratégico en informática no fue posible validar la alineación de este con el de la Municipalidad, lo cual impide un mayor desarrollo y enfoque de las tecnologías de información para el apoyo de sus procesos sustantivos y toma de decisiones estratégicas, así como al desarrollo de la Municipalidad.
2. Por otra parte, la debilidad señalada en el punto anterior implica una carencia de integración de procesos y sistemas que repercute en la calidad y veracidad de la información, situaciones que impiden garantizar la mejor inversión en tecnologías de Información que robustezcan un enfoque estratégico orientado a la administración y gestión.
3. Como producto de la ejecución de las pruebas de Auditoría se concluye que las prácticas actuales implementadas por la Municipalidad de Belén para gestionar cambios sobre el Sistema de Gestión Municipal Belén (SIGMB); provocan:
  - Que no sea posible analizar y priorizar los cambios solicitados y sus impactos.
  - Que no sea posible determinar el nivel de complejidad de los cambios y el tiempo para su solución.
  - Que no se cuente con una práctica estandarizada, en la cual sea el personal respectivo de la Municipalidad de Belén el que determine los cambios que serán analizados en el ambiente de pruebas, antes de ser instalados en el ambiente productivo.
  - Posibles alteraciones en la integridad de la información y continuidad de las operaciones.
  - Falta de control de los cambios implementados.
  - Dependencia total hacia la gestión que tenga el proveedor sobre el control de cambios en el aplicativo.
4. De acuerdo con la administración de cambios en los procesos de informática es posible indicar, que

**Municipalidad de Belén**  
**Auditoría Interna**  
**INF-AI-07-2019**

---

el proveedor del Sistema de Gestión Municipal Belén (SIGMB) posee un ingreso directo para realizar instalaciones en el ambiente productivo de este sistema. Este hecho puede violentar la integridad de la información y puede comprometer la continuidad de las operaciones de la Municipalidad.

5. Una vez analizada la gestión de servicios, incidentes y problemas por parte de la Unidad de Informática se concluye que la misma presenta debilidades, que impiden que ésta se controle de manera adecuada. Lo anterior debido a que:

- Existe una plataforma en la cual se deben registrar todos los casos relacionados con la tecnología de información, sin embargo, no todos los recursos vinculados con la tecnología de información utilizan esta plataforma, lo que impide tener un registro integral de todos los casos y su proceso de solución.
- No se tiene implementado un control que permita monitorear y gestionar proactivamente el cumplimiento de los tiempos de solución de los incidentes y gestión de servicios registrados mediante la plataforma de mesa de servicio.
- La gestión actual de los problemas impide solucionar de forma oportuna una situación desde su raíz, en vez de aplicar medidas paliativas.

6. En cuanto a lo abordado en este estudio para la gestión de usuarios, se concluye que el proceso presenta debilidades de control que se resumen en los siguientes puntos:

- No hay medidas que gestionen la activación, vigencia y renovación de las claves de acceso del Sistema de Gestión Municipal Belén (SIGMB).
- No se encuentra implementadas medidas formales para la aplicación de auto-bloqueo en las máquinas de los usuarios por tiempo de inactividad.
- No existe una práctica formal para comunicar de forma oportuna las acciones de personal (vacaciones, cambios de puestos, licencia de maternidad, entre otros), a la Unidad de Informática.

Por lo que existe el riesgo de que:

- Haya usuarios no autorizados con accesos.
- Haya accesos a los aplicativos que no se encuentren acorde con las funciones de los usuarios.

7. Al evaluar el desempeño en la ejecución de las actividades de alineamiento estratégico y de gestión de control de cambios, usuarios, servicios, incidentes y problemas, de tecnologías de información, en la Municipalidad se puede concluir que los procesos citados no son realizados eficientemente en su totalidad, debido a la ausencia de un marco normativo y de controles aplicables.

## V. RECOMENDACIONES

### A LA ADMINISTRACIÓN

De conformidad con lo descrito, y lo establecido en este documento, de acuerdo con la normativa y los criterios jurídicos citados, a continuación, se presentan las siguientes recomendaciones para su atención:

1. Definir e implementar acciones específicas para garantizar la efectiva ejecución de las Normas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República; esto permitirá contar con un marco formal de controles que colaborará con la minimización de los hallazgos encontrados en el presente estudio de auditoría.
2. Ordenar las acciones necesarias para la elaboración e implementación del Plan Estratégico de Tecnologías de Información, el cual debe contener como mínimo los siguientes aspectos:
  - Vinculación entre los objetivos de tecnología de información y los objetivos estratégicos del negocio.
  - Medición de cómo la tecnología de información colabora en el logro de la estrategia del negocio.
  - Identificación de los recursos de tecnología de información que se necesitan para que ésta pueda colaborar en el logro de la estrategia del negocio.
  - Estrategias de monitoreo sobre el uso de los recursos de tecnología de información en la obtención de la estrategia planeada.
  - Gestión de riesgos asociados a la estrategia de tecnología de información definida.
  - Gestión integral de los proyectos de tecnología de información, con los cuales se podrá dar cumplimiento a la estrategia definida.
3. Elaborar, aprobar e implementar un proceso formal para gestionar los cambios, dicho proceso debe controlar los siguientes aspectos claves:
  - Registro formal de la solicitud de cambio, la cual debió haber sido sometida a un proceso de revisión y autorización por parte de la jefatura de la unidad usuaria respectiva.
  - Definición de un responsable dentro de la Unidad de Informática de analizar las solicitudes de cambio y establecer un orden y prioridad de implementación.
  - El registro de la solicitud de cambio se debe gestionar en un medio que le permita al responsable de la Unidad de Informática, controlar la trazabilidad del proceso de implementación de la solicitud de cambio, desde su registro hasta su cierre.
  - Establecer una práctica formal para gestionar los cambios de emergencia.
  - Determinar de manera formal los casos en los cuales es necesario la ejecución de pruebas, en

**Municipalidad de Belén**  
**Auditoría Interna**  
**INF-AI-07-2019**

---

las cuales debe participar la unidad usuaria que solicitó el ajuste. Para estos casos, se debe definir que no se podrá realizar ninguna instalación en el ambiente productivo hasta que la unidad usuaria dé su aprobación formal.

- Realizar una documentación completa del proceso de solución para los cambios y su impacto en el ambiente productivo.
  - Analizar la efectividad del cambio post-implementación.
  - Administración de cambios de emergencia: debe existir un protocolo que indique como se identificarán y tramitarán los cambios de emergencia. Todo cambio de emergencia debe contar con un proceso de documentación que permita evidenciar los ajustes realizados.
  - El debido cuidado en la implementación de los cambios: la implementación de los cambios se debe realizar en un ambiente controlado, resguardando la integridad de la información.
4. Evaluar como parte del proceso formal de gestión de cambios citado en el punto anterior, continuar con la práctica de que los funcionarios comuniquen y gestionen por medio de correo electrónico las mejoras relacionadas con el Sistema de Gestión Municipal Belén (SIGMB) ante la empresa DECSA.
5. Analizar la viabilidad de eliminar las instalaciones en el ambiente productivo por parte del proveedor del aplicativo.
6. Implementar, capacitar y dar seguimiento un proceso formal para gestionar los servicios y los incidentes, dicho proceso debe controlar los siguientes aspectos claves:
- El registro de toda solicitud de servicio e incidente se debe gestionar en un medio que le permita al responsable de la Unidad de Informática, controlar la trazabilidad de la gestión de forma integral y oportuna, desde su registro hasta su cierre.
  - Utilizar criterios mediante los cuales sea factible clasificar y priorizar las solicitudes de servicio y los incidentes.
  - Dar seguimiento al proceso de solución de las peticiones de servicio e incidentes, teniendo como punto clave de análisis, el cumplimiento de los tiempos de respuestas asociados.
  - Analizar periódicamente los incidentes, para determinar situaciones recurrentes.

Todo lo anterior con el fin de tener una gestión proactiva en el monitoreo de la trazabilidad de los casos, a través de los cuales se identifiquen las causas de incumplimiento de plazos y se logre documentar y subsanar las mismas.

7. Implementar, capacitar y dar seguimiento a un proceso formal para gestionar los problemas, dicho proceso debe controlar los siguientes aspectos claves:
- El registro de problemas en un medio que le permita al responsable de la Unidad de Informática,

- controlar la trazabilidad de la gestión de forma integral, desde su registro hasta su cierre.
- Utilizar criterios mediante los cuales sea factible clasificar y priorizar los problemas.
  - Realizar análisis a profundidad del problema, para poder identificar la causa-raíz de la situación presentada.
  - Mantener una base de conocimiento que sirva como herramienta para solucionar problemas similares que se puedan presentar a futuro.
8. Implementar, capacitar y divulgar la gestión integral de la seguridad de la información, específicamente la gestión de usuarios, de acuerdo con las Políticas aprobadas por el Concejo Municipal, la cual contemple como mínimo los siguientes controles:
- Procedimiento formal para el uso de contraseñas, esta definición debe considerar emisión de contraseña inicial, sintaxis de las contraseñas, vigencia y renovación de contraseñas. Las reglas definidas deben garantizar que las contraseñas utilizadas para acceder a los recursos de la Municipalidad de Belén no facilitan el acceso no autorizado. Todos los recursos que necesiten clave de acceso deben tener implementadas las reglas de contraseñas que se definan.
  - Definir como regla de acatamiento formal la utilización de mecanismos de auto-bloqueo automático con clave de acceso para los equipos que pasen un periodo sin actividad.
  - Procedimiento formal a través de las cuales las unidades responsables informen de manera oportuna a la Unidad de Informática sobre las acciones de personal ejecutadas (renuncias, despidos, incapacidades, licencias, movimientos internos, vacaciones, entre otros), de forma tal que le permita a la Unidad de Informática ejecutar suspensiones de accesos o ajustes sobre los mismos, de una forma proactiva.
  - Las medidas de acceso para el centro de procesamiento principal resguardan el ingreso de acceso no autorizado, por parte de los usuarios; sin embargo, la ubicación de este centro y las condiciones ambientales lo exponen a sufrir problemas serios que provocarían interrupciones en la operación del negocio; por lo que se debe, como parte de una estrategia de continuidad de negocio, definir la estrategia a implementar para subsanar esta situación.
9. Definir e implementar acciones orientadas a fomentar en la Municipalidad un proceso de culturización hacia los usuarios, de forma tal que los mismos comprendan y se involucren en la implementación de las medidas de seguridad definidas en el punto anterior.
10. La Municipalidad debe considerar a futuro dar un mayor aprovechamiento al licenciamiento del software Aranda con el que cuenta para la gestión de la mesa de ayuda por medio de la cual se registra, analiza y da seguimiento a las solicitudes de los usuarios.

De conformidad con los anteriores comentarios y aspectos a considerar, se le solicita informar a esta

**Municipalidad de Belén**  
**Auditoría Interna**  
**INF-AI-07-2019**

---

Auditoria, en un plazo de 30 días hábiles, sobre los resultados de las medidas ejecutadas para dar cumplimiento a lo señalado en este oficio.

Atentamente,

**LICDA. MARIBELLE SANCHO GARCÍA**  
**AUDITORA INTERNA**

Copias: Concejo / Archivo

ORIGINAL FIRMADO