1. No se cuenta con un Plan Estratégico de Tecnología de Información.

De la revisión a los proyectos ejecutados por la Gerencia de Sistemas y Tecnologías de Información (GSTI) se evidenció que dicha Gerencia actualmente trabaja activamente en diversos proyectos tecnológicos, los cuales son ejecutados siguiendo una adecuada gestión de proyectos. Asimismo, se encontró que el Gerente de la GSTI participa como Secretario en la Comisión de Gobierno Electrónico, en donde se revisan los diversos proyectos tecnológicos.

No obstante, la Gerencia no cuenta con un Plan Estratégico de Tecnología de Información que defina los objetivos, estrategias y proyectos de Tecnologías de Información alineados al logro de los objetivos organizacionales de la Compañía.

Esta situación podría dificultar la asignación de los recursos necesarios para que la GSTI implemente adecuadamente soluciones tecnológicas que respondan a las necesidades principales de la Compañía, alineadas al logro de los objetivos organizacionales.

Se recomienda que la Gerencia General disponga que el Gerente de la GSTI formule el Plan Estratégico de Sistemas a largo plazo de al menos 3 años. El plan debe formular la visión, misión, objetivos, estrategias y proyectos de TI alineados al cumplimiento de los objetivos de la Compañía.

2. Los indicadores de Gestión del área Informática son operativos.

De la revisión a los indicadores de Gestión de la Gerencia de Sistemas y Tecnologías de Información (GSTI), se encontró que el área cuenta con los siguientes indicadores:

- Tiene sistema de archivo para la documentación del área de sistemas
- Tienen más del 50% de los programas fuentes de sus aplicaciones
- Tienen más del 60% de la documentación del área
- Respecto a la elaboración del Plan Estratégico de Tecnologías de Información.
- Tiene Plan Operativo de TIC
- La evaluación del Plan Operativo de TIC ha sido registrado en el aplicativo web de la ONGEI

Estos indicadores son internos de la GSTI y por naturaleza son operativos y no permiten medir de manera efectiva la contribución del área a la Compañía.

Esta situación origina que la GSTI no pueda medir su efectividad ni contribuir eficientemente a los objetivos de la Compañía.

Se recomienda que el Gerente de la GSTI defina indicadores de gestión que permitan medir adecuadamente la gestión del área y su contribución a los objetivos estratégicos de la Compañía. Entre los indicadores recomendados se podrían considerar:

- Nivel de satisfacción de los usuarios con el servicio informático
- Nivel de disponibilidad de la infraestructura tecnológica
- Nivel de integración de los proyectos de Informática a los objetivos estratégicos de la Compañía

- Nivel de cumplimiento de los proyectos del Plan Estratégico de Tecnologías de Información

3. <u>La Normatividad del área requiere ser completada.</u>

De la revisión a la documentación normativa con la que cuenta la Gerencia de Sistemas y Tecnologías de Información (GSTI), se encontró que la GSTI cuenta con normatividad parcial para la gestión de sus actividades. En ese sentido, se encontró la existencia de normatividad que principalmente están relacionadas a la seguridad de la información.

Esta situación podría mermar la eficacia de la GSTI y el riesgo de que la GSTI no pueda responder de manera efectiva a las necesidades de los usuarios.

Se recomienda que la Gerencia General disponga que la Gerencia de Sistemas y Tecnologías de Información evalúe la conveniencia de identificar y formular la normatividad faltante; así como la revisión y actualización de la normatividad existente para su respectiva actualización. La Normatividad a contemplar, por ejemplo, podría estar basada en un árbol normativo top-down compuesto de:

- Políticas (documentos de alto nivel que indican la declaración de comportamiento sobre un determinado tema)
- normas, directivas, (documentos de cumplimiento obligatorio y cuyo objetivo es hace cumplir las políticas)
- procedimientos (documentos que describen el paso a paso para realizar algún propósito con el objetivo de hacer cumplir una norma o directiva).
- Instructivos (documentos paso a paso muy detallados, pudiendo contener pantallazos o comandos de ejecución)

4. **<u>La Gerencia de Sistemas y Tecnologias de Información no cuenta con unafunción de Administración de Base de Datos.</u>**

   De la revisión a la estructura organizacional de la Gerencia de Sistemas y Tecnologías de Información (GSTI), se encontró que en dicha área no se cuenta con un rol de Administrador de Base de Datos (DBA) que se encargue de la gestión de las diversas Bases de Datos que son mantenidas por la GSTI.

   Esta situación origina accesos por parte de los analistas y desarrolladores hacia las Bases de Datos, lo cual puede originar riesgos de confidencialidad, integridad y disponibilidad de los datos almacenados en las Bases de Datos.

   Se recomienda que el Gerente General en coordinación con el Gerente de Sistemas y Tecnologías de Información y el Gerente del área de Personal, evalúen la posibilidad de incluir una función de DBA dentro de la estructura organizacional de la GSTI.

5. **El sitio web de la Intranet requieren implementación de controles de protección en el tráfico de información.**

De la revisión a los sitios Web que gestionan la información de la Compañia, se encontró que desde la página Web de la Compañía http://www.lacompamia.pe/ se puede acceder a aplicaciones nternas de la Compañía a través de la Intranet via el link http://digital.lacompania.pe:8080/inicio.html

La navegación por parte de los usuarios a dicha página no se encuentra protegida en su totalidad, por lo que el tráfico de datos intercambiado entre los clientes que acceden a dicha páginas y los servidores web de la Compañía se encuentra en estado vulnerable a diversos ataques informáticos.

Esta situación podría originar una interceptación o fuga de la información procesada por la mencionada página web. Asimismo, debido a la falta de protección referida, se podría un atacante podría registrar información errada en dichas páginas web.

Se recomienda que la Gerencia General disponga que la Gerencia de Sistemas y Tecnologías de Información, priorice la implementación de certificados digitales de 2048 bits en los servidores Web de la Entidad; e implemente el protocolo TLS (antes conocido como SSL) para la transmisión de datos, lo que permitirá conexiones seguras y confiables entre el público usuario que accede a las páginas web indicadas y los servidores web de la Compañía.

6. **La Entidad aún no ha implementado controles para cumplir con la ley de Protección de datos personales.**

A la fecha de nuestra revisión, se evidenció que la Gerencia de Sistemas y Tecnologías de Información (GSTI) aún no ha implementado los controles técnicos exigidos por la Ley 29733 de Protección de Datos Personales. A la fecha de nuestra visita, la GSTI contaba con un informe de la consultora *Consultia Perú* quien realizó un análisis de los controles a implementar, pero que a la fecha de la nuestra revisión aún no se han implementado.

Dado que los Sistemas de Información de la GSTI procesan datos personales y sensibles, deben incorporar los controles exigidos por la Ley 29733 de Protección de datos personales que fue promulgada el 03 de junio del 2011 y reglamentada mediante Decreto Supremo Nº 003-2013-JUS del 22 de marzo del 2013, y que entró en plena vigencia el 08 de mayo del 2015.

Esta situación podría exponer a la Compañía a multas y sanciones de parte de la Autoridad Nacional de Protección de datos del Ministerio de Justicia.

Se recomienda que la Gerencia General, disponga que la Gerencia de Sistemas y Tecnologías de Información (GSTI) prioricen la implementación de los controles técnicos para cumplir con lo dispuesto en dicha Ley.

7. Se requiere mejoras en los controles de los Servidores Windows.

De la revisión a los controles tecnológicos implementados a los Servidores administrados por la Gerencia de Sistemas y Tecnologías de Información (GSTI), se encontró que la mayoría de los servidores están basados en el Sistema Operativo Linux, y cuentan con controles adecuados. Sin embargo, al revisar un Servidor Windows (de Directorio Activo), éste presento 2 debilidades:

- El Servidor de Directorio Activo no contaba con los parches actualizados.
- El acceso remoto a dicho servidor se realizó con el usuario PER\Melissa.Loza, el cual es una cuenta antigua que no es la cuenta que corresponde al Administrador de Servidores.

La falta de parches podría exponer al Servidor a ataques de malware y ataques informáticos. Asimismo, el acceso remoto con otro usuario a un Servidor podría originar que ante la ocurrencia de un evento no se pueda asignar responsabilidad de quien fue la persona que origino el evento.

Se recomienda que la Gerencia Municipal, disponga que la Gerencia de Sistemas y Tecnologías de Información (GSTI) priorice la actualización de los parches en todos los Servidores Windows de la GSTI y la utilización de cuentas individuales e intransferibles para todos los colaboladores de la Compañía.