UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN DEL DEPARTAMENTO DE TI EN EMPRESA DE VENTA DE EQUIPOS ELÉCTRICOS SEGÚN EN EL MARCO DE REFERENCIA COBIT 2019

Trabajo final de investigación aplicada, sometido a la consideración de la Comisión del Programa de Posgrado en Tecnologías de Información y Comunicación para la Gestión Organizacional, para optar al grado y título de Maestría Profesional en Tecnologías de Información y Comunicación para la Gestión Organizacional

ESTRELLA LÓPEZ LÓPEZ

Ciudad Universitaria Rodrigo Facio, Costa Rica

2024

Certificación de Filólogo

San Isidro de El General
Jueves 06 de junio de 2024

Señores

Sistema de Estudios de Posgrado
Universidad de Costa Rica
San José

Estimados señores:

La estudiante Estrella López López, me ha presentado para la revisión de estilo el proyecto de graduación titulado: "*Guía de buenas prácticas para la gestión del departamento de TI en empresa de venta de equipos eléctricos, según el marco de referencia Cobit 2019",* trabajo final de investigación aplicada sometido a consideración de la Comisión del Programa de posgrado en Tecnologías de Información y Comunicación para la Gestión Organizacional para optar al grado y título de Maestría Profesional en Tecnologías de Información y Comunicación para la Gestión Organizacional.

He revisado y corregido los aspectos referentes a estructura, gramática, acentuación, ortografía, puntuación y vicios de dicción que se trasladan al escrito. Además, he comprobado que se han incorporado las correcciones al presente documento.

Atentamente,

Lic. Carlos Bermúdez Vargas

Cédula 1 - 582 - 831
Colegiatura número 8757 (COLYPRO)

Lic. Carlos Bermúdez Vargas
Revisión de estilo de todo tipo de documentos
Tels. 2770-9060 / 83727341
elbermu09@gmail.com

DEDICATORIA

Quiero dedicarle mi trabajo a Dios porque sembró en mi esa semillita de no rendirme a pesar de las tempestades, de mantenerme en pie a pesar de que había cansancio, por tomarme mi mano y no soltarla hasta que este sueño fuera posible.

Por último, a mis padres, quienes me han dado grandes enseñanzas, consejos y momentos que han ido moldeando a la persona que soy hoy.

AGRADECIMIENTOS

Primeramente, agradezco a Dios por ser guía, darme la persistencia y la fuerza que necesito para lograr una meta más en mi vida.

Además, agradezco a la Universidad de Costa Rica por permitirme crecer como profesional darme ese apoyo para continuar en este camino, a mi tutor Mag. Verny Fernández Castro por su tiempo, sus consejos, motivación y orientación en el desarrollo del trabajo, a los lectores M.Sc. Francisco Blanco Chavarría y M.Sc. José Paz Barahona por sus aportes en la investigación.

También, estoy muy agradecida con la empresa de venta de equipos eléctricos por darme la oportunidad de llevar a cabo el trabajo de investigación en su organización.

Finalmente, agradezco a mi familia por escucharme y darme su apoyo para continuar, a mi pareja por estar en cada paso motivándome.

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Posgrado en Tecnologías de Información y Comunicación para la Gestión Organizacional de la Universidad de Costa Rica, como requisito parcial para optar el grado y título en Maestría Profesional en Tecnologías de Información y Comunicación para la Gestión Organizacional".

JAMES FRANCISCUS MC INTOSH MOLINA (FIRMA)
Firmado digitalmente por JAMES FRANCISCUS MC INTOSH MOLINA (FIRMA)
Fecha: 2024.06.18 10:13:21 -06'00'

M.Sc. James Mcintosh Molina
Representante de la Decana Sistema de Estudios de Posgrado

VERNI GERARDO FERNANDEZ CASTRO (FIRMA)
Firmado digitalmente por VERNI GERARDO FERNANDEZ CASTRO (FIRMA)
Fecha: 2024.06.18 18:20:49 -06'00'

M.Sc. Verni Fernández Castro
Profesor Guía

FRANCISCO JOSE BLANCO CHAVARRIA (FIRMA)
Firmado digitalmente por FRANCISCO JOSE BLANCO CHAVARRIA (FIRMA)
Fecha: 2024.06.18 14:30:18 -06'00'

M.Sc. Francisco Blanco Chavarría
Lector

JOSE RAFAEL PAZ BARAHONA (FIRMA)
Firmado digitalmente por JOSE RAFAEL PAZ BARAHONA (FIRMA)
Fecha: 2024.06.18 20:00:12 -06'00'

M.Sc. José Paz Barahona
Lector

YORLENY SALAS ARAYA (FIRMA)
Firmado digitalmente por YORLENY SALAS ARAYA (FIRMA)
Fecha: 2024.06.19 12:31:20 -06'00'

M.Sc. Yorleny Salas Araya
Directora programa de Posgrado en Tecnologías de Información y Comunicación para la Gestión Organizacional

ESTRELLA LOPEZ LOPEZ (FIRMA)
Firmado digitalmente por ESTRELLA LOPEZ LOPEZ (FIRMA)
Fecha: 2024.06.18 20:24:46 -06'00'

Estrella López López
Sustentante

TABLA DE CONTENIDO

RESUMEN EN ESPAÑOL

El objetivo de la presente investigación es desarrollar una guía de mejora para el departamento de TI en una organización de venta de equipos eléctricos a partir del marco COBIT 2019, el cual va a permitir brindar buenas prácticas en el departamento de TI.

La investigación realizada es de tipo aplicada, cuyo diseño utilizado es el estudio de caso, a partir de la documentación creada de una auditoría realizada en la organización, también, se extrae la información de cuestionarios, entrevista y observación directa.

A partir de los resultados proporcionados por los instrumentos aplicados, se hizo la elección de los dominios, objetivos y prácticas que se trabajaron del marco de referencia COBIT 2019, una vez que se determinó cuáles son, se elaboró la guía.

Se concluye que es necesario llevar a cabo este tipo de estudios, ya que así las empresas pueden conocer su situación y donde pueden llegar a mejorar, además que brinda la posibilidad de tomar medidas que generen resultados positivos cuando se apliquen. Además, se debe considerar que el marco de referencia COBIT 2019 puede ser utilizado por empresas pequeñas o grandes ya que para cada una generara beneficios si se pone en práctica.

ABSTRACT

The objective of this research is to develop an improvement guide for the IT department in an electrical equipment sales organization based on the COBIT 2019 framework, which will provide good practices in the IT department.

The research conducted is of applied type, which the design used is the case study, which, was given from the documentation created from an audit conducted in the organization, also, information is extracted from questionnaires, interview and direct observation.

From the results provided by the instruments applied, the choice of the domains, objectives and practices of the COBIT 2019 framework was made, once it was determined what they are, the guide was elaborated.

It is concluded that it is necessary to carry out this type of studies, since this way the companies can know their situation and where they can improve, and it also provides the possibility of taking measures that generate positive results when applied. In addition, it should be considered that the COBIT 2019 framework can be used by small or large companies, as it will generate benefits for each one if it is put into practice.

LISTA DE CUADROS

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA ABREVIATURAS

- **CIO:** Chief Information Officer traducido como director de información. Es un rol que se encarga del área de informática de una empresa.
- **I&T:** se usa en este documento para referirse a toda la información que la empresa genera, procesa y usa para alcanzar sus objetivos, así como la tecnología que lo hace posible en toda la empresa.

UNIVERSIDAD DE COSTA RICA

SEP Sistema de Estudios de Posgrado

Autorización para digitalización y comunicación pública de Trabajos Finales de Graduación del Sistema de Estudios de Posgrado en el Repositorio Institucional de la Universidad de Costa Rica.

Yo, Estrella López López, con cédula de identidad 207830787, en mi condición de autor del TFG titulado GUÍA DE BUENAS PRÁCTICAS PARA LA GESTIÓN DEL DEPARTAMENTO DE TI EN EMPRESA DE VENTA DE EQUIPOS ELÉCTRICOS SEGÚN EN EL MARCO DE REFERENCIA COBIT 2019

Autorizo a la Universidad de Costa Rica para digitalizar y hacer divulgación pública de forma gratuita de dicho TFG a través del Repositorio Institucional u otro medio electrónico, para ser puesto a disposición del público según lo que establezca el Sistema de Estudios de Posgrado. **SI** [X] **NO** *[ ]

***En caso de la negativa favor indicar el tiempo de restricción: _____ año (s).**

Este Trabajo Final de Graduación será publicado en formato PDF, o en el formato que en el momento se establezca, de tal forma que el acceso al mismo sea libre, con el fin de permitir la consulta e impresión, pero no su modificación.

Manifiesto que mi Trabajo Final de Graduación fue debidamente subido al sistema digital Kerwá y su contenido corresponde al documento original que sirvió para la obtención de mi título, y que su información no infringe ni violenta ningún derecho a terceros. El TFG además cuenta con el visto bueno de mi Director (a) de Tesis o Tutor (a) y cumplió con lo establecido en la revisión del Formato por parte del Sistema de Estudios de Posgrado.

INFORMACIÓN DEL ESTUDIANTE:

Nombre Completo: Estrella López López.

Número de Carné: B63925 Número de cédula: 207830787.

Correo Electrónico: estrella.lopez@ucr.ac.cr / estrellalopez2398@gmail.com.

Fecha: 17-06-2024. Número de teléfono: 88769148.

Nombre del Director (a) de Tesis o Tutor (a): M.Sc. Verni Fernández Castro.

ESTRELLA LOPEZ LOPEZ (FIRMA)

Firmado digitalmente por ESTRELLA LOPEZ LOPEZ (FIRMA)
Fecha: 2024.06.18 09:48:23 -06'00'

FIRMA ESTUDIANTE

Nota: El presente documento constituye una declaración jurada, cuyos alcances aseguran a la Universidad, que su contenido sea tomado como cierto. Su importancia radica en que permite abreviar procedimientos administrativos, y al mismo tiempo genera una responsabilidad legal para que quien declare contrario a la verdad de lo que manifiesta, puede como consecuencia, enfrentar un proceso penal por delito de perjurio, tipificado en el artículo 318 de nuestro Código Penal. Lo anterior implica que el estudiante se vea forzado a realizar su mayor esfuerzo para que no sólo incluya información veraz en la Licencia de Publicación, sino que también realice diligentemente la gestión de subir el documento correcto en la plataforma digital Kerwá.

1. PRIMER CAPÍTULO: INTRODUCCIÓN

En este primer capítulo se desarrolla la problemática, se describe la justificación del por qué es importante llevar a cabo la investigación. Además, se presentan una serie de antecedentes que permiten ubicar al lector en otras situaciones similares que han tenido diversas empresas con respecto al tema investigado. Para finalizar, se muestran los objetivos por desarrollar a lo largo del trabajo.

1.1. Problema

La incorporación de herramientas o sistemas que permiten la agilización y automatización de los procesos de una empresa ha tomado fuerza e importancia a través de los años. Debido a esto se busca la forma de centralizar su uso, creando así áreas más específicas en la empresa. Según López y Martí (2014) en los años ochenta del siglo XX, las organizaciones empezaron a incorporar el departamento de Tecnologías de Información (TI) de una forma abrupta y desordenada. Primeramente, inició con la adquisición de la infraestructura, además de incorporar herramientas tecnológicas para cada una de las áreas.

Así mismo, la necesidad de contar con un departamento de TI no cambia a pesar de los años y la forma en la que se lleva a cabo su creación se mantiene, ya que no existe información centralizada que indique los pasos para dar inicio. Esta área se va desarrollando de acuerdo con las necesidades de la organización, por ejemplo, adquieren equipos tecnológicos y sistemas que ayuden al desarrollo de sus actividades, a como crece la empresa, se agregan más elementos. López y Martí (2014) destacan que encontrar un departamento TI con eficacia y eficiencia en la ejecución de sus funciones y alineado con la estrategia de la empresa, no es fácil, se requiere de ciertos conocimientos que se adquieren al utilizar herramientas o marcos de referencia que permite evaluar la alineación de TI con los objetivos de la organización.

Cabe resaltar la relevancia en la claridad de los objetivos de TI y la alineación con la organización. No se debería tener un departamento que no vaya acorde a las metas planteadas por la empresa, ya que irían por caminos diferentes, sería muy difícil generar avances positivos, además se estaría perdiendo una ventaja competitiva si no se logra explotar su potencial.

Por ello, es necesario la concepción de un departamento de TI, que estructure, planifique, administre y decida de manera prudente la utilización de los recursos, así como la infraestructura tecnológica, la información, las aplicaciones para que la empresa satisfaga sus necesidades (López & Martí, 2014)**.** No obstante, la creación de un área de TI no significa que al llevar a cabo su implementación sea la más correcta o bajo estándares de buenas prácticas. El uso de cierta tecnología no garantiza el éxito para una institución, ante esto se deben utilizar marcos o soluciones convenientes que mejoren la forma de realizar los procesos de cada departamento (Argueta, 2006).

Así mismo, involucrar la tecnología no asegura que las empresas vayan a obtener una ventaja, debido a que se requiere de una serie de reglas que permitirán su correcto funcionamiento, primeramente, se debe conocer las acciones y operaciones, además, contar con una estructura detallada de lo que se requiere en tecnología y la acción que se va a implementar, todo con el fin de no llevar a cabo acciones precipitadas o abruptas (Galo, 2018).

La organización en donde se desarrolla el trabajo de investigación aplicada se seguirá denominando empresa de venta de equipos eléctricos. Se resguarda su nombre debido a un acuerdo de confidencialidad. Esta institución tiene 27 años de estar operando en el mercado, dio sus primeros pasos en el área de TI cuando contrató personal para que se encargara de brindarles tercerización de servicios, por lo que se instaló infraestructura, equipos y el cableado para la conexión de redes.

Además, contrataron ingenieros eléctricos para continuar con funciones tecnológicas en áreas como la utilización de sistemas para solicitar informes por medio de consultas en las bases de datos y realizar ciertas actividades relacionadas a la tecnología como la adquisición de herramientas de CRM de Microsoft y el ERP de Softland. Después de un tiempo, específicamente, en el 2020, se adquirieron los servicios de una empresa encargada de auditar los estados financieros y parte de la estructura del control interno, cuyo trabajo se realizó en distintas etapas.

En la primera etapa hicieron la evaluación en el área financiera, después de finalizar ese proceso se enfocaron en una revisión general del área de tecnología la cual abarcó el ambiente de control de TI, su objetivo fue realizar un análisis general de los sistemas utilizados. Al continuar en la segunda etapa, la empresa contratada quería realizar implementaciones o

ajustes del estudio, pero sin antes decir cuáles serían los beneficios de llevarlo a cabo, debido a lo anterior, la implementación que se realizaría se canceló, ya que la institución decidió prescindir de los servicios de la compañía contratada.

La empresa ha intentado poner en práctica pautas de la evaluación previa contratada, como por ejemplo trabajar con la metodología *scrum* y agregar el grupo de trabajo a nuevo personal para que se encargue de funciones más específicas sobre los sistemas con los que cuenta el actual espacio de trabajo de TI, además llevar a cabo la documentación sobre la autorización de accesos a los diferentes sistemas, es decir contar con el mapeo de los usuarios que tiene acceso, además del rol.

Por estos motivos, recientemente se determinó la necesidad de contratar personal especializado en el área de informática para trabajar en las bases de datos y los servicios que ofrecen a sus clientes. Por ello, en la actualidad, cuentan con un área de tecnología, sin embargo, a partir del estudio de auditoría se encontraron varias deficiencias, se destacan las siguientes:

- En los sistemas evaluados se tienen varias cuentas con privilegios administrativos.
- La falta de mapeo de las personas encargadas de dichos accesos.
- Existen cuentas de usuarios genéricas.
- Problemas con las contraseñas, ya que no existe configuración para que tengan vencimiento y un límite de intentos.
- No presenta un registro de bitácora debidamente configurado, no obstante, no son fiscalizados.
- Carencia de actualizaciones de seguridad en los sistemas.
- No existe documentación sobre el plan de continuidad del negocio, contingencias informáticas y del procedimiento de las restauraciones de los respaldos de la información.
- No se cuenta con un plan integral de seguridad de la información.
- Falta ejecución y documentación de un análisis de vulnerabilidades de la infraestructura, plataforma tecnológica, de políticas y procedimientos de administración control de los recursos de información.
- Inexistencia de un monitoreo sobre los diferentes tareas y acuerdos de servicios (SLA) de los proveedores de servicios en el área de TI.

Un factor que agrava la situación es el trabajo que se realiza bajo la marcha, abriendo paso a un análisis apresurado, es decir, se hicieron modificaciones de acuerdo con las necesidades del manejo de datos, optimización de procesos que surgieron en su momento, sin realizar un análisis del impacto y la forma en la que se debería desarrollar. Esta acción llega a generar consecuencias como mala distribución de los recursos, pérdida de oportunidad de realizar flujos de trabajo más efectivos y de calidad, además que no se contemple la seguridad de sus sistemas por reducir el tiempo en las soluciones de los procesos (Argueta, 2006).

1.2. Justificación

La implementación de las TI en la mayoría de las organizaciones ha dado la oportunidad de generar una ventaja competitiva con respecto a otras, debido al valor que genera en el negocio, si se implementan de manera adecuada (Cano & García, 2018). Por lo tanto, es de importancia poder determinar los beneficios que una empresa puede obtener de las TI, no solo la forma en cómo se lleva a cabo, sino establecer los lineamientos y estrategias para estructurar un departamento de TI. Esto se logra a partir de marcos ya establecidos y estudiados que pueden dar una guía para el área de tecnología.

Por lo tanto, a partir de los problemas expuestos por la auditoría y la forma en la que se ha concebido el área de tecnología, se debe considerar realizar un nuevo estudio a partir del marco COBIT 2019 de los procesos y las funciones que se tiene actualmente, ya que han pasado dos años desde que se presentaron estas vulnerabilidades y en este departamento los cambios siempre son constantes. Al llevarlo a cabo, se quiere que la empresa pueda tener oportunidades de mejora, ya sean en el equipo de TI, una correcta gestión de las herramientas tecnológicas y la implementación de nuevas que ayuden a la empresa a generar ventaja competitiva en el mercado.

La utilización de marcos como COBIT 2019 permite evaluar los procesos que lleva a cabo el departamento, esto con el fin de alcanzar las buenas prácticas. Para lograr correctas implementaciones, COBIT 2019 permitirá conseguir una política entendible y transparente para el manejo de las TI en una empresa. Además, se centra en la regulación para que esta se cumpla y brinda la oportunidad de contar con un valor agregado en el departamento de TI, aunque COBIT trabaja en todas las áreas de la institución (Huayhua & Romero, 2019).

La evaluación de COBIT 2019 en el departamento de TI en la empresa de venta de equipos eléctricos va a permitir identificar fortalezas y debilidades en la gestión de TI, además, conocer cuáles son los puntos en los que debe enforcarse para potenciar dicho departamento, entre ellos están alinear los objetivos de TI con los objetivos de la organización, desarrollar valor y proporcionar beneficios a las personas interesadas, optimizar los riesgos al grado de obtener tolerancias aceptables, cuantificar el desempeño del departamento y coordinar los recursos (Hernández, 2018), esta investigación va a marcar pautas, elementos y acciones en las que debe ir trabajando, ya que a partir de la evaluación se elaborará un plan que le permitirá trabajar en los procesos y actividades que requiere modificaciones.

Por esta razón se quiere realizar una evaluación del departamento de TI que permita descubrir las posibilidades que tiene la empresa de mejorar sus procesos y funciones en esta área, además de recomendar buenas prácticas para brindarle un valor agregado en la gestión y seguridad de los sistemas de la organización.

1.3. Antecedentes

En una empresa, las TI gestionan técnicas relacionadas a computadoras y medios de comunicación mediante equipos tecnológicos, permiten el intercambio de comunicación entre clientes y negocios, ya sea de forma interna como externa, así como actividades y funciones que se llevan a cabo en su desarrollo (Argueta, 2006). Se han involucrado en los procesos y acciones de las organizaciones como la forma en la que ofrece los servicios a sus clientes, creación de informes y reportes, automatización de actividades, entre otros (Cortés, 2017).

A pesar de no contar con un departamento de TI, las organizaciones cuentan con tecnologías de información o cierto *software* que les proporciona agilización en sus actividades. Ciertas funciones y procesos se han llegado a automatizar, se ha dejado las hojas electrónicas para el ingreso de datos y ahora se cuenta con sistemas desarrollados específicamente para esto, se sustituye el papel utilizando documentos electrónicos, abriendo la posibilidad de cambiar la forma de almacenaje, dejando de lado los ampos para tener servidores. Además, la forma de dar a conocer la empresa o negocios se transforma, generando el desarrollo de sitios web y empleos de publicidad digital.

Por estas razones, las empresas buscan un acercamiento a las TI, debido a las ventajas competitivas a adquirir mayor captación y fidelidad de los clientes, reconocimiento de imagen de la institución, agilización de los recursos, funciones y operaciones, además la diversificación en el mercado debido al desarrollo de nuevos productos y servicios (Gorbe, 2007). Las organizaciones ven la necesidad de replantearse la estructura, la utilización de los recursos, y la forma en la que llevan a cabo las operaciones para así iniciar su incorporación en el campo tecnológico (Hoyos & Valencia, 2012).

De hecho, las organizaciones andan en busca de una transformación digital, generando un cambio de pensamiento en la forma de desarrollar sus actividades diarias, se traslada e involucra la tecnología en los procesos, dejando atrás la forma tradicional o manual de hacer las funciones para pasar a la agilización, estandarización y el consumo de menos tiempo en el trabajo.

Hay que enfatizar que, al involucrar tecnología, se debe llevar a cabo un análisis y tener conocimiento sobre el campo, por ello, se debe considerar realizar un estudio de la empresa y sus necesidades para saber qué es lo más adecuado, debido a que cada organización es diferente. Además, es un proceso que requiere de tiempo y ciertos marcos que nos van a brindar una guía para ir condicionando de manera correcta un departamento de TI. Cuando ya se cuenta con ciertas bases, lo mejor es analizar lo que se tiene para que, a partir de ahí, tener claridad e iniciar con las mejoras.

Las empresas priorizan o le dan más valor al “cómo” y le restan importancia al “qué”, cuando el primer paso debe ser el “qué”, al comprender el propósito se descubre cuáles son los puntos y las áreas en las que se debe enfocar, una vez que se logre, se continua con la ejecución para disminuir o erradicar el problema (Argueta, 2006).

Del mismo modo, existen estudios internacionales como nacionales que dan a conocer la utilización de los marcos de referencia en el área de tecnología de una organización. Por ejemplo Ati (2018), como parte de su investigación en el Centro de Procesamiento de Datos (CPD) de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Salesiana, diseñó un plan para la continuidad del negocio y recuperación ante desastres utilizando los marcos COBIT, ITIL y la norma ISO 22301. En la metodología utilizó como base las mejores prácticas de los marcos de referencia y la norma seleccionada. Para obtener

información de la institución, realizó una entrevista con el administrador del CPD, además, analizó los escenarios de la infraestructura de TI a nivel físico y lógico, sin dejar atrás la continuidad del negocio. La investigación evidenció la necesidad de intervenir en el tema de prevención, mitigación, corrección y prevención de los desastres en sitios donde se almacenan y procesan los datos. Además, se lograron identificar factores que pueden ocasionar la probabilidad de interrupciones de la continuidad de negocio.

Así mismo, Hidalgo (2015), realizó un diagnóstico y una evaluación de controles basándose en la norma ISO/IEC 27001 y DS5 en una institución pública financiera de Costa Rica. También evaluó los riesgos de TI y la gestión de seguridad considerando el marco de referencia COBIT 5, con el fin de determinar el grado de alineación y en nivel de madurez que tiene el sistema de gestión de seguridad de la información (SGSI) con respecto a las pautas de la norma. Para su elaboración desarrolló plantillas de preguntas abiertas referentes a las normas y pautas, estas se aplicaron mediante entrevistas, de acuerdo con las preguntas se seleccionaba a la persona encuestada. Realizó un análisis de la información y generó un informe. El autor señala la necesidad que tiene la institución de utilizar marcos de control, en especial COBIT, con fin de gestionar las tecnologías de información y saber el nivel de madurez inicial de organización. Se concluyó que el nivel de madurez de la organización es inicial debido a que el sistema de gestión de la seguridad de la información no posee una alineación con el estándar internacional ISO27001:2013.

Por su parte, Arce (2021) diseñó un modelo de gobierno y gestión de TI para el Instituto Costarricense del Deporte y Recreación (ICODER) basado en el marco COBIT 2019, para aplicarlo en la mejora de la gestión empresarial. El autor realiza un análisis minucioso de la organización, lo cual le permitió llevar a cabo el diseño de un modelo de gobierno y gestión que le brindó soporte a la institución y además cubrió sus necesidades. Esto se logró a partir de entrevistas, sesiones de trabajo, además la consulta de información de fuentes primarias y secundarias. El diseño a partir del modelo COBIT 2019 le permitió a la organización la integración de las tecnologías de una mejor manera, además conocer la perspectiva de la empresa, así como los diferentes problemas, el funcionamiento de TI y sus necesidades. Por lo que adquirieron un mayor conocimiento de su entorno empresarial y el aporte que genera TI para la institución.

Por otro lado, Cortés (2021) realizó una evaluación mediante el marco COBIT 2019 del modelo de gestión TIC de la Municipalidad de Carrillo durante el periodo 2020-2021 debido a la implementación de los procesos de migración de sistemas operativos e informáticos. Se utilizaron como instrumentos observación directa y entrevista. Los resultados evidenciaron lo siguiente: en la protección contra *software* malicioso la organización está realizando proyectos de migración de sistemas operativos, además implementan mecanismos de protección. En la parte de vulnerabilidades no se gestiona las vulnerabilidades por lo que le recomiendan levantar métricas y documentación para tener la información. Concluye que, al evaluar el modelo de gestión de las TIC, permitió conocer brechas y oportunidades de mejora en la confrontación de sus acciones con respecto a lo estipulado por el marco. Además, la situación actual de los procesos evaluados les permitió marcar un precedente, es decir, un punto de partida para futuras evaluaciones y comparaciones con los datos históricos para así dar seguimiento a las acciones prioritarias.

De igual forma, Villafuerte (2021) elaboró una estrategia para el manejo de políticas de seguridad informática en una municipalidad de la Región Chorotega, con el fin de minimizar el riesgo y asegurar la integridad del *software* y la información. Realizó encuestas y una observación de participantes, los instrumentos fueron cuestionarios y una guía de observación. Los resultados evidenciaron que en la municipalidad se tiene problemas con la compra de equipos, debilidades en los antivirus, necesidad de capacitaciones, actualización de tecnología. Se concluyó la existencia de manuales de procedimientos y políticas de seguridad, lo que faltaba era la comunicación con los funcionarios.

1.4. Objetivos

1.4.1. Objetivo General

Desarrollar una guía de mejora para el departamento de TI en una empresa de venta de equipos eléctricos mediante el marco de referencia COBIT 2019, con el fin de proporcionar buenas prácticas en distintas áreas de la gestión de TI.

1.4.2. Objetivos Específicos

- Identificar los procesos y funciones del departamento de TI para conocer el funcionamiento del área.

- Evaluar mediante COBIT 2019 los procesos y funciones del departamento de TI, con el fin de identificar las fortalezas y debilidades de su gestión.
- Elaborar una guía de buenas prácticas para el departamento de TI, con el fin de recomendar oportunidades de mejora en funciones, procesos y seguridad.

2. SEGUNDO CAPÍTULO: MARCO TEÓRICO

En este segundo capítulo se desarrolla el marco teórico, este se divide en dos grupos, el marco referencial el cual permite conocer más acerca de la organización, por ello se menciona lo siguiente: descripción de la organización y su entorno, su estructura organizacional, actividades que desarrolla. En el marco conceptual se describen los conceptos relacionados a la tecnología, elementos necesarios para el departamento de TI, marco de referencia, sistemas de aplicaciones empresariales, planes de continuidad, las cuales son fundamentales para la adecuada comprensión del trabajo de investigación.

2.1. Marco referencial

2.1.1. Descripción de la organización y su entorno

2.1.1.1. Descripción de la organización

La empresa de venta de equipos eléctricos fue creada alrededor de la década de los años 90. Su enfoque se centra en brindar equipos eléctricos que marquen la diferencia de manera efectiva en el campo de la energía, favoreciendo a la población y el ambiente.

La organización constantemente se enfoca en innovar y especializarse, está comprometida día con día a brindar en el mercado opciones de servicios de una alta ingeniería, todo esto lo consigue buscando y utilizando tecnologías que brinden eficiencia, por ello, le permite abrir una gama de posibilidades en el mundo para lograr liderar en el campo de la energía.

Por lo tanto, buscan asumir retos y ser propulsores de nuevas soluciones en el campo tecnológico, creando así nuevas formas que permitan generar un cambio positivo en el sector. La organización para cumplir con lo propuesto comienza a trabajar en el campo de la innovación en energía, de la mano de asesorías, servicios y la participación de equipos modernos y de calidad, para brindarle a los clientes las herramientas correctas con el fin de que puedan alcanzar sus objetivos.

2.1.1.2. Entorno donde se desenvuelve

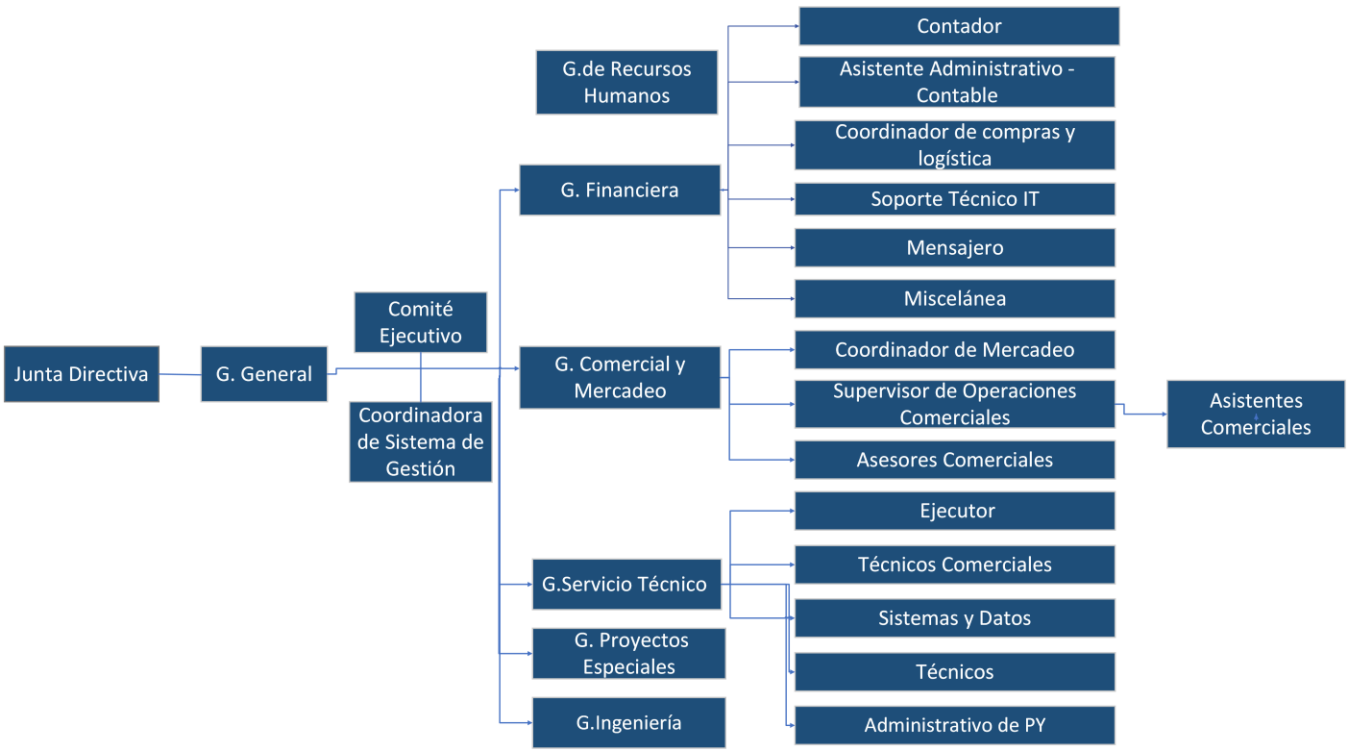
La organización se dedica a la venta de equipos para la medición eléctrica, además ofrece servicios como digitalización y desarrollo de aplicaciones, proyectos de subestaciones, soluciones de mantenimiento y gestión para las empresas que se encargan de la generación de electricidad.

El mercado en el que se enfoca se encuentra en un continuo cambio hacia las nuevas herramientas que ofrecen los fabricantes de equipos de medición y de gestión, donde se integran el internet de las cosas (IoT) en los equipos, lo que obliga a la empresa a no contar con solo personal de ingeniería eléctrica, sino a pensar en colaboradores con conocimiento en informática para ayudar a subsanar el cambio de equipos nuevos en el medio, también esto propicio que la organización explorará otros áreas como lo es el desarrollo de *software* y servicios relacionados a este.

2.1.1.3. *Estructura organizacional*

La empresa, como se mencionó con anterioridad, es pequeña, por ello su estructura organizacional cuenta con pocos departamentos que conviven para mantener a la empresa en el mercado, dicha estructura se compone de la siguiente manera:

Figura 1. *Organigrama de la empresa*



Fuente: Proporcionado por la empresa.

Como se observa en la Figura 1, las distintas ramas tienen a su cargo varios departamentos, donde el de TI está a cargo del gerente de financiero, lo cual no tiene aún en la empresa un gerente de TI que sería lo ideal.

2.1.1.4. Actividades de desarrollo

Las principales actividades de desarrollo de la empresa se basan en la venta de equipos eléctricos, como medidores, equipos de media y alta tensión, además, de venta de soporte para el mantenimiento y la previsión de riesgos eléctricos, así como sistemas de gestión eléctrica.

2.2. Marco conceptual

2.2.1. Tecnologías de Información (TI)

Las tecnologías de información se centran en dispositivos informáticos que permiten la comunicación, se utilizan con el fin de intercambiar información entre los clientes y las relaciones del negocio tanto interno y externo, además de los procesos que se llevan a cabo en la organización (Argueta, 2006).

Por lo tanto, al involucrar TI en las actividades de una organización permite contar con mejoras en la parte de la administración e integración en los procesos de información. También, minimiza el consumo de tiempo de las personas que se involucran en las actividades, además se descartan acciones que puedan generar pérdida de productividad y sea un obstáculo para alcanzar soluciones a problemas de manera más rápida, ágil y en el menor tiempo posible (Argueta, 2006).

Las empresas para tener éxito deben estar constantemente cambiando la forma en la que realizan sus procesos, pues esto va a permitir que puedan ir generando ventajas competitivas sobre otras, ya que su forma de trabajo puede llegar a ser más efectiva, eficiente y de forma automatizada lo que va a generar menos personas participando en el proceso y menos enfoque en actividades que no lo requieren. Según Argueta (2006) las TI "nos ayudan a conocer mejor el medio tanto interno como externo de nuestro negocio, para así detectar nuestras debilidades y potencialidades, atacarlas, y lograr una ventaja comparativa con respecto a las demás empresas del ramo" (p. 2).

2.2.1.1. Gestión de Tecnologías de la Información

La gestión de tecnologías de la información o gestión de TI, consiste en el seguimiento y la administración de los sistemas de tecnología de la información (*hardware*, *software* y redes) de una empresa. Su función principal es la eficiencia en el funcionamiento de los sistemas de información (IBM, s.f.).

En la opinión de Palomino (2022) se trata de un proceso de supervisión de todo lo relacionado a las herramientas de TI utilizadas por una organización. Dicho con palabras de Red Hat (2018) la gestión de TI se enfoca en la coordinación de los recursos como sistemas, plataformas, personas y además entornos de TI. A partir de esta acción se busca la automatización en los procesos de la organización ya que es un elemento estratégico en la modernización y la transformación digital.

2.2.1.2. *Importancia de la Gestión de Tecnologías de Información en las empresas*

Los beneficios que proporcionar la gestión de TI en una organización va desde el mejoramiento de los niveles de productividad hasta la reducción de costos y la garantía de más seguridad. Debido al uso de las nuevas tecnologías que buscan acelerar los procesos productivos mediante el aumento de su eficiencia, además de tener acceso a más sistemas de seguridad informáticos (Palomino, 2022).

2.2.2. Seguridad Informática

Para mencionar el concepto de seguridad informática se debe tener claro el concepto de seguridad y lo que abarca. Primeramente, seguridad es la ausencia de riesgo y en ella se asocian cuatro acciones; prevenir, transferir, mitigar y aceptar el riesgo. Por ello, busca gestionar los riesgos a partir de las acciones anteriormente mencionadas (Romero et al., 2018).

Por lo tanto, la seguridad informática se define como una disciplina que se encarga de construir y brindar normas, procedimientos, métodos y técnicas, con el propósito de obtener sistemas de información con mayor seguridad, conservando la integridad de los datos y la confiabilidad de estos (Avenía, 2017).

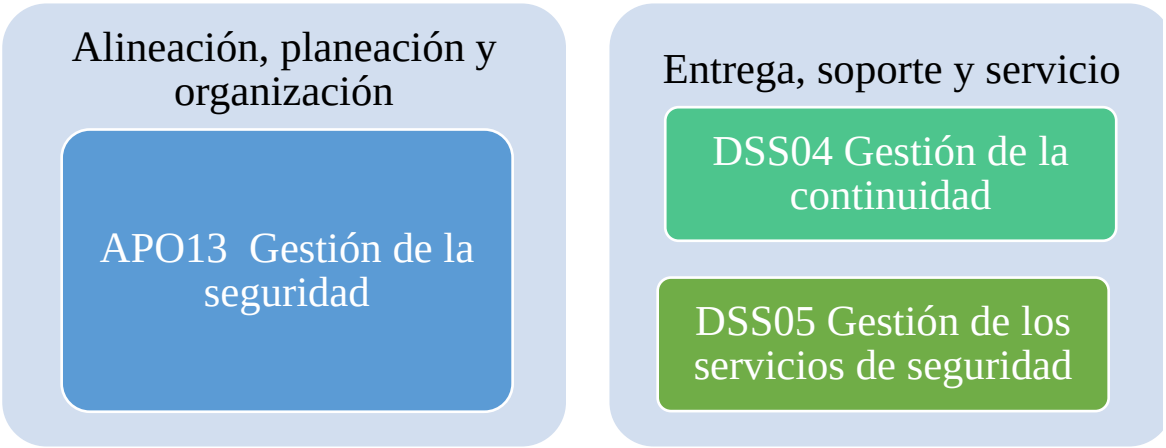
Su principal función es minimizar los riesgos, los cuales ingresan de distintas formas y de cualquier lugar, por ejemplo, entrada de datos, dispositivos con información, los usuarios y por los protocolos que se utilizan (Romero et al., 2018). Al final existen diversas estrategias para poder llegar a vulnerar un programa o un dispositivo, ya que todo está en constante actividad, es decir, la información que se almacena es de acceso, a los dispositivos se les otros elementos, ya sea para almacenar o transportar. Las personas acceden provocando que administren información muy sensible, además de sus accesos, dejando ahí una puerta para que sean la pieza de entrada para los sistemas.

Entonces, la seguridad informática tiene como objetivo "proteger los valiosos recursos informáticos de la organización, tales como la información, *hardware* o *software*. A través de la adopción de las medidas adecuadas…" (Avenía, 2017). Los pilares de la seguridad informática son: integridad, confidencialidad y disponibilidad. Calderón (2015) define cada uno de los elementos de la siguiente manera:

- **Integridad**: El contenido de los datos debe ser el mismo, siempre y cuando este sea modificado por alguien con autorización. Es decir, la información debe estar intacta y contar con consistencia, desde el momento de su concepción, hasta su modificación con permisos de autorización.
- **Confidencialidad**: Brindarle acceso a la información solo a los usuarios que cuentan con autorización. La divulgación debe ser restringida y fiscalizada.
- **Disponibilidad**: La información debe ser accesible en el momento en que un usuario con autorización la solicite.

La seguridad informática según Mendoza (2015) para el marco de COBIT se evidencia en COBIT 5 en sus documentos de seguridad de la información (*COBIT 5 for Information Security*), estos consisten en sentar bases para mejores prácticas en el ámbito de la protección de la información para cualquier nivel de la organización y son complementos para los procesos de los dominios que brinda COBIT, estos consisten en una guía en el sistema de gestión de la seguridad se aprecian en la Figura 2.

Figura 2. *Procesos de los dominios que participan en la seguridad de la información*



Fuente: Elaboración propia

Estos procesos también se encuentran en COBIT 2019, se encuentra en los mismos dominios. Según ISACA (2018) el APO13 Gestión de la Seguridad consiste en "mantener el impacto y existencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa "(p.34), procura que la organización no se vea afectada por las situaciones de riesgo, además al materializarse pueda estar entre los niveles establecidos. En cuanto al DSS04 Gestión de la continuidad "Adaptarse rápidamente, continuar 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 (como amenazas, oportunidades, demandas)" (ISACA, 2018, p.35), por último, DSS05 Gestionar los servicios de seguridad "minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información" (ISACA, 2018, p.35).

2.2.3. Elementos importantes en el departamento de TI

2.2.3.1. Objetivos de TI

Para facilitar este proceso de recolección, comunicación y toma de decisiones, las empresas se apoyan de las tecnologías, creando en ellas un nuevo departamento, el cual pueda gestionar de forma diferente los procesos y actividades que realizan las organizaciones. De acuerdo con Cano (2017), "las TIC son un elemento clave para hacer que nuestro trabajo sea más productivo: agilizando las comunicaciones, sustentando el trabajo en equipo, gestionando las existencias, realizando análisis financieros, y promocionando nuestros productos en el mercado" (p.504), como se puede apreciar, las TIC se van a encontrar en toda la empresa, es decir, que para las organizaciones que lo han implementado no solo afecta a un departamento, sino a todos los departamentos.

Las TIC se han vuelto tan importantes cuando se implementa que existe la posibilidad que si no se maneja adecuadamente puede hacer que la empresa deje de operar debido al grado de incorporación que se tiene. Por ello, las "TIC son la fuente principal de información para la empresa y la información es un recurso estratégico muy importante que sustenta las funciones claves y los procesos de toma de decisiones" (Slusarczyk & Morales, 2016, p.39).

Por lo tanto, si se considera darle un buen uso y optar por todas las medidas necesarias para su correcta implementación se obtendrán ventajas como: "la modernización y agilización de los procesos, incrementar los niveles de productividad y, en definitiva, aumentar la

competitividad de la empresa en un mercado cada vez más globalizado, y en consecuencia mucho más competitivo" (Gorbe, 2017, p.26).

2.2.3.2. Control Interno

Estupiñán (2006) afirma sobre el control interno lo siguiente:

> El control interno se define como un proceso, ejecutado por la junta directiva o consejo de administración de una entidad, por su grupo directivo (gerencial) y por el resto del personal, diseñado específicamente para proporcionarles seguridad razonable de conseguir en la empresa las tres siguientes categorías de objetivos: efectividad y eficiencia de las operaciones, suficiencia y confiabilidad de la información financiera y cumplimiento de las leyes y regulaciones aplicables. (p.25)

Según Calle et al (2020) el control interno

> Se define como un proceso de gestión dinámico e integrado, que propone y adecua altos estándares de seguridad, con relación a los objetivos operacionales, de información y cumplimiento, su función es inherente a la organización y dirección institucional, promoviendo las condiciones necesarias del equipo de trabajo, para causar un mejor desempeño del funcionamiento de la empresa.

El control interno (CI) es el elemento fundamental de la administración que debe estar presente en todas las organizaciones, independientemente de su tipo y conformación. La importancia radica desde el punto de vista de administrar, es decir: no se puede planear, organizar, administrar sin control, por lo tanto, el CI comprende un plan de la organización que permite realizar procedimientos coordinados adoptados por una organización para verificar la razonabilidad y confiabilidad de la información financiera. (p.432 – p.433)

2.2.4. Marcos de referencia

2.2.4.1. COBIT 2019

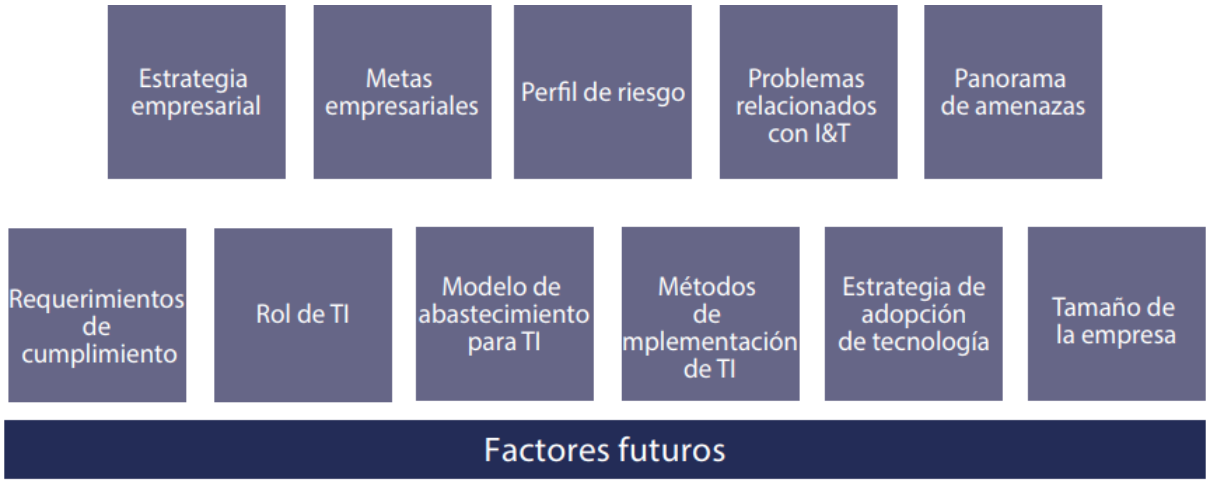
Según ISACA (2018) "COBIT es un marco para el gobierno y la gestión de las tecnologías de la información de la empresa, dirigido a toda la empresa" (p.13). Cuando se tiene pensando la utilización de COBIT se debe considerar que es un marco que nos permitirá integrarlo o utilizarlo en toda la organización, ya que este también se enfoca en otras áreas.

"El marco de referencia COBIT hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos" (ISACA, 2018, p.13).

Factores de diseño

Para posicionar a una empresa y que esta tenga éxito en su trabajo necesita considerar en su diseño y desarrollo de sistema de gobierno los factores de diseño, esto se puede apreciar en la Figura 3.

Figura 3. *Factores de diseño de COBIT*



Fuente: Adaptado de COBIT 2019 (p.23), por ISACA, 2018.

Áreas de enfoque

En el marco de COBIT se indican las áreas principales en las que se puede desarrollar las cuales son: pymes, desarrollo/operación, riesgos, seguridad.

Principios

COBIT 2019 cuenta con nueve principios, los cuales están divididos en dos grupos sistema de gobierno y marco de gobierno. En el sistema de gobierno se pueden observar los seis principios, los cuales son fundamentales para llevar a cabo un sistema para la información y tecnología de la organización, se puede ver en la Figura 4.

Figura 4. *Principios de sistema de gobierno*

Fuente: Adaptado de COBIT 2019 (p.17), por ISACA, 2018.

El marco de gobierno abarca tres principios, a partir de este se puede se utilizar para construir el sistema de gobierno se puede apreciar en la Figura 5.

Figura 5. *Principios de marco de gobierno*

Fuente: Adaptado de COBIT 2019 (p.18), por ISACA, 2018.

Objetivos de Gobierno y Gestión

Los objetivos de gobierno se encuentran distribuido en un solo dominio el cual consiste en: Evaluar, Dirigir y Monitorizar (EDM), “evalúa las opciones estratégicas, direcciona a la alta

gerencia con respecto a las opciones estratégicas elegidas y monitoriza la consecución de la estrategia" (ISACA, 2018, p.20). En la Tabla 1 de puede observar cuales son los objetivos pertenecientes al dominio.

Tabla 1. *Objetivos del dominio Evaluar, Dirigir y Monitorizar (EDM)*

Dominio	Objetivos
Evaluar, Dirigir y Monitorizar (EDM)	**EDM01** Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno
	EDM02 Asegurar la Entrega de Beneficio
	EDM03 Asegurar la Optimización del Riesgo
	EDM04 Asegurar la Optimización de los Recursos
	EDM05 Asegurar la Transparencia hacia las Partes Interesadas

Fuente: Elaboración propia

Según ISACA (20180,) los objetivos de gestión se encuentran asociados o distribuidos en los cuatro dominios pertenecientes a este, entre ellos están: Alinear, Planificar y Organizar (APO), Construir, Adquirir e Implementar (BAI), Entregar, Dar servicio y Soporte (DSS) y Monitorizar, Evaluar y Valorar (MEA). En la Tabla 2 de puede observar cuáles son los objetivos pertenecientes a los dominios mencionados anteriormente.

Tabla 2. *Objetivos de los dominios de gestión*

Dominios	Objetivos
Alinear, Planificar y Organizar (APO)	**APO01** Gestionar el Marco de Gestión de TI
	APO02 Gestionar la Estrategia
	APO03 Administrar la Arquitectura Empresarial
	APO04 Gestionar la Innovación
	APO05 Gestionar la Cartera
	APO06 Gestionar el Presupuesto y los Costes
	APO07 Gestionar los Recursos Humanos
	APO08 Gestionar las Relaciones
	APO09 Gestionar los Acuerdos de Servicio

	APO10 Gestionar los Proveedores
	APO11 Gestionar la Calidad
	APO12 Gestionar el Riesgo
	APO13 Gestionar la Seguridad
	APO14 Datos gestionados
Construir, Adquirir e Implementar (BAI)	**BAI01** Gestionar los Programas y Proyectos
	BAI02 Gestionar la Definición de Requisitos
	BAI03 Gestionar la Identificación y la Construcción de Soluciones
	BAI04 Gestionar la Disponibilidad y la Capacidad
	BAI05 Gestionar la Habilitación del Cambio Organizativo
	BAI06 Gestionar los Cambio
	BAI07 Gestionar la Aceptación del Cambio y de la Transición
	BAI08 Gestionar el Conocimiento
	BAI09 Gestionar los Activos
	BAI10 Gestionar la Configuración
	BAI11 Proyectos gestionados
Entregar, Dar servicio y Soporte (DSS)	**DSS01** Gestionarlas Operaciones
	DSS02 Gestionar las Peticiones y los Incidentes del Servicio
	DSS03 Gestionar los Problemas
	DSS04 Gestionar la Continuidad
	DSS05 Gestionar los Servicios de Seguridad
	DSS06 Gestionar los Controles de los Procesos de la Empresa
Monitorizar, Evaluar y Valorar (MEA)	**MEA01** Supervisar, Evaluar y Valorar Rendimiento y Conformidad

	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno
	MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
	MEA04 Aseguramiento gestionado

Fuente: Elaboración propia

2.2.5. Las aplicaciones empresariales

2.2.5.1. Sistema de Gestión de las relaciones con los clientes (CRM)

Según Sánchez & Moral (2019) Customer Relationship Management (CRM) o su traducción en español Gestión de las relaciones con los clientes consiste en la integración de datos de clientes guardado en diferentes sitios de información, estos se verifican y son accesibles en cualquier momento que se requiera y por cualquier medio de interacción con el cliente, por ejemplo, celular, correo electrónico red social y loca físico de la tienda. Existen diferentes tipos de CRM, aplicaciones operativas, analíticas y colaborativas, el uso de estas va a depender del objetivo de la organización. Al adquirir la operativas se tendrá un acercamiento cara a cara con el cliente, ya que sus funciones están asociadas a ofrecer apoyo a los vendedores, además de servicio al cliente. Las aplicaciones analíticas reciben información de las operativas con el fin de analizarla y apoyar a la empresa en la inteligencia empresarial.

2.2.5.2. Sistemas de planificación de recursos empresariales (ERP)

Según Sánchez & Moral (2019) Enterprise Resource Planning (ERP) o su traducción en español Sistemas de planificación de recursos empresariales consiste en un sistema que se encarga de centralizar el flujo de datos de la organización en un solo sistema, realizando la integración y la coordinación de estos y generando apoyo en las distintas áreas que existen. Este tipo de sistema se vende por módulos o grupos, lo cual permite que su adquisición sea escalable y de acuerdo con las necesidades de la organización, además puede ser integrado y utilizado con los sistemas CRM.

Los módulos que lo componen permiten la automatización e integración de las distintas áreas de la empresa como, contabilidad, ventas, finanzas, compras, recursos humanos entre otras. El sistema obtiene la información de las áreas y las guarda en una única base de datos. Por lo que permite ingresar la información en una única plataforma, además conserva la integridad

y la unicidad de la información de los departamentos, lo que es beneficioso, porque se evita datos duplicados e información repetida en los diferentes sistemas de la organización (Huerta & Zuzuarregui, 2015).

2.2.5.3. Sistemas de Administración de la Cadena de Suministros (SCM)

Según Laudon & Laudon (2014) Supply Chain Management o su traducción en español Sistemas de Administración de la Cadena de Suministro consiste en sistemas de interorganizacionales, ya que automatiza el flujo de información mediante los limites organizacionales. Además, contribuye al proceso que realiza una empresa en relación con la cadena de suministro, va desde el origen, en este caso sería la producción hasta finalizar con el consumo como se aprecia en la Figura 6.

Figura 6. *Cadena de suministro*

Fuente: Elaboración Propia

Este sistema permite que las variables del tiempo y costo reduzcan de forma considerable, permitiendo que se dé una disminución de costos en el transporte y la fabricación, además de acuerdo con la información que almacenan los gerentes pueden tomar decisiones informadas y certeras sobre esta área.

2.2.5.4. Sistemas de administración del conocimiento (KMS)

Según Laudon & Laudon (2014) Knowledge Management System o su traducción en español Sistemas de Administración del conocimiento consiste en recolectar información sobre el conocimiento de fuentes externas e internas, además, la experiencia de empresarial, con el fin de tenerla disponible en cualquier parte y cada vez que lo necesiten para ir mejorando los procesos y las decisiones por parte de la gerencia. Con ellos se da una correcta administración de los procesos, a partir de ahí capturan y aplican el conocimiento y la experiencia.

2.2.6. Transformación Digital

La transformación digital se define como un conjunto de acciones que permiten mejorar y modernizar la mayoría de las actividades que desarrolla la organización, a partir del uso de tecnologías, la empresa podría desarrollar una ventaja competitiva sobre las demás. Al decidir implementar o ingresar al proceso de transformación digital se necesita que la organización

interiorice el modelo de negocios, las acciones y la estrategia tecnológica que implementa, ya que esto provoca un cambio de cultura (AMETIC, s.f).

2.2.7. Consideraciones en el correcto funcionamiento de empresas que ofrecen servicios

2.2.7.1. Plan de continuidad del negocio

El plan de continuidad del negocio es un documento que contiene información del funcionamiento de la organización en caso de suspensión inesperada de los servicios. Es más completo que otros del mismo tipo, ya que contiene planes de contingencias de negocios, de recursos humanos, activos y socios (IBM Services, 2020). Cada uno de los planes anteriormente mencionadas debe considerar un actuar específico, es decir, al llevarse a cabo, se tomarán acciones y caminos diferentes para evacuar la situación, ya que se desarrollan planes específicos para diversas circunstancias, esto debido a las diferencias en las áreas que se puedan presentar (Protege tu empresa, s.f).

Un plan de negocio debe contar con un elemento esencial para su funcionamiento, el cual es un plan de recuperación tras desastres que contiene "estrategias para manejar interrupciones de TI en redes, servidores, sistemas personales y dispositivos móviles" (IBM Services, 2020).

2.2.7.2. Plan de contingencias informáticas

El plan de contingencia consiste en llevar a cabo procedimientos fuera de lo común con el fin de no detener el funcionamiento de la organización. Es decir, se quiere mantener la operabilidad a pesar de presentarse alguna eventualidad ya sea en funciones internas o externas. Estos planes constan de cuatro etapas: evaluación, planificación, pruebas de viabilidad y ejecución. Se recomienda contar con una planificación a pesar de no contar con ningún inconveniente, con el fin de estar preparados cuando se presente. Este plan debe estar anuente al cambio, por lo que debe actualizarse periódica (Mellado, 2014).

2.2.7.3. Acuerdo de nivel de servicio (SLA)

Un acuerdo de nivel de servicio (SLA) se define como un acuerdo antes de adquirir un servicio se realiza en la mayoría de los casos entre un prestador de servicio, ya sea por voz, datos, video u otro, y la persona u organización interesada en adquirir el servicio planteado (Chang et al, 2008).

También se le conoce como el Service Level Agreement (SLA) traducido Acuerdo de Nivel de Servicio consiste en un documento anexado al contrato de prestación de servicios el cual

contiene información acerca de las condiciones y los parámetros que comprometen al proveedor a cumplir niveles de calidad de servicio frente al cliente (Acens Technologies S.A, s.f).

Según Acens Technologies S.A (s.f) los elementos que debe tener el SLA son los siguientes:

- Características del servicio.
- Tiempo transcurrido desde la firma del pedido o contrato hasta la entrega o puesta en marcha del servicio.
- Atención al cliente, como se debe proceder frente a incidencias, la actuación del soporte técnico y el tiempo para asegurar la calidad del servicio.
- Tiempo de respuesta.
- Condiciones del mantenimiento.
- Garantía y compensaciones, cuando incumplan con el contrato.

Importancia del acuerdo de nivel de servicio

El acuerdo de nivel de servicio les asegura a los clientes y a los proveedores que se ha entendido lo definido o pautado, además de la calidad del servicio que se va a brindar (Mangaly, 2022).

Para el cliente, este documento genera tranquilidad, ya que asegura que los servicios que se acordaron se cumplan, además, estos deben ajustarse a las necesidades de la organización. El SLA dicta las normas y mediciones para cada servicio (Mangaly, 2022).

En cuanto al proveedor, le permite la comunicación clara, concisa y precisa entre él y el cliente dejando de lado los malentendidos, en caso de que se presentara alguno, se pueden tomar las medidas definidas en este ya que ofrece un respaldo para el cliente (Mangaly, 2022).

2.2.8. Modelo Carter 10’s

Ray Carter, director de DPSS Consultants escribió un artículo en 1995 en “Purchasing and Supply Management” sobre las 7 C’s de la Evaluación de Proveedores, y luego añadió 3 c’s más, que son:

- **Capacidad:** ¿El proveedor tiene la capacidad de entregar lo que ofrece?

El proveedor al que se quiere contratar tiene los recursos necesarios para cumplir con las peticiones y los requisitos que tiene la organización.

- **Competencia:** ¿El proveedor puede completar la tarea en un periodo de tiempo determinado?

El proveedor es competente para llevar a cabo las actividades de la organización.

- **Consistencia:** ¿El proveedor ofrece los mismos resultados constantes?

El servicio o producto que brinda mantiene la misma calidad en cualquier momento, es decir no hay variación en lo que ofrece.

- **Control del proceso:** ¿El proveedor ofrece flexibilidad y tiene un control sistemático sobre su proceso?
- **Compromiso con la calidad**: ¿Existe un sistema establecido por el proveedor que verifique la gestión de la calidad?
- **Cash (efectivo):** ¿El proveedor es independiente financieramente o trabaja con la participación de terceros?
- **Costo**: ¿Los productos y servicios que ofrece son rentables?
- **Cultura**: ¿El proveedor tiene buena cultura laboral y una buena reputación en el mercado?
- **Clean (limpio):** ¿El proveedor tiene licencia legal para realizar el trabajo que te ofrece?
- **Communication efficiency (eficiencia en la comunicación):** ¿El proveedor cuenta con los medios de comunicación necesarios para responder a las consultas que se le hacen?

2.2.9. Solicitud de servicio

Para la solitud del servicio se consideran los siguientes componentes:

- Esquema de clasificación de incidentes Zendesk (2023) considera la guía del marco de ITIL:
    - *Hardware* (Computador sin funcionamiento).
    - *Software* (Programa defectuoso).
    - Red (Problemas de conexión).
    - Seguridad (intento de intrusión en los sistemas informáticos de la organización).

- Esquema de priorización de incidentes, Zendesk (2023) considera las siguientes categorías a partir del marco de ITIL:
    - Impacto: ¿Cómo afecta el incidente al negocio?
    - Urgencia: ¿Cuánto tiempo de tolerancia se tiene para resolver el problema?
    - Prioridad: La rapidez con la que se requiere una solución. Para estimar este elemento se debe considerar el impacto y la urgencia.
- Pasos para seguir en una solicitud

  Según Zendesk (2023) los siguientes pasos mencionados en el marco de ITIL son:
    - Propuesta: Presentar la solicitud del servicio.
    - Evaluación: Se entiende la solicitud, se determina el grado de urgencia, los recursos y las herramientas que se requiere.
    - Cumplimiento: Se lleva a cabo la gestión de la solicitud.
    - Finalización: La solicitud se cierra y se archiva.
    - Seguimiento.
- Los criterios para el registro de problemas se consideran las siguientes variables que menciona Zendesk (2023) a partir del marco de ITIL:
    - Título o número de ID
    - Descripción
    - Fecha
    - Quien gestiona el incidente

3. TERCER CAPÍTULO: MARCO METODOLÓGICO

En este tercer capítulo se desarrolla el marco metodológico utilizado para llevar a cabo la investigación aplicada. Se incluye el diseño, enfoque, tipo de investigación, población y muestras, fuentes de información consultadas, técnicas e instrumentos utilizados para recolectar datos, además el análisis de estos.

3.1. Diseño de investigación

El diseño de investigación que se utilizó para la TFIA es el método de estudio de caso, debido a que se requiere conocer de forma detallada los procesos y las funciones del departamento de TI de la empresa seleccionada.

Durán (2012) considera lo siguiente:

> El Estudio de Caso (EC) es una forma de abordar un hecho, fenómeno, acontecimiento o situación particular de manera profunda y en su contexto, lo que permite una mayor comprensión de su complejidad y, por lo tanto, el mayor aprendizaje del caso en estudio. Utiliza múltiples fuentes de datos y métodos, es transparadigmático y transdisciplinario.

Por lo tanto, el estudio de caso es un diseño de investigación que permite un involucramiento más cercano y enriquecedor, permite adquirir conocimiento de una forma diferente y más completa, generando resultados favorables en las investigaciones.

Yin (2014 como se citó en Ramírez, Riva y Cardona, 2019) afirma lo siguiente:

> El estudio de caso como estrategia metodológica es una herramienta útil en la investigación, y su validez radica en que a través del mismo se mide y registra la conducta de las personas incluidas en el fenómeno estudiado, mientras que los métodos cuantitativos sólo se centran en información verbal adquirida a través de encuestas por cuestionarios.

Por ello, cuando se da la utilización de un estudio de caso, no solo se centra en una única forma de recaudación de información como se aprecia en los métodos cuantitativos, más bien se puede ampliar considerando así el objeto de estudio, así como la forma de interactuar las personas con respecto a este, en él se puede apreciar el lado cualitativo para recopilar este tipo de información.

3.1.1. Tipo de investigación

El tipo de investigación que se utilizó para la realización de la TFIA se considera como investigación aplicada. Según Muntané (2010) este tipo de trabajo consiste en aplicar o utilizar los conocimientos que se adquieren en la investigación. Además, para su desarrollo tiene como dependencia los resultados y avances que proporciona la investigación básica. Se le conoce como práctica y empírica. Su mayor importancia radica en las consecuencias prácticas que se origina a partir de su construcción.

3.1.2. Método y enfoque de investigación

La presente TFIA utilizó en el método y enfoque el tipo mixto, es decir tanto lo cuantitativo, como lo cualitativo, ya que se considera necesario para el desarrollo de esta, además cada una proporciona valor, a pesar de sus diferencias.

3.2. Población de estudio

La población de estudio este compuesto por tres personas que laboran en la organización. Se observa con mayor detalle en el cuadro 1.

Cuadro 1. *Población de estudio*

Persona	Puesto
Persona 1	Ingeniero eléctrico
Persona 2	Ingeniero en sistemas
Persona 3	Gerente administrativo y financiero

Fuente: Elaboración Propia

También, se requirió el estudio de ciertos procesos y funcionalidades para visualizar el flujo de trabajo en el departamento de TI. Se observa con mayor detalle en el cuadro 2.

Cuadro 2. *Objetos de estudio y sus especificaciones*

Objeto de estudio	Especificaciones
Sistemas	CRM de Microsoft y el ERP de Softland.
Seguridad	Accesos de personas autorizadas en los sistemas. Configuraciones de seguridad. Actualizaciones.
Documentación	Bitácora. Plan de continuidad y de contingencias.
Infraestructura y plataforma tecnológica	Políticas y procedimientos de administración de control de los recursos de información.

Fuente: Elaboración Propia

3.3. Fuente de Información

3.3.1. Fuente primaria

Las fuentes primarias que se utilizaron para el desarrollo de la investigación consistieron en las siguientes:

- Entrevista
- Observación
- Documentación del análisis desarrollado anteriormente por una empresa externa.
- Cuestionario

3.3.2. Fuente secundaria

Las fuentes secundarias que se utilizaron para el desarrollo de la investigación consistieron en las siguientes:

- Marco COBIT 2019
- ISO 27001
- COBIT 2019, Kit de herramientas de diseño
- COBIT 2019, Marco de Referencia, Introducción y Metodología
- COBIT 2019, Diseño de una solución de Gobierno de Información y Tecnología
- Tesis relacionadas a:

    - Propuesta del modelo de implementación del gobierno de TI.
    - Impacto de las tecnologías de la información en los negocios.
    - Modelo de gobierno y gestión de TI basado en el marco de referencia COBIT 2019.
    - Continuidad de negocio basada en COBIT.
    - Evaluación por medio de COBIT 2019.
- Bases de datos utilizadas:
    - Kérwá repositorio institucional de la Universidad de Costa Rica
        - COBIT 2019.
        - Evaluación del marco COBIT 2019.
        - Modelo de implementación COBIT 2019.
    - Dialnet
        - TIC.
        - Modelo de TIC.
        - Marco de referencia COBIT 2019.
        - Tecnologías de Información.
        - Plan de contingencia.

3.4. Técnicas e instrumentos de recolección de información

Las técnicas que se utilizaron en la investigación son las siguientes:

- Observación directa con el fin de observar los sistemas, las configuraciones, funciones y procesos que realizan. Asimismo, ver la forma en la que se encuentra estructurado en la organización. Igualmente, se quiere conocer y entender como realizan ciertos procesos y actividades que no requieren de la presencia de los participantes de la entrevista, para ello se contó una guía de observación que contemple los escenarios para evaluar en TI.
- Entrevista, a una persona de la organización, encargada de área de soporte técnico, se hizo de manera individual, además se utilizó un blog de notas para anotar la información.
- Cuestionario, para recopilar la información del cuestionario se utilizó un Excel, se envió por correo electrónico a una persona de la organización, encargada del departamento de TI, se realizó con el fin de recabar información de manera más específica, se utilizó preguntas cerradas.

- Revisión documental, se revisó la documentación del marco COBIT 2019 e ISO 27001, la documentación de la auditoría proporcionada por la organización.

3.5. Análisis de datos

En el análisis de datos se tiene como objetivo recabar información como la siguiente:

- Tipos de procesos y las funciones que se realizan en el departamento de TI.
- A partir del marco COBIT 2019 analizar y buscar las mejores prácticas para la organización.
- Obtener el mapeo de los procesos.
- Finalizar la guía de buenas prácticas para el departamento de TI.

Cuadro resumen del planteamiento metodológico

Cuadro 3. *Marco metodológico que se utilizará para cumplir los objetivos de la investigación*

Objetivos	Fuente de Información	Instrumentos	Análisis de datos
Identificar los procesos y funciones del departamento de TI para conocer el funcionamiento del área.	Tres personas: un ingeniero eléctrico, un ingeniero en sistemas y por último, una con el cargo administrativo y financiero. Una persona de soporte técnico.	- Entrevista - Observación directa. - Cuestionario	Recopilar los procesos y funciones del departamento de TI.

Evaluar mediante COBIT 2019 los procesos y funciones del departamento de TI, con el fin de identificar las fortalezas y debilidades de su gestión.	Procesos y las funciones del departamento de TI a partir de la información proporcionada del objetivo anterior.	A partir de la revisión documental del marco de trabajo COBIT se realiza un análisis de contenido de la información. Además, del análisis del cuestionario.	A partir de los objetivos brindados por COBIT 2019 se genera una evaluación de la organización.
Elaborar una guía de buenas prácticas para el departamento de TI con el fin de recomendar oportunidades de mejora en funciones, procesos y seguridad.	Resultado de la evaluación del marco.	Análisis de contenido de la información.	Una guía de buenas prácticas ordenada de acuerdo con el resultado de probabilidad e impacto en la organización.

Fuente: Elaboración propia

4. CUARTO CAPÍTULO: PROCESOS Y FUNCIONES DEL DEPARTAMENTO DE TI EN LA ORGANIZACIÓN

En este cuarto capítulo se desarrolla el primer objetivo de la investigación, consiste en identificar los procesos y funciones del departamento de TI a nivel interno (gestionar la infraestructura tecnología, seguridad en la red y los datos, soporte técnico a los colaboradores, gestión de sistemas de comunicación interno o externo) para conocer el funcionamiento del área dentro de la organización. Por ello, antes de comenzar es importante conocer más acerca de la organización, el capítulo estará desarrollado de la siguiente manera: se conocerá el departamento de TI, estructura organizacional del área, procesos y funciones, herramientas utilizadas.

4.1. Departamento de TI

4.1.1. Estructura organizativa del departamento

El área está constituida solo por una persona, la cual se encarga de gestionar todo lo relacionado a TI, desde configurar los correos electrónicos de la organización, la entrega de equipo, reparación de equipos, gestión de las plataformas que usa la empresa y demás funciones.

Y como se mencionó con anterioridad se debe responder al gerente de financiero ya que es un departamento nuevo y no tienen aún una gerencia correspondiente al departamento de TI como tal.

4.1.2. Procesos del departamento de TI

En el departamento de TI realizan varios procesos como los siguientes: peticiones hacia el personal de TI, entrega del equipo tecnológico y gestión de tecnologías de la información TI, cada proceso será explicado a continuación.

- **Peticiones hacia el personal de TI:** se compone de las peticiones que tienen los colaboradores de la empresa hacia el personal de TI, se hace por medio de solicitudes, por lo general escritas y por medio de correo electrónico, o bien de forma verbal, dependiendo del proceso por llevar a cabo.

  Es decir, si es para la compra de algún equipo o bien para reparación de un equipo se debe hacer mediante el correo, expresando la solicitud puntual, para que se dé el visto bueno

por parte del gerente a cargo del departamento, pero si es solo por algún inconveniente menor, se gestiona sin la compra extra, por lo que se hace de forma verbal.

- **Entrega del equipo tecnológico: c**onsiste en proporcionarles a los colaboradores el equipo necesario para cumplir con sus labores, para realizar el proceso correctamente cuentan con un documento que les permite tener garantía y hacer constar que el equipo entregado está en perfectas condiciones para usarse.
- **Gestión de tecnología de información TI:** se tiene la fiscalización tanto del *hardware* y el *software* de los equipos que se ponen a disposición de los colaboradores**,** así como la seguridad ofrecida por los proveedores de distintas herramientas que utiliza la organización. Para llevar a cabo este proceso utilizan un documento que indica requisitos que se debe cumplir.

4.1.3. Funciones del departamento de TI

El personal de TI cuenta con varias funciones, las principales que desarrollan son: servicio técnico, administración de las herramientas utilizadas en el departamento de TI, gestión de equipos informáticos y seguridad, cada proceso será explicado a continuación.

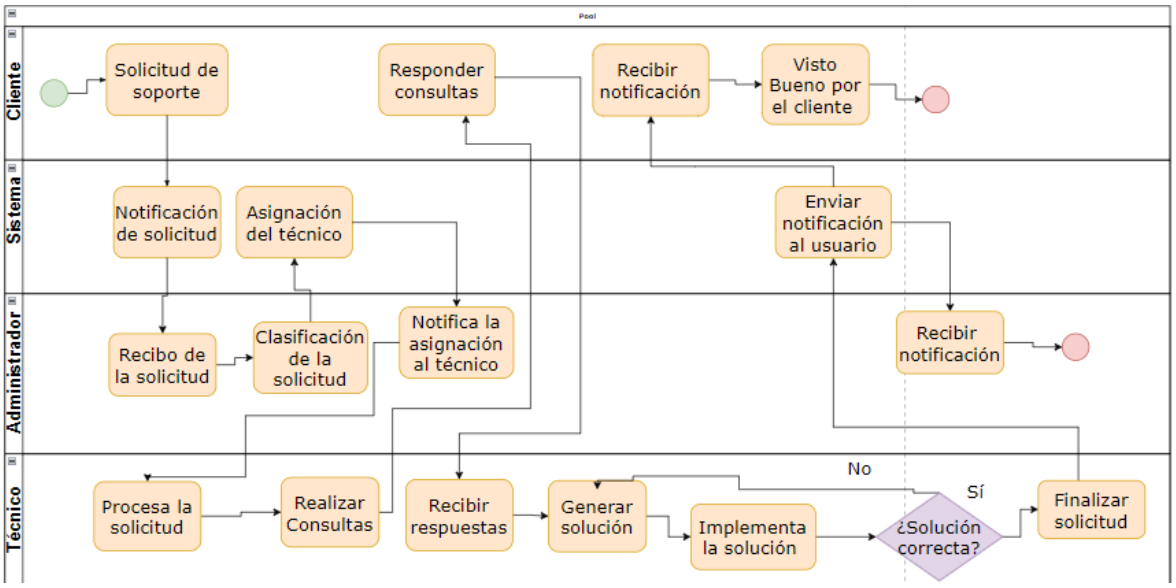
- **Servicio técnico:** para llevar a cabo el proceso de servicio técnico se le solicita al cliente que registre una solicitud, él ingresa nombre, asunto, descripción, nivel de importancia (la prioridad si es 1, 2, 3) en el sistema Portal del CRM de Microsoft. Luego el sistema envía un correo a la persona administradora, ella asigna el caso a el técnico que tiene conocimiento y es responsable del cliente.

El técnico recibe una notificación del caso (se le indica a la persona por medio de Teams sobre el caso asignado). En el proceso lo primero que se realiza, es saber cómo proceder (llamada, correo, Teams, cita), en este caso, se tienen diferentes actividades para desarrollar e involucrar al cliente con el fin de conocer más acerca de lo solicitado.

Una vez que resuelve el caso o la solicitud, se envía un correo para el cliente y el administrador del CRM. Por último, la finalización del caso se da cuando la persona que abrió la solicitud le da el visto bueno mediante un correo o cuando se reactiva nuevamente el caso por disconformidad en la solución utilizada.

Una representación ilustrativa del servicio técnico mencionada anteriormente se puede ver en la Figura 7.

Figura 7. *Diagrama de flujo del servicio técnico*



Fuente: Elaboración Propia

- **Administración de las herramientas utilizadas en el departamento de TI:** el área de TI cuenta con un cuarto de servidores donde se encuentran los servidores físicos, a su vez la administración de los servidores en la nube, además del *software* que usa la compañía.

También se cuenta con sistemas de administración para las cuentas y contraseñas de la organización, a su vez de los recursos para la compra de equipo necesario para los colaboradores y de los implementos necesarios de la oficina como lo pueden ser impresoras, equipo electrónico o bien para los mismos servidores.

- **Seguridad:** La organización cuenta con un cuarto pequeño donde tiene los servidores que se encuentran en uso, además en él también tiene otros dispositivos como herramientas, piezas de cómputo y materiales. Cada uno de estos equipos se encuentran monitorizados por una cámara de seguridad.

Para ingresar al cuarto cualquier persona que lo requiera o lo necesite puede tener acceso a este. Es decir, no se requiere ningún tipo de autorización, tampoco se lleva un registro, ni se

solicita una descripción del motivo del ingreso, solo se requiere de la necesidad de entrar para tener acceso al lugar.

Seguridad de los sistemas: para la seguridad de TI en los sistemas realizan actualizaciones para protegerlos de *software* malicioso. Además, toman medidas en los correos y las descargas que realizan los colaboradores con el fin de evitar ataque de spyware y el phishing. Por esta razón, la empresa concientiza a los trabajadores de los peligros a los que se pueden exponer si cuentan con un mal manejo de las contraseñas, el uso inadecuado del correo y el ingreso de páginas web peligrosas. En menor medida conocen o investigan acerca de las nuevas amenazas de seguridad que hay en el mercado, por ende, de los consejos y los protocolos que deben considerarse al enfrentarse a estos nuevos peligros.

Seguridad de la red: Poseen configuraciones de seguridad en el equipo de red y un control del tráfico entrante y saliente de la red, además aplican un mecanismo de filtrado como el firewall, con el fin de detectar intrusos. Realizan un esfuerzo en la aplicación de protocolos de seguridad en las conexiones de red, aunque puede mejorarse.

- **Gestión de equipos informáticos**

Los dispositivos se encuentran asociados a cada colaborador mediante un documento que se da al inicio de la entrega del equipo. Además, las computadoras o ciertos activos no cuentan con una placa de identificación, con el fin de controlar el activo y en caso de pérdida o de robo pueda identificarse.

4.1.4. Tratamiento de la información y los dispositivos de la organización

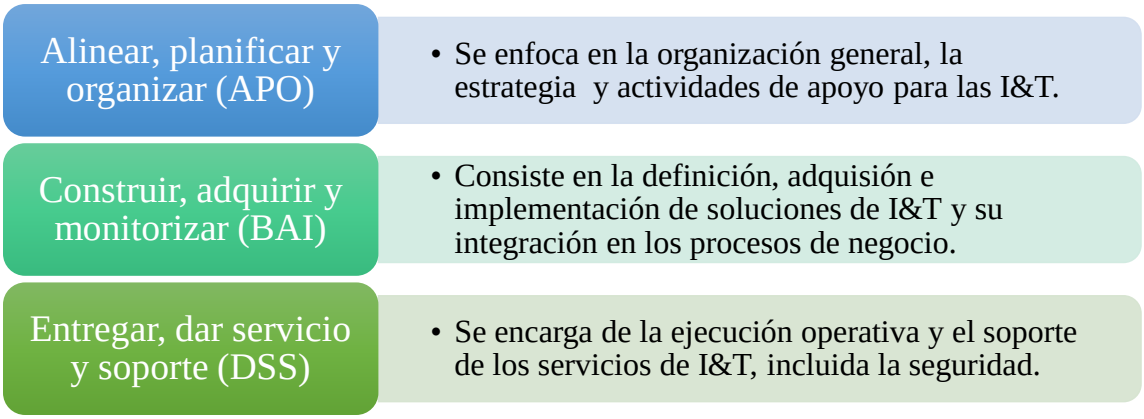
4.1.4.1. Tratamiento de la información

La información sensible no posee un tratamiento diferente a los documentos públicos o no confidenciales, por ello su acceso no es controlado ni se encuentra definido para ciertos trabajadores.

5. QUINTO CAPÍTULO: EVALUACIÓN DE LOS PROCESOS Y FUNCIONES DEL DEPARTAMENTO DE TI, A PARTIR DE COBIT 2019

Para llevar a cabo la selección de dominios en esta investigación se debe tomar en cuenta que COBIT está conformado por cinco dominios: Evaluar, dirigir y monitorizar (EDM), Alinear, planificar y organizar (APO), Construir, adquirir y monitorizar (BAI), Entregar, dar servicio y soporte (DSS), Monitorizar, evaluar y valoras (MEA). De los cuales se trabajará con dos de ellos, debido a su enfoque en los procesos y a los temas que para la organización son más relevantes, cada uno de los procesos de dominios son elegidos debido al crecimiento que tiene la organización si bien es cierto el departamento de TI es pequeño y no sé encuentra totalmente definido es un punto de partida para realizar una evaluación. El objetivo es que lleven a ejecución las mejores prácticas, además antes de aplicar cambios o realizar modificaciones se debe tener un panorama amplio y estos procesos les permite contemplar lo que se requiere para empezar las bases de un departamento de TI, se visualizan en la Figura 8.

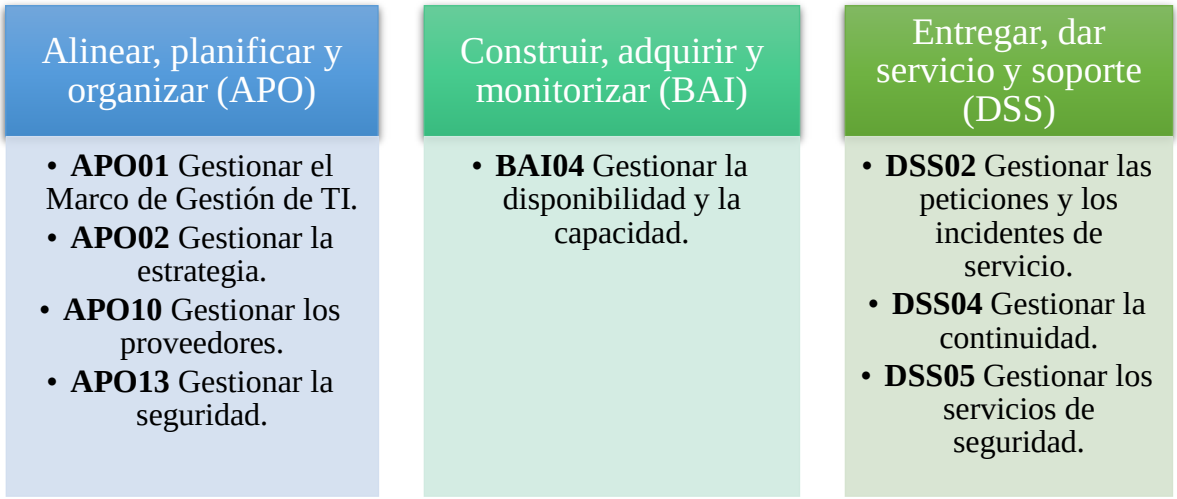
Figura 8. *Selección de los dominios de COBIT y su enfoque*



Fuente: Elaboración Propia

Para llevar a cabo esta elección se consideró la auditoría que previamente se le realizó a la organización por parte de una empresa externa. A partir del documento proporcionado se analizaron los puntos donde se tienen mayores debilidades y se encajaron con los dominios que posee COBIT, pero esto se empieza a desglosar más cuando se da la observación de los objetivos, ya que cada uno conforma el dominio y se dividen en diferentes pautas. En la Figura 9 se puede observar los objetivos seleccionados por dominio.

Figura 9. *Objetivos seleccionados por dominio*



Fuente: Elaboración Propia

Cada uno de estos objetivos esta subdividido en otros puntos de los cuales se eligieron los de mayor interés para la organización.

Dominio 1: Selección de procesos de Alinear, planificar y organizar (APO), ver la tabla 3.

Tabla 3. *Procesos que se tomarán del dominio de APO*

***APO01** Gestionar el Marco de Gestión de TI*	• **APO01.01** Diseñar el sistema de gestión para la I&T de la institución. • **APO01.02** Gestionar la comunicación de los objetivos, dirección y decisiones tomadas. • **APO01.03** Gestionar la implementación de procesos. • **APO01.04** Definir e implementar las estructuras organizativas. • **APO01.05** Establecer roles y responsabilidades • **APO01.06** Optimizar la ubicación de la función de TI. • **APO01.07** Definir la propiedad de la información (datos) y del sistema de información.

	• **APO01.08** Definir las habilidades y competencias objetivo. • **APO01.09** Definir y comunicar políticas y procedimientos. • **APO01.10** Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión.
***APO02** Gestionar la estrategia*	• **APO02.01** Comprender el contexto y la dirección de la empresa. • **APO02.02** Evaluar las capacidades, rendimiento y madurez digital actual de la empresa. • **APO02.03** Definir las capacidades digitales objetivo. • **APO02.05** Definir el plan estratégico y el mapa de ruta.
***APO10** Gestionar los proveedores*	• **APO10.01** Identificar y evaluar los contratos y las relaciones con los proveedores. • **APO10.04** Gestionar el riesgo de los proveedores.
***APO13** Gestionar la Seguridad*	• **APO13.01** Establecer y mantener una información gestión de seguridad (SGSI). • **APO13.02** Definir y administrar una seguridad de la información y riesgo de privacidad plan de tratamiento. • **APO13.03** Supervisar y revisar la información gestión de seguridad (SGSI).

Fuente: Elaboración Propia

Dominio 2: Selección de procesos de Construir, adquirir y monitorizar (BAI), ver la tabla 4.

Tabla 4. *Procesos que se tomarán del dominio de BAI*

***BAI04** Gestionar la Disponibilidad y la Capacidad*	• **BAI04.02** Evaluar el impacto en el negocio.

	• **BAI04.03** Planificar los requisitos de los servicios nuevos o modificados. • **BAI04.05** Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad.

Fuente: Elaboración Propia

Dominio 3: Selección de procesos de Entregar, dar servicio y soporte (DSS), ver la tabla 5.

Tabla 5. *Procesos que se tomarán del dominio de DSS*

DSS02 *Gestionar las Peticiones y los Incidentes del Servicio*	• **DSS02.01** Definir esquemas de clasificación para incidentes y peticiones de servicio. • **DSS02.02** Registrar, clasificar y priorizar las peticiones e incidentes. • **DSS02.06** Cerrar las peticiones de servicio y los incidentes.
DSS04 *Gestionar la Continuidad*	• **DSS04.01** Definir la política de continuidad del negocio, sus objetivos y alcance. • **DSS04.02** Mantener la resiliencia del negocio. • **DSS04.03** Desarrollar e implementar una respuesta de continuidad del negocio.
DSS05 *Gestionar los Servicios de Seguridad*	• **DSS05.01** Proteger contra *software* malicioso. • **DSS05.02** Gestionar la seguridad de la conectividad y de la red. • **DSS05.03** Gestionar la seguridad de *endpoint*. • **DSS05.04** Gestionar la identidad del usuario y el acceso lógico. • **DSS05.05** Gestionar el acceso físico a los activos de I&T.

Fuente: Elaboración Propia

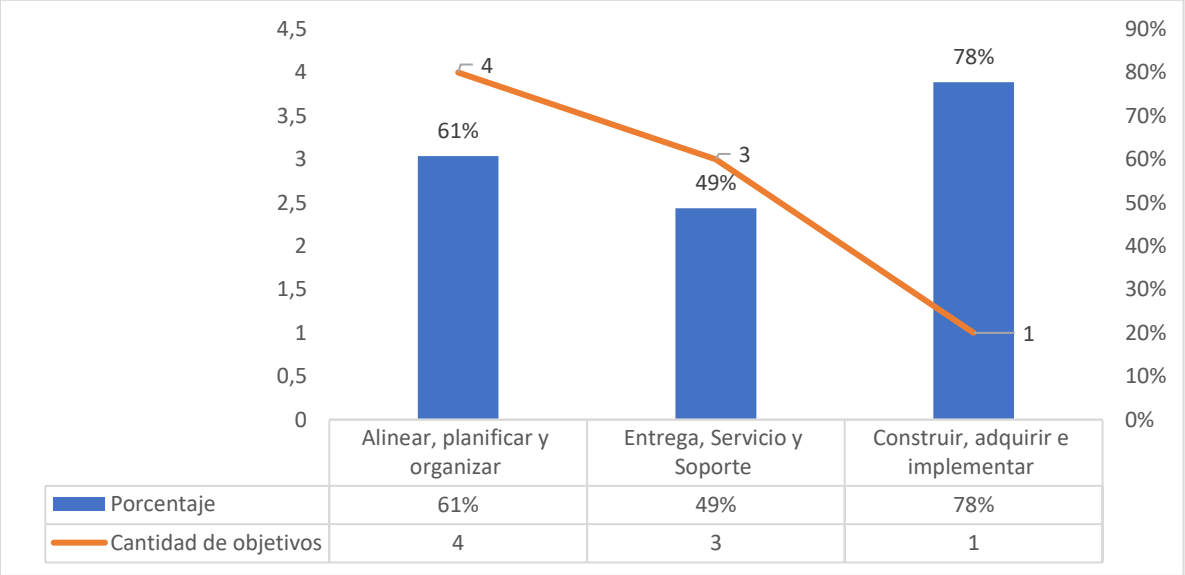
5.1. **Resultado de la evaluación de COBIT 2019 en la empresa de equipos electrónicos**

Para ejecutar la información mencionada anteriormente, se aplicaron cuestionarios que contienen preguntas acerca de los objetivos de COBIT 2019 elegidos, ellos abarcan consultas sobre el grado de los procesos y funciones que se aplican en la organización, nos permite tener el conocimiento para saber en qué condiciones está la empresa asociados en los puntos elegidos del marco COBIT 2019. Los resultados obtenidos se exponen en los siguientes grupos: evaluación por dominio, evaluación por subobjetivos de control y evaluación por objetivos.

5.1.1. Evaluación por dominio

La evaluación de dominios se puede ver en la Figura 10, donde se aprecia los dominios seleccionados, la cantidad de objetivos que se tomaron en consideración, por último, el resultado que se da al evaluar la organización, este es representado por el porcentaje.

Figura 10. *Evaluación de los dominios seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*



Según los resultados que se muestra en la Figura 10, se tiene que el dominio con menor cumplimiento del objetivo es el de entregar, servicio y soporte con un porcentaje de 49%, lo que deja en evidencia problemas en la parte de seguridad, falta de planes de continuidad de negocio, gestión de peticiones e incidentes de servicio.

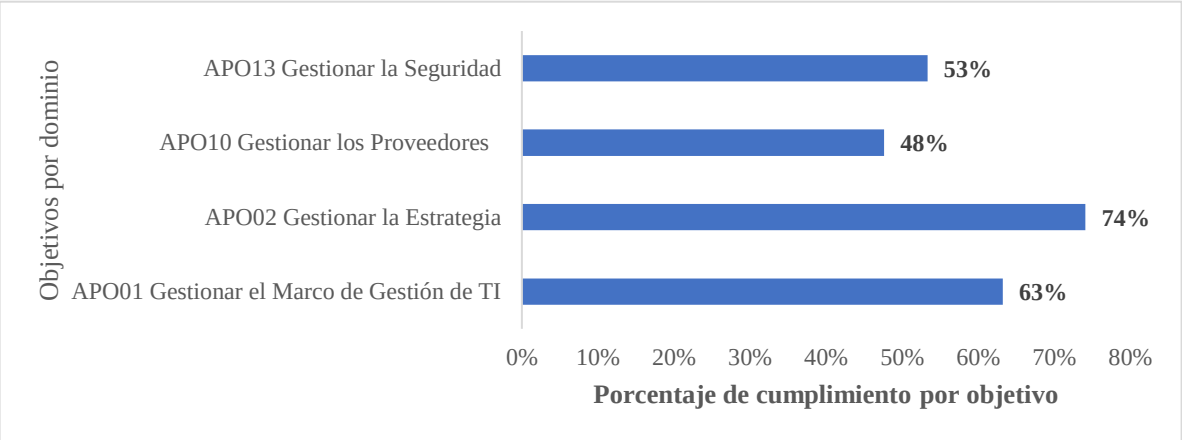
Por otro lado, el objetivo con mayor cumplimiento es construir, adquirir e implementar con un 78%, es mayor al 70%, por lo tanto, es uno de los dominios que se encuentran en el rango aceptable para el marco de trabajo COBIT 2019.

5.1.2. Evaluación por objetivos

En la evaluación que se realizó se presentan los objetivos por dominio que fueron seleccionados, cada uno cuenta con el porcentaje de cumplimiento que tiene en la organización.

5.1.2.1. **Alinear, Planificar y Organizar**

Figura 11. *Evaluación de los objetivos del dominio de Alinear, Planificar y Organizar seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos*



Fuente: Elaboración Propia

Como se puede apreciar en la Figura 11 el objetivo con menor cumplimiento es el APO10 Gestionar los Proveedores con un 48% con respecto a las demás, lo que indica que el departamento no tiene una estrecha relación con los proveedores de servicio, ya que presentan desconocimientos de los contratos que han adquirido, no hay un control o una documentación sobre los servicios adquiridos y la importancia que estos tienen para la empresa.

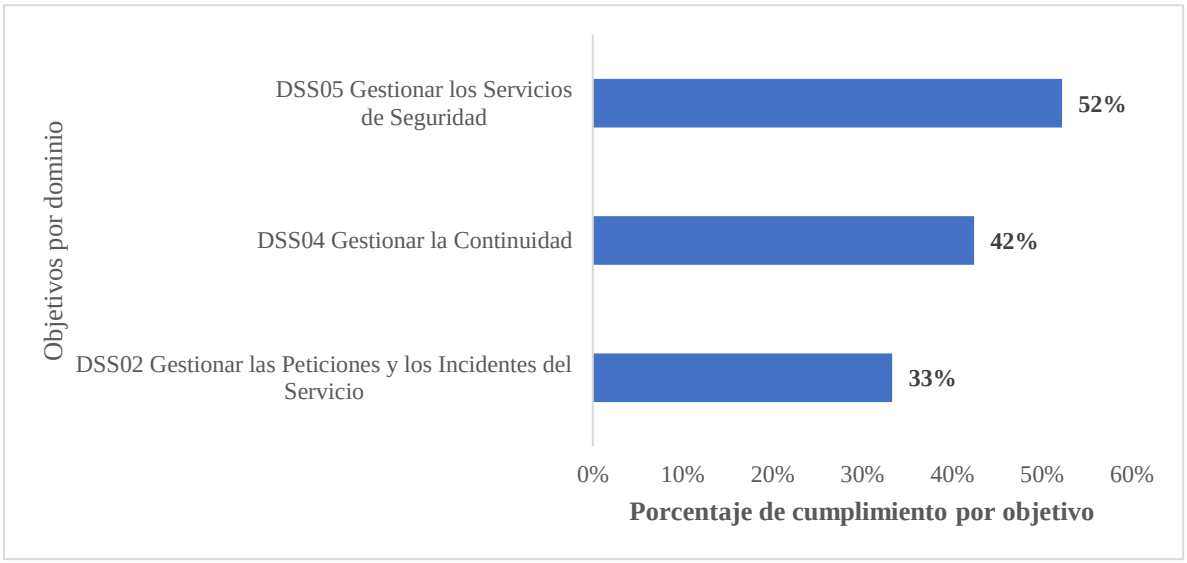
5.1.2.2. **Construir, Adquirir e Implementar**

Al aplicar la evaluación del objetivo BAI04 Gestionar la Disponibilidad y la Capacidad da como resultado 78% de cumplimiento, lo cual indica que la organización en este tema alcanza el 70% que requiere debido a los siguientes puntos: la organización tiene identificado

soluciones o servicios críticos en los procesos de disponibilidad y capacidad, además, cuenta con planes de disponibilidad, rendimiento y capacidad. también posee acciones correctivas.

5.1.2.3. **Entrega, Servicio y Soporte**

Figura 12. *Evaluación de los objetivos de dominio Entrega, Servicio y Soporte del marco COBIT 2019 aplicado a la organización de equipos eléctricos*



Fuente: Elaboración Propia

Como se puede apreciar en la Figura 12 el objetivo con menor cumplimiento es el DSS02 Gestionar las Peticiones y los Incidentes con un 33% con respecto a los demás, las revisiones del departamento presentan oportunidades de mejora en esta área, se debe adquirir o realizar un flujo de proceso para atender la solicitudes de servicio, implementar revisiones de los incidentes atendidos con los usuarios con el fin de recibir el visto bueno, incorporar los informes sobre las incidencias y solicitudes que atiende con el fin de contar con información para la toma de decisiones y realizar modelos de incidentes basados en errores conocidos.

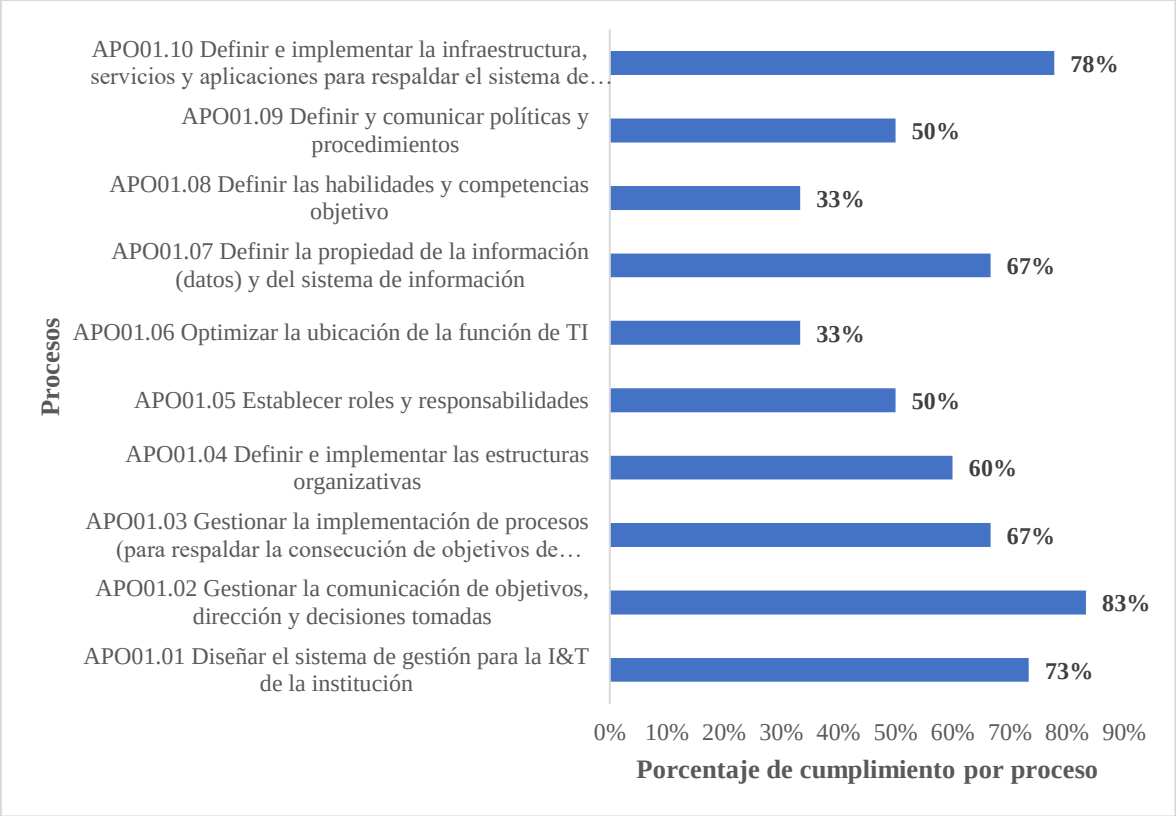
5.1.3. Evaluación por procesos de control

En la evaluación que se realizó se presentan los procesos que fueron tomados de los objetivos, estos se agrupan por dominio y luego por objetivos, cada uno cuenta con el porcentaje de cumplimiento que tienen en la organización.

5.1.3.1. Procesos del dominio Alinear, Planificar y Organizar

5.1.3.1.1. APO01 Gestionar el Marco de Gestión de TI

Figura 13. *Evaluación de los procesos del objetivo APO01 Gestionar el Marco de Gestión de TI seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*

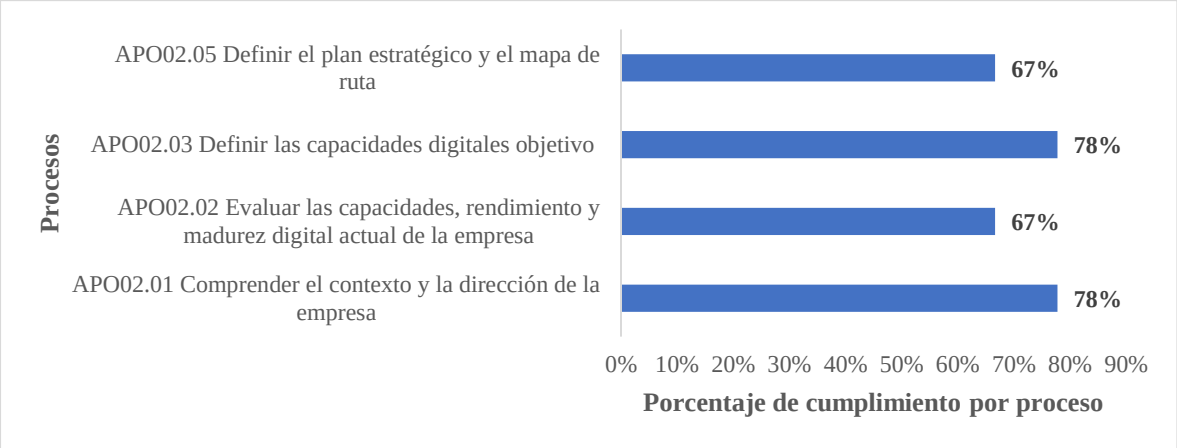


Fuente: Elaboración Propia

Como se puede apreciar en la Figura 13, los objetivos con menor cumplimiento es el APO1.08 Definir las habilidades y competencias objetivo y el APO01.06 Optimizar la ubicación de la función de TI, ambos procesos con un 33%, esta situación indica que la organización no cuenta con claridad en las funciones, la importancia del departamento de TI, además no cuenta con un análisis de las habilidades y capacidades que requieren con respecto a las actuales de la fuerza laboral.

5.1.3.1.2. APO02 Gestionar la estrategia

Figura 14. *Evaluación de los procesos del objetivo APO02 Gestionar la estrategia seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*

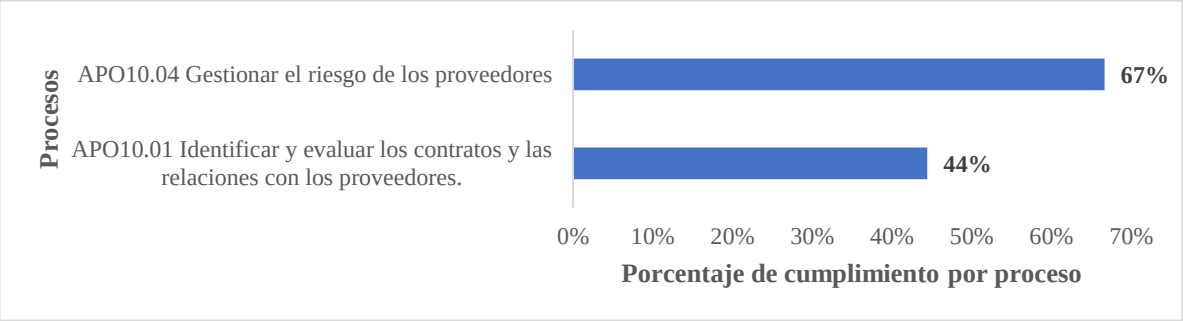


Fuente: Elaboración Propia

Como se puede apreciar en la Figura 14 los objetivos con menor cumplimiento es el APO02.02 Evaluar las capacidades, rendimiento y madurez digital actual de la empresa y APO02.05 ambos con un 67%, lo que indica que el departamento no cuenta con una metodología del trabajo ágil que les permita llevar a cabo los procesos de una forma más ordenada y con una serie de pasos, también se debe considerar mejora en los objetivos de la organización para que estos sean medibles.

5.1.3.1.3. APO10 Gestionar los proveedores

Figura 15. *Evaluación de los procesos del objetivo APO10 Gestionar los proveedores seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*

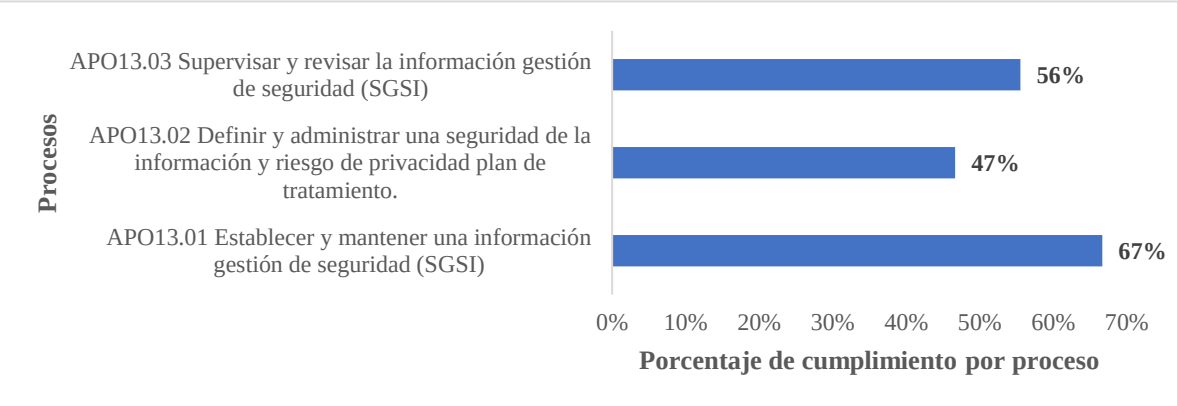


Fuente: Elaboración Propia

Como se puede apreciar en la Figura 15, el objetivo con menor cumplimiento es el APO10.01 Identificar y evaluar los contratos y las relaciones con los proveedores con un 44%, lo que indica es que la organización tiene proveedores, pero se desconoce si los contratos tienen relación con ellos mismos.

5.1.3.1.4. APO13 Gestionar la Seguridad

Figura 16. *Evaluación de los procesos del objetivo APO13 Gestionar la Seguridad seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*



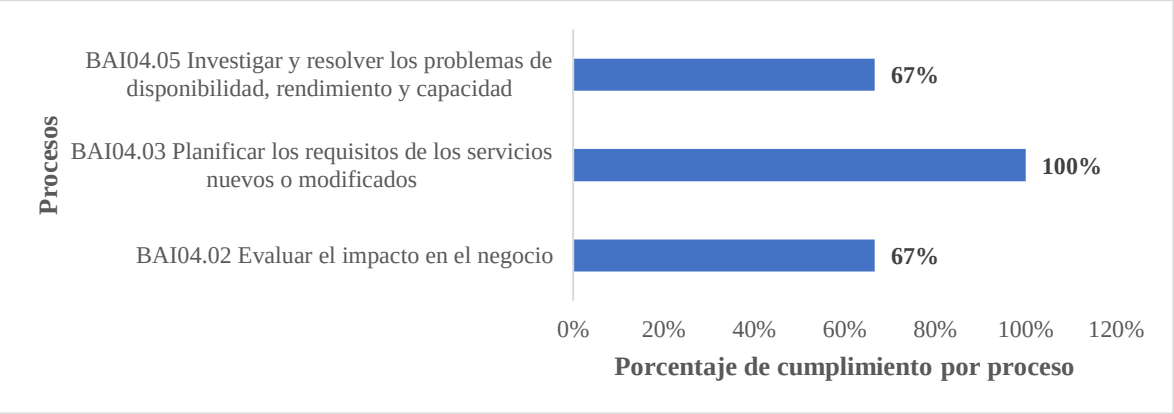
Fuente: Elaboración Propia

Como se puede apreciar en la Figura 16 el proceso con menor cumplimiento es el APO13.02 Definir y administrar una seguridad de la información y riesgo de privacidad plan de tratamiento con un 47%, lo que indica que el departamento cuenta con un plan, pero este no contiene toda información relevante como: práctica de gestión, soluciones de seguridad, recursos, responsabilidades y recursos asociados, además no se tiene información sobre la solución que ha implementado de los riesgos, también requiere que la fuerza laboral sea capacitada sobre los peligros del internet y las medidas que se deben considerar para proteger a la organización.

5.1.3.2. Objetivos del dominio Construir, Adquirir e Implementar

5.1.3.2.1. BAI04 Gestionar la Disponibilidad y la Capacidad

Figura 17. *Evaluación de los procesos del objetivo BAI04 Gestionar la Disponibilidad y la Capacidad seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*



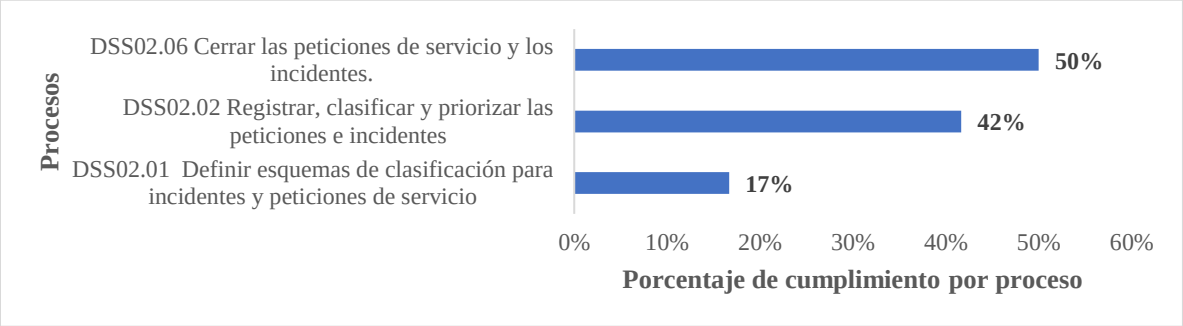
Fuente: Elaboración Propia

Como se puede apreciar en la Figura 17 los procesos con menor cumplimiento son el BAI04.05 Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad 67%, lo que indica en moderadamente se realizan investigaciones y se resuelven problemas relacionados a la disponibilidad, rendimiento y capacidad. El BAI04.02 Evaluar el impacto del negocio 67% lo que indica es que moderadamente se llevan evaluaciones sobre el impacto que tiene los procesos críticos en la organización.

5.1.3.3. Objetivos del dominio Entrega, Servicio y Soporte

5.1.3.3.1. DSS02 Gestionar las Peticiones y los Incidentes del Servicio

Figura 18. *Evaluación de los procesos del objetivo DSS02 Gestionar las Peticiones y los Incidentes del Servicio seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos*

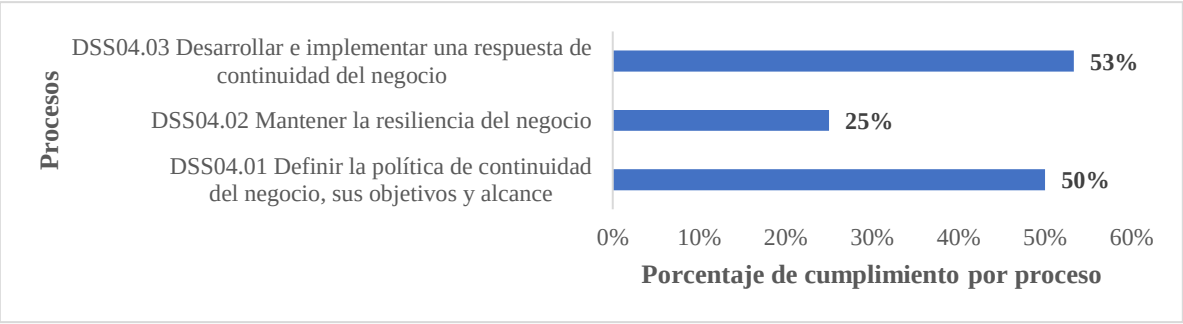


Fuente: Elaboración Propia

Como se puede apreciar en la Figura 18 el proceso con menor cumplimiento es el DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio con un 17% con respecto a los demás, lo que indica que no tiene mucho conocimiento sobre el término SLA (Acuerdo a nivel de servicio), no tienen definido la información que es importante para la organización.

5.1.3.3.2. DSS04 Gestionar la Continuidad

Figura 19. *Evaluación de los procesos del objetivo DSS04 Gestionar la Continuidad seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*

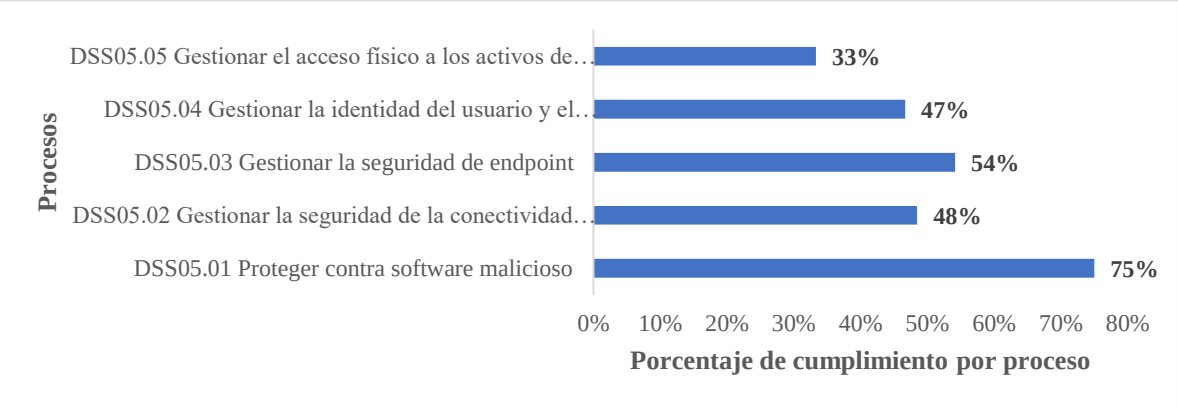


Fuente: Elaboración Propia

Como se puede apreciar en la Figura 19 el objetivo con menor cumplimiento es el DSS04.02 Mantener la resiliencia del negocio con un 25% con respecto a los demás, lo que indica que la organización ha identificado poco los procesos empresariales de apoyo esenciales y los servicios de I&T relacionados, además los escenarios potenciales que dan lugar a eventos que puede causar incidentes disruptivos significativos se evalúan en menor medida, también no han definido los tiempos de recuperación del negocio y cuentan con un plan de negocio poco desarrollado.

5.1.3.3.3. DSS05 Gestionar los Servicios de Seguridad

Figura 20. *Evaluación de los procesos del objetivo DSS05 Gestionar los Servicios de Seguridad seleccionados del marco COBIT 2019 aplicado a la organización de equipos eléctricos.*



Fuente: Elaboración Propia

Como se puede apreciar en la Figura 20 el objetivo con menor cumplimiento es el DSS05.05 Gestionar el acceso físico a los activos de I&T 33% con respecto a los demás, lo que indica que la organización gestiona muy poco los perfiles de acceso, además las personas que se retiran de la empresa continúan usando las cuentas. Además, los colaboradores no tienen conocimiento sobre los temas de seguridad de información física.

6. SEXTO CAPÍTULO: GUÍA DE BUENAS PRÁCTICAS PARA EL DEPARTAMENTO DE TI DE LA ORGANIZACIÓN DE EQUIPOS ELÉCTRICOS

En este sexto capítulo se desarrolla la guía de buenas prácticas para el departamento de TI, a partir de la evaluación realizada anteriormente, esta guía se va a desarrollar a partir de un cuadro que nos indicará como se debe proceder ante las situaciones que afectan el área y que requieren de atención por parte de la organización.

6.1. **Alinear, Planificar y Organizar**

6.1.1. APO01 Gestionar el Marco de Gestión de TI

Según ISACA (2018) el APO01 consiste en lo siguiente:

> Implementar un enfoque uniforme de gestión para permitir que se alcancen los requisitos de gobierno empresarial, con cobertura de componentes de gobierno, como 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. (p.33)

6.1.1.1. APO01.05 Establecer roles y responsabilidades.

Tabla 6. *Plan de acción de práctica de gestión: APO01.05*

Práctica de gestión: APO01.05 Establecer roles y responsabilidades	
Situación actual	**Descripción de la práctica de COBIT 2019**
La organización cuenta con un plan de continuidad. En menor medida se realiza la definición de roles y responsabilidades, la supervisión de estos para saber si aún cuenta con accesos u autoridad o si tienen los recursos suficientes para realizar las funciones asignadas.	Definir y comunicar las funciones y responsabilidades en materia de TI empresarial, incluidos los niveles de autoridad, las responsabilidades y la rendición de cuentas.
Brecha	
No se contemplan los siguientes requerimientos:	

<table>
<tr><td colspan="3">

- La comunicación es escasa, ya que el plan de continuidad no es compartido con los colaboradores.
- Poca definición de las responsabilidades, roles, niveles de autoridad y rendición de cuentas no es la adecuada.
- El plan no cuenta con la información de contacto y las funciones actualizadas.

</td></tr>
<tr><th colspan="3">Plan para ejecutar</th></tr>
<tr><th>Actividad según COBIT 2019</th><th>Acción</th><th>Documentación</th></tr>
<tr><td>1. Establecer, acordar y comunicar las funciones y responsabilidades relacionadas con la I&T para todo el personal de la empresa, en consonancia con las necesidades y objetivos empresariales. Delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la toma de decisiones y las aprobaciones.</td><td>

- Comprender las necesidades y objetivos empresariales.
- Comprender la situación actual de TI.
- Formular las funciones y responsabilidades relacionadas con TI de manera que se encuentren alineadas con las necesidades y los objetivos empresariales.
- De lo generado en el paso anterior comunicárselo a los colaboradores de la organización.
- Con la ayuda de herramientas se requiere definir de manera clara y concisa las responsabilidades y la rendición de cuentas.

</td><td>

- Una guía para llevar a cabo esta acción es utilizar la estructura del Plan estratégico de TI.

Ver anexo 6

- Una guía para llevar a cabo esta acción es la Matriz RACI, la cual consiste en mapear las actividades de la organización o departamento, para a partir de ahí clasificar a los roles, su clasificación va a consistir en responsable, aprobador, consultado e

</td></tr>
</table>

		informado. Al llevar a cabo este proceso nos permite analizar la distribución de responsabilidad dentro de la organización. Ver anexo 7
2. Considerar los requisitos de la continuidad de los servicios de la empresa y de TI a la hora de definir las funciones, incluidos los requisitos de respaldo y formación cruzada del personal.	En el momento de elaborar las funciones, los requisitos de respaldo y además la formación cruzada del personal, se recomienda tener presente los requisitos de continuidad de los servicios y de TI.	No aplica
3. Proporcionar información al proceso de continuidad del servicio de TI manteniendo actualizados los datos de contacto y las descripciones de funciones en la empresa.	Se recomienda que cuando se lleven a cabo cambios de información de la organización o se agreguen nuevos objetivos o metas, estas puedan incorporarse en el plan de continuidad con el fin de evacuar cualquier situación que se pueda presentar cuando falle lo agregado nuevo.	No aplica
4. Incluir requisitos específicos en las descripciones de funciones y responsabilidades en relación con el cumplimiento de las	Al desarrollar las descripciones de funciones y responsabilidades se	No aplica

políticas y procedimientos de gestión, el código ético y las prácticas profesionales.	recomienda involucrar requisitos específicos sobre: - Cumplimiento de políticas y procedimientos de gestión. - Código ético. - Prácticas profesionales.	
5. Asegurar que la rendición de cuentas se defina mediante funciones y responsabilidades.	Para asegurar que se lleva a cabo una adecuada rendición de cuentas se deben considerar los pilares que la conforman información, diálogo y responsabilidad. Por ello, se recomienda que los colaboradores tengan claridad sobre sus funciones y responsabilidades, además que se apropien de estas con el fin de que se hagan responsables de sus acciones.	No aplica
6. Estructure las funciones y responsabilidades para reducir la posibilidad de que una sola función comprometa un proceso crítico.	Al definir responsabilidades y funciones es necesario llevar a cabo un análisis de los procesos que tiene la organización, con el fin de evitar que se vean perjudicados.	No aplica
7. Implantar prácticas de supervisión adecuadas para garantizar que las funciones y responsabilidades se ejerzan correctamente, evaluar si todo	Se requiere que se lleven a cabo los siguientes puntos: - Fiscalizar la autoridad y los recursos de los colaboradores para	No aplica

el personal tiene autoridad y recursos suficientes para ejecutar sus funciones y responsabilidades y, en general, revisar el rendimiento. El nivel de supervisión debe estar en consonancia con la sensibilidad del puesto y el alcance de las responsabilidades asignadas.	proporcionarles lo necesario para que puedan cumplir con sus funciones y responsabilidades. - Revisar el rendimiento. - Contar con una supervisión acorde al puesto y las responsabilidades adquiridas, además desarrollar prácticas en esta área.	

Logros o beneficios que se adquieren

- Responsabilidades claras y establecidas.
- Todo el personal de la empresa cuenta con la misma información, mejorando así la comunicación en ella.
- Reduce la posibilidad de comprometer un proceso critico al definir las funciones y responsabilidades.
- Garantiza que las funciones y responsabilidades se ejercen correctamente, para evaluar si todo el personal tiene autoridad y recursos suficientes, para ejecutar sus funciones y responsabilidades y, en general, para revisar el rendimiento.

6.1.1.2. APO01.06 Optimizar la ubicación de la función de TI.

Tabla 7. *Plan de acción de práctica de gestión: APO01.06*

Práctica de gestión: APO01.06 Optimizar la ubicación de la función de TI	
Situación actual	**Descripción de la práctica de COBIT 2019**
La organización tiene un solo colaborador de TI, él se encarga de actividades como: configuración de correos electrónicos, entrega y reparación de equipos, gestión de las	Posicionar las capacidades de TI en la estructura organizativa general para reflejar la importancia estratégica y la dependencia operativa de las TI dentro de la empresa. La línea jerárquica del CIO y la representación de las TI en la alta dirección

plataformas que usa la empresa, entre otras funciones. El jefe encargado del área es el gerente financiero.	deben ser proporcionales a la importancia de la I&T en la empresa.

Brecha

No se contemplan los siguientes requerimientos:

- El departamento de TI es un área en desarrollo por lo que aún no cuenta con una estructura y situación clara de TI.

Plan para ejecutar

Actividad según COBIT 2019	Acción	Documentación
1. Comprender el contexto para la ubicación de la función de TI, incluida la evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, híbrido), la importancia de la I&T y la situación y las opciones de contratación.	Se debe llevar a cabo un análisis sobre la situación actual de la organización para entender TI en ella. Por lo tanto, se recomienda plantearse los siguientes puntos: - Situación actual de TI. - Situación deseada de TI. - Evaluación interna y externa de la organización. Al realizarse el desarrollo del análisis externo hay que estudiar las tendencias, el mercado, a los clientes, a los agentes económicos. Esto cambia constantemente, hay que salir del día a día de nuestra empresa, estudiar el entorno, otros sectores, otros mercados, otros países… Hay que desarrollar la visión	Plantilla del análisis FODA, una opción para evaluar a la organización. El análisis FODA consiste en evaluar la situación de la empresa tanto a nivel interno como externo, a partir de sus fortalezas, y debilidades (interno) amenazas y oportunidades (externo). Ver anexo 8

	holística (la capacidad de ver no sólo la hoja, sino la rama, el árbol y el bosque completo). Hay que anticiparse para tener capacidad para reaccionar y tomar medidas. (Gorbe, 2007, p.19)	
2. Identificar, evaluar y priorizar opciones para la ubicación organizacional, el abastecimiento y los modelos operativos.	En el momento que se realiza el análisis de la organización, se requiere la identificación y evaluación de las prioridades para observar la ubicación organizativa y el abastecimiento y modelos organizativos.	No aplica
3. Definir la ubicación de la función informática y obtener el acuerdo.	A partir del análisis realizado, definir cuál es la función que posee la informática en la organización y además llegarla a consolidar o darle claridad, para que sea parte importante de la empresa.	No aplica

Logros o beneficios que se adquieren

- Darle valor al TI.
- Claridad en el TI, a partir de la definición de sus elementos.
- Dar a conocer la importancia estratégica y la dependencia operativa de las TI en la organización.

6.1.1.3. APO01.08 Definir las habilidades y competencias objetivo.

Tabla 8. *Plan de acción de práctica de gestión: APO01.08*

<table>
<tr><th colspan="3">Práctica de gestión: APO01.08 Definir las habilidades y competencias objetivo</th></tr>
<tr><th colspan="2">Situación actual</th><th>Descripción de la práctica de COBIT 2019</th></tr>
<tr><td colspan="2">La empresa realiza en menor medida revisiones de las habilidades y capacidades que tiene la fuerza laboral, además de lo que se requiere para cumplir con los objetivos.</td><td>Definir las aptitudes y competencias necesarias para alcanzar los objetivos de gestión pertinentes.</td></tr>
<tr><th colspan="3">Brecha</th></tr>
<tr><td colspan="3">No se contemplan los siguientes requerimientos:
No se plantea un análisis para conocer de la brecha que existe entre las habilidades y capacidades de los colaboradores con respecto a las competencias y aptitudes que se requiere para alcanzar los objetivos de la organización.</td></tr>
<tr><th colspan="3">Plan para ejecutar</th></tr>
<tr><th>Actividad según COBIT 2019</th><th>Acción</th><th>Documentación</th></tr>
<tr><td>1. Identificar las habilidades y competencias necesarias.</td><td>Aplicar herramientas que evalúen las competencias de los colaboradores con el fin de conocer las habilidades y destrezas que poseen.
Identificar y documentar las necesidades que requiere la organización, para cumplir con los objetivos de manera exitosa.</td><td>Las herramientas que se pueden utilizar para evaluar a los colaboradores son:
La rueda de las competencias de Paul J. Meyer. Esta dinámica permite que los empleados autoevalúen el nivel de las competencias Ver anexo 9.
Sistema de evaluación 360°. “Propicia el “cambio de observador”, se da la autopercepción</td></tr>
</table>

		de las competencias de éxito empresarial y la percepción de los demás (Colaboradores, jefes, clientes, entre otros)" (López, 2018). Ver anexo 10 Herramienta para identificar y documentar las necesidades de la organización: • Necesidades basadas en la pirámide Maslow. Permite determinar y priorizar las necesidades que tiene la empresa. Ver anexo 11
2. Analizar la brecha entre las habilidades y capacidades objetivo para la empresa y las habilidades actuales de la fuerza de trabajo.	A partir de la información recopilada anteriormente, se aplica un análisis de las para comparar las habilidades y capacidades que requieren los objetivos de la organización con respecto a la fuerza laboral.	(Consulte APO07-Recursos Humanos Gestionados para el desarrollo de habilidades y prácticas de gestión).
Logros o beneficios que se adquieren		
• Permite alcanzar los objetivos de gestión seleccionados. • Contar con personal calificado para cumplir los objetivos de la organización.		

- Permite conocer cuáles son las habilidades y competencias que poseen la fuerza laboral, además da paso a que estas se puedan mejorar en caso de contar con debilidades en una de ellas.

6.1.1.4. APO01.09 Definir y comunicar políticas y procedimientos.

Tabla 9. *Plan de acción de práctica de gestión: APO01.09*

Práctica de gestión: APO01.09 Definir y comunicar políticas y procedimientos		
Situación actual	**Descripción de la práctica de COBIT 2019**	
La información sensible no posee ningún tratamiento diferente a los documentos no confidenciales. Tiene definidas políticas de seguridad como firewalls, realizan actualizaciones de los equipos y configuraciones en la red. Por otra parte, la organización define políticas que pocas veces se cambian.	Establecer procedimientos para mantener el cumplimiento y la medición del rendimiento de las políticas y otros componentes del marco de control. Aplique las consecuencias del incumplimiento o de un rendimiento inadecuado. Realizar un seguimiento de las tendencias y los resultados y tenerlos en cuenta en el futuro diseño y mejora del marco de control.	
Brecha		
No se contemplan los siguientes requerimientos: • La información sensible debería de tener un tratamiento diferente de los documentos públicos. • No se mantienen informados de las tendencias que existen en el mercado con respecto a la seguridad y protección de la información.		
Plan para ejecutar		
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Crear un conjunto de políticas para impulsar las expectativas de control de TI sobre temas clave relevantes como la calidad, la seguridad,	Verificar si en la organización cuentan con las políticas necesarias para los siguientes temas: calidad, seguridad, privacidad, confidencialidad,	No aplica

la privacidad, la confidencialidad, los controles internos, el uso de activos de I&T, la ética y los derechos de propiedad intelectual (PI).	controles internos, usos de activos de I&T, ética y los derechos de propiedad intelectual. En caso de no contar con algunas políticas en los diversos temas se debe considerar realizar nuevas, para así evacuar en donde se requiere.	
2. Implantar y hacer cumplir las políticas de I&T de manera uniforme para todo el personal pertinente, de modo que se incorporen a las operaciones de la empresa y se conviertan en parte integrante.	Una vez que se revisen y actualicen las políticas que se tienen, se recomienda que estas sean comunicadas al personal de la organización, con el fin de que se les pueda dar el cumplimiento.	No aplica
3. Evaluar y actualizar las políticas al menos una vez al año para adaptarlas a los cambios del entorno operativo o empresarial.	Para evaluar la política sería necesario consultarles a los colaboradores la opinión o comentarios que tenga sobre ella, ya que es en la acción donde se evidencia su utilidad. Una vez que se recopile la información se puede dar un análisis y realizar ajustes en caso de que sea necesario.	No aplica
Logros o beneficios que se adquieren		
• Al evaluar las políticas que se tienen nos permite observar si se tiene todo lo necesario para los diferentes temas que se enfoca la organización.		

- Las políticas actualizadas permiten ir acorde a los cambios realizados en el entorno operativo empresarial, donde las decisiones tomadas puedan ser respaldas por las nuevas políticas, para así evitar diferenciación en lo que se tiene con lo que era antes.

6.1.2. APO10 Gestionar los proveedores

Según ISACA (2018) el APO10 consiste en "optimizar las capacidades disponibles de I&T para apoyar la estrategia y la hoja de ruta de I&T, minimizar el riesgo asociado con proveedores que no rinden o cumplen con los requisitos y asegurar precios competitivos" (p.34).

6.1.2.1. APO10.01 Identificar y evaluar las relaciones con los proveedores y los contratos.

Tabla 10. *Plan de acción de práctica de gestión: APO10.01*

Práctica de gestión: APO10.01 Identificar y evaluar las relaciones con los proveedores y los contratos.	
Situación actual	**Descripción de la práctica de COBIT 2019**
Los socios y proveedores se encuentran definidos en la organización, con menos frecuencia se les aplica mediciones de desempeño.	Buscar e identificar continuamente proveedores y clasificarlos por tipo, importancia y criticidad. Establecer criterios para evaluar proveedores y contratos. Revisar la cartera global de proveedores y contratos existentes y alternativos.
Brecha	
No se contemplan los siguientes requerimientos: • Hay poca documentación de los proveedores o contratos. • Se aplican en menor medida evaluaciones a los proveedores y contratos. • Hay poca clasificación de los proveedores, es decir, no cuenta con un nivel de importancia o prioridad.	
Plan para ejecutar	
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Establecer y mantener criterios relativos al tipo, la importancia y la criticidad de	Algunas preguntas que se recomienda realizar para	No aplica

los proveedores y los contratos con proveedores, que permitan centrarse en los proveedores preferidos e importantes.	responder a los criterios son las siguientes: - ¿Impacto en el servicio de sus operaciones diarias? - ¿Cuánto influye en las actividades de la organización? - ¿Qué problemas se pueden presentar si surge un imprevisto y no se cuenta con ellos?	
2. Identificar, registrar y categorizar a los proveedores y contratos existentes según criterios definidos, para mantener un registro detallado de los proveedores preferentes que deben gestionarse con cuidado.	A partir de los criterios que se han definido clasificar a los proveedores a partir del valor que se le quiera dar.	No aplica
3. Establecer y mantener los criterios de evaluación de proveedores y contratos para permitir la revisión general y la comparación del rendimiento de los proveedores de forma coherente.	Definir los criterios de evaluación, se recomienda considerar los siguientes: - Perfil general del proveedor. - Precio. - Capacidad técnica. - Tecnología e infraestructura. - Acuerdo de nivel de servicio (SLA).	Se recomienda consultar sobre el acuerdo de nivel de servicio (SLA) en el anexo 12.
4. Evaluar y comparar periódicamente el rendimiento de los proveedores actuales y alternativos para identificar	Para evaluar y comparar a los proveedores se recomienda desarrollar un formulario con parámetros de competencia, capacidad, consistencia, calidad,	Se recomienda utilizar el modelo de Carter 10 C's, el cual analiza los aspectos de

oportunidades o una necesidad imperiosa de reconsiderar los contratos actuales con proveedores.	eficiencia, responsabilidad, entre otros.	evaluación de los proveedores antes de ser nombrados.
Logros o beneficios que se adquieren		
• Las evaluaciones periódicas ayudan a mantener el servicio o producto que ofrecen los proveedores eficientes y confiables a largo plazo, además se pueden identificar áreas de mejoras problemas que se estén presentado. • Al tener criterios tanto de evaluación como los relativos permite que se dé claridad en los proveedores que busca la empresa, por ello se toman mejores decisiones sobre estos.		

6.1.3. APO13 Gestionar la seguridad

Según ISACA (2018) el APO13 consiste en "mantener el impacto y la existencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa" (p.34).

6.1.3.1. APO13.02 Definir y gestionar un plan de tratamiento de los riesgos para la seguridad de la información.

Tabla 11. *Plan de acción de práctica de gestión: APO13.02*

Práctica de gestión: APO13.02 Definir y gestionar un plan de tratamiento de los riesgos para la seguridad de la información	
Situación actual	**Descripción de la práctica de COBIT 2019**
La organización cuenta con un plan de tratamiento de riesgos de seguridad de la información. Dicho plan se encuentra alineado con el objetivo estratégico y la arquitectura de la empresa.	Mantener un plan de seguridad de la información que describa cómo gestionar el riesgo de seguridad de la información y alinearlo con la estrategia y la arquitectura de la empresa. Garantizar que las recomendaciones para implantar mejoras de seguridad se basen en casos empresariales aprobados, se apliquen como parte integrante del desarrollo de servicios y soluciones, y funcionen como parte integrante del funcionamiento empresarial.
Brecha	
No se contemplan los siguientes requerimientos:	

<table>
<tr><td colspan="3">

- Los colaboradores están poco capacitados y concientizados en temas de seguridad y privacidad de la organización.
- El plan no cuenta con los componentes necesarios cuando se lleva a cabo, ya que no están elementos como prácticas de gestión, soluciones de seguridad adecuadas y óptimas.
- Carecen de un inventario de componentes de la solución que se va a implementar para administrar el riesgo.

</td></tr>
<tr><th colspan="3">Plan para ejecutar</th></tr>
<tr><th>Actividad según COBIT 2019</th><th>Acción</th><th>Documentación</th></tr>
<tr><td>1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con el objetivo estratégico y la arquitectura empresarial. Garantizar que el plan identifique las prácticas de gestión y soluciones de seguridad adecuadas y óptimas, con los recursos, responsabilidades y prioridades asociados para gestionar el riesgo de seguridad de la información identificado.</td><td>Validar el plan de tratamiento de riesgos que poseen, con respecto al que se proporciona, para verificar si cuenta con los elementos que se requieren como prácticas de gestión y soluciones de seguridad, recursos y responsabilidades y prioridades de cada riesgo. En caso de ser necesario llevar a cabo una actualización.
Además, se aconseja que se desarrollen propuestas del plan de tratamiento que se encuentre respaldado de casos empresariales para llevarlo a su ejecución.</td><td>Plantilla de tratamiento de riesgos.
Ver anexo 13</td></tr>
<tr><td>2. Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución que existen para</td><td>Llevar a cabo la documentación de las soluciones que se aplican a sus respectivos riesgos.</td><td>No aplica</td></tr>
</table>

gestionar los riesgos relacionados con la seguridad.		
3. Implantar programas de formación y concienciación sobre seguridad de la información y privacidad.	Incentivar e involucrar a los colaboradores de la organización a conocer y reforzar los temas de seguridad de la información y la privacidad.	Existen diversas plataformas que permiten de forma gratuita conocer acerca de la seguridad entre ellas están: - Edutin, una plataforma que permite llevar los cursos sin pagar, solo se realiza el pago si se quiere obtener un certificado. - Cursa plataforma que tiene diferentes temas referentes a la seguridad de la información. - Edx, una plataforma que brinda cursos online, gratuitos.
4. Integrar la planificación, el diseño, la aplicación y la supervisión de los procedimientos de seguridad de la información y privacidad y	Desarrollar procedimientos de seguridad que involucre las siguientes etapas planificación, diseño, aplicación y supervisión.	No aplica

otros controles capaces de permitir la prevención rápida, la detección de eventos de seguridad y la respuesta a incidentes de seguridad.		

Logros o beneficios que se adquieren
• Al concientizar a los colaboradores en temas de seguridad va a permitir que se proteja la organización de uno de los tipos de hackeo que existe como lo es la ingeniería social, además se tiene un personal más precavido y alerta de los diferentes mecanismos que utilizan los hackers para robar información. • Contar con un plan de riesgo o un plan de tratamiento, va a permitir saber cómo actuar al materializarse la situación, ya no habría una improvisación de parte de la organización, sino un conocimiento de cómo solucionar ante diferentes situaciones.

6.1.3.2. APO13.03 Supervisar y revisar el sistema de gestión de la seguridad de la información (SGSI).

Tabla 12. *Plan de acción de práctica de gestión: APO13.03*

Práctica de gestión: APO13.03 Supervisar y revisar el sistema de gestión de la seguridad de la información (SGSI).	
Situación actual	**Descripción de la práctica de COBIT 2019**
Se da la revisión del Sistema de Gestión de Seguridad de la Información (SGSI). Se aplican auditorías del sistema de forma planificada, además se les da mantenimiento a los planes de seguridad.	Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de la información. Recopilar y analizar datos sobre el sistema de gestión de la seguridad de la información (SGSI) y mejorar su eficacia. Corregir las no conformidades para evitar que se repitan.
Brecha	
No se contemplan los siguientes requerimientos: • La revisión del Sistema de Gestión de Seguridad es poco frecuente.	
Plan para ejecutar	
Actividad según COBIT 2019	**Acción**	**Documentación**

1. Realizar revisiones periódicas de la eficacia del SGSI. Incluyen el cumplimiento de la política y los objetivos del SGSI y la revisión de las prácticas de seguridad y privacidad.	Realizar revisiones al SGSI periódicamente por las personas a cargo, además por parte de la dirección. La ISO 27001 (s.f) recomienda que sean en intervalos de tiempo planificados, con mayor frecuencia, al menos un año. Aunque el tiempo puede variar dependiendo de las necesidades de la organización y lo que indique la dirección.	No aplica
2. Realizar auditorías del SGSI a intervalos planificados.	Realizar auditorías en intervalos de tiempo, se recomienda una vez al año, aunque puede variar de acuerdo con las necesidades de la organización.	No aplica
3. Registrar las acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI.	Llevar documentación en hojas de cálculo o procesadores de texto de las acciones y eventos generados por el SGSI que sea de impacto para la eficacia o el rendimiento.	No aplica
4. Contribuir al mantenimiento de los planes de seguridad para tener en cuenta las conclusiones de las actividades de supervisión y revisión.	Realizar mantenimientos planificados a los planes de seguridad una vez al año o cuando la empresa lo considere necesario.	No aplica

	Los roles que participan en este mantenimiento son: propietarios de los procesos de negocio, oficina de gestión de proyectos, director (a) de tecnología, oficial de privacidad, gerente de continuidad de negocio, gerente de la seguridad de la información, supervisor, jefe de administración de TI, jefe de operaciones de TI, desarrollo, arquitecto, director de información.	
Logros o beneficios que se adquieren		
• A partir de las revisiones mejora la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI). • El sistema puede estar libre de errores, a partir de las modificaciones realizadas. • Garantiza que su alcance siga siendo adecuado y se identifican mejoras en el proceso del SGSI.		

6.2. **Entregar, Dar servicio y Soporte**

6.2.1. DSS02 Gestionar las peticiones y los incidentes del servicio.

Según ISACA (2018) el DSS02 consiste en lo siguiente:

> Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidentes de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes. (p.35)

6.2.1.1. DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.

Tabla 13. *Plan de acción de práctica de gestión: DSS02.01*

Práctica de gestión: DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio		
Situación actual	**Descripción de la práctica de COBIT 2019**	
La organización cuenta con formalización de los esquemas de solicitudes de servicios e incidentes. Tienen algunas reglas y procedimientos de incidentes.	Definir esquemas y modelos de clasificación de incidentes y solicitudes de servicio.	
Brecha		
No se contemplan los siguientes requerimientos: • Falta de modelos de incidentes basados en errores conocidos. • No cuentan con una documentación para los incidentes y las solicitudes. • Las reglas y procedimientos de escalamiento no se encuentran bien definidos y comunicados en la organización.		
Plan para ejecutar		
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Definir esquemas de clasificación y priorización de incidentes y solicitudes de servicio, así como criterios para el registro de problemas.	Se recomienda utilizar la guía del marco ITIL para desarrollar esquemas de clasificación y priorización de incidentes y solicitudes de servicio.	Para conocer más acerca de la guía de ITIL se recomienda ver el anexo 14
2. Definir modelos de incidencias para errores conocidos que permitan una resolución eficiente y eficaz.	Al desarrollar los modelos de incidencias, según Servicetonic (s.f), utilizando ITIL, se debe incluir los siguientes elementos: - Los pasos para seguir para la resolución de las	No aplica

	incidencias en orden cronológico. - Responsabilidades. - Plazos para la realización de las actividades. - Procedimientos escalados: quién debería ser contactado y cuándo.	
3. Definir modelos de solicitud de servicio según el tipo de solicitud de servicio para permitir la autoayuda y un servicio eficiente para las solicitudes estándar.	A partir de la solicitud del servicio que ya se ha realizado anteriormente, se utiliza de base para sacar los demás modelos, según el tipo de solicitud de servicio que ingresa los cuales son: - *Hardware* - *Software* - Acceso a sistemas	No aplica
4. Definir normas y procedimientos de escalada de incidentes, especialmente para incidentes graves e incidentes de seguridad.	Cuando se habla de la escalada de los incidentes se refiere cuando el colaborador no logra resolver el incidente, este debe pasarse a otra persona con más conocimiento para que lo logre resolver, en estos casos se deben definir ciertos procedimientos o normas para llevarlo a cabo como los siguientes:	No aplica

	- Definir el tipo de escalonamiento (jerárquico, funcional).	

Logros o beneficios que se adquieren
• Contar con una fuente de conocimiento de los incidentes y las solicitudes, va a permitir resolver de manera rápida el error en caso de que se presente el mismo, además son de apoyo para solucionar otro tipo de situaciones. También, permite ver el rendimiento y la cantidad de solicitudes que se han atendido. • Definir cómo proceder ante incidentes y solicitudes de los usuarios permite tener un orden y un control sobre la situación. • Garantiza enfoques coherentes a la hora de gestionar e informar a los usuarios sobre los problemas y realizar análisis de tendencias.

6.2.1.2. DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.

Tabla 14. *Plan de acción de práctica de gestión: DSS02.02*

Práctica de gestión: DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes	
Situación actual	**Descripción de la práctica de COBIT 2019**
La organización atiende peticiones e incidentes cuando estos suceden.	Identificar, registrar y clasificar las solicitudes de servicio y los incidentes y asignarles una prioridad en función de la criticidad de la empresa y de los acuerdos de servicio.
Brecha	
No se contemplan los siguientes requerimientos: • Se tiene poco conocimiento del SLA (Acuerdo de nivel de servicio).	
Plan para ejecutar	
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Registrar todas las solicitudes de servicio y los incidentes, anotando toda la información pertinente, para poder gestionarlos con eficacia y	Toda solicitud debe registrarse.	Consulte el DSS02.01 para conocer el esquema de solicitud. Plantilla de solicitud de servicio

mantener un registro histórico completo.		Ver anexo 14
2. Para permitir el análisis de tendencias, clasificar las solicitudes de servicio y los incidentes identificando el tipo y la categoría.	Cada vez que se realiza una solicitud de servicios, se debe considerar llenar dos elementos claves que permitirán generar un reporte, el primero el tipo de solicitud que requiere y además la categoría.	No aplica
3. Priorizar las solicitudes de servicio y los incidentes basándose en la definición del servicio SLA de impacto y urgencia para la empresa.	Al realizarse las solicitudes de servicio, se debe definir la priorización de acuerdo con el impacto y la urgencia, pero estos deben agregarse a partir de los Acuerdos de nivel de servicio (SLA).	No aplica
Logros o beneficios que se adquieren		
• Permite el análisis de tendencias al llevar a cabo una solicitud de servicio. • Se lleva un orden y control de las solicitudes de servicio. • Al escoger las solicitudes que se deben trabajar, se harán por prioridad, dando importancia a las de mayor urgencia.		

6.2.1.3. DSS02.06 Cerrar las peticiones de servicio y los incidentes.

Tabla 15. *Plan de acción de práctica de gestión: DSS02.06*

<table>
<tr><th colspan="3">Práctica de gestión: DSS02.06 Cerrar las peticiones de servicio y los incidentes</th></tr>
<tr><th>Situación actual</th><th colspan="2">Descripción de la práctica de COBIT 2019</th></tr>
<tr><td>Las solicitudes que se atienden y finalizan no son revisadas en conjunto con el usuario.</td><td colspan="2">Verificar la resolución satisfactoria de las incidencias y/o el cumplimiento de las solicitudes, y cerrarlas.</td></tr>
<tr><th colspan="3">Brecha</th></tr>
<tr><td colspan="3">No se contemplan los siguientes requerimientos:
Se desconoce la satisfacción con los clientes con respecto a las solicitudes atendidas.</td></tr>
<tr><th colspan="3">Plan para ejecutar</th></tr>
<tr><th>Actividad según COBIT 2019</th><th>Acción</th><th>Documentación</th></tr>
<tr><td>1. Verificar con los usuarios afectados que la solicitud de servicio se ha atendido satisfactoriamente o que la incidencia se ha resuelto satisfactoriamente, en un plazo acordado/aceptable.</td><td>Establecer como parte de la etapa de cierre de la solicitud, que el encargado de brindar soporte contacte al usuario para validar la adecuada resolución, de lo contrario la solicitud no puede darse por finalizada</td><td>No aplica</td></tr>
<tr><th colspan="3">Logros o beneficios que se adquieren</th></tr>
<tr><td colspan="3">Permite conocer la disconformidad que puede tener el cliente con el servicio brindado.
La evacuación de las dudas se puede dar en el mismo momento que se presente algún inconveniente al revisar la funcionalidad.
La aprobación y el cierre de la solicitud se da en el mismo momento que la revisión, siempre y cuando sea correcta la solución.</td></tr>
</table>

6.2.2. DSS04 Gestionar la continuidad

Según ISACA (2018) el DSS04 consiste en “adaptarse rápidamente, continuar 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 (como amenazas, oportunidades, demandas)" (p.35).

6.2.2.1. DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance.

Tabla 16.*Plan de acción de práctica de gestión: DSS04.01*

Práctica de gestión: DSS04.01 Definir la política, los objetivos y el alcance de la continuidad de la actividad		
Situación actual	**Descripción de la práctica de COBIT 2019**	
La organización ha analizado poco los procesos empresariales de apoyo esenciales y los servicios de I&T relacionados.	Definir la política y el alcance de la continuidad de las actividades, en consonancia con los objetivos de la empresa y de las partes interesadas, para mejorar la resistencia de la empresa.	
Brecha		
No se contemplan los siguientes requerimientos: • No se tiene un análisis profundo de los procesos internos y subcontratados críticos para las operaciones de la empresa. • Presentan poco análisis sobre los procesos de apoyo y los servicios que se encuentran relacionados al I&T.		
Plan para ejecutar		
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Identificar los procesos de negocio internos y externalizados y las actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir las obligaciones legales y/o contractuales.	Para identificar los procesos y actividades críticas de un negocio se deben seguir los siguientes pasos: - Identificar los procesos actuales. Se debe considerar que las organizaciones cuentan con 3 grandes procesos: Estratégico, operativo y soporte. Se puede hacer el análisis a partir de ellos.	No aplica

	- Determinar la importancia que tiene el proceso para la organización. - A partir de lo anterior se puede identificar los procesos clave.	
2. Determinar las partes interesadas clave y las funciones y responsabilidades para definir y acordar la política de continuidad y su alcance.	Para determinar las partes interesadas se requiere de un personal especifico, ellos son la dirección y los líderes de procesos. Luego se debe conocer cuáles son, para ello se pueden hacer las siguientes preguntas: - ¿Se tienen partes interesadas en los contextos político, económico, social, tecnológico, ambiental y legal? - ¿Se tiene personas que proporcionan recursos, materias primas, servicios, entre otros? - ¿Cuál es la naturaleza de la organización, para ello se conocer el tipo de negocio, los recursos, servicios y soluciones que ofrece entre otros? Una vez que se tenga los proveedores estos se clasifican	Plantilla de partes interesadas matriz. Ver anexo 15

	por prioridad e importancia. Para ello se realizan las siguientes preguntas: - ¿Cuánto impacto genera al negocio si no continua con el contrato? - ¿Deja afectaciones en los procesos en caso de no contribuir con la organización? - Si se retira de la organización, ¿esta puede verse sumergida en el fracaso? Al tener esta información se procede a plasmas este análisis en una matriz de partes interesadas.	
3. Identificar los procesos empresariales de apoyo esenciales y los servicios de I&T relacionados.	Para esta actividad se debe retomar el ejercicio anterior considerando los procesos que aprovisionan recursos a otros procesos. También a partir de ahí identificar los procesos relacionado a I&T.	No aplica
Logros o beneficios que se adquieren		
• Le permite tomar decisiones informadas. • Proporciona conocimiento sobre los procesos críticos de la organización. • Reduce errores y mejora la eficiencia. • Permite la calidad del producto o servicio. • Satisfacción de los clientes.		

6.2.2.2. DSS04.02 Mantener la resiliencia del negocio.

Tabla 17. *Plan de acción de práctica de gestión: DSS04.02*

Práctica de gestión: DSS04.02 Mantener la resiliencia del negocio.		
Situación actual	**Descripción de la práctica de COBIT 2019**	
Se ha evaluado poco las situaciones que se pueden presentar de forma inesperada, por lo que no se tiene claridad si se encuentran preparado para una recuperación adecuada o de inmediata.	Evalúe las opciones de resistencia de la empresa y elija una estrategia rentable y viable que garantice la continuidad de la empresa, la recuperación en caso de catástrofe y la respuesta ante incidentes ante una catástrofe u otro incidente o interrupción importante.	
Brecha		
No se contemplan los siguientes requerimientos: • Se desconoce la capacidad de la organización para eventualidades, por lo que no se sabe la resistencia que puede tener, ni la garantía de la continuidad de negocio ante cualquier situación.		
Plan para ejecutar		
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Identificar los escenarios potenciales susceptibles de dar lugar a sucesos que podrían causar incidentes perturbadores significativos.	Analizar los procesos que conforman las actividades de la organización, a partir de ello, plantear escenarios que podrían causar situaciones no deseadas o que presenten interrupciones el trabajo.	No aplica
2. Llevar a cabo un análisis del impacto en el negocio para evaluar el impacto a lo largo del tiempo de una interrupción en las funciones críticas del negocio y el efecto que	Para llevar a cabo un análisis de impacto del negocio se deben documentar los siguientes pasos: - Identificar las áreas críticas del negocio.	No aplica

una interrupción tendría sobre ellas.	- Conocer las consecuencias que puede tener el área financiera o la operacional si se da la interrupción de un proceso crítico. - Establecer recursos necesarios y tiempo de recuperación.	
3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y la I&T de apoyo, basándose en una duración aceptable de la interrupción del negocio y la interrupción máxima tolerable.	Para establecer el tiempo mínimo necesario para recuperar un proceso se recomienda que se realice por proceso, además se debe considerar la criticidad de cada uno de ellos para sacar así la interrupción aceptable del negocio y la tolerable máxima.	No aplica
4. Determinar las condiciones y los propietarios de las decisiones clave que harán que se invoquen los planes de continuidad.	Decidir los escenarios y quienes pueden proceder con la activación de los planes de continuidad.	No aplica
5. Evaluar la probabilidad de las amenazas que podrían causar la pérdida de continuidad de la actividad. Identificar medidas que reduzcan la probabilidad y el impacto mediante una mejor prevención y una mayor resistencia.	Se recomienda llevar un análisis de las amenazas que se pueden presentar en el negocio, una vez que se tienen, asignar la probabilidad de pérdida de continuidad, además, crear medidas para disminuir la probabilidad asignada, con	No aplica

	el fin de prevenir que se materialice la situación.	
6. Analizar los requisitos de continuidad para identificar posibles opciones estratégicas empresariales y técnicas.	Primeramente, se debe tener definido los requisitos de continuidad, para proceder con su análisis y así identificar las diferentes posibilidades de las opciones estratégicas empresariales y técnicas.	No aplica
7. Determinar las necesidades de recursos y los costes de cada opción técnica estratégica y formular recomendaciones estratégicas.	Se requiere tener los recursos y los costes de las posibles estrategias, además, desarrollar recomendaciones estratégicas.	No aplica
8. Obtener la aprobación empresarial ejecutiva para las opciones estratégicas seleccionadas.	Las posibles estrategias seleccionadas requieren de la aceptación del personal ejecutivo de la organización, por lo cual es necesario que una vez que se desarrollen se presente ante ellos para que todos tengan el conocimiento sobre lo realizado.	No aplica
Logros o beneficios que se adquieren		
• Conocer acerca de la resiliencia con la que cuenta la organización para sobreponerse ante alguna eventualidad permite mejorar los planes y las acciones que se deben tomar para seguir con los procesos sin ningún problema.		

6.2.2.3. DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.

Tabla 18. *Plan de acción de práctica de gestión: DSS04.03*

Práctica de gestión: DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.		
Situación actual	**Descripción de la práctica de COBIT 2019**	
La organización cuenta con un plan de recuperación de desastres poco desarrollado.	Desarrollar un plan de continuidad de las actividades (PCN) y un plan de recuperación en caso de catástrofe (PRC) basados en la estrategia. Documentar todos los procedimientos necesarios para que la empresa continúe con las actividades críticas en caso de incidente.	
Brecha		
No se contemplan los siguientes requerimientos: • El plan de recuperación de desastres se encuentra poco desarrollado.		
Plan para ejecutar		
Actividad según COBIT 2019	**Acción**	**Documentación**
1. Definir las acciones de respuesta a incidentes y las comunicaciones que se llevarán a cabo en caso de interrupción. Definir las funciones y responsabilidades relacionadas, incluida la responsabilidad de la política y su aplicación.	Es necesario que se definan medios de comunicación y acciones para responder a los incidentes que ocasionen interrupciones a la organización. Además, deben tener funciones y responsabilidades de política y la forma en la que se va a aplicar.	No aplica
2. Garantizar que los principales proveedores y socios externos disponen de planes de continuidad eficaces. Obtener las	Los proveedores y socios externos que trabajen con la organización deben contar con planes de continuidad que actúen en situaciones de riesgo, es por ello, la	No aplica

pruebas auditadas necesarias.	necesidad de consultar con ellos para conocer sobre estos planes, además de aplicar pruebas auditadas si se consideran necesarias.	
3. Definir las condiciones y procedimientos de recuperación que permitan reanudar el procesamiento de la actividad. Incluir la actualización y conciliación de las bases de datos de información para preservar la integridad de la información.	Para reanudar el procesamiento de una actividad se requiere determinar las condiciones y los procedimientos de recuperación, además, la actualización y conciliación de la base de datos con el fin de cuidar el aspecto de integridad de la información.	No aplica
4. Desarrollar y mantener plan de continuidad (BCP) y plan de recuperación de desastres (DRP) operativos que contengan los procedimientos por seguir para permitir la operación continua de procesos comerciales críticos y/o arreglos de procedimiento temporal. Incluya enlaces a los planes de los proveedores de servicios subcontratados.	Se recomienda contar con planes de continuidad y planes de recuperación de desastres, ellos deben contener procedimientos para operar de manera continua los procesos comerciales críticos o reparaciones de procedimiento que se presentan temporalmente. También se debe contar con la documentación de los planes que ofrecen las subcontrataciones y proveedores.	No aplica
5. Definir y documentar los recursos necesarios para respaldar los	Antes de respaldar los procedimientos de continuidad y recuperación se debe determinar y	No aplica

procedimientos de continuidad y recuperación, teniendo en cuenta el personal, las instalaciones y la infraestructura informática.	llevar un registro de los recursos que se necesitan, para ello se debe considerar el recurso humano, las instalaciones y la infraestructura informática.	
6. Defina y documente los requisitos de copia de seguridad de la información necesarios para respaldar los planes. Incluya planos y documentos en papel, así como archivos de datos. Considere la necesidad de seguridad y de almacenamiento externo.	Los planes de continuidad deben ser respaldados con copias de seguridad, para realizar estas copias se debe definir y documentar los requisitos que las rigen. Estos respaldos pueden presentar cono archivos de datos, así como guardarse en almacenamiento externo.	No aplica
7. Determinar las competencias necesarias de las personas que participan en la ejecución del plan y los procedimientos.	Para llevar a cabo la ejecución de plan y los procedimientos se recomienda que se conozca las habilidades y competencias de los colaboradores que va a participar.	No aplica
8. Distribuir los planes y la documentación de apoyo de forma segura a las partes interesadas debidamente autorizadas. Asegurarse de que los planes y la documentación	Solo las personas autorizadas deben tener acceso a la documentación y los planes realizados. Además, una vez que se tienen se deben llevar a su ejecución cuando se presenten situaciones catastróficas, por lo	No aplica

sean accesibles en todas las situaciones de catástrofe.	tanto, es necesario que estén a la mano para su utilización.	

Logros o beneficios que se adquieren

- Al presentarse alguna eventualidad inesperada, se puede seguir operando, ya que no se ven afectadas las actividades.
- Si se presenta alguna situación, no se realiza una improvisación si no se tiene conocimiento de qué forma se debe proseguir.

6.2.3. DSS05 Gestionar los servicios de seguridad

Según ISACA (2018) el DSS05 consiste en "Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información" (p.35).

6.2.3.1. DSS05.02 Gestionar la seguridad de la conectividad y de la red.

Tabla 19. *Plan de acción de práctica de gestión: DSS05.02*

Práctica de gestión: DSS05.02 Gestionar la seguridad de la conectividad y de la red	
Situación actual	**Descripción de la práctica de COBIT 2019**
La organización utiliza mecanismos de filtrado como el firewall para la detención de intrusos. Además, posee configuraciones de seguridad en el equipo de red y un control del tráfico entrante y saliente.	Utilice medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los métodos de conectividad.

Brecha

No se contemplan los siguientes requerimientos:

- El acceso a la red de la organización no es restringido, cualquier persona puede ingresar.
- Se aplican pocos protocolos y políticas de seguridad en las conexiones de red.
- No llevan a cabo algún tipo de prueba para comprobar la protección de red y de los sistemas.

Plan para ejecutar

Actividad según COBIT 2019	**Acción**	**Documentación**

1. Permitir que sólo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa. Configurar estos dispositivos para forzar la entrada de contraseñas.	- Solicitar en los dispositivos nuevos la contraseña para conectarse a la red. - En caso de tener carpetas compartidas en la red, que estas cuenten con un mecanismo de acceso al ingresar, para evitar que otras personas accedan.	No aplica
2. Aplicar protocolos de seguridad aprobados a la conectividad de red.	Verificar e implementar protocolos de seguridad a la conectividad de red. Algunos de ellos son: - TCP/IP - HTTP - FTP - SSH - DNS	No aplica
3. Cifrar la información en tránsito según su clasificación.	Se debe considerar el cifrado de la información cuando esta sea sensible, para que al transitar no sea visible en la red.	No aplica
4. Basándose en las evaluaciones de riesgos y los requisitos de la empresa, establezca y mantenga una política de seguridad de la conectividad.	Para desarrollar una política de seguridad se deben contemplar según González (2002) las siguientes recomendaciones: - La política de seguridad debe proteger tres puntos: • La información contenida en los sistemas informáticos. Se debe preservar la	No aplica

	confidencialidad, la integridad y la disponibilidad. • Los recursos de los sistemas de informáticos. • La reputación de cada usuario, del grupo de trabajo, departamento y de la organización completa. - La política de seguridad de una organización debe responder a lo siguiente: • ¿Por qué se establece la protección? • ¿Cuál es el verdadero valor y coste de esta? • ¿Quién es el responsable y de qué autoridad dispone el responsable? - Características que tiene la política de seguridad • Debe ser sencilla, precisa y fácil de entender para la empresa. • Los colaboradores de la organización deben participar en su diseño. • La persona responsable debe disponer también de autoridad para aplicarla.	

	• La política implementada debe proteger la propiedad, reputación y actividad de la organización. • No solo debe cuidar la información de la organización si no también al recurso humano. • Al atender la política desarrollada se resolverán las amenazas y los conflictos.	
5. Realizar pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.	Se recomienda que las pruebas se realicen cada seis meses o cuando se lleven a cabo modificaciones en la red.	No aplica
6. Realizar pruebas periódicas de la seguridad del sistema para determinar la idoneidad de la protección del sistema.	Se recomienda que las pruebas se realicen cada seis meses, pero va a depender de las actualizaciones que sufren los sistemas, porque si se han hecho reciente modificaciones, es recomendado que se haga después de esa actualización.	No aplica
Logros o beneficios que se adquieren		
• Al contar con mecanismos de confianza, permite apoyar la transmisión y recepción de información de forma segura. • Al definir políticas de seguridad tanto de red como en los sistemas, permite mantener a la organización segura y protegida, fuera de peligros.		

• Al realizar periódicamente pruebas a los sistemas y a la red va a permitir tener una apropiada protección de estas, además se pueden encontrar vulnerabilidades y corregirlas.

6.2.3.2. DSS05.03 Gestionar la seguridad de endpoint.

Tabla 20. *Plan de acción de práctica de gestión: DSS05.03*

Práctica de gestión: DSS05.03 Gestionar la seguridad de endpoint		
Situación actual	**Descripción de la práctica de COBIT 2019**	
La organización cuenta con un control de los sitios web maliciosos, así como el correo electrónico. Los dispositivos tienen mecanismos de bloqueos. Además, cuenta con configuraciones de red de forma segura y controlan los accesos y el control remoto.	Garantizar que los puntos finales (por ejemplo, portátiles, ordenadores de sobremesa, servidores y otros dispositivos o programas móviles y de red) estén protegidos a un nivel igual o superior a los requisitos de seguridad y privacidad definidos para la información procesada, almacenada o transmitida.	
Brecha		
No se contemplan los siguientes requerimientos: • Poseen poco filtrado de tráfico de red en dispositivos de punto final. • Los endpoint no son desechados de manera segura. • La información sensible no presenta ningún tipo de procedimiento diferente.		
Plan de acción		
Actividad según COBIT 2019	**Acción**	**Documentación**

1. Implantar el filtrado del tráfico de red en los dispositivos *endpoint*.	No permitir las descargas de programas no autorizados. Impedir el acceso a páginas que no se relacionen con la actividad laboral de la organización. Contar con antivirus que permita la detección de intrusos o documentos infectados. Contar con una VPN para conectarse a la organización.	No aplica
2. Deshágase de los dispositivos endpoint de forma segura.	Los dispositivos que no se estén utilizando, como servidores, celulares, portátiles, deben retirarse o bloquearles en acceso a los sistemas, para que no vaya a utilizarse o ingresar por personas que no deban.	No aplica
3. Cifrar la información almacenada en función de su clasificación.	De acuerdo con la clasificación de información (confidencial o pública), se debería de cifrar cuando esta hacer referencia a la confidencialidad con el fin de protegerla.	No aplica
Logros o beneficios que se adquieren		
• Proporciona seguridad a la organización. • La información solo es accedida por personas con permisos. • Dispositivos protegidos.		

6.2.3.3. DSS05.04 Gestionar la identidad de los usuarios y el acceso lógico.

Tabla 21. *Plan de acción de práctica de gestión: DSS05.04*

<table>
<tr><th colspan="3">Práctica de gestión: DSS05.04 Gestionar la identidad de los usuarios y el acceso lógico.</th></tr>
<tr><th>Situación actual</th><th colspan="2">Descripción de la práctica de COBIT 2019</th></tr>
<tr><td>Procuran gestionar, reducir y supervisar las cuentas de los usuarios con privilegios. Pero omiten las revisiones periódicas, siendo que algunos usuarios dejan de laborar en la institución y las cuentas siguen estando activas y con accesos.
La empresa cuenta con la correcta autenticación de los usuarios cuando lo considera necesario.</td><td colspan="2">Garantizar que todos los usuarios tengan derechos de acceso a la información de acuerdo con la política de privacidad de la unidad de negocio y los requisitos empresariales. Coordinarse con las unidades de negocio que gestionan sus propios derechos de acceso dentro de los procesos empresariales.</td></tr>
<tr><th colspan="3">Brecha</th></tr>
<tr><td colspan="3">No se contemplan los siguientes requerimientos:
Se llevan a cabo pocas revisiones periódicas de las cuentas y los privilegios que tienen los colaboradores.
No se revisan los accesos de los colaboradores.
No se lleva una documentación de los accesos o cambios de los colaboradores de la organización.</td></tr>
<tr><th colspan="3">Plan para ejecutar</th></tr>
<tr><th>Actividad según COBIT 2019</th><th>Acción</th><th>Documentación</th></tr>
<tr><td>1. Mantener los derechos de acceso de los usuarios de acuerdo con la función empresarial, los requisitos de los procesos y las políticas de seguridad. Adaptar la gestión de identidades y derechos de acceso a las funciones y responsabilidades definidas, basándose en los principios de</td><td>Consultar e identificar los accesos que poseen los colaboradores en este momento para verificar que cada uno cuente con las funciones, los requisitos de los procesos y las políticas de seguridad correspondiente.
Además, se debe cerciorar de que los usuarios solo cuenten</td><td>No aplica</td></tr>
</table>

mínimo privilegio, necesidad de tener y necesidad de conocer.	con los privilegios necesarios para las actividades, es decir, asignar los accesos a partir de las funciones que se desempeña, además de la información a la que tienen que acceder para evitar la exposición de documentos a personas que no lo requieren.	
2. Administrar todos los cambios en los derechos de acceso (creación, modificaciones y supresiones) de manera oportuna basándose únicamente en transacciones aprobadas y documentadas autorizadas por las personas de gestión designadas.	Se recomienda llevar una documentación o bitácora con información sobre los cambios que se le ha hecho a los accesos de los colaboradores. Anotar el nombre, el tipo de acceso, el tiempo de asignación, el motivo, cuando se solicita y la firma del responsable, esto por un tema de aceptación y otorgación del permiso.	No aplica
3. Segregar, reducir al mínimo necesario y gestionar activamente las cuentas de usuarios privilegiados. Garantizar la supervisión de toda la actividad de estas cuentas.	Respecto a las cuentas con privilegios, se recomienda que sus actividades sean supervisadas, además que su desarrollo sea mínimo, con el fin de tener un control de la existencia de ellas. Cabe mencionar que es necesario que solo los usen los usuarios que requieran accesos superiores y	No aplica

	de diversas partes de los sistemas.	
4. Identificar de forma única todas las actividades de procesamiento de la información por roles funcionales. Coordinarse con las unidades de negocio para garantizar que todas las funciones se definen de forma coherente, incluidas las funciones definidas por la propia empresa dentro de las aplicaciones de procesos empresariales.	Primeramente, conocer los roles funcionales que posee la organización, además, establecer las actividades de procesamiento de la información, luego asociarlas con el rol que corresponde. Solicitar un proceso de fiscalización de las o la unidad de negocio que tienen establecidas para que aprueben las funciones que se definieron.	No aplica
5. Autenticar todos los accesos a los activos de información en función de las responsabilidades del individuo o de las normas empresariales. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio para garantizar que los controles de autenticación se han administrado correctamente.	Para la autenticación de todos los accesos se requiere que cada colaborador disponga de una cuenta. Al tenerlo de esta manera, se puede solicitar la contraseña para acceder al sistema.	No aplica
6. Garantizar que todos los usuarios (internos, externos y	Cada usuario debe contar con su propio perfil o cuenta en los	No aplica

temporales) y su actividad en los sistemas informáticos (aplicación empresarial, infraestructura informática, operaciones del sistema, desarrollo y mantenimiento) sean identificables de forma única.	sistemas que utilice, con el fin de verificar su actividad dentro de ellos.	
7. Mantener un registro de auditoría del acceso a la información en función de su sensibilidad y de los requisitos normativos.	En el registro por desarrollar se debe llevar en orden cronológico, sin perder algún rastro o información. Además, debe contar con trazabilidad de la información con el fin de que sea consultada en caso de que llegue a presentarse alguna situación.	No aplica
8. Realizar una revisión periódica de la gestión de todas las cuentas y privilegios relacionados.	- Se debe gestionar las cuentas y privilegios relacionados cuando deja de laborar un colaborador para la organización. - Se debe definir revisiones periódicas para fiscalizar las cuentas y los privilegios, ya se cuándo un colaborador deja de trabajar para la organización o cuando se den accesos por un tiempo determinado.	No aplica
Logros o beneficios que se adquieren		

- Los accesos a sistemas tendrían un control y un seguimiento, así no cualquier persona o colaborador podría ingresar.
- El definir los roles en un sistema, permitirá que cada persona pueda visualizar y trabajar en lo que requiere, sin la necesidad de intervenir o revisar otras partes que no le corresponden.
- Llevar una bitácora permite controlar las transacciones que se han llevado a cabo, además si se presenta cierta situación se puede verificar quién fue el último involucrado y saber los cambios realizados, todo con el fin de llegar a solucionar el problema.

6.2.3.4. DSS05.05 Gestionar el acceso físico a los activos de I&T.

Tabla 22. *Plan de acción de práctica de gestión: DSS05.05*

Práctica de gestión: DSS05.05 Gestionar el acceso físico a los activos de I&T		
Situación actual	**Descripción de la práctica de COBIT 2019**	
Cuentan con un sistema que lleva el registro de asistencia de los colaboradores, este consiste en agregar la huella al ingresar al edificio. Se monitoriza por cámara de seguridad un pequeño cuarto donde tiene los servidores que se encuentran en uso. Las personas que lo requieren tienen acceso.	Definir y aplicar procedimientos (incluidos procedimientos de emergencia) para conceder, limitar y revocar el acceso a locales, edificios y zonas, en función de las necesidades de la empresa. El acceso a los locales, edificios y zonas debe estar justificado, autorizado, registrado y supervisado. Este requisito se aplica a todas las personas que entren en los locales, incluidos el personal permanente, el personal temporal, los clientes, los proveedores, los visitantes o cualquier otro tercero.	
Brecha		
No se contemplan los siguientes requerimientos: • No se lleva un registro de las personas que ingresan en el cuarto donde se encuentran los servidores. • Los usuarios no se encuentran concientizados sobre la seguridad de la información física.		
Plan para ejecutar		
Actividad según COBIT 2019	**Acción**	**Documentación**

1. Registrar y supervisar todos los puntos de entrada a los centros de TI. Registre a todos los visitantes, incluidos contratistas y proveedores, del centro.	Llevar un registro o bitácora de las personas que ingresan al cuarto donde se encuentran los servidores, ya sea un libro físico que tenga los siguientes espacios: - Nombre Completo - Cédula - Fecha - Hora de entrada y de salida - Motivo de ingreso - Firma	No aplica
2. Asegúrese de que todo el personal lleve en todo momento una identificación debidamente aprobada.	Se debe considerar que el personal se encuentre siempre bien identificado, ya sea tener un gafete con el nombre completo y el departamento que pertenece el colaborador, además de su foto.	No aplica
3. Realizar periódicamente capacitaciones sobre concientización de la seguridad de la información física.	Incentivar a los colaboradores a conocer sobre la seguridad física de la información, a partir de las siguientes formas: - Mediante charlas impartidas por expertos. - Capacitaciones gratuitas - Cápsulas o panfletos enviados por correo electrónico.	No aplica
Logros o beneficios que se adquieren		

- Mayor control y protección sobre accesos a los elementos informáticos físicos que tiene la organización.
- Prevención de posibles problemas de seguridad al permitirle al colaborador conocer acerca de la seguridad y las medidas que se deben tomar en la información física.

7. SÉPTIMO CAPÍTULO: CONCLUSIONES Y RECOMENDACIONES

En este séptimo capítulo se presenta las conclusiones y recomendaciones del trabajo realizado.

7.1. **Conclusiones**

Siempre existen oportunidades de mejora al gestionar el departamento de TI de una organización, por ello es necesario llevar a cabo un estudio de esta área con el fin de descubrir situaciones que si se deja pasar puede ocasionar problemas mayores. Por esta razón, a través del desarrollo de este trabajo final de investigación aplicada se ha realizado un análisis de la situación del departamento de TI de una empresa con el fin de proporcionarle una guía de buenas prácticas para potenciar el área de tecnología, además, mejorar aspectos que les van a permitir llevar a cabo sus procesos de trabajo más eficientes y con los recursos necesarios.

Un factor clave que se necesitó para llevar a cabo el desarrollo de la guía de mejoras fue conocer acerca del objeto de estudio, que en este caso es el departamento de TI en una organización, para ello fue necesario realizar instrumentos que recopilaron dicha información. Por lo tanto, es fundamental utilizar estos materiales de apoyo, su redacción debe ir acorde a los datos que se quieren recopilar, es decir, al llevar a cabo su aplicación deben recopilar información valiosa y que esta no sea ambigua, para el trabajo. Los instrumentos que se realizaron permitieron conocer a la empresa los procesos y funciones, el entorno, además de su conformación. Todo este primer acercamiento permitió llevar a cabo una evaluación más acertada de lo que la empresa tiene y las mejoras que se pueden aplicar, debido al resultado que se obtuvo.

A partir de la utilización del marco de trabajo COBIT 2019 se pudieron observar datos importantes para la organización. Por lo que algunos procesos de dominios que se eligieron para la empresa no presentaban mayor problema, aunque otros son necesarios trabajarlos, por ello se priorizan en la guía. Uno de los temas a enfatizar son los planes de continuidad, ya que no se encuentran preparados, por ello si sucede una situación inadecuada con los sistemas que tienen, se afectaría el trabajo que deben realizar. Con el uso del marco COBIT 2019 se pudo detectar este problema, así como otros que se necesitan mejorar. Desde la perspectiva de este marco se pudieron encontrar varios hallazgos que permiten conocer a la empresa en ciertos campos, se debe considerar que COBIT es muy amplio y para aplicarlo se requiere que se tomen los dominios y procesos que se quieren evaluar en la organización, además que al

hacerlo se pueda considerar realizarlo por etapas, es decir tomar diez o siete elementos con el fin de hacer el estudio más especializado y sin tanto problema dando un enfoque más centralizado.

Gracias a las actividades que compone cada uno de los dominios de COBIT 2019, se realizó la guía de buenas prácticas, en ella se adjuntaron las plantillas, las cuales se desarrollaron para que sean genéricas y aplicables para cualquier organización, estas se pueden adaptar a las necesidades, ya que la idea es brindarles un camino para que vayan mejorando los aspectos en los que se requiere de trabajar.

Gracias al desarrollo de esta evaluación para una empresa considerada como mediana, podemos concluir que el marco de trabajo COBIT 2019 no está sujeto a que sea solo utilizado por empresas grandes, las pequeñas y medianas empresas (PYMES), pueden considerar estos marcos, ya que se beneficiarían en la mejora de los procesos y funciones que lleva a cabo la organización, por lo tanto, el tamaño de la organización no es un factor para no trabajar de la mano con COBIT 2019.

A partir de la evaluación del marco de COBIT 2019 se concluye que es necesario llevar a cabo este tipo de estudios, ya que así las empresas pueden conocer su situación y donde pueden llegar a mejorar, además que brinda la posibilidad de tomar medidas que generen resultados positivos cuando se apliquen.

7.2. **Recomendaciones**

En la guía se presentan varios dominios estos a su vez conformados por objetivos se debe considerar ir paso a paso con cada uno de ellos cuando se lleve a cabo los cambios, para que no se presente ningún problema, además para que sea más ordenado y controlado.

Una vez que se realice la guía deberían dejar la posibilidad de realizar nuevamente un estudio para observar los otros objetivos de los dominios, ya que COBIT 2019 es muy amplio y se requiere de varias iteraciones para abarcarlo en su totalidad. Utilizar otros objetivos les va a permitir ir mejorando y creciendo en nuevas áreas en el lado de la tecnología e información, además es una herramienta que aporta a la empresa conocimiento necesario para llevar procesos y funciones de manera correcta.

Para este tipo de trabajo se requiere conocer acerca de la organización, por ello es de suma importancia que se coloque énfasis en los instrumentos que se deben elaborar, para así recopilar la información necesaria, ya que una vez que se tiene, se puede aplicar de forma apropiada la evaluación con el marco de trabajo.

Sería ideal no solo considerar el marco COBIT 2019 si no también acercase a normas ISO u otro marco como ITIL, ya que estos pueden formar parte de la guía sin ningún problema, debido a que terminan siendo un complemento que permite reforzar la información.

Un punto importante para considerar es la cantidad de personal que se tiene para el departamento de TI, ya que actualmente solo se cuenta con una persona, por lo que, si se lleva a cabo la implementación de la guía, esta persona no debería ejercer a la vez, el rol de fiscalizador y ejecutor de los cambios, por lo que se debe considerar tener más personal en esta área, con el fin de aplicar la guía de manera adecuada y con el desarrollo apropiado.

8. ANEXOS

8.1. **Anexo 1:** Guía de observación realizada en la organización.

#	Indicadores	SI	Algunas veces	NO	Observaciones
1	Registro de entrada en las instalaciones de TI (cuarto donde se encuentran los servidores).				
2	Cámaras de seguridad cerca del cuarto de servidores y dentro de este.				
3	Cámaras de seguridad dentro del cuarto de servidores.				
4	Monitorización de las entradas cuando se da el ingreso al cuarto de TI.				
5	Solo las personas con autorización ingresan al cuarto de servidores.				
6	El acceso al cuarto de servidores se encuentra restringido y monitorizado mediante dispositivos físicos de seguridad.				
7	Cajas o elementos para guardar documentos sensibles que están en papel.				
8	El colaborador cuenta con una responsabilidad o un rol específico dentro de su papel en la organización.				
9	El trato hacia los clientes es el adecuado.				
10	Dan una respuesta inmediata a los problemas que presentan los clientes.				
11	Dan seguimiento al trabajo realizado.				

8.2. **Anexo 2:** Formulario de Entrevista

Nombre del candidato	**Realizado por**	**Fecha de entrevista**
Puesto en el departamento		

¿Cuál proceso es el que usted atiende en la organización?	
¿En qué consiste el proceso?	
¿Qué herramienta o sistema utiliza para llevar a cabo este proceso?	
¿Quiénes interactúan con el sistema?	
¿De qué forma se llevan las solicitudes que realizan los usuarios en el sistema?	
¿Se les da seguimiento a estas solitudes?	
¿Cómo determinan cuando la solicitud esta tramitada?	
¿Cómo se ingresan las solicitudes o casos?	
¿Cómo se asigna a la persona que lleva el caso?	
¿Cuál es el o son los métodos que se utilizan para recopilar la información que se necesita para entender por completa la solicitud?	
¿Qué sucede si la resolución de la solicitud presentada no satisface al usuario?	

8.3. **Anexo 3:** Cuestionario sobre procesos que lleva a cabo el departamento de TI

1. **¿Qué procesos realizan en el departamento de TI?**

   _____
   _____

2. **En que consiste cada uno de los procesos mencionados anteriormente.**

   _____
   _____

3. **¿Cuáles son las principales funciones que se realizan en cada uno de los procesos mencionados anteriormente?**

   _____
   _

_____
_

4. **¿Proyectos que se encuentran activos en el área?**

_____
_____

5. **¿Cuáles son los sistemas que utilizan?**

_____
_____

6. **En que consiste los sistemas mencionados anteriormente.**

_____
_
_____
_

8.4. **Anexo 4:** Tabulación de preguntas abiertas del cuestionario sobre procesos que llevan a cabo en el departamento de TI

1. **¿Qué procesos realizan en el departamento de TI?**

   1-R-2.1-2-Recibido.

   2-P-2.1 Gestión de Tecnologías de la información TI

2. **En que consiste cada uno de los procesos mencionados anteriormente.**

   - Documento que indica que un colaborador recibió el equipo tecnológico necesario para sus labores en buen estado.
   - Documento que indica los requisitos mínimos tanto en *Hardware* como en *Software* que deben tener los equipos utilizados por los colaboradores de la organización, así como la seguridad ofrecida por los proveedores de distintas herramientas que se utilizan en la organización.

3. **¿Cuáles son las principales funciones que se realizan en cada uno de los procesos mencionados anteriormente?**

   - Entrega y revisión del equipo con la persona que recibe la herramienta de trabajo.
   - Revisión que los equipos cumplen con lo estipulado en los reglamentos de la empresa, además de seguimientos en cuanto a la seguridad de los datos que ofrecen los proveedores de distintas herramientas.

4. **¿Proyectos que se encuentran activos en el área?**

   - Desarrollo e implementación de un nuevo sistema ERP.
   - Desarrollo e implementación de un nuevo sistema tipo Helpdesk, pero a nivel interno.

5. **¿Cuáles son los sistemas que utilizan?**
    - Softland ERP
    - CRM Dynamics
    - Kaspersky Endpoint Security Cloud
6. **En que consiste los sistemas mencionados anteriormente.**
    - ERP – Gestión financiera de la organización.
    - CRM – Gestión de oportunidades de negocio.
    - KESC – Seguridad de punto final para cada dispositivo.

8.5. **Anexo 5**: Cuestionario de evaluación de COBIT 2019 en la organización

Cuestionario

Con el presente cuestionario se desea conocer la forma en la que se lleva a cabo la gestión de algunas tareas y acciones del departamento de TI y la organización en general. Cada una de las preguntas cuenta con las mediciones: No, Poco, Moderado, En Gran Medida y un espacio de observación el cual debe ser utilizado para agregar aportaciones a las preguntas. Es necesario que el cuestionario sea respondido con la mayor sinceridad posible con el fin de llevar la evaluación con información verídica.

¿Los colaboradores tiene claridad con la visión, la dirección y la estrategia de la empresa, la situación y retos actuales?				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con que frecuencia se considera el entorno interno de la empresa, incluida la cultura y la filosofía de gestión, la tolerancia al riesgo, la política de seguridad y privacidad, los valores éticos, el código de conducta, la responsabilidad y los requisitos para la integridad de la gestión.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización aplica algún método o estrategia para seleccionar las prioridades que poseen.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se utilizan reglas, protocolos o medidas para trabajar bajo buenas prácticas las labores que se requieren.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se cuentan con los recursos necesarios para llevar a cabo una correcta comunicación entre los colaboradores.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Considera que entre los miembros de la organización hay una comunicación sólida, adecuada, asertiva, es decir basada en valores.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuando se dicta una directriz los colaboradores entiende la información suministrada y la aplican mediante acciones.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Poseen un modelo donde se aprecian los objetivos de la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con que frecuencia se revisan los objetivos de la organización, con respecto a las prácticas y actividades que están llevando a cabo actualmente.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización tiene métricas que le permitan llevar un seguimiento de las actividades u objetivos que se han cumplido.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con qué frecuencia se lleva a cabo un análisis de las actividades y procesos que realiza la organización en el área de TI.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se realiza un análisis para conocer la brecha que existe entre las habilidades y capacidades que se requieren para cumplir los objetivos de la empresa con respecto a las habilidades actuales de la fuerza laboral.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se cuenta con políticas en el departamento de TI en temas como calidad, seguridad, privacidad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual (PI).				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con que frecuencia se realizan cambios a las políticas ya establecidas.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Ha pensado en la automatización o el cambio de ciertos servicios, aplicaciones o infraestructura.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se utilizan herramientas adecuadas para llevar a cabo las actividades de la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se realizan capacitaciones de las herramientas ingresadas recientemente a la empresa.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se realizan revisiones y se toman medidas sobre el desempeño de los sistemas que se utilizan.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se lleva a cabo un análisis que permita el mejoramiento de las funciones que se realizan dentro de la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se realiza algún estudio de FODA para identificar fortalezas, debilidades, oportunidades y amenazas.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se cuentan con métricas para medir el rendimiento de los objetivos que se llevan a cabo.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Al realizar los procesos y funciones en la organización, estas son llevadas a cabo con eficiencia y eficacia.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los procesos y las funciones que se realizan cuentan con prácticas para una correcta gestión de calidad.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Considera que la institución conserva reglas o normas que un se puede seguir aplicando en la actualidad.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los colaboradores comprenden la forma actual de trabajar, es decir el entorno operativo, la arquitectura empresarial, la cultura empresarial y los desafíos actuales.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se tiene claridad con la dirección futura de la empresa, la estrategia, las metas y los objetivos.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se conocen las partes interesadas clave en la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se realizan evaluaciones de los servicios provistos externamente, las habilidades y competencias relacionadas con TI en toda la empresa.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se llevan a cabo evaluaciones para conocer la madurez digital.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los objetivos y las metas de Información y Tecnología se encuentran definidos.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los servicios y productos relacionados a Información y Tecnología permiten que se alcancen los objetivos de la empresa.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Utilizan metodología de desarrollo (Ágil, scrum, cascada, TI bimodal).				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los objetivos con los que cuenta la organización son medibles				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con que frecuencia se replantean los socios y proveedores que se encuentra relacionados a la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los proveedores se encuentran clasificados (nivel de importancia, prioridad).				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con la documentación de los proveedores y contratos existentes.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se realizan revisiones o se aplican criterios de evaluación a los proveedores y contratos				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con que frecuencia realizan mediciones de desempeño a los proveedores existentes.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Se conoce si los contratos de los proveedores cumplen con los estándares empresariales y los requisitos legales y reglamentarios.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Al adquirir un servicio de terceros se contemplan los riegos a los que ellos pueden estar expuestos y por ende pueda afectar el desarrollo de la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización cuenta con SGSI (Sistema de gestión de seguridad de la información)				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

En caso de contar con SGSI, este se encuentra alineado con el enfoque empresarial.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con un plan de tratamiento de riesgos de seguridad de la información.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

El plan de tratamiento de seguridad de la información se encuentra alineado con el objetivo estratégico y la arquitectura de la empresa.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

El plan contiene prácticas de gestión, soluciones de seguridad adecuadas y óptimas, con los recursos, las responsabilidades y los recursos asociados.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con un inventario de los componentes de la solución que están implementado para administrar el riesgo.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los colaboradores han sido capacitados y concientizados sobre seguridad y privacidad de la organización.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Con que frecuencia se realiza una revisión de SGSI.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Realizan auditorías del SGSI a intervalos planificados.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Proporciona información para el mantenimiento de los planes de seguridad para tener en cuenta los resultados de las actividades de seguimiento y revisión				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuestionario 2

Con el presente cuestionario se desea conocer la forma en la que se lleva a cabo la gestión de algunas tareas y acciones del departamento de TI y la organización en general. Cada una de las preguntas cuenta con las mediciones: No, Poco, Moderado, En Gran Medida y un espacio de observación el cual debe ser utilizado para agregar aportaciones a las preguntas. Es necesario que el cuestionario sea respondido con la mayor sinceridad posible con el fin de llevar la evaluación con información verídica.

La organización realiza una evaluación para conocer la disponibilidad, el rendimiento y la capacidad de los servicios y recursos: requisitos del cliente, prioridades comerciales, objetivos comerciales, impacto presupuestario, utilización de recursos, capacidades de TI y tendencias de la industria.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Identifican todos los incidentes causados por desempeño o capacidad				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Dan seguimiento a todos los incidentes causados por desempeño o capacidad				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Las fallas o errores pasados de las aplicaciones se encuentran documentados.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se evalúa regularmente los niveles actuales de rendimiento para todos los niveles de procesamiento (demanda comercial, capacidad de servicio y capacidad de recursos) comparándolos con las tendencias y los SLA.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La organización tiene identificado soluciones o servicios críticos en el proceso de gestión de disponibilidad y capacidad.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La organización cuenta con planes de disponibilidad, rendimiento y capacidad.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Poseen acciones correctivas (p. ej., cambiar la carga de trabajo, priorizar tareas o agregar recursos cuando se identifiquen problemas de rendimiento y capacidad).				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

¿En qué medida se han formalizado los esquemas de solicitudes de servicios e incidentes?				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

¿Se han desarrollado modelos de incidentes basados en errores conocidos?				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

¿Las reglas y procedimientos de escalamiento de incidentes están bien definidos y comunicados?	Observación

○ No	○ Poco	○ Moderadamente	○ En gran medida	

¿La organización tiene una fuente de conocimiento centralizada para incidentes y solicitudes?				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La información que es ingresada es la más relevante para la organización.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se tiene el conocimiento del servicio SLA (Acuerdo de nivel de servicio).				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Con cuanta frecuencia se producen incidentes				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La organización cuenta con un flujo de proceso predefinido para resolver las solicitudes de servicio.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

¿Las solicitudes una vez atendidas son revisadas con los usuarios?				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

¿Las solicitadas una vez finalizadas por el usuario son cerradas?				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se realizan informes sobre las incidencias y solicitudes que atienden.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Tienen identificado los procesos comerciales internos y subcontratados y las actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La organización ha identificado los procesos empresariales de apoyo esenciales y los servicios de I&T relacionados.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se ha analizado escenarios potenciales que puedan dar lugar a eventos que podrían causar incidentes disruptivos significativos				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La organización ha establecido un tiempo mínimo requerido para recuperar un proceso de negocios y soporte de I&T, basado en una duración aceptable de interrupción del negocio y una interrupción máxima tolerable.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La organización tiene un plan de continuidad de negocio.	Observación

◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con un estudio de probabilidad de amenazas que podrían causar la pérdida de continuidad del negocio.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los proveedores externos con los que trabaja la organización cuentan con planes de continuidad de negocio efectivos.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización cuenta con un plan de recuperación de desastres.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura TI.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con los requisitos de respaldo de información necesarios para respaldar los planes. Incluya planos y documentos en papel, así como archivos de datos.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con el personal para enfrentar o llevar a cabo el plan y los procedimientos ante procedimientos de continuidad y respaldos.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Realizan copias de seguridad a los sistemas, aplicaciones, todo tipo de datos, documentación e información de todo tipo.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Realizan pruebas con las copias de seguridad que se crean de los sistemas.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Llevan a cabo evaluaciones de los planes de continuidad y negocio y del plan de respuesta ante desastres.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Realizan una revisión de efectividad de los planes, capacidades de continuidad, roles, responsabilidades, habilidades entre otras que se tiene.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los planes y las capacidades se les aplican mejoras.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuestionario 3

Con el presente cuestionario se desea conocer la forma en la que se lleva a cabo la gestión de algunas tareas y acciones del departamento de TI y la organización en general. Cada una de las preguntas cuenta con las mediciones: No, Poco, Moderado, En Gran Medida y un espacio de observación el cual debe ser utilizado para agregar aportaciones a las preguntas. Es necesario que el cuestionario sea respondido con la mayor sinceridad posible con el fin de llevar la evaluación con información verídica.

En las instalaciones de procesamiento de TI se cuenta con herramientas actualizadas de protección contra software malicioso.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Existen filtros o reglas en los correos electrónicos y las descargas para proteger a los colaboradores de situaciones de peligro, como spyware y correos electrónicos de phishing.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

En la empresa se concientiza a lo colaboradores sobre los peligros del software malicioso y de las medidas que se debe tener para no brindarles acceso a las personas ajenas por medio de este.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización se informa de las nuevas amenazas que existe, además realizan revisiones sobre consejos de seguridad de manera periódica.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Solo los dispositivos autorizados por la empresa tienen acceso a la red e información corporativa.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Los dispositivos autorizados están configurados para solicitar credenciales.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización cuenta con el control adecuado del tráfico entrante y saliente de la red.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuentan con mecanismos de filtrado como firewalls y software de detección de intrusos.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La organización aplica protocolos de seguridad en las conexiones de red.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

El equipo de red cuenta con configuraciones de seguridad.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

La información en tránsito se encuentra encriptada.				Observación
◯ No	◯ Poco	◯ Moderadamente	◯ En gran medida	

Cuenta con políticas de seguridad de acuerdo con las evaluaciones de riesgo y los requisitos del negocio.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La difusión y recepción de documentos se realiza de manera segura.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Periódicamente se realizan pruebas para comprobar la protección de la red.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Periódicamente se realizan pruebas para comprobar la protección de los sistemas.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Las configuraciones realizadas en los sistemas operáticos se han realizado de forma segura.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Los dispositivos tienen mecanismos de bloqueos.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Las configuraciones de red se han hecho de forma segura.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Controlan los accesos y el control remoto.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Poseen filtrado de tráfico de red en dispositivos de punto final.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Los endpoint so desechados de manera segura.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se tiene un control sobre los sitios web maliciosos, así como el correo electrónico.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Cuenta con procedimientos diferentes para la información sensible. (Como la encriptación)				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Los cambios de acceso o cualquier cambio que se realice se documentan, además se realiza bajo autorización de un superior.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se gestionan, reducen y supervisan las cuentas de los usuarios privilegios.	Observación

○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se cuenta con la autenticación de los usuarios cuando es necesario.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se revisan los accesos que han tenido las personas en los sistemas.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se realizan revisiones periódicas de las cuentas y los privilegios que tienen.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Los perfiles de acceso permanecen en constante actualización.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se les da formación a los colaboradores en el tema de seguridad de información física.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Cuentan con procedimientos para regir la recepción, el uso, la eliminación y la eliminación de documentos confidenciales dentro y fuera de la empresa.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Al hacer uso y retiro de dispositivos de salida dentro de la organización se cuentan con procedimientos o documentación para proceder con la acción.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La información sensible almacenada electrónicamente pasa por un procedimiento criptográfico.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

La información electrónica con cierto grado de sensibilidad es accedida solo por personas interesadas en ella.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

Se tiene un inventario de documentos sensibles y dispositivos.				Observación
○ No	○ Poco	○ Moderadamente	○ En gran medida	

8.6. **Anexo 6**: Plantilla Planificación Estratégica TI

El acceso a la plantilla se encuentra en el siguiente enlace Plantilla Planificación estratégica de TI.docx

8.7. **Anexo 7:** Plantilla Matriz RACI
El acceso a la plantilla se encuentra en el siguiente enlace Plantilla Matriz RACI.

8.8. **Anexo 8:** Herramienta Fortalezas, Oportunidades, Debilidades y Amenazas (FODA)
Plantilla con recomendaciones para llevar a cabo su análisis y desarrollo.

FODA	**Positivo**	**Negativo**
	Fortalezas	**Debilidades**

Internas	Preguntas que se pueden llevar a cabo para descubrir las fortalezas de la empresa: - ¿Cuáles son los puntos fuertes con los que cuenta la organización? - ¿Qué ventaja o ventajas tienen sobre otros? - ¿De qué forma se diferencia de la competencia? - ¿Cuáles son las acciones que realizan que hace que la organización destaque?	Preguntas que se pueden llevar a cabo para descubrir las debilidades de la empresa: - ¿El negocio cuenta con reputación y de que tipo es? - ¿Cuáles son los aspectos que la organización debe mejorar? - ¿Cuáles son los problemas que se presentan a largo o corto plazo?
Externas	**Oportunidades**	**Amenazas**
	Preguntas que se pueden llevar a cabo para descubrir las oportunidades de la empresa: - Existe la posibilidad de expandir el negocio - La organización puede ofrecer otros servicios o productos.	Preguntas que se pueden llevar a cabo para descubrir las amenazas de la empresa: - ¿Cuáles productos se encuentran en el mercado? - ¿Se encuentran otros competidores en esta área de trabajo?

Fuente: Elaboración propia

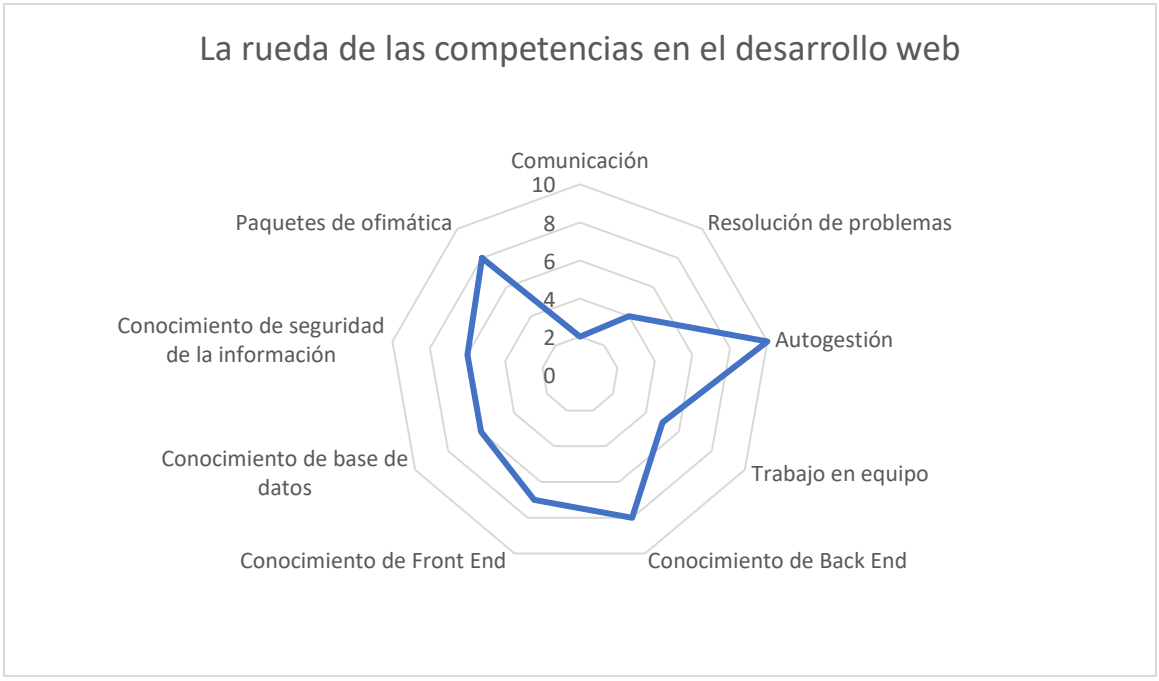
8.9. **Anexo 9:** Herramienta de la rueda de las competencias

Se proporciona una plantilla con un ejemplo de la rueda de las competencias que es adaptado a la rueda de la vida de Paul J. Meyer. Esta rueda consiste en evaluar las habilidades y capacidades que tiene una persona. Los pasos para llevarlo a cabo son los siguientes:

1. Se definen las habilidades que se van a tomar en cuenta: La cantidad va a depender del evaluador.
2. Se define el rango del puntaje que se va a colocar: No hay uno en específico, pero puede ser de 0 a 10 u otro valor.

3. Se evalúa cada opción elegida: Se realiza mediante una línea que sale de la sección de la habilidad hasta el puntaje.
4. Por último, se analiza la evaluación realizada.

Se puede tener mayor claridad en el siguiente ejemplo el cual consiste en evaluar las competencias que tiene una persona en el área de desarrollo web, se consideran tanto habilidades blandas como técnicas.



Fuente: Elaboración propia

8.10. **Anexo10:** Herramienta de Sistema de evaluación 360°

El sistema de evaluación 360° consiste en evaluar el desempeño del colaborador a partir de los comentarios de otras personas. Según Gómez (2022) los pasos a seguir para llevar a cabo esta actividad son los siguientes:

- Seleccione a los participantes de la evaluación: Primeramente, se debe considerar al empleado, a partir de ahí el jefe directo, líder de proyecto, el administrador, entre otros.
- Se debe dar la comunicación de la evaluación de la manera más acertada posible.
- Orientar al evaluado a elegir a sus revisores: La persona encargada de definir a las personas que darán sus comentarios va a ser el colaborador por evaluar, por lo tanto, el encargado debe guiarlo para que busque las adecuadas.

- Formulación de las preguntas de la encuesta: Es recomendables que sean preguntas abiertas, pero puede colocarse cerradas.
- Envío de preguntas a las personas encargadas de evaluar: Cuando se envía la encuesta se debe definir un tiempo y además darle seguimiento para obtener los resultados.
- Compartir los resultados y realizar un plan de acción: Se comparte los resultados con el colaborador y se le indica cuales puntos debe mejorar y una orientación para ayudarlo con las debilidades que se puedan presentar.

8.11. **Anexo 11:** Herramienta de Necesidades basadas en la pirámide de Maslow

En el sitio Mailrelay podemos ver un ejemplo sobre una empresa que utiliza la herramienta. La empresa de redacción de contenidos requiere ampliar su negocio, por ello necesita busca nuevos profesionales para hacerlo utiliza la pirámide de Maslow.

Necesidades fisiológicas: Las necesidades de los futuros empleados como sueldo competitivo, flexibilidad horaria, equilibrio entre la vida laboral y la personal.

Fase de seguridad: Ofrecimiento de un contrato claro, transparente y adecuado a las condiciones laborales. En el lugar de trabajo respetar la privacidad, respeto para todos, trabajo estable.

Necesidades sociales: Ofrecer formaciones grupales por videoconferencia, incentivando a los colaboradores a eventos presenciales de marketing, para así mejora la productividad del equipo de trabajo.

Fase de reconocimiento: Celebrar los logros y objetivos de los colaboradores de manera pública o privada.

Autorrealización: Brindar proyectos más desafiantes.

8.12. **Anexo 12:** Acuerdo de nivel de servicio

Formato de un acuerdo de nivel de servicio en los siguientes enlaces.

- https://repositorio.uisek.edu.ec/bitstream/123456789/2756/6/Formato_SLA.pdf
- https://www.incibe.es/sites/default/files/contenidos/otros/contratacion_sevicios_acuerdo_de_nivel_de_servicio.pdf

8.13. **Anexo 13:** Plantilla de tratamiento de riesgos

El acceso a la plantilla se puede encontrar en el siguiente enlace Plantilla de tratamiento de riesgos.xlsx

8.14. **Anexo 14:** Solicitud de servicio

En el siguiente enlace puede encontrar una plantilla de solicitud de servicio enlace Plantilla Incidentes.xlsx

8.15. **Anexo 15**: Plantilla de Matriz de partes Interesadas

El acceso a la plantilla se encuentra en el siguiente enlace Plantilla de matriz de partes interesadas.docx

9. BIBLIOGRAFÍA

Acents Technologies S.A. (s.f). Información básica ¿Qué es el SLA? https://www.acens.com/comunicacion/file_download/176/acens_que_es_el_sla_baja.pdf

AMETIC. (s.f). *Transformación digital* [Archivo PDF]. TRANSFORMACIÓN DIGITAL: Visión y Propuesta de AMETIC (thinktur.org)

Arce, J. (2021) *Modelo de Gobierno y Gestión de TI basado en el marco de referencia COBIT 2019 para el Instituto Costarricense del Deporte y la Recreación.* [Tesis de maestría, Universidad de Costa Rica]. https://hdl.handle.net/10669/85817

Argueta, M. (2006). *El Impacto de las Tecnologías de la Información en los Negocios*. [Tesis de Maestría, Universidad del Salvador]. https://ri.ues.edu.sv/id/eprint/12315/1/TG-MAF%20658.15%20A686.pdf

Ati, T. (2018). *Diseño del plan de recuperación de desastres y continuidad del negocio basado en Cobit, Itil y de acuerdo a la norma ISO 22301, para el centro de procesamiento de datos (CPD) de la carrera de ingeniería en ciencias de la computación de la Universidad Politécnica Salesiana, sede Quito, campus sur.* [Tesis de Licenciatura, Universidad Politécnica Salesiana]. https://dspace.ups.edu.ec/bitstream/123456789/15904/1/UPS-ST003686.pdf

Avenía, C. (2017). *Fundamentos de seguridad informática*. Fondo editorial Areandino. https://core.ac.uk/download/pdf/326424171.pdf

Calderón, L. (2015). *Seguridad informática y seguridad de la información* (Bachelor's thesis, Universidad Piloto de Colombia). http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Calle, G., Narváez, C., & Erazo, J. (2020). Sistema de control interno como herramienta de optimización de los procesos financieros de la empresa Austroseguridad Cía. Ltda. *Dominio de las Ciencias*, *6*(1), 429-465.

Cano, G., & García, M. (2018) Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. *Dominio de las ciencias, 4(1),* 499-510. https://dialnet.unirioja.es/servlet/articulo?codigo=6313252

Carter, R. (1995). The Seven C's of Supplier Assessment. *Journal of Purchasing and Supply Management*, 44-46.

Chang, H. Y., Wang, P. C., Chan, C. T., & Lee, C. L. (2008, March). A New Service Level Agreement Model for Best-Effort Traffics in IP over WDM. In *22nd International Conference on Advanced Information Networking and Applications-Workshops (aina workshops 2008)* (pp. 1440-1443). IEEE.

Cortés, A. (2021). *Evaluación por medio de COBIT 2019, del modelo de gestión de Tecnologías de Información y Comunicación de la Municipalidad de Carrillo, producto de los procesos de migración de sistemas operativos e informáticos.* [Tesis de Maestría, Universidad de Costa Rica]. https://hdl.handle.net/10669/84448

Durán, M. M. (2012). El estudio de caso en la investigación cualitativa. *Revista nacional de administración*, *3*(1), 121-134.

Estupiñán R. (2006) Control Interno y Fraudes, Análisis de informe coso. Ecoe Ediciones. Bogotá Colombia

Gómez, D. (21 de diciembre de 2022). *¿Qué es la evaluación 360 de desempeño? Concepto, ventajas y ejemplos.* HubSpot. Recuperado el 09 de enero de 2024 de https://blog.hubspot.es/service/evaluacion-360#:~:text=%C2%BFQu%C3%A9%20es%20una%20evaluaci%C3%B3n%20360,y%20debilidades%20desde%20varias%20perspectivas.

González, J. (2002). La seguridad en la red. *Informática y derecho: Revista iberoamericana de derecho informático*,9(34), 117-146. https://dialnet.unirioja.es/servlet/articulo?codigo=1029447

Gorbe, T. (2007). *Las TIC en la estrategia empresarial*. Anetcom. https://datos.portaldelcomerciante.com/userfiles/167/Biblioteca/93d0cb62098a0ea3055eLaTICenlaestrategiaempresarial.pdf

Hernández, H. (2018). COBIT, una metodología que genera valor en las empresas. http://repository.unipiloto.edu.co/handle/20.500.12277/4677

Hidalgo Quirós, N. *Diagnóstico y evaluación de cumplimiento de la norma de los controles de ISO/IEC 27001 Sistema de gestión seguridad de la información (SGSI) desde las 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* [Tesis de Maestría, Universidad de Costa Rica]. https://www.kerwa.ucr.ac.cr/handle/10669/15659

Hoyos, J. & Valencia, A. (2012). *El papel de las TIC en el entorno organizacional de las PYMES.* Revista TRILOGÍA No. 7, pp. 105 – 122.

Huayhua, M. & Romero, A. (2019). *Propuesta de modelo de implementación de gobierno de TI para la gestión de la demanda de requerimientos y proyectos de una empresa del Sector Minero.* [Tesis de Maestría, Universidad Peruana de Ciencias Aplicadas]. http://hdl.handle.net/10757/651592

Huerta, A., & Zuzuarregui, A. (2015). Análisis de las características de los ERPs para pymes: Una guía preliminar de cara a la elección de las soluciones más eficientes. *San Sebastián, España*. https://www.ehu.eus/documents/1432750/3183370/Informe_ERP_Txostena+v1.pdf

IBM Services. (25 de noviembre de 2020). Adaptarse y responder a los riesgos con un plan de continuidad de negocio (BCP). https://www.ibm.com/es-es/services/business-continuity/plan

IBM. (s.f.). ¿Qué es la gestión de Tecnologías de la Información? https://www.ibm.com/mx-es/topics/it-management#:~:text=La%20gesti%C3%B3n%20de%20TI%20o,informaci%C3%B3n%20funcionen%20de%20manera%20eficiente.

ISACA, (2018). Introducción y metodología. ISACA. https://www.isaca.org/credentialing/implementing-the-nist-cybersecurity-framework-using-cobit-2019

ISO 27001. (s.f). *Fase 9 Revisión por la dirección según ISO 27001*. https://normaiso27001.es/fase-9-revision-por-la-direccion-segun-iso-27001/#:~:text=Existe%20un%20requisito%20m%C3%ADnimo%20para,la%20informaci%C3%B3n%20y%20el%20SGSI.

López, D., & Martí, F. (2014). El departamento de SI/TI. https://openaccess.uoc.edu/bitstream/10609/77187/3/Gesti%C3%B3n%20funcional%20de%20servicios%20de%20SI-TI_M%C3%B3dulo%202_El%20departamento%20de%20SI-TI.pdf

López, J. (11 de mayo de 2018). *Las 5 herramientas más eficaces para evaluar las competencias profesionales.* Corporate YACHTING. https://corporateyachting.es/es/las-5-herramientas-mas-eficaces-para-evaluar-las-competencias-profesionales/

Mailrelay. (18 de julio de 2023). Pirámide de Maslow en la empresa + Ejemplos prácticos. https://mailrelay.com/es/blog/2023/07/18/piramide-de-maslow/

Mangaly, S. (17 de agosto del 2022). La guía definitiva del acuerdo del nivel de servicio (SLA). invgate. https://blog.invgate.com/es/acuerdo-de-nivel-de-servicio-sla

Mellando, C. (2014). *Plan de contingencia informático*. [Tesis de grado, Universidad Gabriela Mistral]. http://repositorio.ugm.cl/handle/20.500.12743/244?show=full

Mendoza M. (4 de Agosto de 2015). *COBIT para la seguridad en las organizaciones*. Welivesecurity. https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

Muntané, J. (2010). Introducción a la investigación básica. *Centro de investigación biométrica*, *221*, 227. https://www.researchgate.net/profile/Jordi-Muntane/publication/341343398_Introduccion_a_la_Investigacion_basica/links/5ebb9e7d92851c11a8650cf9/Introduccion-a-la-Investigacion-basica.pdf

Palomino, K. (29 de agosto de 2022). *¿Qué es gestión de Tecnologías de Información?* Southern New Hampshire University. Recuperado el 5 de marzo de 2024 https://es.snhu.edu/noticias/que-es-gestion-de-tecnologias-de-informacion

protege tu empresa. (s.f). Plan de contingencia y continuidad de negocio. https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio

Ramírez, M., Rivas, E. y Cardona, C. (2019). El estudio de caso como estrategia metodológica. Revista ESPACIOS. 4 (23). https://www.revistaespacios.com/a19v40n23/a19v40n23p30.pdf

Red Hat. (9 de marzo de 2018). *El concepto de gestión de la TI.* https://www.redhat.com/es/topics/management

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, Á. & Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L. http://dx.doi.org/10.17993/IngyTec.2018.46

Sánchez, M., Moral, M. (2019). Tecnología de la información en las organizaciones: notas de clase para un curso de grado en administración de empresas. Bahía Blanca: Ediuns. (Docencia) En RIDCA. http://repositoriodigital.uns.edu.ar/handle/123456789/4601

servicetonic. (s.f). *Gestión de incidencias ITIL*. Recuperado de 11 de enero de 2024 de https://www.servicetonic.com/es/itil/itil-v3-gestion-de-incidencias/#Modelos_de_incidencia

Slusarczyk, M. A., & Morales, N. H. M. (2016). Análisis de las estrategias empresariales y de las TIC. 3c Empresa: investigación y pensamiento crítico, 5(1), 29-46. https://dialnet.unirioja.es/servlet/articulo?codigo=5366172

Villafuerte Guerrero, M. (2021). *Estrategia para la gestión de políticas de seguridad informática en una municipalidad de la región chorotega* [Tesis de Maestría, Universidad de Costa Rica]. http://repositorio.ucr.ac.cr/handle/10669/85149

Zendesk. (12 de diciembre, 2023). *Guía introductoria a la gestión de incidentes [Método ITIL]*. Recuperado el 11 de enero de 2024 de https://www.zendesk.com.mx/blog/gestion-de-incidentes/#:~:text=ciclo%20de%20vida.,%C2%BFQu%C3%A9%20es%20un%20incidente%3F,usuario%20hasta%20toda%20la%20empresa.