Universidad CENFOTEC

Maestría Profesional en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Plan de implementación de un Sistema de Gestión de Seguridad de la Información SGSI para el Colegio Universitario de Cartago.

CASTILLO MOLINA FRANK ÁNGEL

Agosto 2023

Declaratoria de derechos de autor

El suscrito Frank Ángel Castillo Molina con cédula de identidad número 1-1291- 0791, declaro bajo fe de juramento, conociendo las consecuencias penales que conlleva el delito de perjurio, que soy el autor del presente trabajo final de graduación para optar por el título de Maestría Profesional de Ciberseguridad de la Universidad CENFOTEC y que el contenido de este trabajo es obra original de Frank Ángel Castillo Molina. Asimismo, autorizo a la Universidad CENFOTEC a disponer de este trabajo para uso y fines de carácter académico, publicitando el mismo en el sitio web.

Ni la Universidad ni el jurado que califica este Proyecto Final de Graduación serán responsables de las ideas expuestas por Frank Ángel Castillo Molina.

A la vez se considera confidencial por el período de 3 años establecido entre el estudiante y la institución. Luego de cumplido ese plazo, se autoriza la consulta y uso con fines exclusivos académicos.

AGRADECIMIENTOS

Agradezco a Dios por bendecirme todos los días y por permitirme completar esta meta que me propuse años atrás

A la Unidad de Tecnologías de la Información del Colegio Universitario de Cartago, por el gran apoyo otorgado a mi persona para la consecución de esta tesis.

A mi amada esposa que ha sido el impulso durante mi carrera y el pilar principal para la culminación de la misma, que gracias a su apoyo incondicional y a su sabiduría me guío en los momentos determinantes para la elaboración de la misma.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Frank Angel Castillo Molina.**

ARTURO RAMIREZ HEGG (FIRMA)
Firmado digitalmente por ARTURO RAMIREZ HEGG (FIRMA)
Fecha: 2024.06.28 10:29:03 -06'00'

M.Sc. Arturo Ramírez Hegg
Tutor

EDGAR EDUARDO RIVERA CALDERON (FIRMA)
Firmado digitalmente por EDGAR EDUARDO RIVERA CALDERON (FIRMA)
Fecha: 2024.06.28 11:13:28 -06'00'

M.Sc. Edgar Rivera Calderón
Lector 1


Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2024.06.28 12:16:07 -06'00'

M.Sc. Miguel Pérez Montero
Lector 2

Índice de contenido

Contenido

Lista de figuras

Resumen

El presente estudio abordó la importancia del resguardo de la seguridad de datos en una institución educativa de la provincia de Cartago, Costa Rica. Específicamente se trabajó en una propuesta a partir del Sistema de Gestión de Seguridad de la Información (SGSI) como un conjunto de políticas, procedimientos, procesos y controles técnicos y organizativos implementados por una organización para gestionar, proteger y garantizar la seguridad de la información.

Sobre la institución en estudio se realizó un análisis de la auditoría realizada en el 2021 que permitió identificar un grado importante de vulnerabilidad en torno a la seguridad de la información. El informe de dicha auditoría fue el insumo utilizado como diagnóstico para establecer la ruta de la propuesta de solución ante dicha necesidad.

El tipo de investigación de este proyecto es aplicada y bajo el enfoque cualitativo, ya que se centra en el análisis de las necesidades de la institución y en el desarrollo de una propuesta que se ajuste a dichas necesidades, utilizando la norma ISO 27001 como referencia. Este enfoque permitió una comprensión profunda y detallada del contexto y de los requisitos específicos de la institución en estudio.

El resultado más valioso de este ejercicio académico e investigativo se centra en la propuesta que surge como solución a la problemática de inseguridad de la información de una institución educativa de importancia en la provincia por la oferta académica que se desarrolla.

Palabras clave: ciberseguridad-informática- Sistema de Gestión de Seguridad de la Información- gestión de la información.

Capítulo I: Introducción

1.1. Generalidades

1.2. Antecedentes del problema

El Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, procesos y controles técnicos y organizativos implementados por una organización para gestionar, proteger y garantizar la seguridad de la información.

En la actualidad, la seguridad de la información es un tema de suma importancia para las organizaciones debido al aumento de las amenazas cibernéticas, la importancia de proteger la confidencialidad, integridad y disponibilidad de la información.

En general se puede decir que existen varios desafíos y tendencias en este campo:

1. Cumplimiento normativo: Las organizaciones deben cumplir con una serie de normas y regulaciones relacionadas con la seguridad de la información, como la ISO 27001, el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, entre otros.

2. Amenazas cibernéticas: Las amenazas cibernéticas están en constante evolución y se vuelven cada vez más sofisticadas. Las organizaciones deben estar preparadas para enfrentar ataques como ransomware, phishing, ataques de denegación de servicio, entre otros.

3. Gestión de riesgos: La gestión de riesgos es un componente clave en la seguridad de la información. Las organizaciones deben identificar y evaluar los riesgos asociados a sus activos de información y tomar medidas para mitigarlos.

4. Educación y concientización: La educación y concientización de los empleados es fundamental para garantizar la seguridad de la información. Las organizaciones deben capacitar a su personal en buenas prácticas de seguridad, como el uso de contraseñas seguras, la identificación de correos electrónicos de phishing, entre otros.

5. Avances tecnológicos: Los avances tecnológicos, como la computación en la nube, el internet de las cosas (IoT) y la inteligencia artificial, presentan nuevos desafíos en términos de seguridad de la información. Las organizaciones deben adaptar sus SGSI para abordar estas nuevas tecnologías.

El SGSI implica enfrentar desafíos como el cumplimiento normativo, las amenazas cibernéticas, la gestión de riesgos, la educación, la concientización y la adaptación a los avances tecnológicos. Las organizaciones deben estar preparadas para enfrentar estos desafíos y garantizar la seguridad de su información.

1.3. Definición y descripción del problema

Desde la revolución tecnológica, la información ha pasado a ser un elemento muy importante, pero a la vez muy sensible y vulnerable para los delitos de distinta índole. Desde esta premisa, se conoce que el Colegio Universitario de Cartago (CUC), no cuenta con un SGSI para poder proteger y administrar la información que maneja. Según MICITT:

> La Institución debe propiciar un ambiente seguro, considerando la seguridad física, lógica y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución. P.13

A partir de lo anterior, el presente estudio pretende a través de la investigación dar respuesta a la pregunta problema: ¿cómo elaborar un plan de implementación de un SGSI para el CUC?

1.4. Justificación

La mayoría de negocios dispone o tiene acceso a información sensible. El hecho de no proteger adecuadamente dicha información puede tener consecuencias operativas, financieras y legales graves, que pueden incluso llevar a la quiebra del negocio. El reto que la mayoría de negocios afronta es proporcionar una adecuada protección. Particularmente, cómo asegurar que han identificado los riesgos a los que están expuestos y cómo gestionarlos de forma proporcionada, sostenible y efectiva.

Además, los usuarios de todas las empresas deberían tener la plena seguridad de que sus datos, activos y otros estén seguros. De aquí radica la importancia para el investigador por elaborar e implementar un plan de SGSI. Si bien muchos negocios y empresas cuentan con certificaciones de seguridad, muchos olvidan dar el soporte y actualización que requiere para que siga siendo efectivo.

La ISO 27001 es la norma internacional para los SGSI, dicho sistema proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. A partir de esta norma se pretende elaborar el instrumento para la recolección de la información necesaria, finalmente el diseño e implementación del plan.

1.5. Viabilidad técnica, operativa y económica

El proyecto, a partir de lo expuesto en las líneas anteriores puede catalogarse como viable en los aspectos técnicos, operativos y económicos. Se contó con el visto bueno de la institución, no se necesitó de ningún tipo de presupuesto para alguna inversión o gasto al que no se pueda hacer frente y que puedan limitar el proyecto. Así mismo, el

investigador ha desarrollado los conocimientos técnicos suficientes, durante sus estudios de maestría, para desarrollar de manera profesional este estudio.

1.6. Objetivo general y específico

1.6.1. General

Elaborar un plan de implementación de un Sistema de Gestión de Seguridad de la Información para el Colegio Universitario de Cartago.

1.6.2. Específicos

1.6.2.1. Identificar oportunidades, riesgos y limitaciones del departamento de Tecnologías de la Información de la institución.

1.6.2.2. Evaluar los resultados de la auditoria AI-03-2021 realizada al departamento como parte del diagnóstico.

1.6.2.3. Diseñar el plan de acción en seguridad informática necesario para el Colegio Universitario de Cartago

1.7. Alcances y limitaciones

Desde el punto de vista de los alcances se puede mencionar que elaborar un plan de implementación de un SGSI para el CUC traerá mucha solidez en cuanto a la confianza del resguardo de información, tanto a funcionarios como a usuarios. A partir del producto de este estudio la institución podrá planificar periodos de revisión y actualización del plan para adecuarse al contexto y los cambios que vayan surgiendo en materia de seguridad informática.

En términos de limitaciones podría mencionarse que el alcance de este proyecto se enfoca en la elaboración del plan de implementación del SGSI, por lo que debe designarse un periodo adicional a la evaluación del plan una vez que se ha puesto en práctica para determinar posibles mejoras.

1.8. Marco de referencia, Organizacional y socioeconómico

En el año 1975 a raíz del problema que afrontaban los egresados de los centros de enseñanza secundaria de Cartago para matricularse en la Universidad de Costa Rica y otros centros de enseñanza superior, un grupo de distinguidas personas, se interesaron por luchar para que los jóvenes cartagineses no perdieran la oportunidad de continuar sus estudios superiores, en razón del principio de igualdad y responsabilidad social que caracteriza nuestro sistema democrático. (CUC, 2023)

Bajo este sentimiento de solidaridad en pro del bienestar de la juventud cartaginesa, el 26 de mayo de 1975 se convocó una asamblea en el salón de sesiones de la Municipalidad de Cartago. En dicha actividad participaron representantes de la Dirección Nacional de Desarrollo de la Comunidad (DINADECO). Después de un análisis de la situación educativa que se vivía en ese momento, los asambleístas tomaron el acuerdo de fundar la Asociación de Desarrollo Específico Universitaria de Cartago (ADEUCA).

Entre los fines que la ADEUCA se planteó la creación de un centro universitario en Cartago para dar cabida a cientos de estudiantes que no encontraron cupo en las universidades, de esta forma la gestación y la creación del CUC se debe a ADEUCA. Con la apertura del CUC se estableció el sistema de enseñanza superior parauniversitaria, el cual tiene como misión impartir carreras cortas y oportunidades de capacitación. El CUC inicia funciones el 8 de noviembre de 1976, como institución de Educación Superior.

Mediante Ley No. 6541 (Gaceta No. 241 del 17 de diciembre de 1980), se establece oficialmente, siendo su objetivo principal ofrecer carreras cortas a personas egresadas de la educación diversificada. Reformado el artículo No. 16 por medio de la Ley No.7015 (Gaceta No. 229 del 29 de noviembre de 1985).

El Reglamento mediante el cual se regula la normativa operativa de la Institución, se dio mediante Decreto Ejecutivo No. 12711-E (Gaceta No. 124 del 2 de julio de 1981), reformado a través del Decreto Ejecutivo No. 30431 -E (Gaceta No. 94 del 17 de mayo del 2002).

La institución fue creada el 8 de noviembre de 1976, mediante la Ley No 6541. Actualmente se rige por la Ley 9625, Ley Orgánica del Colegio Universitario de Cartago, que establece los siguientes fines:

a) Adoptar las nuevas tecnologías para garantizar la más alta calidad en la enseñanza, la investigación y la acción social.
b) Graduar técnicos a nivel de diplomado y pregrado, por medio e carreras cortas, con los requerimientos sociales, científicos y tecnológicos del desarrollo mundial y las necesidades de la provincia y el país, que culminen con la obtención de certificaciones, títulos, pregrados y otros grados académicos de carácter técnico y parauniversitario.
c) Diseñar programas para la educación continua de los graduados del CUC y la ciudadanía en general, que promuevan la actualización constante de conocimientos y los emprendimientos empresariales y culturales.
d) Los demás fines que se establezcan en el Estatuto Orgánico.

Misión

Formamos para transformar vidas

Visión

Brindaremos a la sociedad costarricense personas integras y con las herramientas necesarias para insertarse en el mercado laboral a través de una enseñanza, infraestructura física y tecnología de excelencia

Valores Estratégicos

Excelencia: Capacidad para cumplir con estándares superiores a los establecidos.

Equidad e inclusión: Enfoque que responde positivamente a la diversidad de las personas y a las diferencias individuales para contribuir al desarrollo de la comunidad a través de la cultura, el respeto y la consciencia social.

Transparencia: Orientar la gestión a la satisfacción del interés público en apego al principio de legalidad en la administración de los recursos públicos que permitan una adecuada rendición de cuentas.

Valores Conductuales:

Formación Humanística: Enfoque centrado en la persona como un todo que integra el conocimiento técnico-profesional, valores y creencias para fomentar el respeto y la tolerancia social.

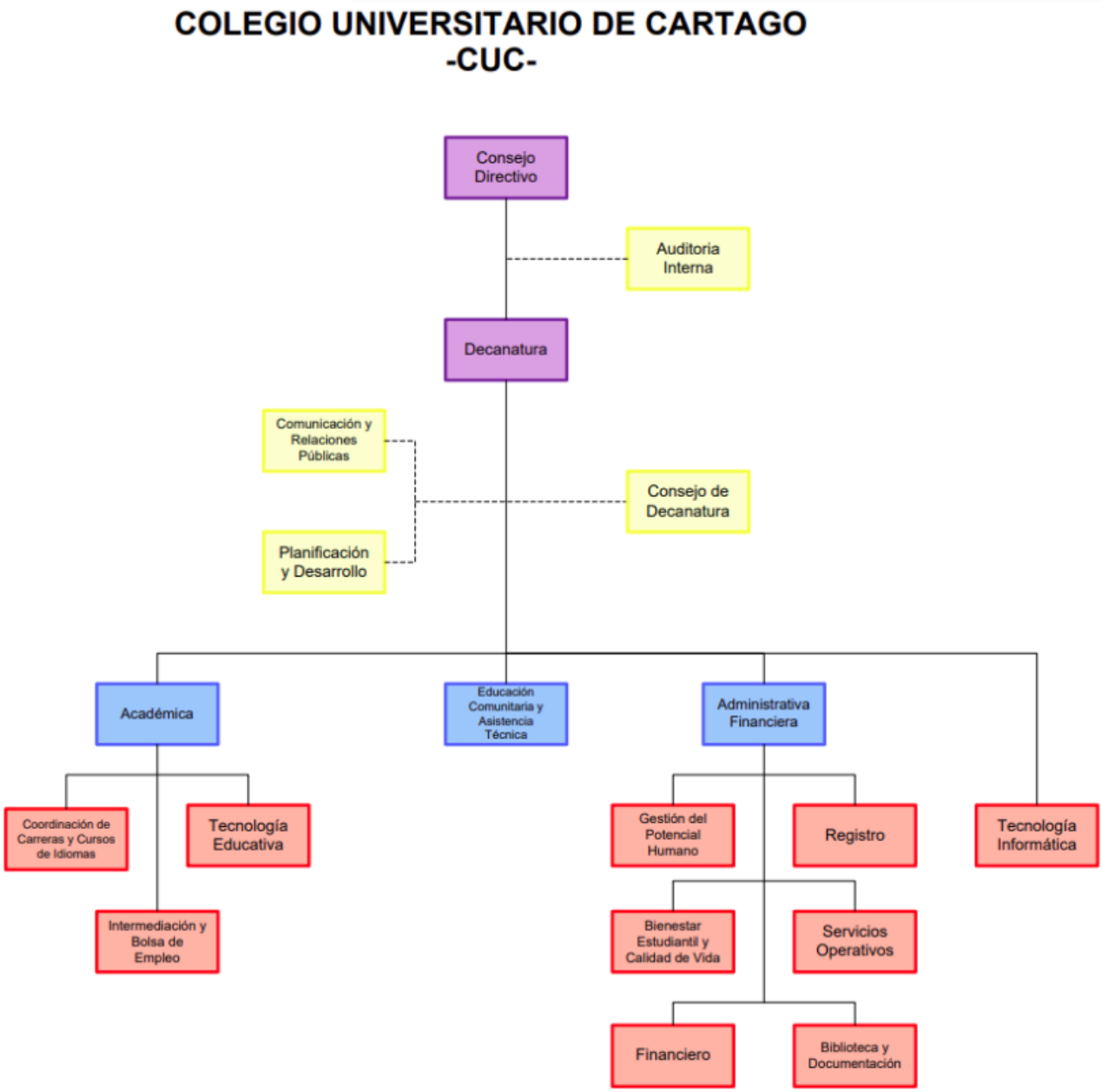
Innovación: Capacidad para proponer y adaptar a iniciativas y proyectos, aportando originalidad e inventiva.

Calidad en el servicio: Capacidad para orientar la gestión según las necesidades del cliente, para lograr y superar los resultados esperados, bajo estándares de calidad establecidos.

Respeto: Capacidad para dar a los otros y a uno mismo un trato digno, franco y tolerante, comportándose de acuerdo con los valores morales.

Conciencia Social: Capacidad para diseñar, proponer, colaborar e identificarse con propuestas orientadas a contribuir con la sociedad, en las áreas en las cuáles estas presentan mayores carencias, por ende, mayor necesidad de ayuda y colaboración.

Figura 1 Marco Organizacional



Fuente: https://www.cuc.ac.cr/institucion/organigrama/

Marco socioeconómico

El CUC se encuentra ubicado en la parte central de la provincia de Cartago. Económicamente la provincia realiza actividades importantes como la agricultura en primer lugar, turismo y el comercio. Según la Municipalidad de Cartago

Cartago desde antes de la conquista y aún más después de ella, vio fortalecida la actividad de cultivar la tierra y es quizás por ello que al día de hoy se mantiene esta forma de subsistencia en gran parte del territorio cartaginés, siendo uno de los mayores proveedores de verduras para el resto del país. 2023

Hablando en términos de salud, la provincia tiene índices de natalidad semejantes al resto del país, pero sobresale por la baja tasa de mortalidad, lo que da un crecimiento poblacional positivo. Se cuenta con servicios públicos a través de la Caja Costarricense de Seguro Social y el Ministerio de Salud, la atención se da a través del Hospital Maximiliano Peralta y los Equipos Básicos de Atención Integral en Salud (EBAIS). Cerca de la institución se encuentra una sede de la Cruz Roja y variedad de servicios de atención privada en clínica, farmacias y otros.

La municipalidad da el servicio de recolección de basura, educación ambiental a los ciudadanos sobre el control de la contaminación y la valoración del recurso hídrico tan importante con el que cuenta la provincia tanto para uso doméstico, industrial y turístico.

Finalmente, se encuentra a pocos metros de la institución, que dicho sea de paso es de educación superior técnica, algunos colegios y escuelas públicas, además de otras del sector privado. El CUC que es la institución en estudio, forma estudiantes en varias carreras entre las cuales se encuentra el turismo, siendo el CUC entidad pionera en la formación de profesionales en turismo en Costa Rica.

1.9. Revisión sistemática de la literatura y estado de la cuestión

En la actualidad, la seguridad de la información se ha convertido en un aspecto crítico para las organizaciones, ya que los avances tecnológicos y la creciente digitalización han aumentado los riesgos y amenazas a la seguridad de los datos. Por lo tanto, muchas organizaciones están implementando SGSI para proteger su información y garantizar la confidencialidad, integridad y disponibilidad de los datos.

En términos de normativas y estándares, existen diversas referencias internacionales que establecen los requisitos y buenas prácticas para la implementación de un SGSI. El estándar más reconocido a nivel mundial es la norma ISO 27001, que establece los requisitos para establecer, implementar, mantener y mejorar un SGSI.

En la actualidad se está dando la importancia a la seguridad de la información y se están implementando estos sistemas. Sin embargo, todavía existen muchas organizaciones que carecen de un SGSI o que no han implementado todas las medidas necesarias para garantizar la seguridad de la información.

Para evaluar el estado de la cuestión de un SGSI, se deben tener en cuenta varios aspectos:

1) Evaluación de riesgos: Se debe realizar una evaluación exhaustiva de los riesgos de seguridad de la información a los que está expuesta la organización. Esto implica identificar las amenazas potenciales, evaluar

su impacto y probabilidad de ocurrencia, y determinar las medidas de control necesarias para mitigar dichos riesgos.

2) Políticas y procedimientos: Se deben analizar y evaluar las políticas y procedimientos existentes en la organización en relación con la seguridad de la información. Esto implica revisar si se cuenta con políticas claras y actualizadas, así como con procedimientos documentados y comunicados adecuadamente a los empleados.
3) Infraestructura tecnológica: Se debe evaluar la infraestructura tecnológica de la organización en términos de seguridad de la información. Esto implica analizar la configuración de los sistemas, la protección de los datos, las medidas de seguridad implementadas, como firewalls y antivirus, y la gestión de accesos y privilegios.
4) Conciencia y capacitación: Se debe evaluar el nivel de conciencia y capacitación en seguridad de la información de los empleados de la organización. Esto implica analizar si se realizan programas de concientización y entrenamiento, si se promueve una cultura de seguridad de la información y si los empleados tienen los conocimientos y habilidades necesarios para proteger la información de la organización.
5) Cumplimiento normativo: Se debe analizar si la organización cumple con las leyes y regulaciones relacionadas con la seguridad de la información. Esto implica evaluar si se tienen en cuenta los requisitos legales reglamentarios, como la protección de datos personales y la privacidad, si se realizan auditorías y controles para asegurar el cumplimiento.

Para este proyecto se realizó una búsqueda de investigaciones relacionadas, de las cuáles se presentan 3 estudios: dos nacionales y una internacional.

Hidalgo (2015), presentó su tesis de maestría profesional en Auditoría de Tecnología de la Información en la Universidad de Costa Rica en el 2015, titulada: Diagnóstico y evaluación de cumplimiento de la norma de los controles de ISO/IEC 27001 Sistema de gestión de seguridad de la información (SGSI) desde la perspectiva del AP12 Evaluar y Administrar los Riesgos de TI (COBIT 5), así como determinar el grado de alineación y nivel de madurez del SGSI en apego a la norma. La empresa por motivos de confidencialidad no se identificó.

Hidalgo realizó un diagnóstico y una evaluación del cumplimiento de la norma ISO/IEC 27001, SGSI junto al DS5: “Garantizar la seguridad de los sistemas” del dominio COBIT: Entregar y dar soporte, para determinar el grado de alineación y nivel de madurez del SGSI en apego a la norma. A partir de esta acción se pretendió crear un plan de gestión de la Seguridad de la información. Aunque no se menciona un problema en concreto, la autora se plantea identificar los riesgos y debilidades que deben mejorarse, lo que podría considerarse que conoce que existen y desea documentarlos.

Para recabar la información, se realizó el diagnóstico a través de plantillas que incluyeron los requerimientos y objetivos de control establecidos por las normas aplicadas por medio de entrevistas. Hidalgo encontró, durante el proceso, que la empresa no contaba con un SGSI alineado con las normas del estándar, colocando este aspecto en madurez inicial, existe desconocimiento por parte de los funcionarios sobre seguridad de la información. Se carece de control de accesos además que se responsabiliza únicamente al departamento de TI cuando se espera haya un trabajo integral en toda la empresa. A partir de estas conclusiones la investigadora realiza las recomendaciones pertinentes.

Es importante mencionar que pese a la antigüedad del estudio se consideró debido a la relevancia metodológica que tiene para esta investigación.

El segundo estudio, desarrollado por Solano (2020) se titula: Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica, investigación realizada para optar por el grado de licenciatura en Ingeniería Informática de la Universidad Latina de Costa Rica

Solano enfocó su investigación en la necesidad actual de las empresas de proteger la integridad, disponibilidad y confidencialidad de su información a través de normas, controles y políticas de seguridad. Menciona que "a pesar de no conocer el resultado, se pueden identificar las fallas en los procesos para que estos puedan remediarse y, posteriormente, se adapten a la situación que presenta la empresa" p. 29.

Fue una investigación de tipo cualitativo y exploratorio utilizando como sujetos de investigación a todo el personal de la empresa. La información se recopiló a través de cuestionarios y guías de observación. Solano concluye su investigación presentando un SGSI como acción ante las vulnerabilidades encontradas por la carencia de procedimientos y controles para proteger la información.

Finalmente, en el ámbito internacional, Guerra (2020) presenta su investigación: Sistema de Gestión para la Seguridad de la Información basado en metodología de identificación y análisis de riesgo en la Biblioteca de la Universidad de la Costa. Este estudio se desarrolló como su trabajo final de graduación en el 2020 para obtener el título de mágister en Gestión de Tecnologías de la Información y la Comunicación de la Universidad de la Costa, Barranquilla, Colombia.

Según Guerra, muchas empresas olvidan considerar entre sus activos la información, que es un elemento muy sensible al tráfico, espionaje y robo. Menciona a INCIBE (2016), que afirma:

> …éstas empresas conformadas por más de 300.000 cuentas de usuarios alrededor del mundo, han sufrido ciberataques generando como resultado el robo de información entre los cuales se destacan: números de tarjetas, cuentas bancarias, direcciones, correos electrónicos y contraseñas entre otros. P. 11.

Guerra realizó una investigación donde utilizó la metodología MAGERIT-OCTAVE. Se desarrolló sobre la base de documentos o revisión bibliográfica y un análisis de riesgos con información recopilada a través de entrevistas no estructuradas, lluvias de ideas, actividades colaborativas y registro de observación, dirigidas al personal del departamento de Sistemas y de Biblioteca.

Guerra encontró que la Biblioteca de la Costa cuenta con certificaciones, sin embargo, no se está cumpliendo con la responsabilidad de la mejora continua, lo que dejó en evidencia riesgos asociados en los procesos. No existe identificación de amenazas y vulnerabilidades, por lo tanto, no hay controles para futuros ataques.

Estas investigaciones aportan al objetivo de esta investigación, tanto desde sus propuestas metodológicas como de los resultados obtenidos, esperando poder incorporar acciones valiosas desde la experiencia en la puesta en práctica de las acciones planteadas.

Debido a lo anterior es que se realiza la necesidad de crear una implementación de un SGSI para el CUC, ya que se determinó que la institución no cuenta con políticas, procedimientos ni controles, por lo que se desea plantear una capa de seguridad que contenga lo anteriormente mencionado, para poder prevenir tanto amenazas internas como externas.

A partir de lo expuesto hasta aquí, el estado de la cuestión de un SGSI implica evaluar y analizar los riesgos, políticas, procedimientos, infraestructura tecnológica, conciencia y capacitación, y cumplimiento normativo en relación con la seguridad de la información dentro de una organización. Esta evaluación proporciona una visión general de la situación actual y permite identificar áreas de mejora y definir acciones para fortalecer la seguridad de la información.

Un SGSI muestra que existe una creciente conciencia sobre la importancia de la seguridad de la información y una mayor adopción de estos sistemas. Sin embargo, todavía hay un camino por recorrer para que todas las organizaciones cuenten con un SGSI completo y efectivo.

1.10. Problema

Hoy en día el avance tecnológico y la información han pasado por elementos muy importantes, pero a la vez muy sensible y vulnerable para los delitos informáticos. A partir de esto, se conoce que el CUC, no cuenta con un SGSI para poder proteger y administrar la información que maneja. Ante este contexto surge la pregunta problema: ¿cómo elaborar un plan de implementación de un SGSI para el CUC?

Capítulo II: Marco conceptual

2. Capítulo II: Marco conceptual

Este estudio pretende dar como producto una propuesta de un sistema de Gestión de Seguridad informática para el CUC, para ello se necesita una fundamentación teórica que respalde las ideas que sustentan la propuesta y así dar al lector un acercamiento más comprensible del estudio realizado. A continuación, se presenta el desarrollo de los conceptos y teorías más representativos que es importante comprender para iniciar la investigación propuesta.

2.1. Seguridad informática

Hoy en día el mundo se encuentra en una era tecnológica sumamente avanzada, como en la naturaleza las personas deben buscar estrategias para sobrevivir y adaptarse a las nuevas condiciones digitales que la sociedad impone para desarrollarse. Esto se convierte en posibilidades de competencia ante la nueva realidad, que aunado a la revolución tecnológica dejó también la pandemia del año 2020, situación que aceleró este contexto.

Es aquí donde entra al escenario la información, información sensible que manejan empresas e instituciones sobre sus procesos, clientes, estrategias, entre muchos otros. Esta información requiere estar segura, las personas necesitan saber que su información personal está resguardada, esto es la seguridad informática. Según EcuRed, al referirse a la seguridad, indique que “es un estado de cualquier tipo de información (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo”. (2020)

La seguridad se convierte en un servicio que las empresas dan a sus clientes, es tan importante que en la actualidad constituye un factor determinante que las personas consideran como determinante en la elección de un servicio o empresa, se trata del resguardo de información confidencial que esté garantizada en su disponibilidad e integridad; es decir, los tres pilares de la seguridad informática.

Toro (2018) define la disponibilidad como “la información deberá permanecer accesible a elementos autorizados”. A partir de esto, habrá usuarios que de manera previa y cuidadosa tendrán acceso a información de los clientes de su empresa, en el momento que la información esté accesible a un rango libre de usuarios, se habrá perdido este pilar de la seguridad.

Sobre la confidencialidad el mismo autor define la confidencialidad como “prevenir la divulgación no autorizada de la información sobre nuestra organización” (Toro, 2018). De la mano de la disponibilidad, la confidencialidad da a los

usuarios la confianza de que su información esté en las manos correctas, además, a la empresa el resguardo de que otras empresas tomen ventaja a partir de la información de sus clientes.

Finalmente, en cuanto a la integridad, Toro (2018) se refiere a información que "se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización", esto garantiza que no haya modificaciones o alteraciones en los datos e información suministrada por usuarios o propios de cada empresa.

A partir de estos aspectos debe iniciar sus estrategias de seguridad de la información, en primera instancia como prevención de ataques informáticos, en caso de que sea tarde, tomar las acciones frente a un posible ataque que ponga en riesgo la información de la empresa. Aquí radica la importancia de la seguridad informática, todas estas estrategias y herramientas que puedan dar confianza a partir de la protección tanto de los datos como del servicio. Esta consideración puede hacer la diferencia en una empresa.

2.2. Ataques informáticos

Tal como se mencionó líneas atrás, la seguridad informática tiene un único objetivo y es la lucha contra los delitos informáticos, por eso es importante referirse a ellos con parte del respaldo en este estudio. Un delito informático es la amenaza más grande a la que se encuentran expuestas las empresas, estos atentan contra los 3 pilares que anteriormente se definieron: confidencialidad, integridad y disponibilidad de la información.

Los delincuentes de la información o ciberdelincuentes utilizan diversos métodos para atacar a usuarios y empresas. El más conocido es la estafa, mediante este método el usuario se ve tentado a liberar información sensible que puede ser utilizada con un objetivo malicioso. Todos los días en los noticieros se menciona el aumento en los ataques cibernéticos y aún con más frecuencia los que tienen que ver con delitos informáticos, contraseñas e información detallada de tarjetas de crédito son la información más perseguida por los delincuentes, esto se respalda con investigaciones que encabezan titulares como "Delitos financieros encabezan la lista de ataques cibernéticos en Latinoamérica" (Prensario IT Latin America, 2023).

Una herramienta utilizada por los delincuentes es el correo electrónico y así lo confirma la empresa japonesa de ciberseguridad Trend Micro In que en un informe determinó que el email fue el principal instrumento de ataques cibernéticos en 2022:

> Trend Micro bloqueó más de 79.900 millones de amenazas en 2022 solo de correo electrónico, de las que 39,9 millones eran de alto riesgo y lograron pasar por alto los filtros nativos de los proveedores de 'email', tal y como se indica desde la plataforma Trend Micro Cloud App Security (CAS), que detecta los ataques que ya están en progreso y los intentos de infiltración de los delincuentes. (Elcomercio.pe, 2023).

Otro de los delitos más tradicionales es el uso de virus informáticos, según Fernández (2020) son "programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta", por otra parte Kaspersky (2018) los define como "programa de software malicioso que puede replicarse a sí mismo en ordenadores o a través de redes de ordenadores sin que te des cuenta de que el equipo está infectado", estos son dos ejemplos de definiciones que al final concluyen que un virus informático tiene la característica de camuflarse para hacerse pasar por un programa original o legítimo, una vez que ha ingresado en el sistema, puede borrar, alterar, pausar y clonar datos.

Por otra parte, existen también los Caballos de Troya o troyanos que tienen la misma característica del virus, pero se reproducen dentro de los equipos de los usuarios o empleados sin necesitar interactuar con la persona que maneja el equipo. Como es conocido para la mayoría de las personas que de alguna forma interactúan con algún aparato electrónico, existen los antivirus, que según EcuRed (2020), "constituyen una herramienta básica de la seguridad informática, que garantiza en principios la protección final de una estación de trabajo contra la infección por programas malignos". Sin embargo, los delitos informáticos podrían burlar estos sistemas.

Actualmente, se dice que muchas personas son vulnerables a los ataques informáticos, para eso los delincuentes se basan en la ingeniería social que Kaspersky (2018) plantea como "un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados" (s. p.). Con esto, la importancia de estrategias y herramientas para combatir la delincuencia informática debe ser prioridad en cualquier empresa, esto incluye al CUC, contexto donde se desarrolla esta investigación.

2.3 Sistemas de Gestión de Seguridad Informática (SGSI)

Tal y como se ha venido mencionando, los SGSI son marcos de trabajo que permiten a las organizaciones establecer, implementar, mantener y mejorar continuamente la seguridad de la información dentro de sus estructuras. Estos sistemas se basan en estándares reconocidos internacionalmente, como la norma ISO 27001, y proporcionan un enfoque sistemático y estructurado para gestionar los riesgos de seguridad de la información.

Un SGSI consta de varios elementos clave:

1. Política de seguridad de la información
2. Análisis y evaluación de riesgos
3. Controles de seguridad:
4. Procesos de gestión
5. Conciencia y capacitación:
6. Auditorías y certificación

Un SGSI es un marco de trabajo que permite a las organizaciones gestionar de manera efectiva la seguridad de la información. Proporciona un enfoque estructurado para identificar y mitigar los riesgos de seguridad, establecer controles adecuados, gestionar procesos y promover la conciencia y capacitación en seguridad de la información.

Capítulo III: Marco metodológico

3. Capítulo III: Marco metodológico

3.1. Tipo de investigación

El tipo de investigación de este proyecto es **aplicada**. Este tipo de investigación busca resolver un problema práctico específico, en este caso, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el Colegio Universitario de Cartago (CUC) basado en la norma ISO 27001.

3.2. Alcance investigativo

El alcance investigativo de este proyecto incluye:

Revisión bibliográfica: Análisis de la literatura existente sobre SGSI y la norma ISO 27001.

Evaluación de necesidades: Identificación de las necesidades específicas del Colegio Universitario de Cartago (CUC) en términos de seguridad de la información.

Desarrollo de propuesta: Diseño de un SGSI adaptado al contexto y necesidades del CUC, basado en la norma ISO 27001.

3.3. Enfoque

El enfoque de la investigación es **cualitativo**, ya que se centra en el análisis de las necesidades de la institución y en el desarrollo de una propuesta que se ajuste a dichas necesidades, utilizando la norma ISO 27001 como referencia. Este enfoque permite una comprensión profunda y detallada del contexto y de los requisitos específicos del CUC.

3.4. Diseño

Las empresas al momento de implementar un SGSI, debe estar enfocada a sus procesos, la norma ISO 27001 implementa el ciclo PHVA (Planear – Hacer, Verificar - Actuar), permitiendo definir los procesos que son afines en el SGSI.

Se procura establecer una metodología general para la ejecución de la propuesta inicial del proyecto, haciendo énfasis a la norma ISO27001, en la unidad de Tecnología Informática del CUC Colegio Universitario de Cartago, permitiendo así realizar un diseño basado en dicha norma.

Para desarrollar este proyecto según los objetivos planteados, se proponen 4 etapas que permitirán establecer, diseñar un SGSI en base a la Norma ISO 27001 para la institución

Etapa 1. Análisis de la situación actual del CUC

Es indispensable realizar un estudio y análisis del estado actual de la seguridad de la información en la unidad de tecnología informática de la institución, para identificar si se cuenta con los procesos, políticas, documentación, entre otras cosas. Que son factores necesarios en la seguridad de la información.

Los procesos para realizar esta actividad son:

- Consultar la documentación existente en el área de informática, respecto a la seguridad de la información.
- Poder indagar sobre los procesos, políticas y procedimientos existentes en la protección de la información.

Etapa 2. Análisis de riesgo

Para realizar un análisis de riesgo, se debe identificar y documentar el inventario de activos existente, con base a los dominios puntualizados en la norma ISO/IEC 27001, se identificarán y aplicarán en la evaluación de riesgos

Los procesos para realizar esta actividad son:

- Identificar, validar, complementar y clasificar los activos del área de TI del CUC
- Determinar el estado actual de la infraestructura tecnológica de la institución
- Realizar el análisis de riesgo según los activos identificados.

Etapa 3. Aplicabilidad bajo la normativa ISO 27001.

Para determinar la aplicabilidad, se realizará luego del análisis de riesgos desarrollado en la etapa 2, el cual se desarrolla con el fin de identificar y analizar los riesgos que fueron encontrados

El desarrollo de la declaración, será donde se registran los controles de seguridad que son aplicables según el tratamiento de riesgos, usando como referencia el Anexo A del estándar ISO 27001 que contiene los controles de seguridad.

Los procesos para realizar esta actividad son:

- Identificar el formato adecuado para la realización de la declaración en la institución.
- Seleccionar y establecer los controles necesarios según la declaración de aplicabilidad, esta selección debe ser según la evaluación de riesgos, requisitos legales, obligaciones adquiridas, requisitos nuevos de la entidad, mejores prácticas, etc.

Etapa 4. Políticas de seguridad de la información para el CUC

Con base a los resultados en el análisis de la situación actual y de riesgos de la entidad, realizado en las etapas anteriores y validando las necesidades que esta requiere se procede a:

- Realizar un análisis de seguridad del estado actual de la entidad con respecto a los requisitos de la norma ISO 27001
- Proponer y documentar las políticas sugeridas para la entidad.

3.5. Población y muestreo

Para esta investigación la población está definida por todos los usuarios de la información contenida en los archivos del CUC. Al ser un estudio que no llega a la etapa de la implementación no se estableció una muestra, sin embargo, la propuesta está planteada a ser aplicada en un mediano plazo.

Capítulo IV: Análisis de la situación

Para poder implementar un SGSI (SGSI) en el Colegio Universitario de Cartago, este no depende solamente del grupo o de la unidad de TI, sino del compromiso y de la cultura organizacional de la institución, permitiendo así la protección y el resguardo de la información.

A continuación se presenta la situación actual del CUC desde de diferentes perspectivas

a. Acceso a la información

Las personas que laboran en el CUC tienen acceso a la información necesaria que requieran en el desarrollo de las actividades laborales. Cada personal nuevo en la institución es reportado a la unidad de TI para que se le otorgue el acceso a la información que es autorizado por la oficina de recursos humanos según el área en donde vaya a elaborar.

b. Seguridad de la información

Todos los funcionarios son responsables de la información que manejan y deben protegerla, para evitar pérdidas, accesos no autorizados, exposición y uso indebido de esta, para esto el departamento de relaciones públicas y comunicaciones y la unidad de tecnología informática desarrollan mecanismos de divulgación que permita sensibilizar a los usuarios de la importancia de la seguridad informática y las responsabilidades de estas, dejando claro que no es solo de la oficina de TI

Toda la información de la entidad, no puede ser vendida, transferida o intercambiada con terceras personas bajo ningún pretexto o propósito. La información se clasifica en diferentes categorías, como lo es confidencia, privada, reservada, pública entre otros.

Los datos o la información son considerados como uno de los activos más importantes y sensibles de la entidad, por esto se debe garantizar la protección de esta, y su uso será solamente de acuerdo a las necesidades y propósitos de la entidad.

c. **Seguridad servicios informáticos**

El correo electrónico es y debe ser usado solo para las funciones propias de la institución. EL CUC se reserva el derecho de acceder y revelar los mensajes enviados por el correo electrónico institucional para cualquier propósito, en efecto la entidad se encarga de realizar auditorías y revisiones de estos ya sea de forma directa o por medios de terceros.

Todo el personal de la institución que se les disponga acceso a internet a través de los recursos informáticos, deberán aceptar, acatar y cumplir las políticas y prácticas de uso de internet que se hallan instaurados por la unidad de TI

El departamento de comunicaciones de la institución tiene a cargo el funcionamiento del portal WEB, todos los trámites de publicaciones o cambios en este, se realizarán por medio de este departamento para este fin, la supervisión de la información que se publique o maneja en la web, deberá ser aprobada por el jefe de cada departamento

Los mecanismos de control de los sistemas de información, para garantizar la integridad, confidencialidad, autenticidad y aceptación son dispuestos desde la jefatura e infraestructura de la oficina de TI

El software que comprometa o que se requiera por los usuarios, será administrado y solicitado única y exclusivamente al área de soporte de informática

d. Seguridad en recursos informáticos

Administración de usuarios: Menciona cómo son creadas las claves de acceso a los recursos informáticos, indica los parámetros de qué longitud mínima debe ser las contraseñas, el periodo de cambio de la clave y la vigencia de esta, entre otras.

El acceso a los sistemas de información de la institución, tienen un control por medios de códigos de identificación y palabras clave de las contraseñas de cada usuario.

Las contraseñas o claves asignadas al personal de la institución, es responsabilidad de cada uno de ellos y estas no deben ser reveladas a terceros, siendo responsables de lo que pueda suceder si es divulgada.

La información que se encuentra en la base de datos, la cual es sensible, crítica y valiosa, cuenta con controles de acceso y *backups*, garantizando que no sea accedida, modificada o eliminada por personal no autorizado.

La información en la institución se encuentra clasificada o salvaguardada, es responsabilidad de los funcionarios velar por la integridad, confidencialidad, disponibilidad, accesibilidad y confiabilidad de la información que maneja.

En la institución se establece que toda la información generada en las computadoras del CUC, es propiedad de este.

Los usuarios por ningún motivo deben manipular técnicamente el software o hardware asignado, así sospechen de algún fallo, este debe ser informado al área o persona de soporte.

Los ambientes de pruebas y producción son separados y su operación, control y seguridad son independientes.

e. Actualización de hardware

Para realizar cualquier cambio en los equipos de cómputo se debe tener una evaluación técnica previa por parte del personal de soporte de la institución y posteriormente la autorización del área responsable para posteriormente continuar con el cambio.

Cuando se requiere una apertura de un equipo, solo podrá realizarse por el personal autorizado, sea interno o externo a la entidad.

f. Almacenamiento y respaldo

Se cuenta con una estrategia para realizar los *backups* de la información de las bases de datos y de los discos críticos de la institución, se desarrolla de manera semanal por medio del proveedor adjudicado que tiene a cargo el servidor institucional, este esquema incluye almacenamientos de discos externos con verificación constante de restauración.

La información crítica es almacenada en medios físicos, tiene control de acceso y custodia, evitando pérdidas o accesos no autorizados.

g. Contingencia

Los servicios informáticos que se prestan en el CUC cuentan con un plan de contingencia en caso de inoperatividad de servidores, bases de datos, servidores de seguridad, aplicaciones, equipos de comunicaciones, entre otros, con el fin de mantener la operación en la entidad.

h. Seguridad física

El CUC cuenta con un *datacenter* con acceso restringido, al cual solo puede acceder el personal autorizado.

Los centros de cómputo cuentan con elementos de control de incendios, alarmas, entre otros. De igual forma cuentan con zonas demarcadas como de circulación o restringidas.

La zona donde se encuentran los *racks*, cajas de paso, tableros, entre otros, se cataloga como zona de alto riesgo y está limitado el acceso.

Los equipos portátiles, modem, equipos de comunicación se registran al ingreso y a la salida, estos no salen de la institución al menos que tengan una autorización previa por parte del jefe de área.

Los equipos de cómputo no se mueven o se reubican si no se tiene una autorización previa por el área encargada.

Las personas ajenas que no tengan relación con la institución, no pueden acceder a los recursos informáticos de esta.

Análisis de brecha contra las buenas prácticas

Este análisis corresponde a la evaluación de los niveles de cumplimiento, madurez de los procesos, riesgos y situación evidenciada en cada una de las áreas: En esta sección se desarrollará el reporte sobre el estado de preparación del SGSI, en el cual se incluye el resumen de calificación obtenida de niveles de madurez, porcentaje de cumplimiento de los controles, análisis del contexto y las brechas existentes en el sistema.

La matriz de cumplimiento está basada en preguntas abiertas que están alineadas a los requerimientos del ISO/IEC 27001 y a identificar los niveles de madurez de los requerimientos y controles del ISO 27001.

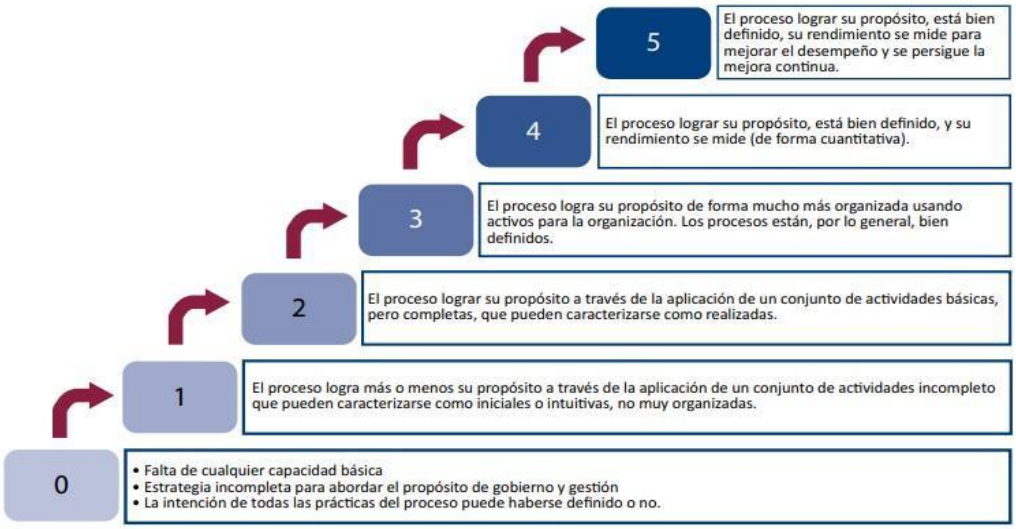
Nivel de Madurez y Cumplimiento

El Marco de Gobierno y Gestión de COBIT 2019 describe el nivel de madurez o capacidad de 18 objetivos que fueron analizados durante las sesiones de evaluación de gobierno y gestión de TI llevadas a cabo dentro del CUC.

Nivel de Capacidad

Cada uno de los objetivos que conforman el Marco COBIT 2019 están conformados por distintas actividades; cada una de estas actividades tiene asignados diferentes niveles de capacidad, permitiendo una clara definición acerca de cómo alcanzar dicho nivel. Los niveles de capacidad están respaldados por el Modelo de Madurez de la Capacidad (CMMI), basado en una escala de 0 a 5. El nivel de capacidad es una medida de lo bien que un proceso se ha implementado. A continuación, en la siguiente figura se detalla cada uno de los niveles con su respectiva descripción.

Figura 2 NIveles de capacidad



Nota*:* Información Obtenida del Marco de Referencia COBIT® 2019: Objetivos De Gobierno y Gestión.

Nivel de Cumplimiento

El nivel de Cumplimiento se encarga de medir si la institución cumple o no cumple con cada una de las actividades que conforman los objetivos del Marco de Gobierno y Gestión de Tecnologías de la Información según lo estipulado por COBIT 2019 y lo recomendado por el Ministerio de Ciencia, Innovación y Tecnologías y Telecomunicaciones (MICITT), esto servirá para llegar a un puntaje que refleje el cumplimiento actual de la institución.

Por otra parte, el nivel de cumplimiento se obtiene de la evaluación de los cuarenta objetivos de COBIT2019 que se realizó en conjunto con la dirección de TI, Planificación y Auditoría en sesiones planificadas, para ir verificando el nivel actual que posee la institución.

Resultados de la Evaluación

A continuación, se describen los resultados de la evaluación por cada uno de los componentes que integran el Marco de Gestión de Tecnologías de la Información según el Ministerio de Ciencia, Innovación y Tecnologías y Telecomunicaciones (MICITT).

Gestión de TI

APO01 - Gestionar el Marco de Gestión de TI

El propósito del objetivo APO01 es brindar un enfoque del marco de gestión de TI consistente para permitir que se alcancen los requisitos de gobierno institucional, con cobertura de componentes de gobierno, es decir, los procesos de gestión, las estructuras organizativas, los roles y las responsabilidades, las actividades confiables y repetibles, los elementos de información, las políticas y procedimientos, las habilidades y las competencias, la cultura y el comportamiento, y los servicios, infraestructura y aplicaciones.

Figura 3. APO01 Gestionar el Marco de Gestión de TI.

Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 25,76% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
APO01.01 DISEÑAR EL SISTEMA DE GESTIÓN PARA LA TI DE LA INSTITUCIÓN	
Hallazgo o avance	***Recomendación***
El CUC se encuentra en el proceso de desarrollo de su Marco de Gobierno y Gestión de I&T, sin embargo, el proceso de diseño del Sistema de Gobierno aplicando los Factores de Diseño y la cascada de metas de COBIT no ha sido desarrollado; por lo tanto, no es posible determinar los objetivos de gobierno y de gestión prioritarios.	Documentar una metodología de gestión de I&T la cual incluya el proceso de implementación del sistema de gobierno, esta metodología, debe abordar el ajuste de los 7 componentes del mismo.
APO01.02 GESTIONAR LA COMUNICACIÓN DE OBJETIVOS, DIRECCIÓN Y DECISIONES TOMADAS	
La unidad de TI realiza diversos informes durante el año, estos responden a la ejecución presupuestaria y avance de los proyectos y metas definidos para esta; no obstante, estas comunicaciones no responden a una identificación de partes interesadas y sus necesidades de información.	Desarrollar un Plan de Comunicaciones asociados al proceso de implementación del Marco de Gobierno y Gestión de I&T el cual establezca las reglas básicas de comunicación basado en las necesidades de comunicación de las partes interesadas, este plan podría incluir los siguientes elementos: tipos de informes que debe presentar TI, frecuencia, canales de comunicación y a quien deben ir dirigidos.
APO01.03 GESTIONAR LA IMPLEMENTACIÓN DE PROCESOS (PARA RESPALDAR LA CONSECUCIÓN DE OBJETIVOS DE GOBIERNO Y GESTIÓN)	
La institución ha realizado la contratación de una empresa consultora para determinar el nivel de cumplimiento de los procesos asociados a los objetivos de gobierno y gestión para posteriormente, desarrollar una hoja de ruta que permita cerrar las brechas entre el modelo actual y el modelo objetivo.	**Ninguna**

APO01.04 DEFINIR E IMPLEMENTARLAS	
Hallazgo o avance	***Recomendación***
Actualmente se posee una estructura organizacional formal y aprobada por MIDEPLAN, publicada en la página web de la institución, donde se establecen las unidades y departamentos.	Se recomienda realizar un análisis de todas las estructuras organizativas propuestas por COBIT y su estado actual en la institución, con el propósito de determinar las brechas entre las estructuras actuales y las estructuras sugeridas. Posteriormente, basado en las capacidades de la institución realizar los ajustes requeridos para cerrar las brechas identificadas.
APO01.05 ESTABLECER ROLES Y RESPONSABILIDADES	
Actualmente se posee una estructura organizacional formal y aprobada por la alta dirección, publicada en la página web de la Institución, donde se establecen las unidades y departamentos; sin embargo, la unidad de Tecnología Informática no posee unidades adscritas y se mantiene como unidad y no departamento.	Valorar la transición de la Unidad de Tecnología Informática a departamento, de modo que se encuentra posicionada como un socio estratégico y pueda apoyar la toma de decisiones de una manera más oportuna.
APO01.07 - DEFINIR LA PROPIEDAD DE LA INFORMACIÓN (DATOS) Y DEL SISTEMA DE INFORMACIÓN	
Actualmente la institución no posee una metodología para la clasificación de la información, del mismo modo, no se poseen activos de información identificados con sus respectivos dueños y custodios.	**1.**Desarrollar un inventario de activos de información el cual establezca todos los activos de información, sus dueños, custodios, medios de soporte, ubicación, plazo de retención, criticidad y requisitos especiales asociados al uso de estos como requisitos legales o regulatorios. (esto puede ser desarrollado como parte del objetivo DSS05 Gestionar los Servicios de Seguridad) 2. Desarrollar un Metodología de Clasificación y Etiquetado de la información la cual establezca los tipos de información, los tipos de etiquetas y los mecanismos para etiquetar y clasificar. (esto puede ser desarrollado como parte del objetivo DSS05 Gestionar los Servicios de Seguridad)

APO01.08 - DEFINIR LAS HABILIDADES Y COMPETENCIAS OBJETIVO	
Hallazgo o avance	***Recomendación***
1. La Institución, en su Manual de Puestos define los requisitos de habilidades y competencias requeridos para desempeñar el puesto, sin embargo, estos carecen de la profundidad requerida para abordar los nuevos requisitos asociados al Marco de Gobierno y Gestión de I&T. **2.** El área de Recursos Humanos, de manera anual genera un Plan de Capacitaciones el cual está sujeto a las capacidades presupuestarias de la institución.	**1.** Desarrollar una matriz de habilidades actuales y requeridas, asociadas a la operación del Marco de Gobierno y Gestión de I&T, con el propósito de identificar las brechas entre las habilidades actuales y las habilidades requeridas. **2.** Desarrollar un Plan de Capacitaciones basado en las brechas previamente identificadas, este debe incluir las capacitaciones a recibir, los recursos que las recibirán y los mecanismos para validar que el conocimiento es obtenido y aplicado; priorizar aquellas capacitaciones que permitan atender puntos de dolor actuales y procesos no definidos. Este plan podría incluir áreas de conocimiento como, por ejemplo: Gestión de Seguridad de la Información, Gestión de Proyectos, Gestión de Servicios de TI, Gestión de Riesgos, Gestión de Calidad, Gestión de Datos, entre otros.
APO01. 09 - DEFINIR Y COMUNICAR POLÍTICAS Y PROCEDIMIENTOS	
1. La institución ha desarrollado algunos documentos internos para la operación de los procesos de negocio y de TI, sin embargo, debido al nuevo proceso de implementación del Marco de Gobierno y Gestión de I&T se deben desarrollar documentos asociados a componentes del marco que no habían sido identificados, como por ejemplo Seguridad, Calidad, Continuidad, Privacidad, Datos, Disponibilidad, Capacidad, entre otros. **2.** En base a la revisión documental, no se identifican revisiones periódicas a la documentación con el propósito de asegurar que esta se encuentre actualizada.	1. Recopilar la documentación requerida para operar los diferentes objetivos de gobierno y gestión, esto puede incluir el desarrollo de políticas, procedimientos, formularios, herramientas, directrices, entre otros. 2. Establecer una directriz de actualización anual de toda la documentación.

APO01. 10 - DEFINIR E IMPLEMENTAR LA INFRAESTRUCTURA, SERVICIOS Y APLICACIONES PARA RESPALDAR EL SISTEMA DE GOBIERNO Y GESTIÓN	
El área de TIC y la institución en general posee diversos sistemas de información que les apoyan en la operación de los procesos de negocio, como por ejemplo el proyecto de implementación de la Mesa de Ayuda ARANDA el cual está en desarrollo; sin embargo, debido a que se encuentran en proceso de implementación no se han identificado posibles sistemas que apoyen la automatización de objetivos de gobierno y gestión.	Desarrollar una matriz de los objetivos de gobierno y gestión y posibles herramientas (sistemas de información) que permitirán la optimización y automatización de estos.
APO01.11 - GESTIONAR LA MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE TI	
Debido a que el Marco de Gobierno y Gestión está en desarrollo este aún no ha es evaluado para determinar su rendimiento y aplicar mejora continua, sin embargo, el área de TIC y las demás áreas de negocio realizan actividades de mejora continua periódica. No obstante, estas no se documentan.	**1.** Desarrollar un procedimiento para la Gestión de la Mejora Continua, que permita documentar y registrar todas las actividades desarrolladas como parte del ciclo de la mejora continua. **2.** Una vez que la primera iteración de implementación del marco haya finalizado, se recomienda realizar evaluaciones del desempeño para determinar componentes obsoletos y oportunidades de mejora.

APO09 - Gestionar los Acuerdos de Servicios

El propósito del objetivo APO09 es asegurarse que los productos, servicios y niveles de servicio de TI satisfagan las necesidades actuales y futuras de la institución.

Figura 4. APO09 Gestionar los acuerdos de servicio.

Nota: elaboración propia

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 24,92% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
APO09.01 - IDENTIFICAR LOS SERVICIOS DE TI	
Hallazgo o Avance	**Recomendación**
1. El área de TIC mediante el documento "CATALOGO DE SERVICIOS TI_v1" ha desarrollado su catálogo de servicios de TI el cual identifica todos los servicios, las ofertas de servicios, los canales de contacto, la prioridad, el impacto y otra serie de componentes asociados al servicio; no obstante, este fue un esfuerzo realizado unilateralmente por el área de TIC por lo que no se analizaron actividades de negocio para determinar la compatibilidad de los requerimientos de este con la oferta de servicios de TI. 2. Debido a la ausencia de un Portafolio de Servicios de TIC, no se identifica que se realicen revisiones periódicas a este u otro portafolio.	**1.** Documentar una metodología de gestión de servicios de TI, la cual aborde todo el ciclo de vida del servicio y posteriormente de los niveles de servicio. **2.** Actualizar el catálogo de servicios de TI para que incluya una evaluación de las actividades de negocio. Esta evaluación debe identificar los requerimientos de los clientes y asegurar que la oferta de servicios de TI cumpla con estos requerimientos. **3.** Desarrollar un Portafolio de Servicios de TI, el cual incluya todos los servicios; incluyendo aquellos en desarrollo y aquellos retirados. **4.** Se recomienda desarrollar fichas de servicio para cada uno de los servicios presentes en el portafolio, esto permitirá identificar todos los componentes de los servicios de TI y su oferta de valor. **5.** Documentar procedimientos operativos para la gestión del portafolio de servicios de TI. (crear, actualizar, retirar).

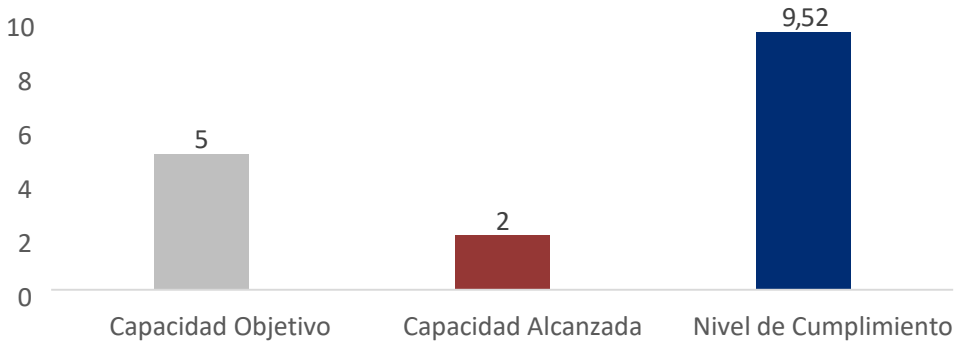
APO09.02 - CATALOGAR LOS SERVICI OS HABILITADOS POR TI	
Hallazgo o Avance	**Recomendación**
1. En el documento "CATALOGO DE SERVICIOS TI_v1" se establece la categorización de los servicios en 4 tipos los cuales se detallan a continuación: a. Aplicaciones de Negocio. b. Servicios de Telecomunicaciones. c. Servicio de soporte a Operaciones. d. Servicio de soporte a Hardware. 2. Debido a la ausencia de la figura del Gestor de Relaciones, no es posible asegurar que se le comunican las actualizaciones del portafolio o catálogo.	Incluir dentro del procedimiento la comunicación de todos los cambios al portafolio a través de la figura del Gestor de Relaciones.
APO09.03 - DEFINIR Y PREPARAR ACUERDOS DE SERVICIO	
A pesar de que dentro del documento "CATALOGO DE SERVICIOS TI_v1" se definen algunos niveles de servicios, estos al ser desarrollados unilateralmente no representan un Acuerdo de Nivel de Servicio (SLA). Debido a lo anterior, no es posible asegurar que se realicen borradores de SLA para posteriormente finalizarlos con el cliente del servicio. Actualmente, el área de TIC no posee acuerdos de nivel operativo (OLA). Dentro de los contratos de servicio, el área de TIC solicita algunos requisitos asociados a los niveles de servicio que estos deben	**1.** Documentar un procedimiento para gestionar los niveles de servicio de TI. **2.** Desarrollar Acuerdos de Nivel de Servicio (SLA) basados en los requisitos del negocio, estos SLA podrían incluir los siguientes elementos: a. Servicios asociados b. Horario de operación c. Horario de Soporte d. Horario de Mantenimiento e. Tiempos de respuesta f. Canales de Comunicación g. Requisitos de disponibilidad, capacidad, seguridad, continuidad, privacidad, entre otros.

cumplir; sin embargo, estos no tienen relación con los niveles de servicio actuales.	**3.** Desarrollar los acuerdos de nivel operativo (OLA) requeridos para respaldar los Niveles de Servicio definidos en los Acuerdos de Nivel de Servicio (SLA), estos acuerdos deberán incluir las diferentes partes involucradas en la prestación del servicio y las responsabilidades de cada.
APO09.04 - MONITORIZAR Y REPORTAR LOS NIVELES DE SERVICIO	
Hallazgo o Avance	**Recomendación**
1. Actualmente, el área de TIC realiza actividades operativas con el propósito de mantener los diferentes servicios operativos; no obstante, esto no está directamente alineado al cumplimiento de los niveles de servicio (SLA). **2.** Debido a que los niveles de servicio no son monitoreados, no es posible desarrollar planes de acción en caso de incumplimiento.	**1.** Incluir dentro del procedimiento de gestión de niveles de servicio, la monitorización y reporte de los niveles de servicio; este procedimiento debe incluir el desarrollo de acciones correctivas en caso de no cumplir los niveles de servicio acordados.
APO09.05 - REVISAR LOS ACUERDOS Y LOS CONTRATOS DE SERVICIO	
1. Debido a la ausencia de acuerdos de nivel de servicio (SLA), estos no son revisados y actualizados. **2.** Debido a lo anterior, los Acuerdos de Nivel Operativo (OLA) y Contratos de Servicio (UC) tampoco son revisados y actualizados en caso de ser requerido.	**1.** Incluir dentro del procedimiento de gestión de niveles de servicio, la revisión y actualización de los Acuerdos de Nivel de Servicio, Acuerdos de Nivel Operativo y Contratos de Servicio periódicamente; esto con el propósito de asegurar la validez de estos y valorar la necesidad de cambios y/o actualizaciones.

DSS02 -Gestionar las Peticiones y los Incidentes De Servicio

El propósito del objetivo DSS02 es lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Además de evaluar el impacto de los cambios, hacer frente a los incidentes del servicio y resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes.

Figura 5. DSS02 Gestionar las peticiones y los incidentes del servicio.



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 2 y el nivel de cumplimiento es de 9,52% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
DSS02.01 - DEFINIR ESQUEMAS DE CLASIFICACIÓN PARA INCIDENTES Y PETICIONES DE SERVICIO	
Hallazgo o Avance	***Recomendación***
1. Actualmente la unidad de TIC se encuentra en el proceso de implementación de la Mesa de Ayuda ARANDA; no obstante, este proyecto aún está en desarrollo por lo que la gestión de peticiones e incidentes es realizada de manera empírica a través de correo electrónico. Debido a lo anterior, la institución no posee esquemas de priorización y clasificación, procedimientos de escalamiento ni fuentes de conocimiento para las peticiones e incidentes de servicio. Adicionalmente, no se identifican niveles de atención o escalamiento dentro de la unidad de TIC.	**1.** Documentar una metodología de gestión de peticiones e incidentes la cual establezca los siguientes elementos: a. Los canales de registro y comunicación. b. Los esquemas de priorización y clasificación. c. Los niveles de atención y escalamiento. d. Las fuentes de conocimiento sobre peticiones e incidentes. **2.** Se recomienda documentar un procedimiento para la gestión de peticiones e incidentes que permita ejecutar lo establecido en la metodología.
DSS02.02 - REGISTRAR, CLASIFICAR Y PRIORIZAR LAS PETICIONES E INCIDENTES	
1. Todas las peticiones e incidentes son gestionados a través de correos o llamadas telefónicas, por lo que no es posible asegurar que exista un registro único con toda la información relevante. 2. Derivado de lo anterior, y debido a la ausencia de datos estandarizados no se desarrollan análisis de tendencias. 3. Adicionalmente, no se identifican mecanismos para la priorización ni tipificación de las peticiones e incidentes.	**1.** Se recomienda incluir dentro de la metodología los siguientes elementos: a. La priorización de peticiones e incidentes basado en los posibles Acuerdos de Nivel de Servicio (SLA) asociados. b. El desarrollo de análisis de tendencias utilizando como insumo los registros de peticiones e incidentes.

DSS02.02 - REGISTRAR, CLASIFICAR Y PRIORIZAR LAS PETICIONES E INCIDENTES	
Hallazgo o Avance	***Recomendación***
1. Todas las peticiones e incidentes son gestionados a través de correos o llamadas telefónicas, por lo que no es posible asegurar que exista un registro único con toda la información relevante. Derivado de lo anterior, y debido a la ausencia de datos estandarizados no se desarrollan análisis de tendencias. **2.** Adicionalmente, no se identifican mecanismos para la priorización ni tipificación de las peticiones e incidentes. **3.**	**1.** Se recomienda incluir dentro de la metodología los siguientes elementos: c. La priorización de peticiones e incidentes basado en los posibles Acuerdos de Nivel de Servicio (SLA) asociados. d. El desarrollo de análisis de tendencias utilizando como insumo los registros de peticiones e incidentes.

DSS02.03 - VERIFICAR, APROBAR Y RESOLVER PETICIONES DE SERVICIO	
1. que deben ser registradas u aprobadas únicamente por un jefe de departamento, sin embargo, no se poseen documentación al respecto. La institución no posee un proceso de gestión de cambios por lo que no es posible aprobar los cambios estándar asociados.	**1.** Se recomienda incluir dentro de la metodología los siguientes elementos: a. La confirmación de los niveles de autoridad requeridos para peticiones que así lo requieran (por ejemplo, solicitudes de permisos y/o ejecución de compras) b. La ejecución de cambios de acuerdos al proceso de gestión de cambios cuando este sea necesario.

DSS02.04 - INVESTIGAR, DIAGNOSTICAR Y ASIGNAR INCIDENTES	
Hallazgo o Avance	***Recomendación***
1. No se identifica el registro de la causa raíz de los incidentes, así como tampoco su relación con fuentes de conocimientos como errores conocidos debido a la ausencia de estos. **2.** Dado que no existe un registro de errores conocidos, no se identifican los criterios requeridos para el registro de estos. **3.** La jefatura de la unidad de TIC asigna las peticiones e incidentes a los agentes que poseen mayor conocimiento en el tema y lo escalan a nivel jerárquico cuando es requerido.	**1.** Incluir dentro de la metodología los siguientes elementos: a. La identificación de la causa raíz de los incidentes utilizando como insumo el registro de errores conocidos o incidentes anteriores. b. La asignación del incidente a grupos específicos de agentes en caso de ser requerido. c. El registro de un nuevo error conocido en caso de que esto aplique.

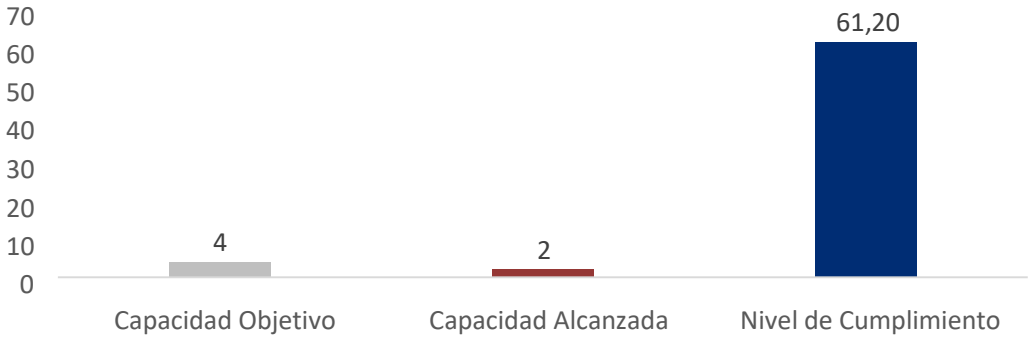
DSS02.05 – RESOLVER Y RECUPERARSE DE LOS INCIDENTES	
Hallazgo o Avance	***Recomendación***
1. Debido a la ausencia de una herramienta que apoye la gestión, no se poseen registros asociados a soluciones temporales o permanentes y los conocimientos asociados a estos; no obstante, los técnicos de la unidad de TIC resuelven los incidentes según sus posibilidades y conocimientos.	**1.** Se recomienda incluir dentro de la metodología los siguientes elementos: el uso y registro de soluciones temporales en caso de que no sea posible establecer una solución permanente.
DSS02.06 - CERRAR LAS PETICIONES DE SERVICIO Y LOS INCIDENTES	
1. Debido a la ausencia de una herramienta que apoye la gestión, no se realizan cierres de las peticiones e incidentes de manera formal. **2.** Del mismo modo, no es posible asegurar que se confirma con los usuarios afectados la correcta atención de las peticiones e incidentes.	Incluir dentro de la metodología los siguientes elementos: a. El cierre de las peticiones e incidentes una vez estas han sido atendidas. b. La comprobación con los usuarios afectados que la petición se ha cumplido de forma satisfactoria o el incidente se ha resuelto de forma satisfactoria dentro de un plazo de tiempo acordado/aceptable.
DSS02.07 - HACER SEGUIMIENTO AL ESTADO Y PRODUCIR INFORMES	
1. Debido a la ausencia de una herramienta que apoye la gestión, no se realiza un seguimiento a escalamientos o incidentes no atendidos. **2.** A su vez, no se poseen informes asociados a la atención de peticiones o incidentes por lo que esta no es utilizada para la mejora continua de los servicios de TI.	Incluir dentro de la metodología los siguientes elementos: a. El seguimiento de las atenciones a incidentes y peticiones dentro de los límites acordados en los Acuerdos de Nivel de Servicio (SLA). b. La creación y remisión de informes periódicos referente a la atención de peticiones e incidentes.

Planificación Tecnológica Institucional

APO02 - Gestionar la Estrategia

El propósito del objetivo APO02 es apoyar la estrategia de transformación digital de la institución y proporcionar el valor deseado a través de una hoja de ruta con cambios incrementales. Además de usar un enfoque holístico en cuanto a TI, asegurando que cada iniciativa esté claramente conectada con una estrategia global para habilitar el cambio en todos los diversos aspectos de los canales y procesos a los datos, cultura, habilidades, modelo operativo e incentivos.

Figura 6. APO02 Gestionar la estrategia.



Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 2 y el nivel de cumplimiento es de 61,20% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, no está completamente documentada.

Estado General Del Proceso	
APO02.01 - COMPRENDER EL CONTEXTO Y LA DIRECCIÓN DE LA INSTITUCIÓN	
Hallazgo o Avance	***Recomendación***
1. La unidad de TIC posee un documento llamado "PETIC Final 2019-2023 – CUC" donde se refleja la estrategia de I&T. **2.** En el documento mencionado anteriormente existe un apartado llamado "Análisis de Negocio" en el cual se realiza un reconocimiento extenso de todas las diversas áreas de la institución incluyendo las "Prioridades de Negocio" y los "Requerimientos Globales del Negocio".	Documentar un procedimiento para el desarrollo del PETIC, que permita alinear el PETIC con la estrategia de transformación digital de la institución.

APO02.02 - EVALUAR LAS CAPACIDADES, RENDIMIENTO Y MADUREZ DIGITAL ACTUAL DE LA INSTITUCIÓN	
1. En el documento mencionado anteriormente, existe un apartado denominado "Situación actual de TI" en la cual se explora a profundidad las capacidades del equipo de TI, mostrando sus procesos, funcionarios, sistemas e infraestructura. **2.** A pesar de lo mencionado anteriormente, no se identifica una evaluación o declaración sobre el nivel de madurez actual de la institución.	Incluir dentro del Plan Estratégico de Tecnologías de Información y Comunicación (PETIC) un análisis sobre el nivel de madurez actual de la institución.

APO02.03 -DEFINIR LAS CAPACIDA DES DIGITALES OBJETIVO	
Hallazgo o Avance	***Recomendación***
1. A lo largo del documento mencionado previamente, se definen diversos componentes objetivos a los cuales se proyecta llegar a manera de "Recomendaciones" para subsanar las brechas identificadas en los diferentes análisis realizados. 2. Adicionalmente, se define un Cuadro de Mando Integral del cual se deriva una serie de iniciativas que permitirán el cumplimiento de este; sin embargo, estas iniciativas carecen de estrategias o metodologías asociadas que permitan su logro (Agile, Scrum, Waterfall, Bimodal IT).	Asociar a las distintas iniciativas las posibles estrategias y metodologías que pudiesen apoyar en el desarrollo de estas.

APO02.04 LLEVAR A CABO UN ANÁLISIS DE BRECHAS	
Hallazgo o Avance	***Recomendación***
1. A lo largo del documento mencionado previamente, se identifican las múltiples brechas resultado de las situaciones deseadas en varias dimensiones (personal, infraestructura, sistemas); sin embargo, debido a la ausencia de una arquitectura empresarial, estas brechas no están alineadas con los dominios del negocio, la información, los datos, las aplicaciones y la tecnología. **2.** Adicionalmente, no es posible identificar las implicaciones de alto nivel de todas las brechas, el valor de los posibles cambios en las capacidades de I&T y del negocio, los servicios y la arquitectura institucional de TI, así como las implicaciones de no lograr ningún cambio.	**1.** Incluir dentro del PETIC, los posibles cambios en la Arquitectura Empresarial una vez esta haya sido desarrollada. **2.** Agregar al PETIC las implicaciones de alto nivel de todas las brechas acompañadas, las implicaciones de no lograr ningún cambio y el valor obtenido a partir de los cambios propuestos.
APO02.05- DEFINIR EL PLAN ESTRATÉGICO Y EL MAPA DE RUTA	
Posteriormente, se definen algunos proyectos de TI con sus respectivos casos de negocio y hoja de ruta; sin embargo, estos no reflejan la presencia de portafolios o programas con sus respectivas dependencias, solapamientos o sinergias. Adicionalmente, no se identifica que el Plan Estratégico de TI sea apoyado y aprobado formalmente por parte de los interesados.	1. Incluir dentro del PETIC, los diferentes proyectos o iniciativas como parte de un portafolio o programa, esto implica que se deben identificar las dependencias, solapamientos, sinergias e impactos entre proyectos, y priorizar. 2. Incluir dentro del PETIC la aprobación formal de todas las partes interesadas para asegurar su compromiso con la hoja de ruta.

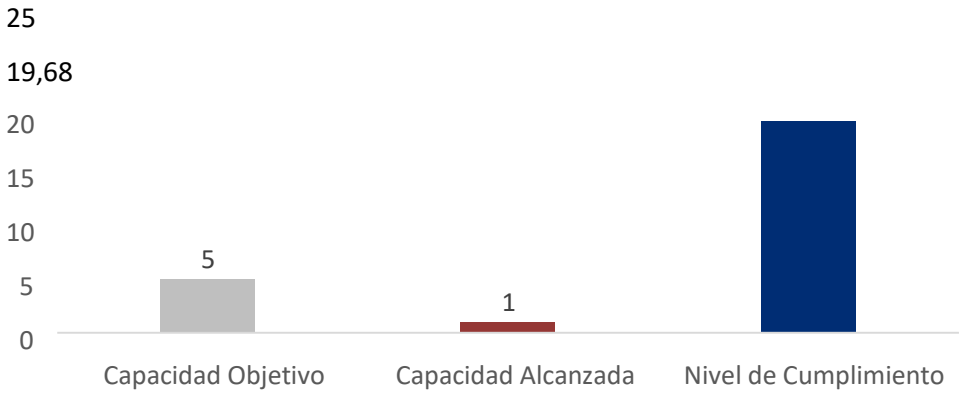
APO02.06 COMUNICAR LA DIRECC IÓN Y ESTRATEGIA DE TI	
Hallazgo o Avance	***Recomendación***
1. Finalmente, se plasma un apartado denominado "Plan de comunicaciones del PETI" en el cual se establecen algunos actores y las comunicaciones requeridas en torno al plan; no obstante, no se identifica que exista retroalimentación por parte de las partes interesadas externas e internas que permita la actualización del plan.	**1.** Incluir dentro del PETIC mecanismos para la obtención de retroalimentación y mejora de este por parte de los interesados.

Gestión de Riesgos Tecnológicos

APO12 - Gestionar el Riesgo

Este objetivo tiene como propósito integrar la gestión del riesgo institucional relacionado con la TI, con la gestión del riesgo institucional global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo institucional relacionado con las TI.

Figura 7. APO12 Gestionar el riesgo.



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 19,68% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
APO12.01 - RECOPILAR DATOS	
Hallazgo o Avance	**Recomendación**
1. La unidad TIC realiza su propia gestión de riesgos alineado a lo establecido en el Sistema Especifico de Valoración de Riesgos Institucionales (SEVRI). De manera anual, la unidad de TIC realiza la identificación de sus riesgos dentro del alcance definido por el documento "MATRIZ DICCIONARIO DE RIESGOS CUC" el cual establece 5 categorías de alto nivel (relevancia de la información, integridad de la información, acceso a la información, disponibilidad de la información, infraestructura tecnológica), esto permite el desarrollo del documento "SEVRI-TI ENCARGADO_TI (1)" el cual documenta de manera más específica los riesgos asociados a TI; sin embargo en base a la revisión documental se identifica una cantidad significativamente reducida de riesgos identificados. **2.** A pesar de los riesgos registrados poseen una fecha de registro, estos no son estudiados ni analizados para identificar factores causantes comunes.	**1.** Documentar una Metodología de Gestión de Riesgos Tecnológicos la cual establezca el proceso de recolección de datos asociados a los riesgos, esto alineado a lo establecido en el Marco Orientador SEVRI. 2. Ajustar el documento "MATRIZ DICCIONARIO DE RIESGOS CUC" con el propósito de incluir nuevas categorías de riesgo que expandan el alcance de la gestión de riesgos tecnológicos. 3. Incluir dentro de la metodología el estudio y analices de los datos históricos de riesgos de I&T con el propósito de identificar factores causantes comunes.

APO12.02 - ANALIZAR EL RIESGO	
Hallazgo o Avance	**Recomendación**
1. En el documento "MATRIZ DICCIONARIO DE RIESGOS CUC" se define el alcance general de gestión de riesgos tecnológicos mediante la definición de 5 categorías. **2.** El proceso desarrollado actualmente, consiste en evaluar el riesgo inherente, evaluar los controles actuales y establecer medidas de control de riesgos; estas medidas no están asociadas a casos de negocio para el desarrollo de proyectos o programas. A pesar de lo mencionado anteriormente, no se identifica una clara vinculación de las actividades actuales con el Análisis de Impacto en el Negocio (BIA) debido a la ausencia de este.	**1.** Incluir dentro de la metodología el análisis de los riesgos utilizando como parámetro lo establecido por el Marco Orientador SEVRI. **2.** Incluir dentro del paso de proponer respuestas (planes de acción) la definición de casos de negocio para posibles proyectos, estos casos de negocio deben indicar su coste/beneficio y el impacto en el nivel de riesgo residual.

APO12.03 MANTENER UN PERFIL DE RIESGO	
Hallazgo o Avance	**Recomendación**
Actualmente no se posee un inventario de los procesos de negocio con su respectiva dependencia con los procesos de gestión de servicios de I&T; a su vez, tampoco es posible identificar cuáles son aquellos acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. En base a la revisión documental, no se identifica la presencia de un perfil de riesgos. Debido a la ausencia del perfil de riesgos, no se poseen indicadores asociados a la gestión de este.	**1.** Desarrollar un Análisis de Impacto al Negocio (BIA) con el propósito de identificar: a. Los procesos de negocio con su respectiva dependencia con los procesos de gestión de servicios de I&T. b. Los recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. **2.** Incluir dentro de la metodología la valoración de los riesgos en base a los parámetros anteriormente mencionados resultantes del BIA para identificar su nivel de riesgo inherente. **3.** Incluir dentro de la metodología el desarrollo de un Perfil de Riesgos de I&T, el cual establezca de manera resumida y estructurada los riesgos a los cuales la institución se encuentra expuesta, este perfil debe ser desarrollado como parte de un proceso integral de captura de información de otros procesos como la Gestión de Incidentes o la Gestión de Problemas. **4.** Incluir dentro de la metodología un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del perfil de riesgo actual y las tendencias de riesgo.

APO12.04 ARTICULAR EL RIESGO	
Hallazgo o Avance	**Recomendación**
1. La unidad TIC remite el resultado de la evaluación realizada internamente al encargado institucional del SEVRI, sin embargo, no se realiza un seguimiento de los niveles de riesgo de I&T. **2.** En casos específicos, donde el riesgo es de muy alto impacto y los proyectos para minimizar su nivel son grandes, la unidad de TIC los eleva a la Alta Dirección en busca de apoyo y contenido presupuestario para el desarrollo de estos. **3.** Debido a la ausencia de un perfil de riesgos, este no es comunicado a las diversas partes interesadas. **4.** Actualmente, no se identifica la revisión de resultados de evaluaciones de terceros debido a la ausencia de estas.	**1.** Incluir dentro de la metodología la generación de informes relacionados a riesgos de manera periódica, estos informes deben estar alineados a los indicadores establecidos para medir el Perfil de Riesgos de I&T. **2.** Incluir dentro de la metodología, la identificación de oportunidades que pudiesen derivar en la capacidad de aceptación de un riesgo mayor y un mayor crecimiento y retorno. **3.** Se recomienda incluir dentro de la metodología, la ejecución de evaluaciones externas en caso de que estas sean necesarias.

APO12.05 DEFINIR UN PORTAFOLIO CON A	CCIONES DE GESTIÓN DE RIESGOS
Hallazgo o Avance	**Recomendación**
1. Dentro del documento "Sevri 2020 Tecnología Informática general" en el apartado "Resultados de las medidas de administración del riesgo" es posible identificar los riesgos fuera y dentro del apetito y niveles de tolerancia en general; no obstante, no se identifican las distintas actividades y planes de acción a realizar en respuesta a esto. **2.** Todas las unidades poseen la responsabilidad de registrar y analizar sus riesgos, así como de dar tratamiento a aquellos que se encuentren fuera del apetito.	**1.** Incluir dentro de la metodología la generación de informes relacionados a riesgos de manera periódica, el establecimiento de un portafolio de acción con gestión de riesgos que permita dar seguimiento al estado del perfil de riesgos y los avances de los programas o proyectos.

APO12.06 RESPONDE R AL RIESGO	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC no posee procedimientos operativos que permitan responden ante la materialización de diversos riesgos, sin embargo, posee el apoyo de proveedores para la atención de incidencias en sistemas o aplicaciones tercerizados. **2.** Debido a que los procesos de riesgos e incidentes no están relacionados, no se realizan análisis de causa raíz de estos para mejorar el proceso de gestión de riesgos.	**1.** Incluir dentro de la metodología la definición de procedimientos operativos como respuesta a los riesgos de mayor impacto. **2.** Comparar los diferentes incidentes y problemas resultantes de estos procesos, con los niveles de tolerancia al riesgo con el propósito de examinar eventos adversos/pérdidas y oportunidades del pasado no consideradas y determinar las causas raíz.

Arquitectura Institucional

APO03 - Gestionar la Arquitectura Institucional

El propósito del objetivo APO03 se encarga de representar los diferentes bloques de construcción que conforman la institución y sus interrelaciones, así como los principios que guían su diseño y evolución a lo largo del tiempo, para posibilitar una prestación estándar, responsable y eficiente de los objetivos operativos y estratégicos.

Figura 8. APO03 Gestionar la arquitectura empresarial

Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 0 y el nivel de cumplimiento es de 0% de un 100%, por lo que indica que la institución no cumple con las

prácticas para gestionar la arquitectura institucional y mejorar el alineamiento, aumentar la agilidad, mejorar la calidad de la información.

Estado General del Proceso	
APO03.01 DESARROLLAR LA VISIÓN DE LA ARQUITECTURA INSTITUCIONAL	
Hallazgo o Avance	***Recomendación***
1. Actualmente la institución no posee una arquitectura empresarial formalmente definida, sin embargo se han realizado esfuerzos aislados para desarrollar componentes como lo son el Mapa de Procesos o la definición la Arquitectura de Información como se aprecia en el documento "Modelo de Arquitectura de la Información" el cual establece 6 componentes de este dominio los cuales son: procesos de negocio, servicios de TI, sistemas de información, gestión de información, personal involucrado y datos municipales. **2.** Debido a la definición incompleta de la arquitectura empresarial, no se han identificado las partes interesadas clave y sus propósitos y/o preocupaciones; asimismo no se poseen los objetivos de arquitectura con su respectiva alineación con las metas y objetivos institucionales en torno a esta. **3.** Adicionalmente, no se ha desarrollado la visión de la arquitectura deseada con su respectivo alcance, principios, riesgos y metas; esto debido a la ausencia de un caso de negocio asociado al desarrollo de todo el modelo de arquitectura empresarial.	**1.** Documentar una Política de Arquitectura Empresarial que contemple los siguientes elementos: **a.** Las partes interesadas clave y sus preocupaciones/objetivos en torno a la arquitectura empresarial para definir los requisitos clave de la institución que deben abordarse, así como las visualizaciones de la arquitectura que deben desarrollarse para satisfacer los requisitos de las partes interesadas. **b.** Las metas y motivadores estratégicos de la empresa para definir las limitaciones que deben abordarse, incluidas las limitaciones de la institución en su conjunto y las específicas de los proyectos. **2.** Se recomienda establecer formalmente un modelo de arquitectura empresarial que incluya, como mínimo los siguientes componentes: **a.** Los objetivos de la arquitectura con las prioridades del programa estratégico en la política de arquitectura. **b.** Las capacidades y metas institucionales e identificar opciones para conseguir dichas metas. **c.** El alcance de la arquitectura de referencia y la arquitectura objetiva enumerando elementos que están dentro del alcance y aquellos que no lo están.

APO03.02 DEFINIR LA ARQUITECTURA DE REFERENCIA	
Hallazgo o Avance	***Recomendación***
1. Actualmente, la institución no posee una arquitectura de referencia por lo que carece de un repositorio de arquitectura que contenga los estándares, componentes reutilizables, los artefactos de modelado, las relaciones, las dependencias y las visualizaciones asociados a esta. **2.** Debido a lo anterior, no se pueden seleccionar puntos de vista de referencia del repositorio de la arquitectura que permite demostrar cómo se abordan las preocupaciones de las partes interesadas en la arquitectura. **3.** Adicionalmente, la institución carece de la de los componentes detallados asociados a los distintos dominios (Negocio, Aplicaciones, Datos e Infraestructura).	**1.** Crear un repositorio de arquitectura, que contenga estándares, componentes reutilizables, los artefactos de modelado, las relaciones, las dependencias y las visualizaciones, para permitir la uniformidad de la institución y el mantenimiento de la arquitectura. Además, asegurarse que cuente además con puntos de vista de referencia que permitan demostrar cómo se abordan las preocupaciones de las partes interesadas en la arquitectura. **2.** Como parte del modelo de arquitectura empresarial se recomienda incluir los siguientes elementos: **a.** Las descripciones de dominio arquitectónico de referencia, usando el alcance y nivel de detalle necesario para respaldar la arquitectura objetivo y, hasta donde sea posible, identificando los bloques de construcción relevantes de la arquitectura del repositorio de arquitectura. **b.** Los dominios del negocio, la información, los datos, las aplicaciones y la tecnología y crear un documento de definición de la arquitectura.

APO03.03 - SELECCIONAR OPORT UNIDADES Y SOLUCIONES	
Hallazgo o Avance	***Recomendación***
1. Debido a la ausencia de un proceso de desarrollo de la arquitectura empresarial, no se identifican los atributos de cambios institucionales clave ni factores que podrían limitar la implementación. **2.** Debido a la ausencia de la arquitectura de referencia y la arquitectura objetivo, no se evalúan los requisitos, brechas, soluciones y otros factores para identificar un conjunto mínimo de requisitos funcionales cuya integración en paquetes de trabajo llevarían a una implementación más eficaz y eficiente. Ante la ausencia de los aspectos anteriores, no se desarrolla una arquitectura de transición que permita alcanzar de forma parcial los objetivos y **3.** que posteriormente, es mejorada a través un enfoque iterativo.	**1.** Documentar un procedimiento el cual permita operativizar el modelo de arquitectura de información sugerido en el punto anterior, que contemple: **a.** Los atributos de cambios institucionales clave. **b.** Los factores institucionales que limitaría la secuencia de implementación. **c.** Los resultados del análisis de brechas entre las arquitecturas de referencia y la objetivo. **d.** La evaluación de los requisitos, brechas, y soluciones para identificar un conjunto mínimo de requisitos cuya integración en paquetes de trabajo llevarían a una implementación más eficaz y eficiente de la arquitectura objetivo.

APO03.04 DEFINIR LA IMPLEMENTA CIÓN DE LA ARQUITECTURA	
Hallazgo o Avance	***Recomendación***
1. Debido a la ausencia de un procedimiento de implementación, no se establecen los elementos requeridos para el plan de implementación de la Arquitectura objetivo. **2.** Ante la ausencia de un proyecto de implementación, no se posee una hoja de ruta con incrementos y fases de la arquitectura de transición.	1. Incluir dentro del procedimiento los siguientes elementos: a. La identificación de los elementos requeridos para el plan de implementación. b. La definición de los incrementos y las fases de la arquitectura de transición. c. La implementación de la arquitectura y el plan de migración. d. La creación de una hoja de ruta de para la obtención de la arquitectura objetiva.

APO03.05 PROPORCIONAR SERVICIOS DE ARQUITECTURA INSTITUCIONAL	
Hallazgo o Avance	***Recomendación***
1. Actualmente la Institución no posee un modelo de arquitectura implementado, por lo que no existen directrices para desarrollar e implementar soluciones. **2.** Del mismo modo, no se gestionan los requisitos de la arquitectura, así como tampoco se respalda al negocio y TI con consejos e información experta sobre principios, modelos y bloques de construcción. **3.** Ante la ausencia de un portafolio de servicios de la arquitectura empresarial, este no se gestiona el con el propósito de garantizar el alineamiento con los objetivos estratégicos y el desarrollo de soluciones. **4.** Finalmente, no se identifican las prioridades de la arquitectura empresarial ni se posee un foro de tecnología que permita proporcionar directrices de arquitectura, asesorar proyectos y guiar la selección de tecnología en base a las necesidades de arquitectura.	**1.** Incluir dentro del procedimientos los siguientes elementos: a. La definición del alcance y las prioridades para proporcionar directrices para desarrollar e implementar soluciones por medio de un proceso definido en la política de arquitectura. b. Los requisitos de la arquitectura empresarial para ofrecer al negocio y TI consejos e información experta sobre principios, modelos y bloques de construcción. c. El portafolio de servicios de la arquitectura empresarial y garantizar el alineamiento con los objetivos estratégicos y el desarrollo de soluciones. d. Las prioridades de la arquitectura empresarial. e. Establecer un foro de tecnología para proporcionar directrices de arquitectura, asesorar proyectos y guiar la selección de tecnología.

BAI09 - Gestionar los Activos

El propósito del objetivo BAI09 es tener en cuenta todos los activos de TI y optimizar el valor proporcionado por su uso.

Figura 9. BAI09 Gestionar los activos

Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 42,59% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
BAI09.01 - IDENTIFICAR Y REGISTRAR LOS ACTIVOS ACTUALES	
Hallazgo o Avance	**Recomendación**
1. Actualmente la unidad de TIC ha realizado recientemente un levantamiento del 100% de los activos tecnológicos de la institución, adicionalmente el área administrativa posee un inventario contable de todos los activos. **2.** Dentro del inventario de activos de TI, se establece el estado del activo para determinar si este está en buen o mal estado; es decir, si continúa generando valor o no. **3.** De manera periódica la unidad de TIC realiza control cruzado con el área administrativa para asegurar la existencia de todos los activos; no obstante, esta periodicidad no está definida.	**1.** Documentar una Metodología de Gestión de Activos de TI la cual establezca las siguientes actividades: a. El desarrollo de un inventario de activos de TI. b. La revisión periódica del inventario de activos con el propósito de asegurar la existencia de todos los activos registrados.

BAI09.02 - GESTIONAR ACTIVOS CRÍTICOS	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC posee identificados los activos críticos de la infraestructura, sin embargo, estos no están documentados y no poseen mecanismos específicos para evitar fallos en estos debido a una insuficiente cantidad de recursos disponibles. **2.** Cuando se realizan actividades de mantenimiento estas son comunicadas a todas las partes interesadas internas y externas. **3.** Las actividades de mantenimiento son realizadas de manera periódica, sin embargo, no se posee un calendario de mantenimiento. **4.** Debido a la ausencia de la identificación de activos críticos, no se identifica un mantenimiento asignado a estos específicamente, sin embargo, el equipo de TIC realiza mantenimiento general a todos los activos tecnológicos bajo demanda. Se poseen algunas contrataciones para el mantenimiento de diversos activos; sin embargo, no se poseen procedimientos para habilitar los diferentes accesos remotos únicamente cuando es requerido.	**1.** Incluir dentro de la metodología las siguientes actividades: a. La identificación de todos los activos críticos para la prestación de los servicios de TI. b. La definición de mecanismos que permitan responder a posibles fallos de los activos críticos. c. El desarrollo de actividades de mantenimiento a los activos críticos como un parte de un Plan de Mantenimiento. d. La planificación de las actividades de mantenimiento dentro del calendario global de producción y la comunicación de las posibles afectaciones a los partes interesados. e. La habilitación de accesos remotos a proveedores que desarrollen actividades de mantenimiento.

BAI09.03 - GESTIONAR EL CICLO DE VIDA DEL ACTIVO	
Hallazgo o Avance	**Recomendación**
La adquisición de activos es realizada mediante lo establecido en la ley 9986 de contratación pública y son realizadas mediante el Sistema Integrado de Compras Públicas (SICOP); una vez es adjudicada la compra a un proveedor, se realiza la entrega en las instalaciones donde se verifican los entregables y posteriormente se registra y plaquea; finalmente se realizan los pagos. Debido a la ausencia de un proceso de Gestión de Cambios, este no se incorpora al ciclo de vida de implementación de los activos; tampoco se identifican pruebas de aceptación. Una vez el activo es plaqueado, registrado y configurado el mismo es asignado a un usuario, la unidad de TIC genera un correo electrónico a las partes interesadas para comunicar la asignación del activo. Los diferentes activos son reutilizados y optimizados a su máxima capacidad mediante la reutilización y reasignación de estos. La unidad de TIC posee un plan de renovación de equipos en los cuales se planificaba el cambio y retirada de estos. Actualmente, no se poseen mecanismos o procedimientos para el desecho seguro de activos de TI.	**1.** Incluir dentro de la metodología las siguientes actividades: a. Los canales y mecanismos para la solicitud y provisión de activos mediante el ciclo de vida de estos, incluyendo la gestión de cambios y pruebas de aceptación. b. El desarrollo de un plan de renovación de activos por obsolescencia o daño. c. Los mecanismos para el desecho seguro de activos, incluyendo la eliminación de toda la información.

BAI09.04 - OPTIMIZAR EL VALOR DE LOS ACTIVOS	
Hallazgo o Avance	**Recomendación**
1. Anualmente, se realiza la preparación del presupuesto en donde se considera la necesidad de nuevos equipos; sin embargo, esto no implica revisiones regulares a la base de activos para identificar si está alineada con las necesidades o identificar opciones de estandarización o suministro único. **2.** Los costes de mantenimiento no son evaluados para determinar posibles nuevas opciones de menor coste. **3.** Al no monitorizar el uso en disponibilidad y capacidad de los activos no es posible utilizar esta información para determinar activos subutilizados.	**1.** Incluir dentro de la metodología las siguientes actividades: a. La revisión regular de la base de activos para identifica si esta está alineada con las necesidades de la institución u opciones de estandarización o suministro único. b. La evaluación de los costes de mantenimiento en busca de opciones de menor coste. c. La identificación de activos subutilizados utilizado como insumo los datos provenientes del monitoreo de la disponibilidad y capacidad.

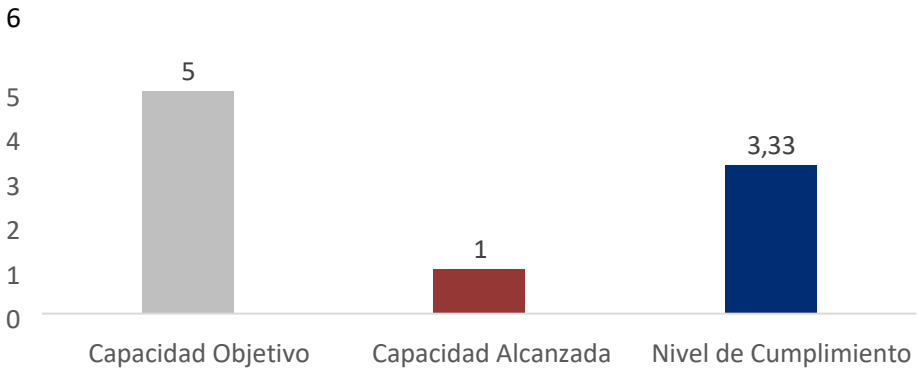
BAI09.05 - GESTIONAR LAS LICENCIAS	
Hallazgo o Avance	**Recomendación**
1. El área administrativa posee licencias registradas como activos, adicionalmente, la unidad de TIC posee un inventario propio de las licencias adquiridas. **2.** A pesar de lo anterior, no se identifica que se realicen revisiones periódicas con el propósito de asegurar que la cantidad de licencias en uso concuerda con las licencias adquiridas. **3.** El número de licencias que se poseen es bastante ajustado a la cantidad de licencias requeridas y el personal que se posee, y en caso de requerir más o menos se realiza en el proceso de renovación de contratos.	**1.** Incluir dentro de la metodología las siguientes actividades: a. La inclusión de las licencias de software dentro del inventario de activos. b. La revisión periódica de la cantidad de licencias adquiridas vs. la cantidad de licencias instaladas. c. La adquisición o eliminación de licencias en base a la cantidad requerida por el negocio.

Calidad de los Procesos Tecnológicos

APO11 - Gestionar la Calidad

El propósito del objetivo APO11 es asegurar la prestación consistente de soluciones y servicios tecnológicos para satisfacer los requisitos de calidad de la institución y las necesidades de las partes interesadas.

Figura 10. APO11 Gestionar la calidad.



Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 3,3% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
APO11.01 - ESTABLECER UN SISTEMA DE GESTIÓN DE CALIDAD	
Hallazgo o Avance	**Recomendación**
1. Actualmente la institución posee algunos elementos asociados a calidad como, por ejemplo, un mapa de procesos y un encargado de procesos; sin embargo, no tiene formalmente definido un Sistema de Gestión de Calidad (SGC). Debido a esto no se evidencia que la definición de roles, tareas, derechos de decisión y responsabilidades para la gestión de la calidad. Hoy en día no se obtienen insumos de la dirección y de las partes interesadas externas e internas sobre la definición de los requisitos de calidad y los criterios de gestión de la calidad, lo anterior debido a que no tiene un SGC formalmente definido. Al no tener establecido un SGC, la institución no puede revisar regularmente el sistema de gestión de calidad frente a los criterios de aceptación acordados para obtener retroalimentación y tomar medidas correctivas.	**1.** Tomar las medidas necesarias para establecer formalmente un SGC institucional basado en la ISO 9001, que contenga como mínimo: a. Una política de gestión de calidad que describa la implementación de un SGC. b. Roles, tareas y derechos de decisión y responsabilidades para la gestión de la calidad en la estructura organizativa. c. Requisitos de calidad y los criterios de gestión de la calidad. d. Plan de Calidad de los Servicios de TI. Una vez definido el SGC se recomienda realizar revisiones periódicas (al menos una vez al año) con la finalidad de garantizar que los criterios de aceptación acordados se estén cumpliendo.

APO11.02 - ENFOCAR LA GESTIÓN DE LA CALIDAD EN LOS CLIENTES	
Hallazgo o Avance	**Recomendación**
1. La institución no determina los requisitos del cliente interno y externo para asegurar el alineamiento de los estándares y las prácticas de información y tecnología con sus necesidades, sin embargo TI, con el fin de buscar el cumplimiento de los requisitos establecidos al inicio del proyecto y la conformidad a la hora de concluir el proyecto, en los procesos de desarrollo de software, elabora requisitos (lista de requerimientos) y aceptación en donde realiza pruebas del desarrollador y pruebas de usuario final. **2.** En cuanto a gestionar las necesidades y expectativas institucionales para cada proceso de la institución, servicio operativo y nuevas soluciones de TI no se evidencia que la institución cumpla con lo detallado anteriormente.	**1.** Aplicar las recomendaciones de la práctica APO11.01 Establecer un Sistema de Gestión de Calidad, de manera que se considere lo siguiente: Requisitos del cliente interno y externo para asegurar el alineamiento de los estándares y las prácticas TI con sus necesidades. a. Los roles y responsabilidades relacionados con la resolución de conflictos entre el usuario/cliente y la organización de TI. b. Criterios de aceptación de calidad para los procesos institucionales y servicios de TI. **2.** Se recomienda que la institución en conjunto con TI desarrolle encuestas o evaluaciones para determinar la calidad de los procesos de negocio y de los servicios de TI, esto con el objetivo de obtener las opiniones de los diferentes clientes desde un enfoque de mejora continua.

APO11.03 - GESTIONAR LOS ESTÁNDARES, PRÁCTICAS Y PROCEDIMIENTOS DE CALIDAD E INTEGRAR LA GESTIÓN DE LA CALIDAD EN LOS PROCESOS Y SOLUCIONES CLAVE	
Hallazgo o Avance	**Recomendación**
1. Actualmente no hay evidencia de que estén definidos los estándares para la gestión de calidad a nivel Institucional. 2. Asimismo, no se suministró evidencia que permita verificar la definición formal de un procedimiento para la gestión de calidad de los procesos. 3. Al no tener definidos los estándares o prácticas para la gestión de calidad, no es posible que la institución cuantifique los beneficios y costes de las certificaciones de calidad. 4. Derivado de lo anterior no hay evidencia de que la institución realice programas de capacitación sobre calidad. 4. Actualmente no se revisan regularmente la relevancia, eficiencia y eficacia continua de los procesos específicos de gestión de calidad.	1. Definir los estándares y prácticas que regirán la gestión de calidad a nivel municipal, algunos de estos podrían ser: a. ISO 9001: 2015 b. COBIT 2019 2. Realizar una evaluación de los posibles beneficios y costes asociados con las certificaciones de calidad con el objetivo de generar un valor agregado a la institución. 3. Se recomienda definir un procedimiento para la gestión de calidad de los procesos de la institución, donde se considere la monitorización de los datos de calidad y las revisiones regulares de los procesos que formarán parte del SGC. 4. Se recomienda que la institución realice programas de capacitación sobre calidad que permitan comunicar el enfoque de gestión de calidad dentro de la institución. 5. Se recomienda que la institución revise regularmente la relevancia, eficiencia y eficacia continua de los procesos que conforman la gestión de calidad. 6.

APO11.04 LLEVAR A CABO LA MONITORI CALIDAZACIÓN, CONTROL Y REVISIONES DE D.	
Hallazgo o Avance	**Recomendación**
1. Actualmente no hay evidencia de que la institución realice un monitoreo de la calidad para los procesos. 2. A nivel institucional no se evidencia que estén definidas las métricas de calidad basadas en los objetivos de calidad de la institución, debido a la ausencia de estos.	Definir métricas de calidad que permitan evaluar el rendimiento asociado a la calidad de los procesos. Se recomienda desarrollar un registro de las evaluaciones que permiten monitorear la satisfacción del cliente respecto a la calidad de los procesos.

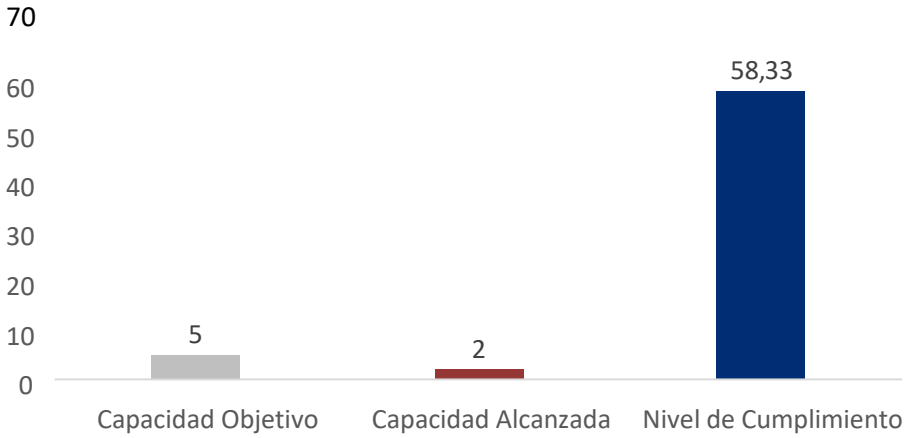
APO11.05 MANTENER LA MEJORA CONTINUA	
Hallazgo o Avance	**Recomendación**
1. A nivel institucional no se evidencia un repositorio donde se puedan compartir buenas prácticas y captar información sobre la gestión de la calidad. 2. Actualmente no se identifica, comunica y utiliza como ejemplo aquellos procesos que sobresalen por su nivel de calidad.	1. Implementar una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos. 2. Diseñar e implementar herramientas que permitan darle seguimiento a las posibles desviaciones o no conformidades bajo un esquema de mejora continua de los procesos.

Contratación y Adquisición de Bienes y Servicios Tecnológicos

APO10 - Gestionar los Proveedores

El propósito del objetivo APO10 es optimizar las capacidades de TI disponibles para apoyar la estrategia y la hoja de ruta de TI, además de minimizar el riesgo asociado con proveedores que no rinden o cumplen con los requisitos y asegurar precios competitivos

Figura 11. APO10 Gestionar los proveedores



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 2 y el nivel de cumplimiento es de 58,33% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
APO10.01 - IDENTIFICAR Y EVALUAR LOS CONTRATOS Y LAS RELACIONES CON LOS PROVEEDORES	
Hallazgo o Avance	***Recomendación***
1. La unidad de TIC se encarga de constantemente identificar nuevos proveedores y socios comerciales, mediante conversaciones y reuniones con estos, en las cuales se exponen los portafolios y catálogos de productos en búsqueda de oportunidades de mejora para la institución. Mediante el Sistema Integrado de Compras Públicas (SICOP) la institución identifica sus proveedores y contratos activos; no obstante, no se identifican aquellos que son críticos. Actualmente no se plasma requisitos de evaluación dentro de los pliegos de condiciones, los cuales establezcan los criterios para la evaluación de estos. portafolios y catálogos de productos en búsqueda de oportunidades de mejora para la institución. Mediante el Sistema Integrado de Compras Públicas (SICOP) la institución identifica sus proveedores y contratos activos; no obstante, no se identifican aquellos que son críticos. Actualmente no se plasma requisitos de evaluación dentro de los pliegos de condiciones, los cuales establezcan los criterios para la evaluación de estos.	**1.** Documentar una Metodología para la Gestión de Proveedores y Contrataciones de I&T, esta debe incluir al menos los siguientes elementos: a. Mecanismos para identificar nuevos proveedores y su nivel de apoyo. b. La clasificación de los diferentes proveedores y contratos en base a su criticidad. c. El establecimiento de criterios de evaluación y evaluaciones para los proveedores dentro del pliego de condiciones para posteriormente utilizar los resultados para mejorar las relaciones con estos.

APO10.02 - SELECCIONAR PROVEEDORES	
Hallazgo o Avance	***Recomendación***
1. Para seleccionar proveedores la unidad y/o área solicitante prepara en conjunto con la unidad de proveeduría un pliego de condiciones donde se establece el alcance y los requisitos que debe cumplir el proveedor para poder participar, además de los criterios de evaluación que están desarrollados. La adjudicación es realizada en SICOP mediante el cumplimiento de los **2.** criterios de adjudicación establecidos en el pliego de condiciones. Según las condiciones del proyecto a desarrollar, se establecen requisitos especiales para estos; no obstante, esto no **3.** está estandarizado. En caso de ser requerido, se busca el apoyo del área jurídica.	**1.** Incluir dentro de la metodología, la selección de proveedores mediante la definición de cláusulas específicas en los pliegos de condiciones, dentro de los cuales destacan: a. La definición de la titularidad de licencias de software, niveles de servicios, acuerdos de mantenimiento, garantías, procedimientos de arbitraje, términos de actualizaciones, seguridad, privacidad, metodologías de proyectos, desarrollo y pruebas, gestión de la calidad y cumplimiento de políticas internas. b. La revisión de los pliegos de condiciones por parte de la unidad legal en caso de ser requerido.

APO10.03 - GESTIONAR LOS CONTRATOS Y LAS RELACIONES CON LOS PROVEEDORES	
Hallazgo o Avance	***Recomendación***
1. Para cada contrato, se asigna un administrador de contrato quien es el encargado de gestionar las relaciones con este. **2.** La comunicación es realizada según los canales establecidos en el pliego de condiciones o bien a través de SICOP. **3.** Para renovar un contrato, la unidad solicitante debe asegurarse de que el proveedor cumple con todos los requisitos para posteriormente formalizarlo en SICOP. **4.** En el pliego de condiciones, se establecen los roles y responsabilidades del proveedor. **5.** Para establecer mejoras en las relaciones prima la negociación con el proveedor para posteriormente, si es requerido es posible optar por instancias contractuales o judiciales las cuales están basadas en la ley de contratación pública.	**1.** Incluir dentro de la metodología, la gestión de los contratos y relaciones con proveedores mediante los siguientes elementos: a. La asignación de un administrador de contrato quien se encargue de dar seguimiento a este. b. La definición de roles y responsabilidades del proveedor. c. La evaluación de la eficacia de la relación e identificar y gestionar la mejora continua.

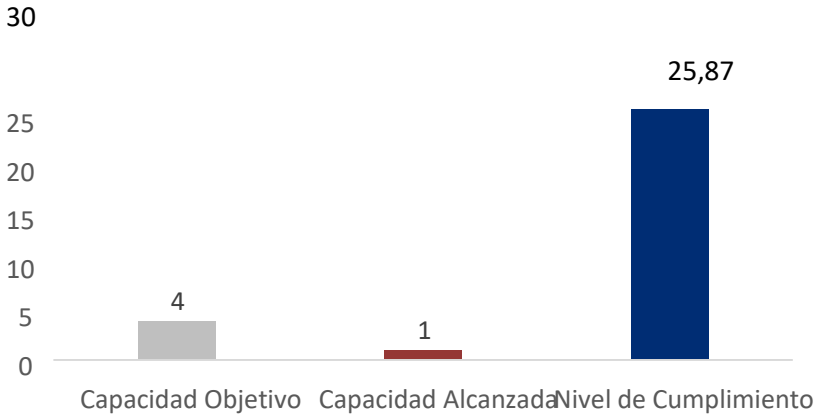
APO10.04 GESTIONAR LOS RIESGOS DE LOS PROVEEDORES	
Hallazgo o Avance	***Recomendación***
1. La institución plasma en el cartel algunas cláusulas de penalización en aras de mitigar riesgos; adicionalmente estos deben realizar un depósito de dinero el cual es utilizado como garantía. **2.** Debido a la ausencia de un proceso de gestión de cambios, gestión de la disponibilidad, entre otros; estos no son incluidos como parte de los pliegos de condiciones de modo que el alcance de estos procesos internos pueda expandirse a componentes tercerizados.	**1.** Incluir dentro de la metodología, la gestión de los riesgos asociados a contratos y proveedores mediante los siguientes elementos: a. La inclusión de cláusulas de penalización en aras de mitigar riesgos, esto dentro del pliego de condiciones. b. La inclusión de cláusulas que permitan integrar los procesos de gestión de servicios de TI internos de la institución con los del proveedor. c. La evaluación de la eficacia de la relación e identificar y gestionar la mejora continua.
APO10.05 SUPERVISAR EL RENDIMIENTO Y EL CUMPLIMIENTO DEL PROVEEDOR	
1. Cuando una contratación llega a su fin, la unidad de TIC realiza una revisión de que los entregables solicitados cumplan con lo establecido originalmente dentro del pliego de condiciones; sin embargo, no existe evidencia documental al respecto. **2.** Actualmente, dentro de los pliegos de condiciones no se incluyen cláusulas que permitan solicitar revisiones independientes de las prácticas y controles internos del proveedor, si fueses necesario. **3.** El administrador del contrato es quien asegura que las contrataciones cumplen con los criterios de calidad y demás requerimientos establecidos en el pliego de condiciones.	**1.** Incluir dentro de la metodología, la supervisión del rendimiento y cumplimiento mediante los siguientes elementos: a. La ejecución de las evaluaciones del servicio en conjunto con el proveedor, utilizando como insumo los criterios de evaluación definidos en el pliego de condiciones. b. El uso de los resultados para la mejora continua de las relaciones.

Gestión de Proyectos que Implementan Recursos Tecnológicos

BAI11 - Gestionar los Proyectos

El propósito del objetivo BAI11 es definir los resultados definidos en el proyecto y reducir el riesgo de retrasos inesperados, costes mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Para de esta manera garantizar el valor y la calidad a los entregables del proyecto.

Figura 12. BAI11 Gestionar los proyectos



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 25,87% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
BAI11.01 - MANTENER UN ENFOQUE ESTÁNDAR EN LA GESTIÓN DE PROYECTOS	
Hallazgo o Avance	***Recomendación***
1. La institución posee múltiples plantillas que apoyan y guían el desarrollo de proyectos en la institución; no obstante, carece de una metodología el cual guie la ejecución de todo el proceso. Adicionalmente, se carece de una Oficina de Gestión de Proyectos (PMO) que dé mantenimiento a las diversas plantillas y metodologías. Derivado de lo anterior, no es posible asegurar que se haga uso de la mejora continua en las estructuras y herramientas de gestión de proyectos.	**1.** Documentar una metodología para la gestión de portafolios, programas y proyectos. **2.** Establecer una oficina de gestión de proyectos PMO que mantenga una estrategia estándar para la gestión de programas y proyectos en toda la organización.
BAI11.02 - ESTABLECER E INI CIAR UN PROYECTO	
1. La institución posee el documento "Plantilla Charter", el cual establece los elementos requeridos para la definición del proyecto; como, por ejemplo, perfil del proyecto, información general (caso de negocio), enfoque, alcance y otros elementos. **2.** Adicionalmente, mediante el documento "Plantilla Declaración del Alcance" se hace una definición de los distintos entregables y sus criterios de aceptación.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Garantizar que cada proyecto tenga uno o más patrocinadores b. Nombrar a un gestor dedicado para el proyecto. c. Asegurar que la definición del proyecto describe los requisitos de un plan de comunicación del proyecto que identifique las comunicaciones internas y externas del proyecto.

BAI11.03 GESTIONAR LA PARTICIPACIÓN DE LAS PARTES INTERESADAS	
Hallazgo o Avance	***Recomendación***
1. La institución posee el documento "Plantilla Charter", el cual establece los elementos requeridos para la definición del proyecto, sin embargo, este carece de una identificación de partes interesadas, sus requisitos y como estos se involucrarán dentro del proyecto. Debido a lo anterior, no es posible asegurar que se implementen acciones correctivas en caso de ser requerido.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Planificar cómo las partes interesadas dentro y fuera de la organización se identificarán, analizarán, involucrarán y gestionarán durante el ciclo de vida del proyecto. b. Analizar los intereses, requisitos y compromiso de las partes interesadas. Implementar medidas correctivas si fuera necesario. **2.** Se recomienda desarrollar una herramienta de identificación de interesados que apoye lo establecido en la metodología.
BAI11.04 DESARROLLAR Y MANTENER EL PLAN DEL PROYECTO	
1. El área de TIC realiza un plan de proyecto (cronograma) en el cual se establecen las diferentes actividades y recursos a utilizar dentro del proyecto; esto les permite dar seguimiento y controlar su progreso. **2.** A pesar de lo anterior, no es posible asegurar que los diferentes planes adicionales (calidad o riesgos) se actualicen conforme al cronograma.	**3.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Mantener el plan del proyecto y los planes dependientes (p. ej., plan de riesgos, plan de calidad, plan de obtención de beneficios). b. Asegurar que los planes estén actualizados y reflejen el progreso actual y los cambios materiales aprobados.

BAI11.05 GESTIONAR LA CALIDAD DEL PROYECTO	
Hallazgo o Avance	***Recomendación***
1. Dentro de los diferentes proyectos, se realizan actividades para asegurar la calidad de los proyectos individuales; esto de cara a los procesos de contratación pública; sin embargo, estas actividades asociadas a la calidad no se incluyen dentro de los cronogramas como tareas específicas con responsables asociados. **2.** Derivado de la ausencia de un Sistema de Gestión de Calidad (SGC) no es posible asegurar que el plan de calidad y la gestión de calidad de los proyectos en general, esté alineada con el SGC.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Identificar las tareas y prácticas de aseguramiento requeridas. b. Realizar actividades de aseguramiento y control de calidad conforme al plan de gestión de calidad y el SGC. **2.** Documentar una herramienta de Plan de Calidad que permita ejecutar lo establecido en la Metodología.
BAI11.06 GESTIONAR EL RIESGO DEL PROYECTO	
Hallazgo o Avance	***Recomendación***
1. La institución posee un proceso de gestión de riesgos institucionales asociadas al SEVRI; sin embargo, no se identifica que se realizan planes de gestión de riesgos como parte integral de la gestión de proyectos. **2.** El riesgo del proyecto no se revalúa periódicamente, incluyendo un inicio a cada fase del proyecto principal como parte de evaluaciones de solicitudes de cambio mayores.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Realizar la evaluación de riesgos del proyecto, identificando y cuantificando el riesgo continuamente durante todo el proyecto de acuerdo con la metodología institucional. b. Reevaluar el riesgo del proyecto periódicamente, incluyendo un inicio de fase o solicitudes de cambio mayores. c. Se recomienda documentar un Plan de Riesgos que permita ejecutar lo establecido en la Metodología.

BAI11.07 SUPERVISAR Y CONTROLAR LOS PROYECTOS	
Hallazgo o Avance	***Recomendación***
1. La institución da seguimiento a los proyectos para asegurar que estos son completados en tiempo y forma; no obstante, no se identifica la presencia de informes periódicos hacia las partes interesadas. A su vez, la institución posee el documento **2.** "Plantillas_Contratos" en cual se da seguimiento a los cambios en los contratos/proyectos; no obstante, el proceso de aprobación no está basado en criterios de aceptación definidos antes del comienzo de la fase del proyecto o iteración.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Informar a las partes interesadas identificadas clave acerca del progreso del proyecto o desviaciones. b. Evaluar el proyecto en las fases, liberaciones o iteraciones mayores acordadas. Documentar una herramienta de informe de proyecto que permita ejecutar lo establecido en la Metodología.
BAI11.08 Gestionar los recursos del proyecto y los paquetes de trabajo.	
1. La gestión de las adquisiciones es gestionada de conformidad con los procesos de contratación pública a través de SICOP; no obstante, no se identifica un plan de adquisiciones asociado al proyecto.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Identificar las necesidades de recursos del negocio y de TI para el proyecto. b. Definir y acordar claramente la responsabilidad de la adquisición y gestión de productos. Se recomienda documentar una herramienta de Plan de Adquisiciones que permita ejecutar lo establecido en la Metodología.

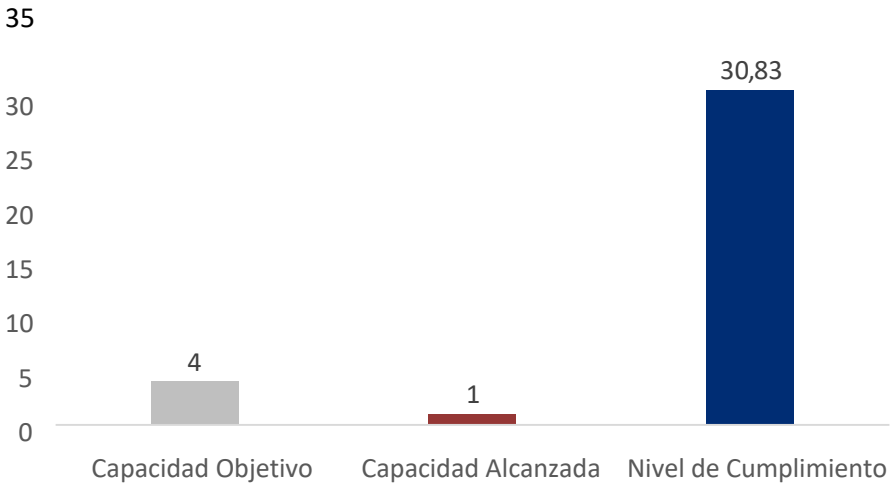
BAI11.09 CERRAR UN PROY ECTO O ITERACIÓN	
Hallazgo o Avance	***Recomendación***
1. La institución posee el documento "Plantilla Acta Cierre Proyecto" el cual permite hacer un cierre ordenado del proyecto, mediante la aceptación de todos los entregables y la confirmación de que se han validado todos los criterios de calidad. **2.** Adicionalmente, mediante el documento "Plantillas_Contratos" se realiza una "lista de chequeo" y se captan las lecciones aprendidas.	**1.** Incluir dentro del apartado de proyectos, los siguientes elementos: a. Obtener la aceptación de las partes interesadas para los entregables del proyecto y transferir la propiedad. b. Ejecutar revisiones postimplementación para determinar si los proyectos ofrecen los resultados esperados. c. Recopilar las lecciones aprendidas de los participantes del proyecto.

Desarrollo, Implementación y Mantenimiento de Sistema de Información

BAI03 - Gestionar la Identificación y Construcción de Soluciones

El propósito del objetivo BAI03 es garantizar una prestación ágil y escalable de los productos y servicios digitales. Es decir, se encarga de establecer soluciones oportunas y rentables para cumplir con los objetivos estratégicos y operativos de la institución.

Figura 13. BAI03 Gestionar la identificación y la construcción de soluciones.



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 30,83% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
BAI03.01 - DISEÑO DE SOLUCIONES DE ALTO NIVEL	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC realiza reuniones con el usuario solicitante para el levantamiento de requisitos y posteriormente establecen un diseño de alto nivel o prototipo de la solución, generalmente enfocado en la interfaz de usuario y ocasionalmente en procesos de negocio; finalmente se busca la aprobación del patrocinador y se realiza le proceso de contratación o desarrollo interno. **2.** Actualmente, la unidad de TIC no posee estándares de desarrollo formalmente definidos; únicamente se conocen algunas directrices las cuales son plasmadas en las contrataciones cuando estas aplican.	**1.** Documentar una Metodología de Desarrollo de Soluciones, en la cual se desarrolle un apartado sobre el diseño de la solución; este apartado deberá incluir como mínimo los siguientes elementos: a. El diseño de alto nivel de la solución, incluyendo procesos de negocio. b. El cumplimiento de los estándares de diseño de la institución. c. La definición y el alineamiento de los criterios de calidad con el Sistema de Gestión de Calidad. d. La aprobación final de los requisitos por parte de todas las partes interesadas. **2.** Se recomienda documentar estándares para el diseño y construcción de soluciones en la institución, estos podrían incluir elementos como, por ejemplo: a. Uso de lenguajes y frameworks de programación específicos. b. Uso de patrones de diseño comunes. c. Uso de pruebas unitarias, de integración y de sistema. d. Implementación de prácticas de seguridad. e. Nomenclatura de los componentes. f. Uso de herramientas y aplicaciones específicas.

BAI03.02 DISEÑAR COMPONENTES DETALLADOS PARA LA SOLUCIÓN	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC realiza o solicita al proveedor encargado, algunos diseños de la solución, por ejemplo, diseños de interfaz de usuario, diagramas entidad-relación y/o ubicación de la solución. **2.** A pesar de lo mencionado anteriormente, los diversos componentes a diseñar no están estandarizados.	**1.** Incluir dentro de la metodología, en el apartado de diseño, el desarrollo de los siguientes componentes: a. Procesos de negocio. b. Entradas y salidas de datos. c. Interfaces de sistemas. d. Interfaces de usuario. e. Ubicación del almacenamiento. f. Redundancia y datos de auditoría. g. Controles de información. **2.** Incluir dentro de cada diseño un apartado sobre el versionamiento asociada a cada uno.

BAI03.03 - DESARROLLAR LOS COMPONENTES DE LA SOLUCIÓN	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC posee ambientes separados de desarrollo, pruebas y producción. **2.** Cuando los terceros se ven involucrados en un proyecto, estos deben cumplir lo establecido en el contrato. **3.** Los cambios en los componentes son revisados y abordados según las capacidades del equipo de TI, no obstante, no se identifica un control de versiones para los diferentes componentes de la solución. **4.** Durante los procesos de estudio de mercado previos al comienzo del proyecto, se evalúan diferentes opciones con el propósito de identificar el impacto en el presupuesto y la institución del desarrollo de un producto a la medida o la compra de una ya hecho.	**1.** Se recomienda incluir dentro de la metodología, en el apartado de desarrollo, los siguientes elementos: a. La separación de los ambientes de desarrollo, pruebas y producción. b. La gestión de cambios en los requisitos, evaluando el impacto de estos en el alcance del proyecto y ajustando las versiones de los diferentes componentes y sus diseños. c. La responsabilidad del uso de componentes de alta criticidad en términos de seguridad de la información.

BAI03.04 - ADQUIRIR LOS COMPONENTES DE LA SOLUCIÓN	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC identifica aquellos componentes requeridos para su adquisición y realiza los procedimientos respectivos; sin embargo, esto no responde un plan de adquisiciones asociado al proyecto.	**1.** Incluir dentro de la metodología, en el apartado de desarrollo, los siguientes elementos: a. El desarrollar un plan de adquisiciones para la solución propuesta de acuerdo con lo establecido en la Metodología de Proyectos.

BAI03.05 - CONSTRUIR SOLUCIONES	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC instala y configura las soluciones de TI, de acuerdo con el criterio experto del equipo. **2.** Todas las adquisiciones (hardware, por ejemplo) son registradas en el inventario de activos. Debido a que la unidad de TIC no posee un portafolio de servicios de TI, en el cual se identifiquen aquellos servicios en desarrollo; no es posible asegurar que se creen productos y servicios los cuales se vean reflejados en este portafolio.	**1.** Se recomienda incluir dentro de la metodología, en el apartado de desarrollo, los siguientes elementos: a. La configuración de los componentes según las necesidades de la institución y los diseños aprobados. b. La presencia de registro de auditoria durante la integración del hardware y software. c. La definición de catálogos de productos y servicios para los grupos objetivos como parte del Portafolio de Servicios de TI.

BAI03.06 - REALIZAR EL ASEGURAMIENTO DE CALIDAD (QA)	
Hallazgo o Avance	**Recomendación**
1. El encargado de proyecto es el encargado de asegurar la calidad del proyecto; no obstante, al no poseer un plan de calidad asociado este es realizado de manera limitada y no controlada.	Se recomienda incluir dentro de la metodología en el apartado de aseguramiento de la calidad, los siguientes elementos: Definir un plan de aseguramiento de la calidad que incluya, por ejemplo, la especificación de los criterios de calidad, procesos de validación y verificación, definición sobre cómo se revisará la calidad, cualificaciones necesarias de los revisores de la calidad, y roles y responsabilidades para lograr la calidad, mecanismos a utilizar. a. Supervisar todas las excepciones de calidad y abordar todas las acciones correctivas. b.Mantener un registro de todas las revisiones, resultados, excepciones y correcciones. Se recomienda documentar un plan de calidad del proyecto el cual establezca todos los componentes requeridos por la metodología.

BAI03.07 PREPARAR LAS PRUEBAS DE LA SOLUCIÓN	
Hallazgo o Avance	**Recomendación**
1. Existe un entorno de pruebas / desarrollo para la ejecución de pruebas de calidad el cual es administrado y configurado por la unidad de TIC o proveedores externos según sea el proyecto. **2.** La unidad de TIC genera un plan de pruebas con sus respectivas pruebas, esto incluye los pasos a realizar, los resultados esperados y los resultados obtenidos.	**1.** Incluir dentro de la metodología, en el apartado de aseguramiento de la calidad, los siguientes elementos: a. El desarrollo de procedimientos de pruebas según lo establecido en el plan de pruebas, en el entorno destinado a esto.
BAI03.08 - EJECUTAR LAS PRUEBAS DE LA SOLUCIÓN	
1. La unidad de TIC o los proveedores realizan pruebas asociadas a las soluciones de TI y sus componentes. **2.** La mayoría de estas tienden a ser pruebas guiadas por los usuarios finales. **3.** En caso de que las pruebas fallen, estas son corregidas por el equipo de TIC o proveedores externos según corresponda.	**1.** Incluir dentro de la metodología, en el apartado de aseguramiento de la calidad, los siguientes elementos: a. La ejecución de las pruebas según el procedimiento de pruebas y los guiones de pruebas. b. Identificar, registrar y clasificar los errores (p. ej. menores, significativos, de misión crítica) durante las pruebas. Repetir las pruebas hasta que se hayan resuelto todos los errores significativos. a. Registrar los resultados de las pruebas y comunicarlos a las partes interesadas.
BAI03.09 - GESTIONAR LOS CAMBIOS A LOS REQUISITOS	
1. Los cambios en los componentes y el proyecto son revisados y abordados según las capacidades del equipo de TI.	**1.** Guiar la gestión de cambios en los requisitos, evaluando el impacto de estos en el alcance; esto de acuerdo con lo sugerido en la metodología de gestión de proyectos.

BAI03.10 - MANTENER LAS SOLUCIONES	
Hallazgo o Avance	**Recomendación**
1. Actualmente no se desarrollan planes de mantenimiento para las soluciones en desarrollo.	**1.** Incluir dentro de la metodología, en el apartado de mantenimiento de la solución, los siguientes elementos: a. Desarrollar plan de mantenimiento para las soluciones en desarrollo, este plan podría incluir actividades como por ejemplos: gestión de parches, estrategias de actualización, riesgo, privacidad, análisis de vulnerabilidades y requisitos de seguridad.
BAI03.11 DEFINIR PRODUCTOS Y SERVICIOS DE TI Y MANTENER EL PORTAFOLIO DE SERVICIOS	
Hallazgo o Avance	**Recomendación**
1. Las nuevas soluciones no se encuentran documentadas en el portafolio de servicios de TI debido a la ausencia de este.	**1.** Incluir dentro de la metodología, en el apartado de mantenimiento de la solución, los siguientes elementos: a. Desarrollar una declaración formal del servicio a incluir en el portafolio de servicios de TI a partir de fichas de servicio e incluir como un servicio en desarrollo.
BAI03.12 DISEÑAR SOLUCIONES CONFORME A LA METODOLOGÍA DE DESARROLLO DEFINIDA	
Hallazgo o Avance	**Recomendación**
1. La unidad de TIC selecciona la metodología de desarrollo a utilizar mediante la experiencia de aquella que mejor se adapta y ha dado mejores resultados, generalmente se trabaja con una metodología en cascada; sin embargo, cuando participan proveedores estos utilizan metodologías agiles. El establecimiento del equipo de trabajo se valora con el encargado de la unidad de TIC considerando la experiencia de los diferentes integrantes del equipo de TI, sus responsabilidades actuales y sus áreas de conocimiento.	**1.** Incluir dentro de la metodología, en el apartado de políticas de desarrollo de la solución, los siguientes elementos: a. La valoración y selección de dinámicas de desarrollo en base a las necesidades del proyecto (cascada o agiles). a. La conformación de los equipos del proyecto de acuerdo con las dinámicas seleccionadas.

BAI04 - Gestionar la Disponibilidad y Capacidad

El propósito del objetivo BAI04 es mantener la disponibilidad del servicio, la gestión eficiente de los recursos y la optimización del rendimiento del sistema a través de la predicción de los requisitos futuros de rendimiento y capacidad.

Figura 14. BAI04 Gestionar la disponibilidad y la capacidad.

.

Según el gráfico anterior, se puede verificar que el nivel de capacidad y el nivel de cumplimiento es de 0% de un 100%, esto implica que el proceso se no se ha establecido.

Estado General del Proceso	
BAI04.01 EVALUAR LA DISPONIBILIDAD, RENDIMIENTO Y CAPACIDAD ACTUALES, Y CREAR UNA LÍNEA DE REFERENCIA	
Hallazgo o Avance	***Recomendación***
1. Actualmente la institución realiza la gestión de la disponibilidad y capacidad de manera manual, debido a esto no poseen una línea base de su rendimiento y capacidad actuales. **2.** Debido a lo anterior y sumado a la ausencia de herramientas (sistemas de información) que apoyen la ejecución del proceso de incidentes y monitore; no es posible asegurar que se realiza un registro y seguimiento de todos los incidentes derivados de problemas de disponibilidad y/o capacidad. **3.** Adicionalmente, debido a la ausencia de un modelo de monitoreo; no se identifica la presencia de umbrales definidos que puedan ser monitoreados. **4.** A pesar de que dentro del Catálogo de Servicios de TI se poseen algunos niveles de servicio definidos; no es posible asegurar que su cumplimiento sea evaluado periódicamente utilizando como insumo el proceso de gestión de la disponibilidad y capacidad.	**1.** Desarrollar una metodología de disponibilidad y capacidad la cual incluya los siguientes elementos: a. El desarrollo de una línea base de disponibilidad y capacidad. b. El monitoreo de los recursos de TI mediante el uso de una herramienta automatizada la cual sea configurada utilizado como insumo el modelo de monitoreo. c. El registro, atención y seguimiento de los incidentes asociados según lo establecido en el proceso de Gestión de Incidentes. **2.** Se recomienda documentar un modelo de monitoreo el cual establezca los diferentes activos a monitorear con sus respectivos umbrales. **3.** Se recomienda la implementación de una herramienta para la gestión del monitoreo, como, por ejemplo, Pandora FMS, Ansible o MS Systemcenter.

BAI04.02 EVALUAR EL IMPACTO EN EL NEGOCIO	
Hallazgo o Avance	***Recomendación***
1. Actualmente, la institución posee una cierta noción sobre cuales son aquellos servicios críticos para estos; no obstante, esto no se encuentra documentado. **2.** Debido a la ausencia de servicios y activos de TI críticos formalmente identificados, estos no son monitoreados como parte del alcance del proceso de gestión de disponibilidad y capacidad. **3.** Debido a la ausencia de datos referentes al monitoreo; no es posible asegurar que se realicen análisis de tendencias para predecir fallos o incidentes futuros; asimismo, no se identifican escenarios de disponibilidad o capacidad desarrollados en base a esta información. **4.** Derivado de lo anterior, no se identifican escenarios de disponibilidad y capacidad con sus respectivos impactos en el negocio.	**1.** Incluir dentro de la metodología los siguientes elementos: a. El monitoreo específico de los activos críticos mediante la herramienta de monitoreo. b. El desarrollo de análisis de tendencias a partir de los resultados de la herramienta de monitoreo. c. El desarrollo de escenarios de rendimiento y capacidad en base a los análisis de tendencias. d. La aceptación de los diferentes usuarios de negocio sobre los escenarios y sus implicaciones.

BAI04.03 PLANIFICAR LOS REQUISITOS DE LOS SERVICIOS NUEVOS O MODIFICADOS	
Hallazgo o Avance	***Recomendación***
1. De manera empírica, la unidad de TIC planea las mejoras respectivas para la infraestructura; sin embargo, no se dispone de información de referencia que sean utilizados como insumo para la planificación de estas mejoras. **2.** Debido a los aspectos mencionados anteriormente, no se identifica la presencia de planes de capacidad. Asimismo, los Acuerdos de Nivel de **3.** Servicio (SLA) no son ajustados en base los diferentes planes de capacidad.	Incluir dentro de la metodología los siguientes elementos: a. El desarrollo de un plan de disponibilidad y capacidad que permita alcanzar los niveles requeridos por el negocio. b. El ajuste de los Acuerdos de Nivel de Servicio (SLA) en caso de ser requerido.
BAI04.04 MONITORIZAR Y REVISAR LA DISPONIBILIDAD Y LA CAPACIDAD	
1. Actualmente, no se identifica la presencia de informes de capacidad para los procesos de negocio. **2.** Ante la ausencia de informes, estos no son revisados periódicamente por TI y las diferentes partes interesadas. **3.** Asimismo, los resultados de estos informes no son utilizados para la planificación de actividad iterativas para mejorar los rendimientos.	Incluir dentro de la metodología los siguientes elementos: a. Emitir de manera periódica informes de disponibilidad y capacidad. b. Utilizar los informes como insumo para le mejora de los servicios de TI.

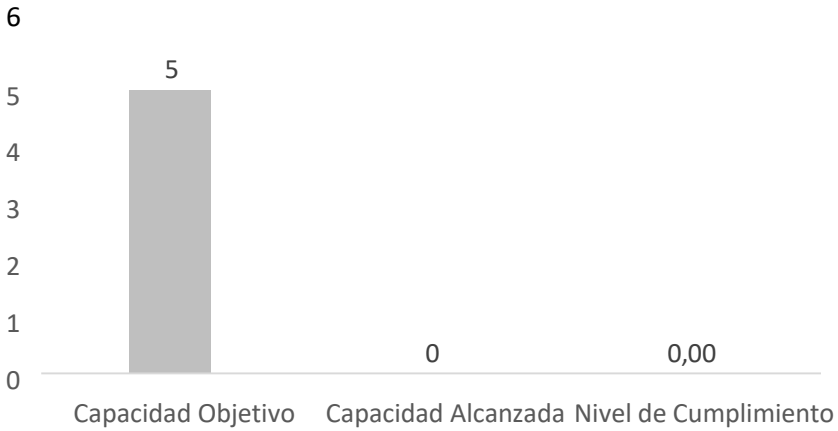
BAI04.05 INVESTIGAR Y RESOLVER LOS PROBLEMAS DE DISPONIBILIDAD, RENDIMIENTO Y CAPACIDAD	
Hallazgo o Avance	***Recomendación***
1. Generalmente, la unidad de TIC busca el apoyo de proveedores para la configuración y optimización de los respectivos productos. **2.** Adicionalmente, en los diferentes contratos se establecen los mecanismos para el escalamiento de solicitudes o incidentes. **3.** Finalmente, no se identifican que se realicen acciones correctivas en línea con el proceso de gestión de cambios.	**1.** Incluir dentro de la metodología los siguientes elementos: a. La optimización del rendimiento de los servicios de TI mediante el apoyo de los proveedores externos. b. El escalamiento de incidentes y peticiones de servicio a proveedores cuando este sea necesario. c. La aplicación de acciones correctivas en línea con el proceso de gestión de cambios como herramienta para la atención de incidentes.

Seguridad y Ciberseguridad

APO13 – Gestionar la Ciberseguridad

El propósito del objetivo APO13 es mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la institución.

Figura 15. APO13 Gestionar la ciberseguridad.



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad y el nivel de cumplimiento es de 0% de un 100%, esto implica que el proceso se no se ha establecido.

Estado General del Proceso	
APO13.01 ESTABLECER Y MANTENER UN SGSI (SGSI).	
Hallazgo o Avance	***Recomendación***
1. La institución no posee un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente definido. 2. Debido a lo anterior, la institución carece de los componentes básicos de un SGSI dentro de los cuales destacan: Objetivos Institucionales en materia de Seguridad de la Información para su alineamiento con el SGSI. Definición del Alcance. Autorización de la alta dirección para operar y gestionar el SGSI. Declaración de aplicabilidad para los controles. Roles y responsabilidades formalmente definidos. Estrategia del SGSI.	**1.** Se recomienda la definición formal de un SGSI, como parte de este sistema de gestión se debe incluir al menos lo siguientes elementos: a. La definición de objetivos institucionales en materia de Seguridad de la Información. b. Definición del Alcance del SGSI. c. Autorización por parte de la Alta Dirección para la implementación y operación. d. Declaración de aplicabilidad de controles. e. Roles y responsabilidades en materia de Seguridad de la Información. f. Estrategia comunicada en materia de Seguridad de la Información. g. Política General de Seguridad de la Información. h. Análisis de riesgos de Seguridad de la Información.

APO13.02 DEFINIR Y GESTIONAR UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD.	
Hallazgo o Avance	***Recomendación***
1. Actualmente, el perfil de riesgos de la institución no considera la Seguridad de la Información como uno de los ámbitos de este. **2.** La institución carece de un inventario de activos de información. **3.** La institución posee una plantilla de "Perfil de Proyecto", sin embargo, no se identifican iniciativas que apoyen al desarrollo del Plan de tratamiento de Riesgos de Seguridad de la Información. A pesar de realizar capacitaciones de manera ocasional esto no implica la presencia de un Programa de Capacitación y Concientización de materia de Seguridad de la Información. Debido a la ausencia de controles definidos formalmente mediante la declaración de aplicabilidad, no se poseen indicadores asociados a la eficacia de los controles.	**1.** Se recomienda incluir al SGSI los siguientes componentes: a. Inventario de Activos de Información. b. Plan de Tratamiento de Riesgos de Seguridad de la Información, el cual debe incluir los controles seleccionados en la declaración de aplicabilidad. c. Casos de negocio que apoyen a la implementación de los controles establecidos en el Plan de Tratamiento de Riesgos. c. Programa de Capacitación y Concientización en materia de Seguridad de la Información.

APO13.03 MONITORIZAR Y REVISAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	
Hallazgo o Avance	***Recomendación***
Se Derivado de la ausencia de un SGSI, este no es monitorizado ni revisado por parte de la alta dirección para asegurar que los objetivos han sido alcanzados o su alcance se ha visto modificado. Del mismo modo, no se identifican eventos que podrían afectar el rendimiento del SGSI. Finalmente, no es posible asegurar que existan acciones de mejora para atender problemas de rendimiento asociados al SGSI.	**1.** Se recomienda documentar un procedimiento de revisión y mantenimiento del SGSI que contemple las siguientes actividades: a. Revisiones periódicas del rendimiento. b. Auditorias periódicas. c. Revisiones para determinar si el alcance ha sufrido cambios. d. Identificar eventos que podrían afectar el rendimiento e. Identificar acciones de mejora para el SGSI, resultante de hallazgos asociados a la monitorización y revisión.

DSS05 - Gestionar Los Servicios De Seguridad

El propósito del objetivo DSS05 es minimizar las vulnerabilidades e incidentes operativos de la seguridad de la información en la institución, es decir, se encarga de proteger la información para mantener el nivel de riesgo de la seguridad de la información aceptable para la institución, conforme con la política de seguridad.

Figura 16. DSS05 Gestionar los servicios de seguridad

Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 66,46% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
DSS05.01 PROTEGER CONTRA SOFTWARE MALICIOSO	
Hallazgo o Avance	***Recomendación***
1. El área de TIC posee la herramienta para la protección del software malicioso "ESET", esta se encuentra desplegada en todos sus dispositivos. **2.** Mediante la seguridad perimetral (firewall) y una integración con las herramientas de correo electrónico de Microsoft Office 365, el tráfico es filtrado para evitar la descarga de software malicioso. **3.** No se identifica la presencia de un plan de concientización en temas de Seguridad de la Información, el cual incluya temas sobre software malicioso; sin embargo, se realiza concientización de manera periódica. **4.** Mediante la plataforma administración de la herramienta para la protección de software malicioso se administran los parches de seguridad y actualizaciones de manera centralizada. **5.** Mensualmente, la unidad de TIC se mantiene en constante actualización sobre nuevas amenazas mediante la revisión de la consola del antivirus; adicionalmente se busca la cooperación y apoyo de entes externos como el MICITT.	**1.** Inclusión de la concientización sobre software malicioso dentro del plan de concientización del SGSI (SGSI). **2.** Documentar una política de prevención de software malicioso.

DSS05.02 GESTIONAR LA SEGURIDAD DE LA CONECTIVI DAD Y D E LA RED	
Hallazgo o Avance	***Recomendación***
1. La unidad de TIC ha configurado la infraestructura tecnológica de tal manera que únicamente aquellos dispositivos autorizados propiedad de la municipalidad tengan acceso a la información y a los sistemas. La institución posee diversas capas de seguridad, dentro de las cuales destacan la presencia de un firewall de seguridad perimetral en el cual se establecen perfiles y políticas asociadas a los perfiles. Dentro de la seguridad perimetral se poseen bloqueados protocolos no seguros; sin embargo, no existe una documentación que establezca estos protocolos seguros. Los equipos son configurados de manera segura mediante la experiencia del equipo de TIC y el apoyo de proveedores expertos. La institución se apoya en mecanismos de envío y recepción asociados a la suite colaborativa de Microsoft como lo son MS Sharepoint, MS Teams y MS OneDrive. Actualmente, no se realizan pruebas de penetración o análisis de vulnerabilidades debido a temas presupuestarios.	**1.** Se recomienda un procedimiento de configuración de equipos de red de forma segura, este procedimiento debe establecer todos los componentes a configurar en los diferentes activos para cumplir con la línea base de configuración y los requisitos de seguridad de la institución. Se recomienda documentar una política de seguridad de las comunicaciones la cual establezca los diferentes protocolos a permitir dentro de las comunicaciones; posteriormente ajustar las políticas de las herramientas perimetrales para cumplir con esta. Documentar una política de transferencia de información la cual establezca los mecanismos oficiales y seguros para la transmisión de información, tanto a nivel interno como externo. Valorar la ejecución de pruebas de penetración y/o análisis de vulnerabilidades.

DSS05.03 GESTIONAR LA SEGURIDAD DE PUNTO FINAL	
Hallazgo o Avance	***Recomendación***
Los sistemas operativos son configurados de manera segura mediante la experiencia del Equipo de TIC y el apoyo de proveedores expertos. **2.** La institución posee configurado el bloqueo de las sesiones de usuarios aproximadamente después de 5 minutos. **3.** Para la gestión de dispositivos móviles y teletrabajo, se poseen políticas configuradas en el firewall para su operación, adicionalmente se requiere el uso de una VPN. **4.** Las redes son configuradas de manera segura mediante la experiencia del equipo de TIC y el apoyo de proveedores expertos. **5.** Los equipos finales poseen filtrado de tráfico mediante la solución de antivirus. **6.** Para poder realizar modificaciones a los sistemas, se requiere de usuarios administradores y se poseen políticas en el Active Directory para evitar modificaciones no autorizadas. **7.** Todos los equipos están dentro de oficinas o laboratorios cerradas con llave, adicionalmente la institución posee mecanismos de seguridad física como puertas con cerraduras electrónicas y guardias. **8.** A la hora de la eliminación o desecho de endpoint se retiran todos los dispositivos de almacenamiento y posteriormente se coordina el desecho respectivo. **9.** Dentro de la seguridad perimetral se poseen configurados diversos perfiles de acceso a internet, de	establecer todos los componentes a configurar en los diferentes activos para cumplir con la línea base de configuración y los requisitos de seguridad de la institución. **2.** Documentar una política de escritorio y pantalla limpios la cual establezca la directriz del bloqueo de los equipos de trabajo en todo momento cuando no están en uso; adicionalmente incluir directrices que asegurar que los escritorios y pantallas se mantengan limpios de información confidencial. **3.** Documentación de política de dispositivos móviles y teletrabajo, la cual establezca las reglas y directrices para el uso de dispositivos móviles y el teletrabajo. **4.** Documentar una política de clasificación y etiquetado de la información la cual establezca los mecanismos para clasificar y etiquetar la información en base a su criticidad e importancia para la institución. **5.** Documentar una política sobre el uso de controles criptográficos la cual establezca los protocolos y mecanismo a utilizar para la encriptación de la información que así lo requiera. Valorar la implementación de una herramienta DLP (Data Loss Prevention que permita proteger la información sensible de la institución, tanto en reposo como en tránsito.

modo que algunos sitios están bloqueados según los requerimientos de negocio. **10.** No se identifica una clasificación de la información que permita cifrar otra información según su categoría.	
DSS05.04 GESTIONAR LA IDENTIDAD DEL USUARIO Y EL ACCESO LÓGICO.	
Hallazgo o Avance	***Recomendación***
1. Los diferentes roles y permisos configurados en sistemas y dispositivos de seguridad han sido desarrollados de acuerdo con las necesidades de la institución. **2.** Los cambios en accesos son gestionados a través del correo electrónico y pueden ser solicitados únicamente por aquellos jefes de departamento. **3.** Únicamente aquellos usuarios del equipo de TIC que requieren accesos administradores los poseen; no obstante, la gestión de usuarios como “root” o “admin” no está normado. **4.** La autenticación en los diferentes sistemas es realizada a través de Active Directory. **5.** Los sistemas poseen registros de auditoria para identificar las acciones realizadas. **6.** Se posee una coordinación con la unidad de recursos humanos para llevar a cabo revisiones periódicas de accesos.	**1.** Documentar una política de control de accesos que tenga como objetivo proteger los activos de información de los riesgos de seguridad; la política debe cubrir todos los usuarios, sistemas y dispositivos de seguridad y debe definir las responsabilidades de la unidad de TIC y negocio. **2.** Documentar una política de desarrollo seguro que establezca los parámetros que deben cumplir los sistemas desarrollados por la municipalidad, incluyendo la autenticación de un solo punto (SSO).

DSS05.05 GESTIONAR EL ACCESO FÍSICO A LOS ACTIVOS DE TI.	
Hallazgo o Avance	***Recomendación***
Las oficinas de TIC se encuentran aisladas y protegidas mediante un encierro; adicionalmente, se posee una bitácora de accesos. Los funcionarios poseen un carné institucional y deben portarlo en todo momento. Los visitantes son acompañados en todo momento por personal de TI, esto dentro de las posibilidades y naturaleza del trabajo. Los diferentes roles de la municipalidad no establecen áreas de acceso restringidos o autorizados. No se realiza concientización en temas de seguridad física.	**1.** Documentar una política de seguridad física y ambiental la cual establezca claramente las medidas de seguridad física y ambiental que deben implementarse en la institución, dentro de estas medidas se destacan las siguientes: a. El uso de carné institucional en todo momento. b. El acompañamiento de visitantes y proveedores en todo momento. c. La documentación de todas las solicitudes de acceso. d. La documentación de los roles de accesos en base a las necesidades del negocio y el principio de menor privilegio. e. La concientización de temas de seguridad física.
DSS05.06: GESTIONAR DOCUMENTOS SENSIBLES Y DISPOSITIVOS DE SALIDA.	
Hallazgo o Avance	**Recomendación**
La institución no posee un procedimiento para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa. Se poseen algunos controles criptográficos para proteger información almacenada, sin embargo, no se poseen criterios para la clasificación de la información. La unidad de TIC realiza las configuraciones de los accesos basándose en el principio de menor privilegio.	Documentar un inventario de activos de información con el propósito de identificar aquellos activos críticos para la institución.

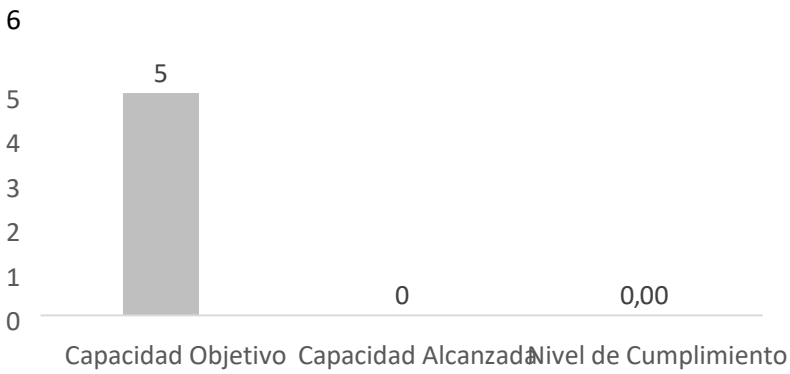
	No se identifica la presencia de un inventario de documentos sensibles y dispositivos de salida. La información física se encuentra protegida en las diferentes dependencias o departamentos bajo llave.	
DSS05.07 GESTIONAR LAS VULNERABILIDADES Y MONITORIZAR LA INFRAESTRUCTURA PARA DETECTAR EVENTOS RELACIONADOS CON LA SEGURIDAD		
	Hallazgo o Avance	***Recomendación***
1.	La institución posee contratado un servicio externo de monitoreo de eventos de seguridad, quienes revisan regularmente los eventos y gestionan los posibles eventos de seguridad.	**1.** Ninguna.

Administración de la Infraestructura Tecnológica

BAI10 - Gestionar la Configuración

El propósito del objetivo BAI10 es proporcionar información suficiente sobre los activos de servicio para facilitar que el servicio se gestione de forma eficiente. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.

Figura 17. BAI10 Gestionar la configuración



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad y el nivel de cumplimiento es de 0 de un 100%, esto implica que el proceso se no se ha establecido.

ESTADO GENERAL DEL PROCESO	
BAI10.01 ESTABLECER Y MANTENER UN MODELO DE CONFIGURACIÓN	
Hallazgo o Avance	***Recomendación***
1. Actualmente la unidad de TIC no posee un proceso para la gestión de la configuración, debido a esto, no se posee un modelo de configuración el cual defina el alcance y nivel de detalle sobre la gestión de la configuración. **2.** Del mismo modo, no se identifica la presencia de un modelo lógico para la gestión de la configuración, incluida la información de los tipos de elementos de configuración (CI), atributos, tipos de relaciones, atributos de relaciones y códigos de estado.	**1.** Se recomienda documentar una metodología para la gestión de la configuración, en la cual se establezca la necesidad de un modelo de configuración, el cual detalle el alcance y el nivel de detalle de los elementos de configuración a registrar. **2.** Se recomienda documentar un Modelo de Configuración el cual defina la información de los tipos de elementos de configuración (CI), atributos, tipos de relaciones, atributos de relaciones y códigos de estado.

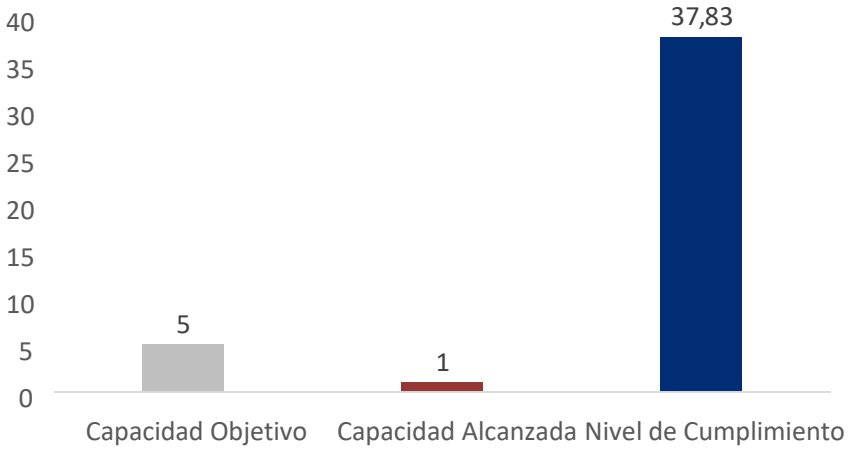
BAI10.02 ESTABLECER Y MANTENER UN REPOSITORIO DE LA CONFIGURACIÓN Y UNA LÍNEA DE REFERENCIA	
1. Debido a lo anteriormente mencionado, la unidad de TIC no posee un repositorio de configuración (CMDB). **2.** Derivado de lo anterior, no es posible poblar el repositorio con las líneas de referencia actuales de los servicios de TI. **3.** Asimismo, no es posible poblar el repositorio con las líneas de referencia actuales de los servicios de TI debido a la ausencia de ambos elementos.	**1.** Establecer dentro de la metodología la presencia de un repositorio de configuración (CMDB) desarrollado a partir del Modelo de Configuración. **2.** Identificar todos los Elementos de Configuración (CI) y sus relaciones, posteriormente poblar el repositorio con esta información. **3.** Valorar la adquisición de una herramienta para la gestión de la configuración.

BAI10.03 MANTENER Y CONTROLAR LOS ELEMENTOS DE CONFIGURACIÓN	
Hallazgo o Avance	***Recomendación***
1. Ante la ausencia de un repositorio de configuración y un proceso de gestión de cambios, no se identifican regularmente los cambios a los elementos de configuración (CI). Debido a lo anterior, no es posible asegurar que los cambios sigan un proceso ordenado para su revisión, aprobación y aplicación.	**1.** Establecer dentro de la metodología la valoración, aprobación y aplicación de los cambios a los CI's; esto de acuerdo con el proceso de Gestión de Cambios.
BAI10.04 – GENERAR INFORMES DE ESTADO DE LA CONFIGURACIÓN	
1. Debido a la ausencia del repositorio de configurar y acciones realizadas en torno a este, no se identifican informes sobre cambios de estado en este.	**1.** Establecer dentro de la metodología la identificación de requisitos asociados a los informes de gestión de configuración y desarrollarlos en base a estos.
BAI10.05 – VERIFICAR Y REVISAR LA INTEGRIDAD DEL REPOSITORIO DE CONFIGURACIÓN	
1. Debido a la ausencia del repositorio de configuración, no se verifica la integridad de la información presente en este.	**1.** Se recomienda establecer dentro de la metodología la revisión periódica de los elementos físicos presentes y su comparación con lo establecido dentro de los registros, comunicar desviaciones y aplicar los cambios requeridos para asegurar que la información presente es precisa.

DSS01 – Gestionar las Operaciones

El propósito del objetivo DSS01 es proporcionar los resultados de los productos y servicios operativos de TI según lo planeado. Es decir, se encarga de coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de TI, internos y externalizados.

Figura 18. DSS01 Gestionar las operaciones.



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 37,83% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
DSS01-01 EJECUTAR PROCEDIMIENTOS OPERATIVOS	
Hallazgo o Avance	***Recomendación***
1. La unidad de TIC posee algunos procedimientos operativos los cuales están aprobados y publicados en su página web; estos procedimientos apoyan el desarrollo y ejecución de tareas operativas. A pesar de poseer diversos procedimientos operativos, la unidad de TIC carece de un calendario de operaciones el cual establezca las actividades a realizar, su frecuencia y el responsable de ejecutarlas. Debido a la ausencia del calendario de operaciones, no es posible monitorizar su cumplimiento y rendimiento. Actualmente, el proceso de incidentes aún no está completamente desarrollado e implementado; por lo tanto, no es posible asegurar que los incidentes derivados de actividades operativas son registrados y atendidos según este proceso.	**1.** Desarrollar una Metodología de Gestión de Operaciones de TI, la cual establezca directrices para garantizar la gestión e implementación efectiva de todos los servicios de I&T para satisfacer los requisitos del negocio. Se recomienda el desarrollo de un calendario de operaciones el cual incluya todas las operaciones requeridas para operar los servicios de IT, posterior a su implementación; supervisar su cumplimiento. Se recomienda incluir dentro de la metodología de gestión de incidentes, el registro de los incidentes asociados a la ejecución de actividades operativas.

DSS01-02 GESTIONAR SERVICIOS TERCERIZADOS DE TI	
Hallazgo o Avance	***Recomendación***
Los servicios tercerizados son gestionados cuidadosamente por la unidad de TIC, esto es realizado mediante el desarrollo de pliegos de condiciones con cláusulas que establezcan requisitos de seguridad y de soporte que los proveedores deben cumplir. La unidad de TIC se encuentra en proceso de implementación de los procesos asociados a la gestión de servicios de TI (ITSM) como lo es la gestión de cambios o la gestión de la configuración, por lo que no es posible asegurar que estos procesos se integren con los servicios tercerizados. Si fuese necesario, el área de TIC se encuentra dentro de la potestad de realizar una auditoría o revisión para asegurar que los diferentes proveedores cumplen con los requisitos establecidos en el pliego de condiciones.	Incluir dentro de la metodología, la gestión de los servicios tercerizados a través de los diversos procesos internos de gestión de servicios de TI. Alinear el desarrollo de pliegos de condiciones con los niveles de servicios requeridos por parte del negocio, así como otros requisitos derivados de la implementación de otros componentes del sistema de gestión de I&T; por ejemplo, seguridad, continuidad o privacidad.

DSS01-03 MONITORIZAR LA INFRAESTRUCTURA DE TI	
Hallazgo o Avance	***Recomendación***
1. Actualmente la unidad de TIC realiza el monitoreo de la infraestructura de manera manual, lo que no permite el registro de eventos. **2.** Debido a lo mencionado en los hallazgos anteriores, no se identifican incidentes asociados a actividades de monitoreo.	**1.** Incluir dentro de la metodología de gestión de incidentes, el registro de los derivados de eventos de advertencia o excepción.
DSS01-04 GESTIONAR EL MEDIOAMBIENTE	
1. La institución posee una brigada, la cual se encarga de coordinar las respuestas los posibles desastres naturales. **2.** Las instalaciones de TI se encuentran protegidas de amenazas medioambientales; además, se prohíbe el consumo de comida, bebida y fumar en áreas sensibles. **3.** La unidad de TIC realiza mantenimiento para asegurar que las instalaciones de TI se encuentran limpias en todo momento, libres de papelería y/o cajas de cartón. **4.** Las instalaciones de TI poseen diversos mecanismos para la prevención de amenazas medioambientales, como detectores de humo y extintores. **5.** La institución no posee pólizas de seguros, por lo que no se identifican esfuerzos para el cumplimiento de los requisitos asociados a estas pólizas.	**1.** Incluir dentro del perfil de riesgos de I&T, los riesgos medioambientales a los cuales están expuestas las instalaciones de TI. **2.** Se recomienda documentar una Política para la Gestión de las Instalaciones la cual documente las directrices para la protección del centro de datos y las instalaciones de TI.

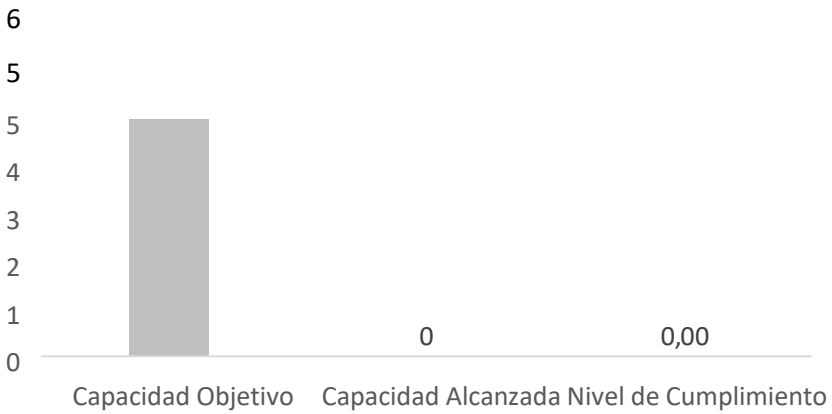
DSS01-05 GESTIONAR LAS INSTALACIONES	
Hallazgo o Avance	***Recomendación***
1. El centro de datos de la Institución se encuentra protegido contra amenazas eléctricas, esto mediante la presencia de UPS y planta eléctrica. **2.** De manera periódica; la planta eléctrica es puesta a prueba para asegurar que mantiene funcionando correctamente. **3.** En materia de telecomunicaciones, se poseen dos enlaces de internet de diversos proveedores para asegurar una alta disponibilidad. **4.** El cableado de telefonía y red se encuentra parcialmente ordenado y etiquetado. **5.** Debido a que el proceso de incidentes aún no está completamente desarrollado; no se poseen incidentes resultantes alarmas medioambientales.	**1.** Se recomienda incluir dentro de la Política para la Gestión de las Instalaciones los diversos mecanismos de seguridad actualmente implementados en esta. **2.** Se recomienda incluir dentro de la metodología de gestión de incidentes, el registro de los incidentes derivados de alarmas medioambientales (alarmas de humo, incendio o humedad); adicionalmente, valorar la posible integración de estos mecanismos de detección con herramientas de monitoreo para asegurar la centralización de los datos

Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos

DSS04 - Gestionar la Continuidad

El propósito del objetivo DSS04 es que la institución pueda adaptarse rápidamente, continuar con las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la empresa en caso de una interrupción significativa (p.ej., amenazas, oportunidades, demandas).

Figura 19. DSS04 Gestionar la continuidad.



Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad y el nivel de cumplimiento es de 0% de un 100%, esto implica que el proceso se no se ha establecido.

Estado General del Proceso	
DSS04.01 DEFINIR LA POLÍTICA DE CONTINUIDAD DEL NEGOCIO, SUS OBJETIVOS Y ALCANCE	
Hallazgo o Avance	***Recomendación***
1. La institución debe definir una política y alcance para la continuidad del negocio, en línea con sus objetivos y estrategias, para mejorar su resiliencia. A continuación, se describen los hallazgos encontrados: a. La institución aún no ha realizado un inventario completo de los procesos y actividades de servicio, tanto internos como externos, que son esenciales para sus operaciones. b. Las partes interesadas clave que deben participar en la definición de los objetivos y políticas de continuidad del negocio aún no han sido identificadas. No se encontró evidencia suficiente que respalde la afirmación de que el CUC cuenta con una política de continuidad de las operaciones.	**1.** La Institución debe documentar una política que contribuya al establecimiento del alcance de la continuidad de las operaciones de negocio, alineada con su realidad y objetivos estratégicos, con el objetivo de garantizar que el CUC pueda mantener sus operaciones en caso de interrupciones. **2.** La Institución debe realizar un inventario completo de los procesos y actividades de servicio que son críticos para la ejecución de sus operaciones, tanto internos como externos, incluyendo los procesos clave y los procesos de apoyo, con el objetivo de identificar los procesos y actividades que son esenciales para el funcionamiento del CUC. **3.** Desarrollar una política de gestión de crisis, en la que se definan las directrices y la secuencia de la respuesta ante crisis en áreas claves del CUC con el objetivo de garantizar una respuesta rápida y efectiva ante situaciones críticas. Se sugiere que la institución establezca un enfoque integral para la gestión de la continuidad del negocio y la gestión de crisis, con el objetivo de garantizar que el CUC pueda mantener sus operaciones en caso de interrupciones y responder efectivamente a situaciones críticas. Esto incluye la documentación de políticas claras y alineadas con los objetivos estratégicos, así como la realización de un inventario completo de los procesos críticos de la institución (BIA). También es importante que la Institución desarrolle planes de respuesta de crisis y establezca un proceso de revisión y actualización regular de estos planes.

DSS04.02 MANTENER LA RESILIENCIA DEL NEGOCIO	
Hallazgo o Avance	***Recomendación***
1. La institución debe evaluar las opciones de resiliencia ante posibles desastres naturales, tecnológicos o humanos, y elegir una estrategia viable y rentable para asegurar la continuidad de sus operaciones. Se identificaron los siguientes hallazgos: a. La institución no ha evaluado opciones de resiliencia ni ha elegido estrategias viables y rentables para garantizar la continuidad y recuperación de sus operaciones ante posibles desastres. b. No se ha encontrado evidencia suficiente para afirmar que se ha realizado un análisis de impacto en el negocio (BIA). c. Como resultado de lo anterior, aún no se han identificado los RTO (tiempo de recuperación objetivo) y los RPO (punto objetivo de recuperación) para los procesos críticos de negocio. c. Al no haber estrategias de recuperación definidas, tampoco se han comunicado ni aprobado por la dirección de la institución.	**1.** El CUC debe realizar un Análisis de Impacto en el Negocio (BIA) para identificar el impacto que tendría una interrupción en sus operaciones. a. Como resultado del análisis de impacto en el negocio, se deben identificar los RTO (tiempo objetivo de recuperación) y los RPO (punto objetivo de recuperación) para la institución en caso de desastre. b. Además, es importante identificar los posibles escenarios de desastre que podrían afectar a la institución y llevar a cabo una evaluación preliminar de riesgos para establecer las estrategias de recuperación correspondientes. c. c. Para cada estrategia de recuperación, se debe identificar los requisitos y costos de recursos necesarios para su implementación.

DSS04.03 DESARROLLAR E IMPLEMENTAR UNA RESPUESTA DE CONTINUIDAD DEL NEGOCIO	
Hallazgo o Avance	***Recomendación***
1. La institución debe desarrollar un plan integral de continuidad de negocio y recuperación ante desastres que esté alineado con su estrategia. Para ello, la institución debe considerar cualquier interrupción que pueda afectar su funcionamiento y desarrollar un proceso de recuperación que permita la reanudación del procesamiento de negocio en el menor tiempo posible. El plan debe contener, como mínimo, los siguientes componentes: a. Acciones y comunicaciones de respuesta a incidentes que deben tomarse en caso de interrupción. b. Condiciones y procedimientos de recuperación que permitan la reanudación del procesamiento de negocio. c. Recursos necesarios para respaldar los procedimientos de continuidad y recuperación, considerando las personas, las instalaciones y la infraestructura de TI. d. Requisitos de copias de seguridad de la información necesarias para respaldar los planes. Habilidades requeridas para los individuos involucrados en la ejecución del plan y los procedimientos.	**1.** Documentar su plan de continuidad de negocio y su plan de recuperación ante desastres, los cuales deben contener, como mínimo, los siguientes elementos: a. Acciones y comunicaciones de respuesta ante incidentes que se deben tomar en caso de interrupción. b. Condiciones y procedimientos de recuperación que permitirán la reanudación del procesamiento de negocio. c. Recursos necesarios para respaldar los procedimientos de continuidad y recuperación, incluyendo personas, instalaciones e infraestructura de TI. d. Requisitos de copias de seguridad de la información necesarios para respaldar los planes. e. Habilidades requeridas para las personas involucradas en la ejecución del plan y los procedimientos. **2.** Una vez documentados los planes, deben ser distribuidos de forma segura a las partes interesadas autorizadas y asegurarse de que sean accesibles en todos los escenarios de desastre. c. Es importante realizar la creación de un plan de gestión de crisis y un plan de comunicación para garantizar una comunicación efectiva con los funcionarios en caso de un desastre. Estos planes deben ser desarrollados previamente y actualizados periódicamente para asegurar que se encuentren vigentes y en línea con los objetivos y necesidades del negocio.

DSS04.04 REALIZAR EJERCICIOS, PROBAR Y REVISAR EL PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) Y EL PLAN DE RESPUESTA ANTE DESASTRES (DRP)	
Hallazgo o Avance	***Recomendación***
1. La Institución debe realizar pruebas periódicas de continuidad para verificar el comportamiento de los planes frente a los resultados predeterminados, mantener la resiliencia del negocio y permitir el desarrollo de soluciones innovadoras. Sobre este particular, se ha identificado que la institución no lleva a cabo estas pruebas debido a la falta de un Plan de Continuidad de Negocio y un Plan de Recuperación Ante Desastres.	**1.** Una vez que se hayan documentado los planes de continuidad y recuperación ante desastres, la institución debe seguir los siguientes pasos: a. Definir y acordar con las partes interesadas ejercicios realistas que validen los procedimientos de continuidad. Esto debe incluir la definición clara de roles y responsabilidades, así como acuerdos de retención de datos que minimicen la disrupción de los procesos del negocio. b. Asignar roles y responsabilidades para la ejecución de los ejercicios y pruebas del plan de continuidad. **2.** Se recomienda programar ejercicios y actividades de prueba de acuerdo con lo definido en los planes de continuidad. Estas pruebas deben realizarse periódicamente para evaluar la efectividad de los planes y asegurar la resiliencia del negocio. **3.** Realizar ejercicios de concientización sobre la continuidad del negocio, con el fin de verificar el nivel de comprensión de las partes interesadas sobre los planes y procedimientos de continuidad del negocio, estos se pueden realizar por medio de charlas o talleres de concientización.

DSS04.05 REVISAR, MANTENER Y MEJORAR LOS PLANES DE CONTINUIDAD	
Hallazgo o Avance	***Recomendación***
1. La institución debe realizar revisiones periódicas de la capacidad de continuidad para asegurar su idoneidad, adecuación y efectividad. En este sentido, se identificaron los siguientes hallazgos: a. La institución no realiza revisiones periódicas de los planes de continuidad y su capacidad contra las hipótesis consideradas y los objetivos estratégicos y operativos actuales del negocio. b. De igual forma, no se revisan regularmente los planes de continuidad para considerar el impacto de nuevos o mayores cambios a lo interno del CUC.	**1.** La institución debe establecer procedimientos de revisión periódica de sus planes de continuidad de negocio, esto con el fin de garantizar su actualización y la preparación de la institución ante posibles escenarios de desastre, estos planes deben incluir la siguiente información: a. Objetivos. b. Alcance. c. Activación del plan. d. Procedimientos de continuidad de negocio.
DSS04.06 REALIZAR FORMACIÓN SOBRE EL PLAN DE CONTINUIDAD	
1. En la actualidad, la Institución no ofrece sesiones periódicas de formación a todas las partes internas y externas involucradas sobre los procedimientos y sus roles y responsabilidades en caso de interrupción.	**1.** La institución debe incluir como parte de sus programas de capacitación y entrenamiento relacionadas con continuidad de negocio y con los planes, estrategias, procedimientos de continuidad de negocio documentados.
DSS04.07 ADMINISTRAR LOS ACUERDOS DE RESPALDO	
1. La institución debe establecer prácticas que permitan mantener la disponibilidad de la información crítica para el negocio. Sobre este particular se debe indicar que no se obtuvo evidencia suficiente para respaldar el cumplimiento de esta práctica.	**1.** Documentar procedimientos de respaldos y recuperación luego de la ejecución de un ejercicio de continuidad de negocio, donde se identifiquen los activos de información críticos para la Institución, su periodo de retención y prioridad según las necesidades del negocio y alineado con el RTO y el RPO definidos por la Institución.

ASEGURAMIENTO

MEA04 – Gestionar el Aseguramiento

El propósito del objetivo MEA04 es facilitar a la institución el diseño y desarrollo de iniciativas de aseguramiento eficaces y eficientes proporcionando una guía sobre la planificación, alcance, ejecución y seguimiento de las revisiones de aseguramiento con una hoja de ruta basada en estrategias de aseguramiento.

Figura 20. MEA04 Gestionar el aseguramiento.

Nota: elaboración propia.

Según el gráfico anterior, se puede verificar que el nivel de capacidad alcanzado por el objetivo es de 1 y el nivel de cumplimiento es de 19,44% de un 100%, esto implica que, el proceso se ha establecido de manera básica y se llevan a cabo algunas actividades relacionadas con el mismo. Sin embargo, la implementación es informal o improvisada y no está completamente documentada.

Estado General del Proceso	
MEA04.01 ASEGURAR QUE LOS PROVEEDORES DE ASEGURAMIENTO SEAN INDEPENDIENTES Y ESTÉN CUALIFICADOS	
Hallazgo o Avance	***Recomendación***
1. La institución posee un área de auditoría interna totalmente independiente, quien guía las diversas iniciativas de aseguramiento; no obstante, su alcance para con I&T se ve limitado debido a que no es su área de expertis. **2.** Adicionalmente, la institución posee un Código de Ética el cual rige el comportamiento esperado de todos los funcionarios de la institución.	**1.** Ninguno.
MEA04.02 DESARROLLAR UNA PLANIFICACIÓN DE INICIATIVAS DE ASEGURAMIENTO BASADA EN RIESGOS	
1. El área de auditoria realiza iniciativas en diferentes departamentos, unidades y procesos de la institución; sin embargo, no se identifica la presencia de un programa integral de auditoria que incluya a I&T.	**1.** Documentar un Programa de Auditoria que abarque las diferentes unidades de negocio, incluyendo la unidad de TIC.

MEA04.03 DETERMINAR LOS OBJETIVO S DE LA INICIATIVA DE ASEGURAMIENTO	
Hallazgo o Avance	***Recomendación***
1. En la planificación de las iniciativas se definen los límites y los objetivos de estas; no obstante, las auditorias asociadas a la unidad de TIC aún no incluyen componentes asociados a COBIT como lo son la cascada de metas la cual incluye las metas institucionales y las metas de alineamiento.	**1.** Documentar una metodología para la gestión de aseguramientos de I&T la cual incluya los siguientes elementos: a. Entender la estrategia, prioridades, contexto interno y externo de la institución. b. Evaluar de manera específica aquellos aspectos diferenciadores a tomar en cuenta con las iniciativas de I&T, como, por ejemplo, la revisión de la correcta aplicación de la cascada de metas para asegurar un correcto alineamiento entre I&T y el negocio.
MEA04.04 DEFINIR EL ALCANCE DE LA INICIATIVA DE ASEGURAMIENTO.	
1. Como parte de la definición del alcance de la auditoria, se definen los diferentes componentes a incluir dentro de esta. **2.** A pesare de lo anterior, no es posible asegurar que el alcance se encuentra perfeccionado y alineado con la arquitectura empresarial y la ausencia de esta.	**1.** Incluir dentro de la metodología, el aseguramiento de que el alcance esté alineado con la arquitectura empresarial, una vez esta haya sido desarrollada.

MEA04.05 DEFINIR EL PROGRAMA DE TRABAJO PARA LA INICIATIVA DE ASEGURAMIENTO	
Hallazgo o Avance	***Recomendación***
1. Actualmente, no se identifica que se desarrollen pasos detallados para la recopilación y evaluación de la información considerada dentro del alcance de la iniciativa de aseguramiento. **2.** Asimismo, no se identifica que se definan las buenas prácticas o prácticas esperadas para los controles de gestión.	**1.** Incluir dentro de la metodología los siguientes elementos: a. La definición de pasos detallados para la recolección de la información requerida. b. La definición de las buenas prácticas esperadas.
MEA04.06 EJECUTAR LA INICIATIVA DE ASEGURAMIENTO, ENFOCÁNDOSE EN LA EFECTIVIDAD DEL DISEÑO	
1. Las iniciativas son ejecutadas de acuerdos los procedimientos internos; sin embargo, no se identifica que se revise si se han asignado las responsabilidades globales del componente de gobierno y de la rendición de cuentas. Asimismo, no se identifica que se considere el esfuerzo dedicado a mantener **2.** los controles y su rentabilidad asociada.	**1.** Se recomienda incluir dentro de la metodología los siguientes elementos: a. Preguntar al dueño del control si se han asignado las responsabilidades globales del proceso. b. Considerar el esfuerzo dedicado a mantener los controles de gestión y su rentabilidad asociada.

MEA04.07 EJECUTAR LA INICIATIVA DE ASEGURAMIENTO, ENFOCÁNDOSE EN LA EFICACIA OPERATIVA	
Hallazgo o Avance	***Recomendación***
1. Las iniciativas son ejecutadas de acuerdos los procedimientos internos; sin embargo, no se identifica que se evalúa si un control puede ser más eficiente.	**1.** Incluir dentro de la metodología los siguientes elementos: a. Evaluar si se han alcanzado los resultados esperados para cada uno de los controles. b. Investigar si un control de gestión puede ser más eficiente.
MEA04.08 INFORMAR Y HACER SEGUIMIENTO A LA INICIATIVA DE ASEGURAMIENTO	
1. Una vez finalizada la auditoría, se genera un informe donde se documentan los hallazgos y el impacto de estos.	**1.** Incluir dentro de la metodología los siguientes elementos: a. Documentar el impacto de las debilidades del control. b. Proporcionar a la dirección un informe que sustente los resultados de la iniciativa. c. Garantizar que el trabajo está finalizado, cumple con los objetivos y tiene una calidad aceptable
MEA04.09 HACER SEGUIMIENTO A LAS RECOMENDACIONES Y A LAS ACCIONES	
1. Cuando se identifican oportunidades de mejora, los diferentes encargados de área o jefes de unidades / departamentos son los responsables de ejecutarlas y dar seguimiento al cumplimiento de estas.	**1.** Incluir dentro de la metodología los siguientes elementos: a. Acordar e implementar las acciones necesarias para resolver las debilidades y brechas identificadas. b. Hacer un seguimiento para determinar si se llevaron a cabo acciones correctivas.

Capítulo V. Propuesta de solución

Con base en el análisis de brechas que se realizó en los capítulos anteriores, se confeccionó un plan de implementación del SGSI a la medida del CUC. A continuación se detalla cada una de las fases propuestas para la implementación.

Fase 1

Responsable: alta gerencia.

1. **Definición de la política:** Definir parte normativa, tener ese cimiento, ¿por qué? ¿Es importante la SGSI?, ¿para qué? ¿Cuál es su objetivo? En esta fase debe asignarse la persona o equipo responsable de cada fase.

2. **Definición de la organización:** Definir los roles, responsabilidades y autoridades de las personas, en seguridad desde el inicio garantizar el compromiso. Se debe formalizar la organización para que haga parte de la definición y establecimiento del SGSI

3. **Definición del alcance del SGSI:** Definir cuáles procesos estarán en el alcance del SGSI basados en criterios o requerimientos de la dirección. Aprobar el alcance inicial del SGSI y evaluar posibles mejoras con base en los activos y riesgos identificados. Conocer información crítica de la empresa.

4. **Capacitación y entrenamiento:**

   Dirigida a la organización de la seguridad en:

   - ü Implementación de SGSI
   - ü Auditoría de SGSI
   - ü Gestión de riesgos
   - ü Seguridad de la información
   - ü Gestión de incidentes
   - ü Gestión de vulnerabilidades

5. **Análisis de brechas (Gap):** Verificar cómo se cumple la ISO 27001 y aprovechar recursos actuales, evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito. Gap se refiere al espacio entre "dónde estamos" (el presente) y "dónde queremos estar" (el objetivo a alcanzar). Un análisis de deficiencias también puede denominarse análisis de necesidades, permitiéndonos determinar lo que nos falta y los recursos

necesarios para alcanzar los objetivos. Realizar un Gap anualmente y compararlo con el año anterior. Reportar los avances en el SGSI.

En esta fase debe definirse un documento formal que defina y establezca el alcance del SGSI y que determine las partes o procesos de la organización que van a ser incluidos, así como los procesos críticos que se quieren proteger y por donde se va a iniciar, además de la definición de las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del SGSI. Esta cláusula determina la creación del primero de los documentos que constituyen el SGSI, "el alcance del sistema".

Así como que determine las partes o procesos de la organización que van a ser incluidos, así como los procesos críticos que se quieren proteger, por dónde se va a iniciar, además de la definición de las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del SGSI.

Se recomienda definir un proceso formal que establezca los procedimientos para la definición, implantación, mantenimiento y mejora continua del SGSI. Esta fase estaría a cargo de

Fase 2
Responsable: Funcionarios de TI

Esta fase consiste en explicar cada gestión

1. **Gestión de activos:**

   - Ø Definir una metodología práctica y adecuada a la institución.
   - Ø Identificar los activos valorarlos y clasificarlos.
   - Ø Entregar estas tareas a los procesos.
   - Ø Todo esto para saber qué es lo que hay que proteger.

2. **Gestión de vulnerabilidades:**

   - Ø Identificar y valorar vulnerabilidades no solo en las TIC sino en las personas y en la normatividad.
   - Ø Definir un ciclo de gestión de vulnerabilidades y que sea administrado continuamente.

- Ø Todo esto para conocer qué tipo de debilidades están presentes, para eso se puede contratar pruebas de intrusión, pruebas de ethical hacking, pruebas de vulnerabilidades, generando un valor dando así un análisis total y actual de qué tan expuesta está la institución ante los ataques cibernéticos, todo esto bajo un ambiente controlado

3. Gestión de Riesgos.

Si se conocen vulnerabilidades de punto anterior eso se convierte en riesgos, por lo tanto, es una fuente importante de los riesgos que posee la organización.

Este tipo de gestión se alimenta del estado actual de los controles, que vulnerabilidades posee la institución:

- Ø Integrarse a ciclos de identificación, valoración y tratamiento de riesgos existentes.
- Ø Es clave la planificación, documentación y seguimiento efectivo del tratamiento de los riesgos.
- Ø Solo las vulnerabilidades reales permiten identificar riesgos actuales.

4. Definición de controles

Integrar los controles técnicos, normativos y del recurso humano, importante para cada control definir:

- Ø Objetivo
- Ø Cómo se medirá su efectividad
- Ø Quién lo diseña
- Ø Quién lo administra
- Ø Quién lo revisa

5. Definición de planes de tratamiento:

- Ø Los planes deben ser entregados formalmente a las áreas implementadoras
- Ø Se debe hacer un seguimiento eficaz a estos planes de tratamiento y entregarlos a la operación.

La política de seguridad de la información debe delimitar que es lo que va a protegerse, de quién y por qué. Debe explicar que es lo que está permitido y qué no. Debe determinar los límites del comportamiento aceptable y cuál sería la respuesta si estos se incumplen, e identificar los riesgos a los que está sometida la organización. La política debe cumplir, al menos, con los siguientes requisitos:

a. Ser redactada en una manera accesible para todo el personal de la organización
b. Debe ser aprobada por el consejo directivo y publicada por la misma.
c. Debe ser de dominio público dentro de la organización.
d. Debe definir las responsabilidades teniendo en cuenta que éstas van asociados a la autoridad dentro de la institución.
e. Debe indicar que es lo que se protege en la organización (personal, información, imagen)
f. Debe ser personalizada para la institución.
g. Debe señalar las reglas y normas que va adoptar la organización y las medidas de seguridad que serán necesarias.
h. Debe definir lo que es seguridad de la información.
i. Debe definir un objetivo global de la política de seguridad de la información.
j. Debe definir el alcance e importancia de la seguridad como mecanismo de control que permite compartir la información.
k. Declaración formal por parte de la dirección apoyando los objetivos y principios de la seguridad de la información.
l. Debe definir las responsabilidades generales y específicas, en las que se incluirían los roles, pero nunca a las personas en concreto.
m. Referencias de documentación que pueda sustentar la política.

Adicionalmente, dentro de los temas la política debe incluir: el control de accesos, clasificación de los riesgos, la seguridad física y ambiental.

Se recomienda definir un período, al menos, una vez al año para revisión de la política de seguridad, además también se recomienda efectuar actualización cada vez que sucedan grandes incidentes de seguridad, después de auditorías sin éxito y/o frente a cambios que afectan a la estructura de la organización.

Fase 3

Responsable: equipo de gestión del SGSI: diversas gerencias y líderes de áreas del CUC, que podrían participar en la planificación y ejecución de las actividades del SGSI.

1. **Gestión de cultura:** Dirigido a todos los empleados, medir el conocimiento y comportamiento en cuanto a:

    - Ø La importancia de la seguridad de la información
    - Ø Qué es el SGSI
    - Ø La normatividad relacionada
    - Ø Responsabilidades

Implementación de controles

Se refiere específicamente a los controles derivados de la fase anterior.

- Ø Realizar la implementación de los controles tecnológicos, normativos y de los recursos humanos.
- Ø Apoyarse en expertos para la implementación de controles.

2. **Medición de controles**

Se debe establecer:

- Ø Cómo se mide la efectividad de cada control.
- Ø Cómo el control mitiga el riesgo para el cual fue implementado.

3. **Gestión de indicadores del SGSI**

Demostrar cómo el SGSI genera valor a la entidad, a través de:

- Ø La disminución de vulnerabilidades
- Ø La mitigación de riesgos
- Ø La gestión eficaz de incidentes
- Ø El incremento del cumplimiento

4. **Gestión de Incidentes:**

   - Ø Definición de procedimientos de gestión de incidentes integrados (TI, Seguridad, Continuidad, Físicos, etc.)
   - Ø Sensibilizar efectivamente la gestión de incidentes.
   - Ø Medir la efectividad de la gestión de incidentes.

Existe el riesgo de que algún funcionario que cambie rol o función dentro de la organización, que la jefatura correspondiente no deshabilite los accesos y privilegios que le competen al puesto anterior provocando que en el actual los mantenga. Para lo anterior se recomienda revisar la implementación de controles que garantice el mantenimiento de los accesos a los servicios de la institución. Se recomienda emitir un procedimiento formal y debidamente aprobado para la des habilitación de accesos y privilegios de todo el personal que: cambie de puesto o rol dentro de la institución, se encuentre incapacitado por un período prolongado, renuncie o despido laboral, personas pensionadas o jubiladas, vacaciones prolongadas. Este procedimiento debe definir el mecanismo y canal a utilizar para la comunicación, así como la frecuencia con la que debe realizarse.

Adicionalmente se recomienda definir un control para la revisión frecuente sobre el manejo de los accesos con el fin de garantizar una adecuada segregación de las funciones en los sistemas y aplicaciones institucionales. Dentro de la metodología de gestión de proyectos no se tienen definidos los requisitos a nivel de seguridad de la información en la gestión de proyectos. Los mismos se aplican dependiendo del tipo de proyecto que se encuentre en desarrollo. Por lo tanto, se recomienda incorporar dentro de la metodología de gestión de proyectos los requisitos necesarios para abordar el tema de seguridad de la información en la gestión de los proyectos, en todas sus fases.

Fase 4

Responsable: auditor interno

1. **Mecanismos de mejora continua:**

   - Ø Incentivar las acciones de mejora en el SGSI
   - Ø El SGSI debe estar integrado en la documentación y mejora continua de los procesos.

2. **Auditorías y revisión:**

    - Ø La auditoría interna del SGSI debe ser parte de los planes de auditoría anuales
    - Ø Se debe contar preferiblemente con auditores especializados en ISO 27001

3. **Cierre de hallazgos de auditoría:** Y a partir de la auditoria cerramos los hallazgos, siempre van a existir hallazgos, razón por la cual el SGSI siempre mejorará después de una auditoria y el cierre de sus hallazgos

    - Ø Garantizar los recursos para el cierre de los hallazgos

4. **Automatización y optimización:** Implementar herramientas tecnológicas para operar, y mantener el SGSI

    - Ø Software de gestión y reporte del SGSI (activos, riesgos, incidentes, medición, cumplimiento)
    - Ø Herramientas de gestión de vulnerabilidades
    - Ø Servicios de monitoreo y gestión de seguridad
    - Ø Herramientas de gestión de proyectos

Realizar en cada fase la forma en que se va a evaluar o documentar la ejecución o preparación de cada fase. El SGSI requiere de inversión real continua, por lo cual hay que garantizar tiempo y dinero para su operación y mejora. La implementación de Sistema de información para la gestión y el reporte de las actividades claves del SGSI es una necesidad natural que brinda los siguientes beneficios:

- Ø Información centralizada y con fácil acceso
- Ø Evidencia objetiva de la realización de actividades
- Ø Estandariza los métodos y los mecanismos utilizados
- Ø Generación de reportes oportunos
- Ø Toma de decisiones bien informadas
- Ø Medición efectiva del SGSI
- Ø Permite la integración entre diferentes gestiones
- Ø Brinda a los usuarios un entendimiento práctico de un SGSI

Para la última fase lo que se recomienda monitorear y medir los procesos de seguridad y controles. Por lo que es necesario contar con:

a) los métodos para monitorizar, medir, analizar y evaluar, cuando sea aplicable, para asegurar unos resultados adecuados.
b) definir cuándo deberán ser realizadas las monitorizaciones y mediciones
c) quién deberá monitorizar y medir.
d) cuando deberán ser analizados y evaluados (rangos de normalidad y anomalía) los resultados de la monitorización y medición
e) quién analizará y evaluará estos resultados.

Para lo anterior, es necesario definir una serie de indicadores sobre los procesos del área de seguridad, pero para ello es indispensable contar con la definición formal de un modelo de gobierno de seguridad y definir posterior los indicadores de desempeño del SGSI.

Es indispensable en el proceso de gestión de la seguridad de la información un alto compromiso de la dirección. El proceso de gestión de la seguridad de la información es vital para la consecución de los objetivos del negocio, aspecto que es de interés de los altos jerarcas. Para ello es necesario que al menos se establezca una sesión de los altos jerarcas y los responsables de la gestión del SGSI para valorar los temas y decisiones sobre la adecuada gestión del SGSI. Se podría definir que en forma cuatrimestral se ejecuten sesiones de seguimiento para valorar los temas del SGSI en conjunto con la alta dirección. Al menos deben cubrirse los siguientes puntos y que los mismos queden debidamente documentados.

- Cambios internos y externos que afecten la seguridad de la información
- Comentarios sobre el desempeño del SGSI
- Seguimiento y medición del SGSI
- Resultados de la auditoría interna sobre el SGSI
- Cumplimiento de los objetivos del SGSI.
- Retroalimentación de las partes interesadas.
- Resultados de las evaluaciones de riesgo y planes de tratamiento
- Oportunidades de mejora continua al SGSI

Capítulo VI Conclusiones

Después del proceso sistemático de recopilación, análisis y síntesis de información disponible en la literatura científica y académica sobre la realidad se concluye lo siguiente a partir de cada objetivo planteado:

1. Identificar oportunidades, riesgos y limitaciones del departamento de Tecnologías de la Información de la institución.

Oportunidades: Mediante estudios y análisis como éste, los profesionales de TI pueden identificar oportunidades para automatizar tareas, mejorar la eficiencia operativa, reducir costos mediante la implementación de sistemas y herramientas tecnológicas adecuadas.

La unidad de TI está al tanto de las últimas tendencias y avances tecnológicos, lo que le permite proponer soluciones innovadoras que impulsen la competitividad y el crecimiento de la empresa.

Los datos y análisis proporcionados por la unidad de TI pueden ayudar a la dirección de la institución a tomar decisiones informadas y estratégicas basadas en información relevante y actualizada.

Riesgos: La Unidad de TI debe procurar proteger y garantizar los datos confidenciales de la institución, implementando medidas de seguridad para prevenir ataques cibernéticos, pérdida de información y violaciones de privacidad, sin embargo, no se está cumpliendo al 100% con esta acción.

Limitaciones: Un departamento de TI es fundamental para garantizar el correcto funcionamiento de la infraestructura tecnológica de la empresa, proteger sus activos digitales, fomentar la innovación y mejorar la eficiencia operativa. Pese a que es un aspecto primordial en el CUC no se considera a TI como departamento sino como una unidad, hecho que limita la toma de decisiones importantes como la seguridad informática.

2. Evaluar los resultados de la auditoría AI-03-2021 realizada al departamento como parte del diagnóstico.

La información revela varias áreas de mejora en la Unidad de TI y la Seguridad de la Información del Colegio Universitario de Cartago (CUC):

Estructura y roles en la Unidad de TI

- **Actual**: Estructura jerárquica con un encargado y áreas de soporte técnico, análisis y desarrollo de sistemas.
- **Faltante**: Rol de Gestor de Servicios de TI y la necesidad de reevaluar la relevancia del área de análisis/desarrollo dado que los sistemas principales son adquiridos de proveedores externos.

Seguridad de la Información y Seguridad Informática

- **Debilidades**: El centro de datos presenta vulnerabilidades significativas.
- **Falta de Plan de Seguridad**: No hay un plan de seguridad de la información, haciendo a la institución vulnerable.
- **Cumplimiento Incompleto**: Solo un 64% de cumplimiento en el marco de seguridad, seguridad física y ambiental, seguridad de operaciones y comunicaciones, y controles de acceso.
- **Causa Principal**: Ausencia de un responsable que supervise y asegure el nivel adecuado de seguridad informática y de la información.

3. Diseñar el plan de acción en seguridad informática necesario para el Colegio Universitario de Cartago

La implementación de un SGSI es una Iniciativa de negocio y no de TI, la cual está diseñada para asegurar la protección de todos los activos de información. El proceso de la implementación final del SGSI consta de veintitrés pasos divididos en cuatro fases basadas en el ciclo de mejora continua PDCA (Planear, Hacer, Verificar, Actuar).

Adicionalmente, se debe desarrollar una política de seguridad de la información donde se establezcan las directrices para preservar las características de confiabilidad, integridad, confidencialidad y disponibilidad de los activos de información.

El Oficial de Seguridad de la Información será el encargado a nivel Institucional de establecer las pautas que permitan abordar la seguridad de la información de una forma integral, el proceso debe considerar todos los aspectos que intervienen en la seguridad de la información como son personal, tecnologías, controles de seguridad, servicios, productos, infraestructura, competencias y habilidades y la cultura organizacional.

Bajo este panorama, algunas las actividades a desarrollar son las siguientes:

1. Realizar un diagnóstico de los controles actuales y estado del SGSI.
2. Obtener la aprobación de la Alta Dirección para Operar el SGSI.
3. Diseñar la Política de Seguridad, en conjunto con la alta dirección la cual debe incluir al menos requisitos internos y externo
4. Desarrollar un Análisis de Aplicabilidad (SOA) para determinar cuáles son los controles que aplican a la institución.

5. Realizar una evaluación exhaustiva de los controles basados en una mejor práctica como ISO 27002.
6. Incluir dentro del plan de tratamiento de riesgos institucional, los riesgos de seguridad de la información y asegurar que los mismos son gestionados.
7. Implementar un plan de concientización asociado a la seguridad de la información, el cual debe abordar diferentes áreas como:

    - Seguridad de la Información.
    - Software Malicioso.
    - Seguridad Física.
    - Alcance
    - Objetivos
    - Roles y responsabilidades
    - Compromiso de la alta dirección

Referencias bibliográficas

Etek International. (2024, junio 25). Delitos financieros encabezan la lista de ataques cibernéticos en Latinoamérica. Prensario Tila. https://prensariotila.com/delitos-financieros-encabezan-la-lista-de-ataques-ciberneticos-en-latinoamerica/

Grados, R., Berrios, C., & Rocha, M. (2015, 6 de noviembre). Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO/IEC 27001. Repositorio Académico UPC. https://repositorioacademico.upc.edu.pe/handle/10757/581891?show=full&locale-attribute=es

Instituto Nacional de Ciberseguridad. (2021, 12 de abril). INCIBE publica el ranking de los 10 principales incidentes de Ciberseguridad a nivel mundial de 2016. Instituto Nacional de Ciberseguridad. https://www.incibe.es/incibe/sala-de-prensa/incibe-publica-el-ranking-los-10-principales-incidentes-ciberseguridad

López, T. (2023, 20 de enero). SGSI: Qué es y Cómo Implementarlo Conoce qué es un SGSI, por qué lo necesitas en tu empresa y cómo implementarlo para que sea exitoso. INNEVO. https://blog.innevo.com/que-es-sgsi

Martínez, J. (2015, septiembre). Seguridad de la información en pequeñas y medianas empresas (pymes). Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00002332.pdf

Norma ISO 27001. (n.d.). Que es un análisis de brechas GAP en ISO 27001. NORMA ISO 27001. https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

Toro, R. (2015, abril 23). La importancia de la norma ISO 27001. PMG-SSI. https://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/

Toro, R. (2017, enero 26). ¿Seguridad informática o seguridad de la información? PMG-SSI. https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Toro, R. (2018, febrero 1). Confidencialidad, integridad y disponibilidad. PMG-SSI. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/