UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

Proyecto Integrador, previo a la obtención del Título de Licenciada en Contabilidad y Auditoría C.P.A.

Tema:

“Evaluación a los procesos informáticos en la empresa DChristian Maryuri de la ciudad de Ambato "

Autora: Vargas Guzmán, Leslie Ingrid

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de identidad No. 180293423-0, en mi calidad de Tutora del proyecto integrador sobre el tema: **"EVALUACIÓN A LOS PROCESOS INFORMÁTICOS EN LA EMPRESA DCHRISTIAN MARYURI DE LA CIUDAD DE AMBATO"**, desarrollado por Leslie Ingrid Vargas Guzmán, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, Marzo 2022.

TUTORA

……..……..

Dra. Patricia Paola Jiménez Estrella

C.I. 180293423-0

DECLARACIÓN DE AUTORÍA

Yo, Leslie Ingrid Vargas Guzmán con cédula de identidad No. 180548365-6, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"EVALUACIÓN A LOS PROCESOS INFORMÁTICOS EN LA EMPRESA DCHRISTIAN MARYURI DE LA CIUDAD DE AMBATO"** así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este Proyecto Integrador.

Ambato, Marzo 2022.

AUTORA

……..

Leslie Ingrid Vargas Guzmán

C.I. 180548365-6

CESIÓN DE DERECHOS

Autorizo a la Universidad Técnica de Ambato, para que haga de este proyecto integrador, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi proyecto integrador, con fines de difusión pública; además apruebo la reproducción de este proyecto integrador, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autora.

Ambato, Marzo 2022.

AUTORA

……..

Leslie Ingrid Vargas Guzmán

C.I. 180548365-6

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema**:** **"EVALUACIÓN A LOS PROCESOS INFORMÁTICOS EN LA EMPRESA DCHRISTIAN MARYURI DE LA CIUDAD DE AMBATO"**, elaborado por Leslie Ingrid Vargas Guzmán, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

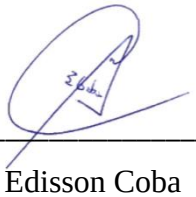
Ambato, Marzo 2021.

Dra. Mg. Tatiana Valle

PRESIDENTE

Dra. Rocío Cando

MIEMBRO CALIFICADOR



Dr. Edisson Coba

MIEMBRO CALIFICADOR

DEDICATORIA

El presente proyecto integrador se lo dedico principalmente a Dios por darme fuerza para seguir a delante y sobre todo por permitirme alcanzar esta meta y llegar a uno de los momentos más importantes de mi vida.

Se la dedico a mis padres, quienes han sido mi apoyo incondicional en toda esta travesía, y que gracias a su amor y esfuerzo he podido cumplir este sueño.

Leslie Ingrid Vargas Guzmán

AGRADECIMIENTO

Quiero expresar mi gratitud a mi familia, amigos y mascota, por ser los principales motores de este sueño.

A la Dra. Patricia Jiménez por orientarme con sus conocimientos en la ejecución de este proyecto integrador.

De igual manera mis agradecimientos a la Universidad Técnica de Ambato y a todos mis docentes por impartirme conocimientos en el transcurso de la carrera.

Y por último a la empresa D'Christian Maryuri por brindarme las facilidades de recolectar información necesaria para realizar este trabajo.

Leslie Ingrid Vargas Guzmán

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "EVALUACIÓN A LOS PROCESOS INFORMÁTICOS EN LA EMPRESA DCHRISTIAN MARYURI DE LA CIUDAD DE AMBATO"

AUTORA: Leslie Ingrid Vargas Guzmán
TUTORA: Dra. Patricia Paola Jiménez Estrella
FECHA: Marzo 2022

RESUMEN EJECUTIVO

El presente proyecto integrador titulado "Evaluación a los procesos informáticos en la empresa D´CHRISTIAN MARYURI de la ciudad de Ambato" se enfocó en el campo de la auditoría de sistemas y tiene como objetivo el diseño de un Marco de Referencia para llevar un óptimo sistema de control y dar soporte a los procesos del negocio. Mediante la ejecución a los procesos informáticos de la empresa D'Christian Maryuri y bajo la aplicación de dos metodologías los cuales corresponden a: COSO ERM 2017 y COBIT 2019 apoyaron a la institución en la detección de falencias, vulnerabilidades y riesgos a través de una evaluación documental y matrices que ayudaron al análisis y revisión de las actividades relacionadas con los procesos de gobierno y gestión de TI. Para la realización del proyecto se establecieron tres fases en las cuales se identificó y determinó que la empresa no implementaba controles, procedimientos y políticas que ayuden a delimitar riesgos potenciales, y aseguren la confidencialidad de la información. De igual manera no adoptaban prácticas de gestión de riegos lo que puede facilitar el robo de información y fraude, así mismo se identificaron varias actividades con brechas significativas que muestran un complejo rendimiento por parte de la institución, una vez encontrado todos estos hallazgos se determinaron acciones de mejora como recomendación para que la empresa los apliques de manera más frecuente.

PALABRAS DESCRIPTORAS: PROCESOS INFORMÁTICOS, RIESGO, COSO ERM, GESTIÓN DE RIESGOS, COBIT.

TECHNICAL UNIVERSITY OF AMBATO
FACULTY OF ACCOUNTING AND AUDITING
ACCOUNTING AND AUDITING CAREER

TOPIC: "EVALUATION OF THE COMPUTER PROCESSES IN THE COMPANY D'CHRISTIAN MARYURI OF THE CITY OF AMBATO".

AUTHOR: Leslie Ingrid Vargas Guzmán
TUTOR: Dra. Patricia Paola Jiménez Estrella
DATE: March 2022

ABSTRACT

This integrative project entitled "Evaluation of the IT processes in the company D'CHRISTIAN MARYURI in the city of Ambato" focused on the field of systems auditing and aims to design a framework of reference to bring an optimal control system and support the business processes. Through the execution to the IT processes of the company D'Christian Maryuri and under the application of two methodologies which correspond to: COSO ERM 2017 and COBIT 2019 supported the institution in the detection of weaknesses, vulnerabilities and risks through a documentary evaluation and matrices that helped the analysis and review of activities related to governance processes and IT management. To carry out the project, three phases were established in which it was identified and determined that the company did not implement controls, procedures and policies that help to delimit potential risks and ensure the confidentiality of information. Likewise, they did not adopt risk management practices, which can facilitate information theft and fraud. Likewise, several activities were identified with significant gaps that show a complex performance by the institution, once all these findings were found, improvement actions were determined as a recommendation for the company to apply them more frequently.

KEYWORDS: IT PROCESSES, RISK, COSO ERM, RISK MANAGEMENT, COBIT.

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

ÍNDICE DE GRÁFICOS

CONTENIDO **PÁGINA**

CAPÍTULO I

MARCO TEÓRICO

1.1 Introducción

1.1.1 Antecedentes del proyecto integrador

1.1.1.1 Historia de la empresa

D´Christian Maryuri se encuentra domiciliada en la ciudad de Ambato, provincia de Tungurahua, se dedica a la producción y comercialización de ropa interior para niños, niñas, damas y caballeros, con una amplia gama de productos y marcas para cada tipo de cliente como son: Maryuri, D'Christian, Joe, Pitbool, Polette, entre otras.

Inició sus actividades empresariales en el año 2006, siendo fundada por su propietario Sr. Mario Lara quién con su visión y con la ayuda de su esposa arriendan una propiedad en la cual se establecen donde incursiona diseñando y confeccionando las prendas que son promocionadas y ofertadas en el mercado textil.

Con el pasar de los años la empresa crece rentablemente, lo que le permite al propietario invertir en la construcción de su fábrica ubicada en el Barrio Solís en las calles Bustamante Celi y Julio César Cañar. Para el año 2018 se extiende y construyen una planta física ubicada en Santa Rosa cantón Ambato, con el fin de satisfacer la creciente demanda de sus productos, es por ello que D'Christian Maryuri incorpora nuevas líneas de producción con altos estándares de calidad, convirtiéndola en una empresa líder en ropa interior del país hasta la actualidad.

Datos de la empresa

Razón Social: Lara Lara Mario Oswaldo

RUC: 1802205250001

Nombre Comercial: D'Christian Maryuri

Clase de Contribuyente: Especial

Fecha de inicio de actividades: 24 de julio del 2006

1.1.1.2 Detalles estratégicos

1.1.1.2.1 Misión

“Somos la empresa con mayor crecimiento nacional en la comercialización de ropa interior, con un personal altamente, calificado y comprometido en proporcionar lo mejor en ropa íntima. Trabajamos constantemente para cumplir las expectativas de nuestros clientes. Actualmente, cuenta con el servicio de compras online para facilitar la adquisición de nuestros productos en todo el territorio nacional”.

1.1.1.2.2 Visión

“Ser una empresa líder a nivel nacional por la exclusividad de nuestros diseños elegantes y genuinos, calidad en nuestros productos y excelente servicio en la fabricación y distribución de ropa interior garantizando la satisfacción de nuestro cliente”.

1.1.1.2.3 Valores

Solidaridad: Apoyamos las actividades de los colaboradores internos y externos son olvidarnos de la responsabilidad social con las personas más vulnerables.

Respeto: Respetamos las opiniones y esfuerzos de las personas de nuestra empresa, a través del cumplimiento de las políticas internas, lo que permite mantener un buen clima laboral.

Honestidad: Fomentemos y practicamos la honestidad en todas las actividade4s que se desarrollan en la empresa, avalando el desempeño de cada colaborador.

Calidad: La empresa busca la calidad integral de nuestros colaboradores, procesos y productos, aplicando la innovación, creatividad y cumplimiento de estándares en el mercado.

Cumplimiento: Somos puntuales en la entrega de productos cumpliendo con los contratos establecidos, de esta manera se demuestra responsabilidad y respeto de la empresa con cada uno de los clientes.

1.1.1.2.4 Logotipo de la empresa

Gráfico No. 1 Logotipo D´Christian Maryuri

Fuente: D´Christian Maryuri

Elaborado por: D'Christian Maryuri

1.1.1.2.5 Ubicación

Se encuentra ubicada en la provincia de Tungurahua, cantón Ambato, calle s/n y Bernardino Echeverría, San José de Santa Rosa.

Gráfico No. 2 Ubicación de la empresa

Fuente: D´Christian Maryuri

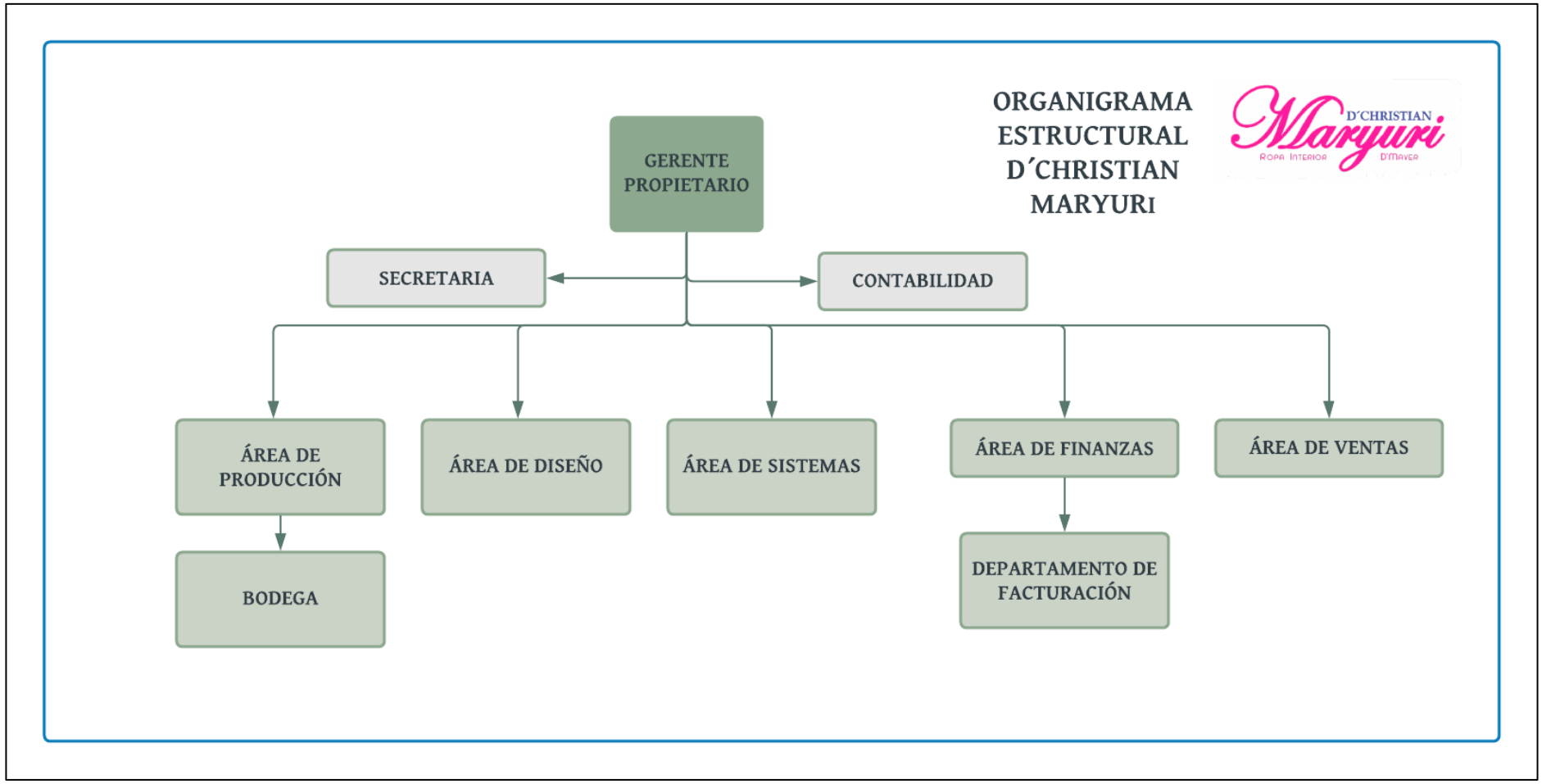
Elaborado por: Google maps

1.1.1.2.6 Organización estructural

La empresa D´Christian Maryuri está compuesta por una organización estructural distribuida entre los departamentos de: contabilidad, producción, diseño, sistemas finanzas, ventas y departamento de facturación.

A continuación, el organigrama estructural de la empresa.

Gráfico No. 3 Organigrama estructural



Fuente: D´Christian Maryuri

Elaborado por: Vargas (2021)

1.1.1.2.7 Estructura funcional

- **Área administrativa**

  Gerente: Está a cargo del propietario de la empresa Sr. Mario Oswaldo Lara Lara responsable de la mando, control y organización de la misma. Lidera, coordina y toma decisiones de manera eficiente.

  Contador y administrador: El Ing. Jorge Aucanshala encargado de la parte contable y tributaria de la empresa, también cumple la función de administrador donde planifica, organiza y controla todas las áreas de la empresa.

- **Área de producción**

  Se cuenta con maquinaria de punta, insumos y materiales de calidad, la Sra. Verónica Ocaña está a cargo del taller de producción, que tiene a su cargo 38 trabajadores, quienes se encargan de producir, empacar las prendas que son entregadas a la bodega de producto terminado.

  Esta área está conformada por los siguientes pasos:

  Corte: Reciben el corte con la ficha de código a producir, verifican que las piezas y colores sean acorde a las mismas cantidades a producir.

  Confección: Se procede a fundillar la prenda para pasar a igualar la tela en la igualadora, se pone las piernas, después se las cierra y se coloca etiquetas, se procede a poner cintura para la colocación de sesgo o elástico según el diseño de la prenda. Se cierra la pierna para rematar las costuras con la atracadora.

  Pulida: Se encarga de cortar los hilos de las prendas finales de la producción.

  Empacado: Se separan las prendas por 12 colores para comenzar a empacar en las cajas respectivas que constituyen a tres prendas por cada caja, las cuales son enviadas al área de producto terminado.

  Producto terminado: Distribuyen las cajas en las perchas de acuerdo al código elaborado.

  Despachado: La bodega de producto terminado trabaja conjuntamente con los vendedores y clientes, quienes realizan sus pedidos, encargándose de despachar a todos los puntos de distribución a nivel nacional.

- **Área de ventas**

  Los puntos de venta principales es la planta principal y los vendedores externos.

Gráfico No. 4 Planta principal D'Christian Maryuri

Fuente: D´Christian Maryuri

Elaborado por: D´Christian Maryuri

1.1.1.3 Detalles de operación

D´Christian Maryuri es una empresa dedicada a la producción de ropa interior para hombres, mujeres, niños y niñas. Cada prenda intima es realizada con materiales de calidad, y sus diseños se encuentran acorde a las tendencias que existe en el mercado. Los productos que brinda son detallados a continuación:

Interiores para dama: Acariciamos tu piel con una alta gama de prendas de vestir, diversos tipos de ropa interior confortables para la mujer, con varios modelos que te hará sentir segura de ti misma.

Interiores para hombre: Nuestras prendas brindan la máxima seguridad intima en cada una de nuestras prendas de ropa interior al hombre vanguardista, brindándole comodidad en su día a día.

Interiores para niña: Maryuri la marca de ropa interior para niñas más bonitas. Encuentra ropa diferente y preciosa para vestir a tus hijas siguiendo las últimas tendencias y al mejor precio.

Interiores para niño: ¡Si lo que buscas es ropa interior de niño, en D'Christian Maryuri la has encontrado! Porque su ropa interior está pensada para que tu hijo sea el más guapo y el mejor vestido.

1.1.1.4 Detalles legales

D´Christian Maryuri se rige a través de la siguiente normativa:

La empresa se encuentra legalmente constituida para el desarrollo de sus actividades económicas, cumpliendo con todas las obligaciones legales, laborales, contables, tributarios que este tipo de empresa requiere como son: Instituto Ecuatoriano de Seguridad Social, Ministerio de Trabajo, Servicio de Rentas Internas. Así también cumple con las normas y leyes reglamentarias como son: Código de Trabajo, Código de la Producción, Constitución de la República del Ecuador, Ley de Seguridad Social, entre otros. Lo que le permite estar al día con sus empleados y entidades de control como: la Contraloría General del Estado, Procuraduría General del Estado, Ministerio Público, Comisión de Control Cívico de la Corrupción y la Superintendencias.

En la Constitución de la República del Ecuador, en su artículo 284 señala que el incentivar la producción nacional, mantener una estabilidad económica y promover un intercambio justo de bienes y servicios se constituyen como políticas económicas, así mismo en el artículo 320 reconoce que la producción estará sujeta a principios y normas de calidad que aseguren un buen vivir y cumplan con la demanda del mercado.

La empresa D´Christian Maryuri se constituye como una Persona Natural obligado a llevar contabilidad, y se considera como una empresa mediana, con 79 empleados y ventas anuales de $ 1 800 000. De acuerdo a la Ley de Régimen Tributario Interno al tener ingresos mayores a $ 300 000 toda persona natural es obligada a llevar contabilidad, así mismo establece que obligaciones tributarias tiene la empresa conforme a su tipo de actividad y contribuyente, también establece que la contabilidad se deberá llevar de acuerdo a los Principios de Contabilidad Generalmente Aceptados.

Con relación a lo anterior a continuación, se detalla las obligaciones tributarias de la empresa D’Christian Maryuri:

Tabla No. 1 Obligaciones tributarias

TIPO	OBLIGACIÓN	PERIODO
TRIBUTARIO	Anexo Relación de Dependencia	Anual
	Declaración del Impuesto a la Renta - Personas Naturales	
	Anexo Transaccional Simplificado	Mensual
	Declaración de IVA	
	Declaración de Retenciones en la Fuente	

Fuente: D´Christian Maryuri

Elaborado por: Vargas (2021)

1.1.2 Descripción del entorno

D'Christian Maryuri realiza sus actividades diarias mediante un sistema que abarca varios procesos, cabe mencionar que la misma actualmente no cuenta con un marco de referencia que ayude en la ejecución de estos procesos informáticos, y contribuya al desarrollo e implementación de estrategias para identificar y administrar riesgos de mayor impacto que pueden afectar directamente a la organización.

Por ende, es sustancial revisar que procesos no se realizan o no se dan prioridad, para así sugerir correcciones que ayuden a una mejor toma de decisiones.

1.1.2.1 Análisis y desarrollo de las TIC en la actualidad

Las Tecnologías de Información son herramientas que facilitan el procesamiento, acceso y control de la información, cabe recalcar que actualmente la información es el recurso más importante de la empresa, pues un buen uso de la misma puede significar una ventaja competitiva que ayudara a obtener mejores resultados. En un mundo cada vez más rígido y exigente las TIC posibilitan tratar la información de manera fácil y veraz, tomando en cuenta los cambios que se realizan a menudo en la sociedad con respecto a los avances tecnológicos. Como lo menciona Díaz et al. (2011) en la actualidad, ya sea para una persona, una empresa u una organización, el acceso a las TIC es un requisito indispensable para incorporarse en un círculo social cada vez más dependiente de la tecnología. Por esta razón en los últimos años, en varios países se han aplicado normas y estrategias que promueven el uso de las TIC con el fin de aprovechar los beneficios y aportes que estas brindan (Prieto et al., 2011).

Igualmente hay que considerar que las TIC han sido de gran ayuda para la globalización, puesto que con el tiempo se han ido desarrollando y han contribuido en el avance tecnológico y por ende en el mejoramiento de la vida humana. Con relación a lo anterior Ortiz (2011) menciona que dentro de un mundo globalizado se ha dado lugar a un proceso de creciente interdependencia social, ya que países que no están preparados para los cambios que las TIC implican, son consideran poco avanzados. Así mismo hay que tener en cuenta que hoy en día los mercados mercantiles, financieros, los sistemas, la información, los procesos productivos, la gestión, la tecnología, entre otros se basan en función a las redes globales.

1.1.2.2 La Implementación y el uso de los sistemas de informática e información como herramientas prácticas

Los Sistemas de Información (SI) comprende un conjunto de manuales y sistemas informáticos que automatizan el almacenamiento, la recopilación, recuperación y disposición de la información en toda la institución. Como lo menciona Trasobares (2003) aparte de los datos, los componentes básicos que constituyen un SI son los usuarios, que conforman la organización empresarial y los equipos como software y hardware. Debido a la importancia que tienen los sistemas de información en la planificación estratégica de una empresa, existen varios modelos que permiten evaluar los procesos informáticos. De acuerdo con Pesado et al. (2013) en los últimos años el software se ha desarrollado constantemente, debido a la necesidad de implementar modelos que garanticen un mejor desarrollo a los procesos de gestión y de calidad.

Sin embargo, un SI tiene el fin suministrar información relevante de la organización para su correcto funcionamiento y control de sus actividades, capaz de procesar datos de forma eficaz y eficiente. Cabe recalcar que para implementar un SI la empresa deberá tomar en cuenta las necesidades de la misma, como sus objetivos y recursos, ya que el seguimiento de los planes estratégicos es fundamental para lograr mejores resultados. Con relación a lo anterior y en referencia a los procesos tecnológicos, el emplear un enfoque de procesos podrá determinar que métodos se utilizarán para el control de los resultados. El realizar una evaluación a los procesos informáticos surge con el fin de conocer deficiencias, vulnerabilidades y errores que pueda llegar a tener el sistema.

En estudios enfocados al sector textil la aplicación de un sistema de información es un elemento primordial dentro de la organización, puesto que al implementar y ejecutar estrategias para la tomar decisiones fortalece la estrategia competitiva. De acuerdo con Serna (2007) para que las PYMES sigan ingresando en el mercado y se diversifiquen, es necesario desarrollar un sistema de información de marketing, crear un estructura estable y una visión a futuro de la empresa, para generar, procesar y almacenar información que pueda respaldar la toma de decisiones.

En cambio, la seguridad informática permite digitalizar todo un volumen de información al reducir la cantidad de espacio ocupado y al facilitar el análisis y procesamiento de la información (Calderón, 2015). Como lo menciona Voutssas (2010) la seguridad informática es el proceso de establecer y seguir un conjunto de lineamientos, pautas, practicas, estrategias, entre otros, diseñados para prevenir y proteger los recursos informáticos de la empresa de daños o robos. En la actualidad las empresas manipulan grandes cantidades de información la mismas que pueden estar expuestas a ser interceptadas por personas no autorizadas como hackers, al no poseer un sistema de seguridad informática y de información aumenta la posibilidad de riesgos, amenazas y vulnerabilidades.

Para las PYMES la seguridad informática es un aspecto importante, ya que a partir de los procesos y procedimientos especializados es posible proteger los datos mediante un Sistema de Gestión de la Seguridad Informática (SGSI), para proteger eficazmente los registros confidenciales, mediante un mecanismo que sostenga la confidencialidad, integridad y disponibilidad de la información tomando en consideración los parámetros de seguridad permitidos por la ley (Guzmán & Taborda, 2015) .

1.1.3 Justificación

1.1.3.1 Justificación teórica

Los sistemas informáticos han sido una herramienta de ayuda para todas las empresas sean estas grandes, medianas o pequeñas, ya que tiene como objetivo principal el almacenar y procesar información y datos relevantes de la organización (Díaz et al., 2014). Este estudio menciona la relevancia que tiene realizar esta evaluación, sus

enfoques teóricos, el para que se debe realizarla y se enfoca en la problemática: Desconocimiento de la ejecución de los procesos informáticos.

Esta evaluación a los procesos informáticos se centra en el campo de la auditoría de sistemas, como lo cita Ramírez & Álvarez (2003) una auditoría se define como la actividad de emitir una opinión experta sobre si el tema sometido a análisis representa adecuadamente la realidad que se espera que se refleje o cumpla con los requisitos ya especificados. Sin embargo, Trasobares (2003) menciona un sistema de información va más allá de la computación, ya que no solo se toma en cuenta las herramientas que lo componen, si no también interviene el cómo organizar dichas herramientas y obtener información necesaria y suficiente para el correcto manejo de la empresa. Por lo que la auditoría de sistemas se puede denominar como la verificación del control en el procesamiento de la información, desarrollo e instalación del sistema con el fin de evaluar su efectividad y efectuar recomendaciones a la gerencia que ayude a la toma de decisiones (Naranjo, 2009). Así mismo, un elemento importante en este trabajo es el Marco de Referencia COBIT 2019. Según Armendáriz (2017) este marco es una metodología distribuida por ISACA y las mejores prácticas de ITIL, que permiten evaluar la gestión de tecnología de información mediante la auditoría.

Martínez et al. (2012) señala que en esta época la información es el activo más importante de las empresas, por eso se ha invertido mucho dinero y tiempo en la creación de sistemas de información. De acuerdo con los autores es relevante resaltar que para que la información sea segura y confiable, el sistema deberá tener un conjunto de controles adecuados para la empresa. Como lo mencionan Salazar & Campos (2009) existe mucha inseguridad relacionada con los equipos y sistemas de información y comunicación ya que al no implementar controles de seguridad las TIC pueden enfrentarse a amenazas globales, es una tema que preocupa tanto a grandes, medianas y pequeñas empresas ya que al existir ladrones de información puede ocasionar interrupción en los servicios y existir fallas en el sistema.

Por consiguiente, realizar una evaluación a los sistemas informáticos permitirá evaluar y analizar los procesos y controles que lleva la empresa, con el fin de dar una opinión en el entorno tecnológico que ayude a la misma en la toma de decisiones, a adoptar

medidas que resguarden la seguridad de la información, y aseguren la confidencialidad y confiabilidad de la misma (Fernández & Casas, 2017). De acuerdo con Suñagua & Félix (2013) si se desea realizar una Evaluación a la Seguridad de la Información, se debe contar con el apoyo y conciencia de la dirección, del personal administrativo y ejecutivo de la empresa y a la vez poseer de una visión estratégica de negocio a corto, mediano y largo plazo que permita la aplicación de modelos de seguridad empresarial y ciclos de seguridad.

Para finalizar, los marcos de referencia COBIT y COSO como ayuda para el trabajo, pueden ser considerados como un elemento de control en la empresa, ya que todo el desarrollo tecnológico debe regirse bajo un control interno informático y evidentemente al descubrimiento de sistemas de controles recientes, administración de los recursos, gestión de TI y sistemas informáticos (Rodríguez, 2004). Al investigar y analizar casos en diferentes empresas se puede llegar a la conclusión de que es necesario generar e implementar políticas, evaluar los procesos informáticos, emplear objetivos, metas y procedimientos de control que ayuden a mejorar la eficiencia y eficacia del sistema (Comas et al., 2014)

1.1.3.2 Justificación práctica

En la actualidad la tecnología ha sido un recurso fundamental para el desarrollo, mantenimiento, optimización y mejora de procesos en las empresas, por consiguiente, la implementación de un sistema informático ayuda a almacenar y procesar información relevante, considerándose como una herramienta eficaz para intercambiar información y construir redes informáticas.

Considerando la relevancia práctica que tiene este trabajo, al representar un tema de gran interés abarcando una revisión y evaluación a los procesos informáticos en los sistemas informatizados se validará la eficiencia de los controles que aplica la empresa en cuanto al uso de las Tecnologías de información y la seguridad de la información. Detectando posibles amenazas, vulnerabilidades, riesgos que pueden afectar la disponibilidad, confidencialidad e integridad de la información, que comprende el sistema de información entre las áreas de contabilidad, producto terminado y ventas debido a que existe una estrecha comunicación y relación de actividades, por una parte

contabilidad consolidando la información contable, producto terminado por ser realizar un inventario detallado de la mercadería y ventas enfocadas a la generación de utilidades.

El presente trabajo es factible ya que se contará con toda la información necesaria, y la aplicación práctica de la ejecución a los procesos informáticos servirán como herramienta para que la gerencia tome decisiones en cuanto a la salvaguarda de la información que maneja y la aplicación de controles eficientes que permitan mantener datos reales en cuanto a su sistema de información. La Auditoría de sistemas, Tecnologías de la Información y Comunicación, Metodologías de la investigación, y la Administración son áreas que engloban al tema.

La elaboración del estudio fortalece el aprendizaje por lo que podrá ser beneficioso para el entorno laboral y académico, realizar esta ejecución aporta a la ciencia de la auditoría la implementación de principios metodológicos y teóricos para la revisión, ejecución y control de procesos y sistemas, aportando así a la tecnología y al ámbito profesional para futuros trabajos.

1.1.4 Objetivos

1.1.4.1 Objetivo general

- Ejecutar los procesos informáticos en la empresa D´Christian Maryuri de la ciudad de Ambato evaluando a través de marcos de referencia la gestión de riegos y niveles de capacidad para la comprobación de la fiabilidad de la información.

1.1.4.2 Objetivos específicos

- Identificar los activos de información que dispone la empresa en las áreas de contabilidad, producto terminado y ventas para la detección de amenazas, vulnerabilidades y riesgos.
- Delimitar el nivel de riesgo mediante la utilización de matrices aplicados a los procesos informatizados en las actividades de la empresa considerando los componentes y principios del COSO ERM 2017.
- Emplear la metodología COBIT 2019 para la determinación del nivel de capacidad de los procesos informáticos alineados a los objetivos de gobierno y gestión de TI.

1.2 Revisión de la literatura

1.2.1 La calidad de los procesos informáticos y la orientación estratégica en las empresas

Actualmente existen varias instituciones o empresas que carecen de una metodología correcta que ayude a llevar un control en los procesos informáticos, puesto que las mismas no son aptos para alcanzar metas u objetivos institucionales. De acuerdo con Martínez & Peralta (2014) el proponer estrategias que ayuden en el desarrollo de proyectos y programas permite medir el desempeño de los procesos en las organizaciones que generan valor para la investigación, el desarrollo y la tecnología. La calidad del software deberá cumplir con los estándares de funcionalidad, requerimientos y necesidades de la empresa, para así poder definir que parámetros o indicadores de calidad pueden ser medidos.

Considerando que el entorno donde la empresa desarrolla sus actividades cada vez es más complejo y competitivo, para su supervivencia y crecimiento organizacional, la información deberá ser considera como elemento clave para la gestión (Trasobares, 2003). Al mejorar la sistematización de los elementos estructurales que componen la empresa, el uso eficiente de los recursos y un máximo rendimiento mejorarán la productividad y competitividad de la empresa.

1.2.2 Teoría de sistemas

La Teoría de Sistemas se comprende como un todo, ya que trata de encontrar propiedades que sean comunes en un sistema, constituyéndose en un mecanismo que integra varios elementos, permite comprender como las organizaciones se relacionan formando uno solo, y a la vez puede ser utilizada en cualquiera ámbito de las ciencias sociales. Cabe recalar que esta teoría busca generar un pensamiento sistemático por lo que ha contribuido dentro de la informática al desarrollo de teorías como: la de información, la dinámica de sistemas y cibernética. Como lo menciona Zubenko et al (2001) las propiedades informáticas son algunas de las diferentes propiedades de la materia, al organizarse de diferentes modos estás realizan alguna función, por lo que se puede decir que esas propiedades están organizadas en forma de un sistema. Enfocándose así a la Teoría General de Sistemas a la hora de dividir otros tipos de sistemas y subtipos como: sistemas de ayuda, de computación, operativos, de

programación, entre otros. Como lo menciona Tamayo (1999) esta teoría fue presentada por Ludwig Von Bertalanffy como un movimiento científico importante, y según el autor enfatiza que esta teoría formula principios básicos que hacen posible agrupar el conocimiento sobre todos los sistemas vivos y no vivos.

1.2.3 Conceptualización

1.2.3.1 Auditoría

Como bien afirma Biler (2017) la auditoría es el campo más avanzado de la ciencia contable, esta revisa las cuentas de una empresa u organización, siendo su fin el investigar si cumplen con las disposiciones y directrices estipuladas, para así revisar si están fueron implementadas con eficacia. Con relación a lo anterior se podría decir que la Auditoría emite un diagnóstico a los procedimientos de una entidad, evalúa los riesgos que puedan existir en la misma y ayuda a la toma de decisiones.

Según Montilla & Herrera (2006) la auditoría es una práctica de interés económico y social, que establece varias relaciones de distinta índole entre agentes económicos, debido a la confianza que se deposita en el trabajo de los contadores cuando otorgan una garantía personal, involucrando una investigación laboral denominada auditoría.

1.2.3.2 Auditoría informática

La Auditoría Informática comprende una evaluación a los procesos informáticos de una empresa. Como lo afirma Arias (2010) la auditoría informática incorpora un diagnóstico, evaluación y estudio del marco de TI como: el hardware, software, sistemas, redes, entre otras, tomando en consideración marcos de referencia, estándares y normas, que hacen énfasis en la mejor forma de gestionar.

Desde el punto de vista de Ramírez & Álvarez (2003) la Auditoría Informática es una herramienta para la gestión de la tecnología de la información en las organizaciones y les permite buscar los recursos para alcanzar los estándares internacionales con su uso adecuado, además muestra si la empresa puede identificar y controlar los riesgos de mayor impacto.

1.2.3.3 Seguridad informática

La seguridad Informática es aquella que protege la infraestructura computacional, anticipa y detecta el uso incompetente de un sistema informático. Para López (2010) es una disciplina que diseña normas, técnicas, procedimientos y métodos que ayudan a conseguir un sistema veraz y seguro. Así mismo para Zambrano & Valencia (2017) la seguridad informática es aquella que mantiene al mínimo los riesgos, vulnerabilidades y amenazas sobre los recursos informáticos y garantiza la continuidad de las actividades que realiza la organización, por medio de estructuras organizacionales técnicas, administrativas, gerenciales o legales.

1.2.3.4 Planificación estratégica informática

En palabras de Martínez & Peralta (2014) la Planificación Estratégica Informática surge de la necesidad y oportunidad del desarrollo de una estrategia competitiva organizacional, esta planificación se puede considerar como un proceso sistematizado que define y desarrolla la estrategia tecnológica de información que deberá mantenerse en la organización (Rodríguez & Martínez, 1998).

Así mismo para Torres (2017) la Planificación Estratégica Informática está basada netamente en una planificación organizacional, donde se realiza un plan que se determina en un documento, reflejando estrategias a seguir por los recursos informáticos que maneja la empresa.

1.2.3.5 Control interno informático

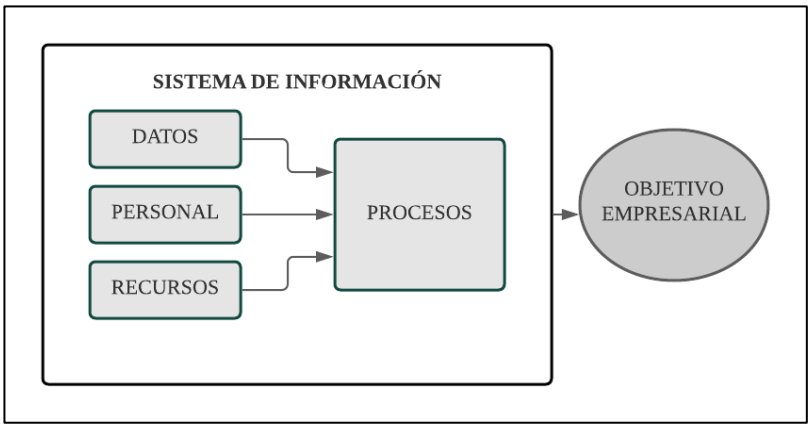
Llevar un Control Interno Informático favorece al control de las operaciones que se realizan a diario en los sistemas de información, en el cual se realiza una evaluación para controlar el cumplimiento de los procedimientos, estándares y normas determinados por la organización. Como lo menciona Rodríguez (2018) este control es aquel que asegura que las medidas obtenidas por parte de los equipos informáticos, sean utilizados de forma óptima y además satisfagan los requerimientos de la organización, protegiendo a su vez los activos de información y asegurando que los datos sean íntegros y fiables.

1.2.3.6 Sistemas de información

Un sistema de información es un conjunto de componentes que administran, recopilan, procesan y almacenan datos de manera más eficiente, para que el personal de la organización interactúe directamente con la información. Como lo afirma Trasobares (2003) cada sistema de información utiliza como materia prima los datos que al ser procesados obtienen un resultado final, el cual se pone a disposición de los diferentes usuarios del sistema, existiendo un proceso de retroalimentación donde se evalúa si la información obtenida cumple con las expectativas o no.

Por otra parte, López (2010) afirma que un SI es un conjunto de elementos que se organizan, relacionan y coordinan entre sí, con el fin de facilitar el funcionamiento de la empresa y favorecer al cumplimiento de sus objetivos institucionales.

Gráfico No. 5 Sistema de información



Fuente: López (2010)
Elaborado por: Vargas (2021)

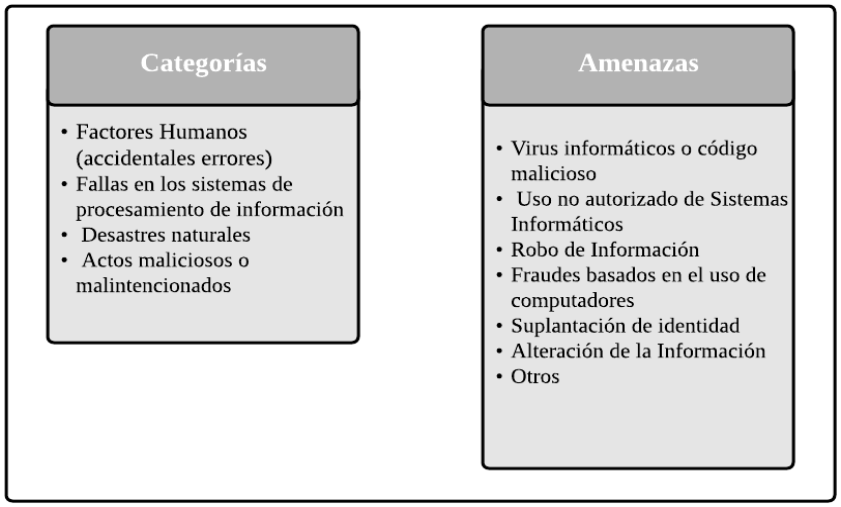
1.2.3.7 Seguridad de la información

Según Figueroa et al. (2018) la Información de la Seguridad se encarga de proporcionar una evaluación a los riesgos y amenazas, es considerada como una disciplina y a su vez realiza un plan de acción y adecuación que ayuda a la minimización de riesgos, respetando las buenas prácticas que garanticen la seguridad, la integridad y la disponibilidad de la gestión de la información de activos.

1.2.3.8 Amenazas de la información

De acuerdo con Figueroa et al. (2018) se pueden agrupar las amenazas de la información en cuatro categorías.

Gráfico No. 6 Amenazas de la información



Fuente: Figueroa et al. (2018)

Elaborado por: Vargas (2021)

1.2.3.9 Tecnologías de información y comunicación

Las Tecnologías de Información y Comunicación (TIC) es un implemento que ayuda en el proceso, control y difusión de la información, facilitando el acceso rápido y fácil a la misma, por lo que se considera un elemento esencial para las organizaciones y la sociedad. Sánchez (2008), expresa que las TIC son las tecnologías que gestionan y transforman la información, junto con el uso de ordenadores y programas permiten crear, modificar, almacenar, proteger y recuperar esa información.

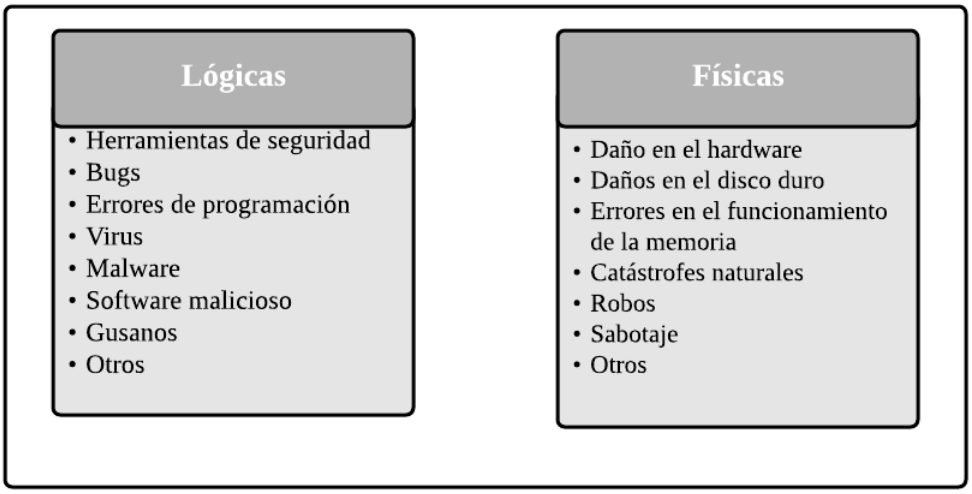
Del mismo modo Cruz et al. (2019) afirma que las TIC se basan en los avances científicos producidos en el campo de la información y de las telecomunicaciones, que son esenciales para el acceso de la tecnología a la producción, interacción, procesamiento y comunicación de la información.

1.2.3.10 Amenazas informáticas

Para Ballesteros et al. (2010) las amenazas se definen como situaciones que surgen del entorno, se consideran un riesgo significativo y pueden amenazar contra el prestigio de una organización**.** En efecto, una amenaza es cualquier situación o evento que pueda

afectar la capacidad de una organización o persona para realizar sus actividades, impactando directamente a la información o los sistemas que la procesan (Tarazona & Cesar, 2007).

Gráfico No. 7 Amenazas informáticas



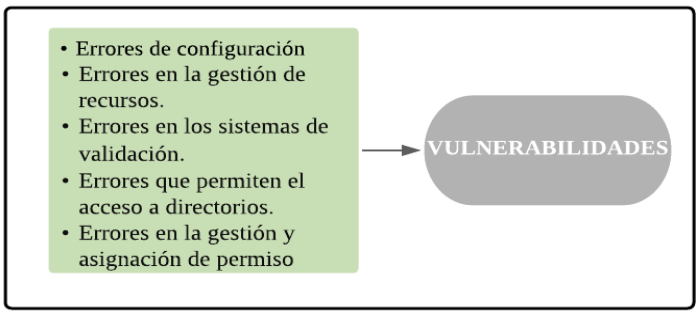
Fuente: Tarazona & Cesar (2007)

Elaborado por: Vargas (2021)

1.2.3.11 Vulnerabilidades informáticas

La vulnerabilidad se podría definir como algo que implica fragilidad, debilidad o amenaza que a su vez puede causar un daño físico o moral. Según Tarazona & Cesar (2007) las vulnerabilidades informáticas son un punto débil de la tecnología o de los procesos de la información, por lo que se consideran características del sistema de información o de la infraestructura que los contiene. Dando a entender que es un riesgo para la seguridad de los datos, ya que al ser vulnerable podría causar que un atacante ponga en peligro la integridad y confidencialidad de la información.

Gráfico No. 8 Vulnerabilidades informáticas



Fuente: Tarazona & Cesar (2007)

Elaborado por: Vargas (2021)

1.2.3.12 Riesgos informáticos

Un riesgo es considerado como la probabilidad de que una amenaza ocurra, existiendo algún daño o peligro que pueda ser perjudicial para la información. Como lo menciona Hernández et al. (2019) los riesgos informáticos comprende toda aquella amenaza y vulnerabilidad de la seguridad que puede afectar a la organización en todos los aspectos, las consecuencias pueden ser importantes con respecto a la información que se maneja.

1.2.3.13 Marco de referencia COBIT

El marco de Referencia COBIT es considerado como apto para toda empresa, un marco para el gobierno y la gestión de la TI e identifica que componentes ayudan a construir y mantener un sistema de gobierno que se acople a las necesidades de la organización, así mismo engloba asuntos de gestión de gobierno mediante la agrupación de los objetivos de gobierno y de gestión administrados con los niveles de capacidad requeridas. (ISACA, 2018).

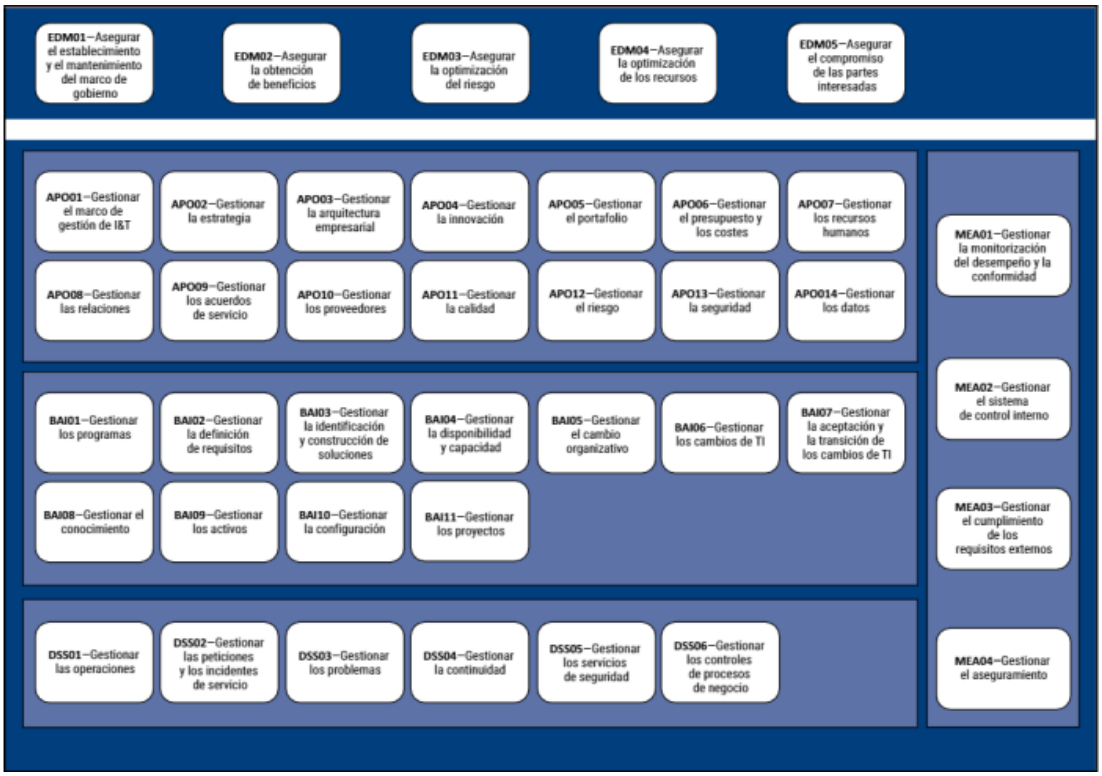
1.2.3.13.1 COBIT

Según Cobit proporciona un marco de trabajo integral para contribuir a las organizaciones alcance de sus objetivos de gestión de TI y gobierno, es decir, facilita a que la empresa cree un valor optimo a partir de IT al equilibrar la generación de ganancias, optimización de los riesgos y el uso de recursos. Este marco permite que la TI se ejecute y se administre de manera integral para toda la empresa, dirigiéndola de principio a fin, tomando en cuenta los intereses relacionados con TI de las partes interesadas internas y externas (ISACA, 2012).

1.2.3.13.2 Modelo de referencia de procesos

Para ISACA (2018) el modelo de referencia de procesos de COBIT desglosa los procesos de gestión y gobierno de TI en dos dominios de procesos: Gobierno y Gestión.

Gráfico No. 9 Modelo de referencia de procesos de COBIT

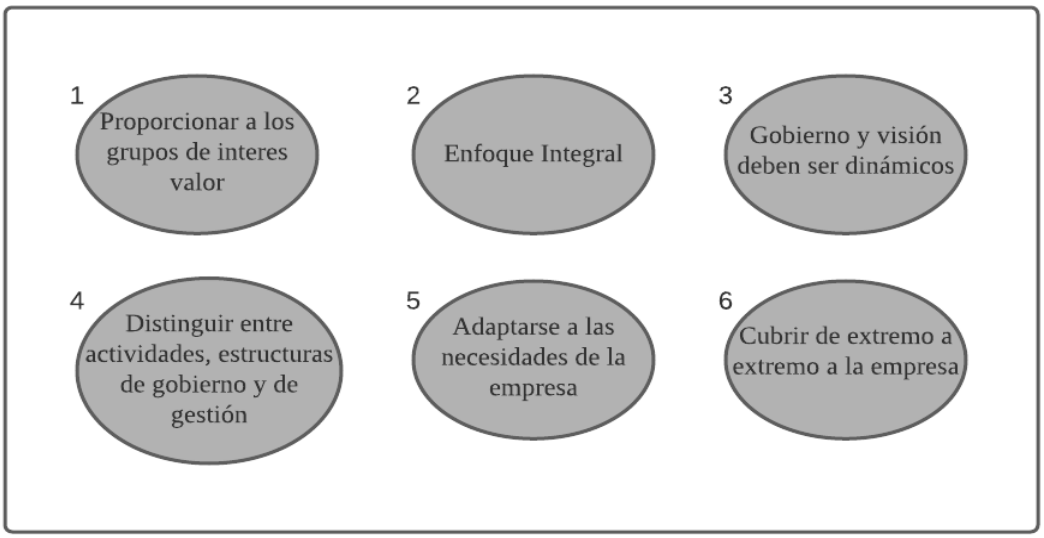


Fuente: ISACA, Marco de referencia COBIT 2019: Modelo de Referencia de los procesos de COBIT 2019 (2018)

1.2.3.13.3 Principios para un sistema de gobierno

Para ISACA (2018) los seis principios de un sistema de gobierno son:

Gráfico No. 10 Principios del sistema COBIT



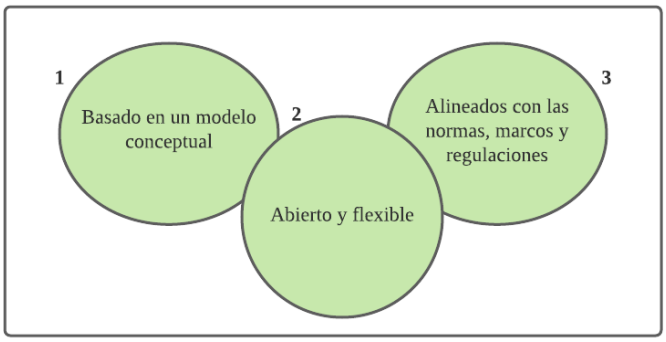
Fuente: ISACA, Marco de referencia COBIT 2019: Principios del sistema COBIT 2019 (2018)

Elaborado por: Vargas **(**2021)

1.2.3.13.4 Principios para un marco de gestión

Para ISACA (2018) los tres principios para un marco de gestión son:

Gráfico No. 11 Principios del marco de gestión COBIT



Fuente: ISACA, Marco de referencia COBIT 2019: Principios del Marco de Gestión 2019 (2018)
Elaborado por: Vargas **(**2021)

1.2.3.14 Marco de Referencia de control interno COSO ERM

Para Sánchez (2015) COSO ERM es un proceso constante el cual debe ser llevado a cabo en todos los niveles de la organización por el personal, afirma que no solo es una combinación de políticas, encuestas o formularios, sino de involucrar a toda la empresa en aquellos niveles con el fin de identificar posible eventos que puedan afectar a la organización.

1.2.3.14.1 Creación de valor

Según Roa et al. (2017) para crear valor en los grupos de interés es necesario desarrollar un Mapa de Valor que representa la relación entre el valor para los accionistas y el desempeño comercial, puesto que ayuda a planificar, estructurar, argumentar y priorizar las oportunidades de mejora, lo que resulta un mayor valor en el crecimiento de los ingresos, el desempeño, el margen de utilidad, entre otros.

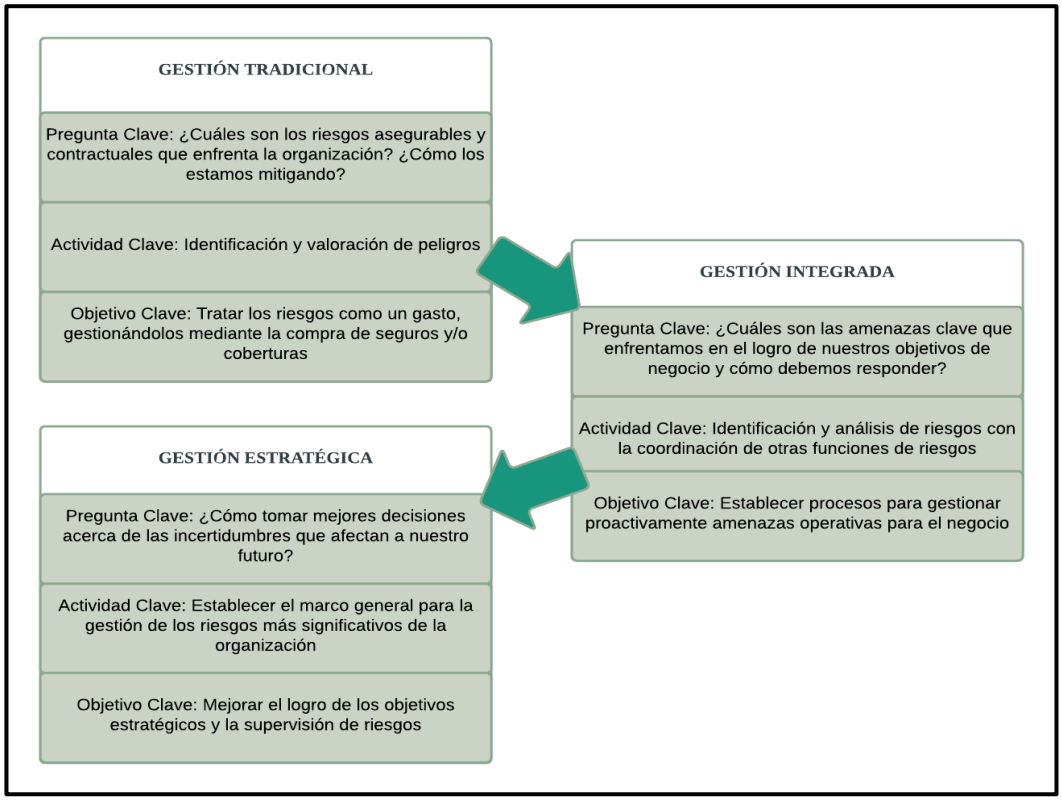
Gráfico No. 12 Valor para el accionista

Fuente: Roa et al. (2017)
Elaborado por: Roa et al. (2017)

1.2.3.14.2 Gestión de riesgos

El COSO ERM es una herramienta de apoyo para el proceso de gestión de riesgos, permite a los administradores de las empresas operar de manera más efectiva en un entorno libre de riesgos, aumentando la capacidad para ajustar el nivel de riesgo, unificar el crecimiento y rendimiento con mejores decisiones de respuesta al riesgo, minimizando pérdidas, e identificando y administrando estos riesgos y la racionalidad del uso de recursos (Sánchez, 2015).

Gráfico No. 13 Evolución de la gestión de riesgos



Fuente: Roa et al. (2017)

Elaborado por: Vargas (2021)

1.2.3.14.3 Gestión de riesgos empresariales y sus componentes

El Marco de Gestión de Riesgos Empresariales explica la importancia de la gestión de riesgos en la planificación estratégica y la integra con toda la organización, ya que el riesgo incide en las estrategias y el desempeño de todas las áreas.

1.2.3.14.4 Componentes

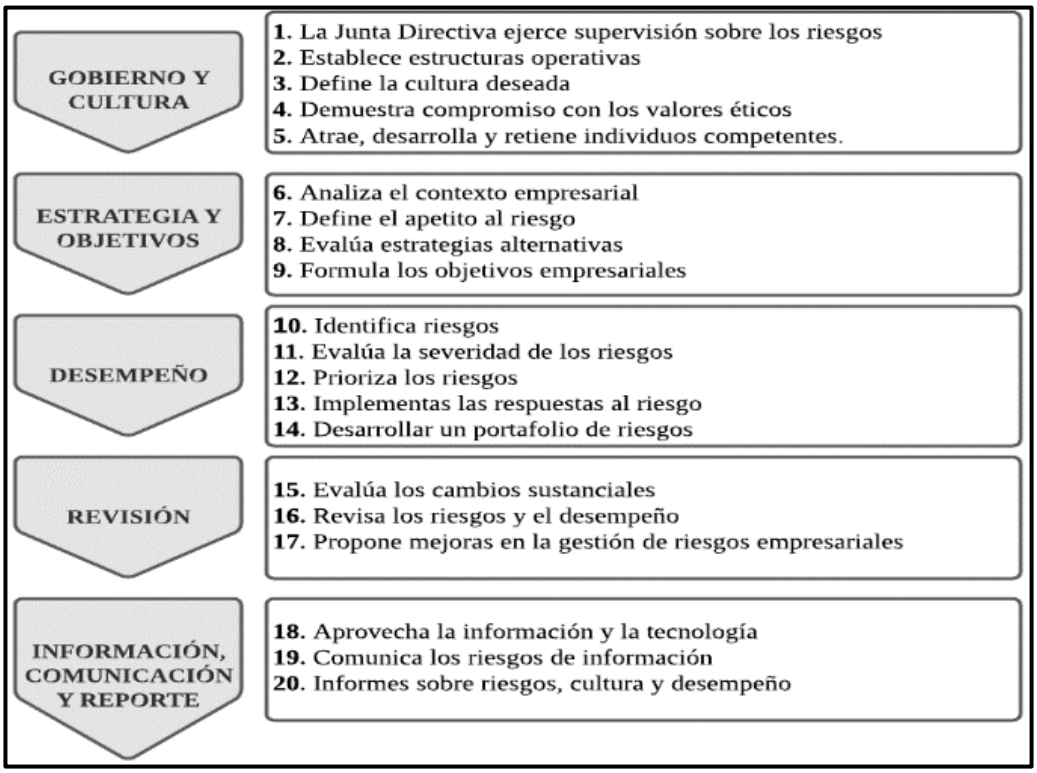
Gráfico No. 14 Componentes del COSO ERM

Fuente: Roa et al. (2017)

Elaborado por: Vargas (2021)

1.2.3.14.5 Principios

Gráfico No. 15 Evolución de la gestión de riesgos



Fuente: Roa et al. (2017)

Elaborado por: Vargas (2021)

CAPÍTULO II

METODOLOGÍA

2.1 Descripción de la metodología

2.1.1 Nivel y tipo de investigación

2.1.1.1 Nivel descriptivo

En palabras de Grajales (2000) el nivel descriptivo busca ampliar una representación firme de las variables estudiadas a partir de sus características, al medir estas variables se especifican las propiedades del estudio dándole un mayor énfasis al mismo. Se aplico este nivel para el diseño de la investigación, ya que en el estudio se analizó cada de una de las variables tomando en cuenta cada una de sus características de manera independiente, mediante un enfoque cualitativo con el fin interpretar como el personal actúa frente a la ejecución de los procesos. La modalidad básica de investigación a utilizar será la de campo debido a que la investigación se realizará en las instalaciones, y se complementará con una investigación bibliográfica.

La información se obtendrá de fuentes primarias en las que se recolectarán directamente de la empresa por medio de entrevistas y listas de control al personal encargado de las áreas de aplicación. Así mismo se trabajará con fuentes secundarias tomadas de investigaciones realizadas como artículos científicos, repositorios académicos enfocados al tema, libros, base de datos digitales y fuentes de información como el internet y las bibliotecas virtuales, contribuyendo a la fundamentación del marco teórico.

2.1.1.2. Tipo observacional o no experimental

Para Veiga & Zimmermann (2008) los estudios observacionales tienen como objetivo describir un fenómeno en una población estudiada y comprender cómo se distribuyen en la misma, por lo que el investigador no interviene de manera directa, ya que solo se limita a estudiar y medir el fenómeno o caso en estudio. Se aplico esta investigación para observar datos anteriores de la organización que son relevantes para el estudio, con el fin de ver que decisiones ha tomado la empresa y analizar el efecto que han causado las mismas, mediante el análisis de los procesos informáticos sin intención de

establecer o intervenir en dichos procesos, así mismo se trabajó con una investigación retrospectiva y transversal.

2.1.2 Unidad de análisis

Para el proyecto integrador se ha considerado como unidad de análisis a la empresa D'Christian Maryuri del cantón Ambato, dedicada a la producción y comercialización de ropa interior, cuyo sistema de información se basa en los procesos informáticos del software contable que utiliza la entidad denominada FENIX para la sistematización contable. Se considera ejecutar una evaluación a los procesos informáticos como un mecanismo de ayuda que permita observar el modo de trabajo que tiene su sistema informatizado e identificar si es necesario realizar mejoras a los procedimientos del registro, actualización, almacenamiento y salida de datos a través de la emisión de reportes y el seguimiento al proceso contable de forma automatizada.

Se procedió a identificar los activos de información para la detección de ciertas vulnerabilidades, amenazas y riesgos a los que están expuestos, de igual manera se elaboró la matriz de riesgo a las áreas de contabilidad, producto terminado y venta. En cuanto a los procesos se comprobó la inexistencia de políticas, normas o procedimientos que ayudan a salvaguardar la información que se maneja en cada proceso. Puesto que se dispone de un bajo nivel de capacidad y control se ejecutó a través de COSO ERM 2017 y COBIT 2019 una revisión y administración a los procesos informáticos de la empresa con el fin de determinar el nivel de capacidad de los mismos.

2.1.3 Fuentes y técnicas de recolección de información

Fuentes de información primaria

La información fue solicitada a los departamentos de informática, producto terminado y ventas debido a que son las principales áreas que manejan y conocen el sistema informático, por ende, las personas entrevistadas fueron tres, además se aplicó una lista de control para revisar los procesos implementados que se llevan para la administración de los activos de información.

Entrevistas

La entrevista fue realizada en diciembre del 2021, mediante un guion de entrevista, cada una se aplicó a través de una serie de preguntas enfocadas a la evaluación informática, fueron efectuadas a cuatros trabajadores quienes comprenden y manejan el sistema, con el fin de recopilar información y conocer como esta lleva el control, la seguridad y cuidado del mismo.

Guion de entrevista. - Se realizaron 15 preguntas, con un tiempo estimado de 10 minutos cada una.

Tabla No. 2 Preguntas de la entrevista

PREGUNTAS	CATEGORÍA
¿Cómo considera usted la forma en que actualmente se maneja la información en la empresa?	***Ambiente de control***
¿Qué aspectos considera más vulnerables en el proceso informático que utiliza la empresa?	
¿La empresa ha implementado alguna metodología para la evaluación de procesos informáticos?	***Evaluación de riesgos***
¿Existen deficiencias o errores al momento de manejar los datos e incluirlos al sistema contable?	
¿La empresa tiene procedimientos para la gestión de la seguridad de la información en los equipos informáticos y dispositivos?	***Actividades de control***
¿Cuáles son los controles que la empresa aplica en los procesos informáticos?	
¿Cómo es el proceso de comunicación que existe entre los departamentos que manejan el sistema informático?	
¿Existe un manual de procedimientos para la gestión de la información?	
¿La empresa maneja perfiles de usuarios para el sistema contable?	
¿Cuáles son los procesos que considera medulares en cuanto a manejo de información?	***Información y comunicación***
¿Qué reportes genera el sistema actual y cómo se utilizan?	
¿Los reportes que se emiten desde el sistema informático son correctos o tienen alguna deficiencia?	
¿Con que frecuencia se da soporte y actualización al sistema informático?	***Soporte y mantenimiento***
¿Con que frecuencia se hacen correcciones a los registros en el sistema informatizado?	
¿Se realiza una revisión frecuentemente a todos los equipos de cómputo con el fin de detectar si existe algún virus o software malicioso? ¿Cada que tiempo?	

Fuente: García & Gavilanes (2015)

Elaborado por: Vargas (2021)

Observación

La Observación fue aplicada en diciembre del 2021, mediante una lista de control (Check-list), con el fin de controlar, verificar y examinar aspectos importantes dentro de los procesos informáticos, y a su vez analizar que componentes pueden influir negativamente en los mismos.

Tabla No. 3 Check list preguntas para la gestión de riesgos

ASPECTO EVALUADO	CATEGORÍA
¿Se realizan reuniones con el fin de actualizar las prácticas de gestión de riesgos?	***Gobierno y Cultura***
¿Existe una asignación de responsabilidades para supervisión y control continuo de los procesos dentro de la empresa?	
¿Cuándo se toman decisiones dentro de la empresa existe un responsable que las notifique mediante procesos pertinentes?	
¿Existe un plan de acción para mitigar los riesgos de la infraestructura tecnológica de forma segura?	
¿Existen normas, leyes y reglamentos que guíen los procesos dentro de la empresa?	
¿Existen políticas y procedimientos internos para los procesos dentro de la empresa?	
¿La entidad tiene prácticas de gestión de riesgos?	
¿El software que se utiliza cumple con los estándares de funcionalidad, requerimientos y necesidades de la empresa?	
¿La persona encargada de la supervisión y control de los procesos informáticos es independiente a la persona que los administra?	
¿Se realizan actividades de supervisión continuas sobre los riesgos existentes?	
¿La organización ha definido políticas de la seguridad de la información?	
¿Las políticas de seguridad están debidamente socializadas con el personal de la empresa?	
¿Existen normas de control interno donde se garantice la protección de los recursos para su disponibilidad e integridad?	
¿Existe un inventario de todos los activos asociados a las instalaciones de procesamiento de información?	
¿Se ha implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	

¿Se han establecido competencias habilidades y conocimientos necesarios para cada puesto de trabajo?	***Gobierno y Cultura***
¿Se han cumplido con los objetivos planteados en la empresa?	
¿Se realizan reuniones periódicas con todo el personal para identificar nuevos riesgos?	
¿Se definen indicadores para identificar situaciones y tendencias relacionadas a los estándares de conducta de la organización, incluyendo a los proveedores y clientes?	
¿Se cumple con los plazos acordados para cada uno de los procesos informáticos?	
¿Se toma en cuenta la opinión del personal para la toma de decisiones dentro de cada proceso?	
¿Existe algún responsable de orientar la ruta a seguir cuando existen dudas en los procesos informáticos??	
¿Se puede cometer algún error sin que incida en forma crítica dentro de los procesos?	
¿La cantidad de información que abarca cada uno de los procesos es razonable?	
¿Existe un responsable del control de los procesos informáticos?	
¿Se ha definido quien es el responsable de los activos de información?	
¿La empresa cuenta con una misión dentro de su plan estratégico?	***Estrategia y Objetivos***
¿Se ha definido la visión dentro de la empresa?	
¿La empresa ha definido valores institucionales?	
¿Existen canales de comunicación para informar sobre el plan estratégico que mantiene la empresa?	
¿Se tiene identificado los riesgos dentro de cada área que maneja procesos informáticos?	
¿Se han establecido alternativas para gestionar los riesgos?	
¿Se actualizan en forma periódica las estrategias establecidas?	
¿Se han establecido estrategias alternativas para el logro de los objetivos?	
¿La empresa cuenta con un procedimiento para identificar riesgos potenciales en los procesos informáticos que desarrollan?	***Desempeño***
¿Se han encontrado errores en el sistema contable de la empresa? Especifique cuales en la casilla de observaciones	
¿Existen procedimientos establecidos que aseguren el cumplimiento de las leyes y regulaciones que conciernen al manejo de los recursos de la empresa?	

¿El riesgo de fraude o robo de datos es evaluado en los diferentes procesos de la empresa?	***Desempeño***
¿Se detecta y previene la fuga de información, perdida de datos y las amenazas e intrusiones a nivel del software?	
¿Existen controles en el manejo del sistema contable para el ingreso de las transacciones en el sistema?	
¿Se realiza una evaluación de los riesgos que pueden afectar la infraestructura tecnológica mediante la utilización de una metodología?	
¿Se monitorea el plan de acción en contra de los riesgos de la infraestructura tecnológica?	
¿La empresa tiene medidas de protección física para prevenir desastres naturales, ataques maliciosos o accidentes?	
¿Existen controles preventivos como claves de acceso, etc.?	
¿Existe algún proceso para asegurar que los empleados y los contratistas hagan devolución de los activos de información de propiedad de la empresa a la terminación de su contrato laboral?	
¿La empresa toma acciones para identificar factores críticos de riesgos potenciales en los procesos?	
¿Se hace uso de una herramienta de gestión de autoevaluación para la identificación de riesgos?	
¿La empresa cuenta con procedimientos establecidos para mitigar riesgos identificados por fraude, robo datos, substracción de información confidencial con el fin de prevenirlos o detectarlos?	
¿Los procedimientos informáticos incluyen actividades de control para evaluar el desempeño?	
¿En el área de contabilidad se monitorea nuevos riegos originados en los reportes financieros?	
¿El área de ventas cuenta con un sistema de información confiable para la obtención de reportes de ventas?	
¿El sistema de información genera reportes confiables en el área de producto terminado?	
¿Los procesos informáticos son evaluados para determinar su impacto en el cumplimiento de la estrategia de la gestión de riesgos?	***Revisión***
¿Se evalúan los cambios relevantes que se hayan producido en el procesamiento de la información?	
¿En los procedimientos informáticos de las áreas de contabilidad, producto terminado y ventas se han identificado riesgos?	

¿Para el seguimiento de las estrategias se evalúa el cumplimiento de los objetivos periódicamente?	***Revisión***
¿Se realizan auditorías en la empresa para medir la razonabilidad de la información en los diferentes procesos?	
¿Existe un marco de referencia para la evaluación sistemática de los riesgos a los que está expuesta la infraestructura tecnológica de la institución?	***Información, comunicación y reporte***
¿La empresa maneja alguna app para la realización de ventas?	
¿Realiza procesos de concientización con los empleados por mantener la seguridad de los activos?	
¿Los activos de información se codifican o etiquetan mediante algún programa?	
¿Se posee bitácoras de fallas detectadas en los equipos?	
¿Se realizan copias de seguridad de la base de datos?	
¿Los usuarios respaldan información en cada uno de sus equipos a cargo?	
¿Se tienen actualizados los inventarios de activos físico y lógicos de la red?	
¿La empresa trabaja con sistema en red?	
¿En el modo en que se establece nuevas políticas y procedimientos son estos comunicados?	
¿Se comunica oportunamente al gerente los riesgos identificados que afectan el cumplimiento de los objetivos empresariales?	
¿Los diferentes departamentos presentan informes sobre riesgos identificados y posibles medidas de mitigación?	

Fuente: Yessenia (2021)

Elaborado por: Vargas (2021)

2.1.4 Procesamiento de la información

La entrevista se aplicó con la finalidad de recabar información esencial para realizar esté proyecto integrador y para contribuir al análisis de los resultados obtenidos en la fase II se lo tabulo mediante el siguiente esquema:

Gráfico No. 16 Estructura

Pregunta	Entrevistado 1 Área Sistemas	Entrevistado 2 Área Producto terminado	Entrevistado 3 Área Ventas	Entrevistado 4 Área Contabilidad	Resumen Conclusión
1. ¿Cómo considera usted la forma en que actualmente se maneja la información en la empresa?					
2. ¿Qué aspectos considera más vulnerables en el proceso informático que utiliza la empresa?					
3. ¿La empresa ha implementado alguna metodología para la evaluación de procesos informáticos?					
4. ¿Existen deficiencias o errores al momento de manejar los datos e incluirlos al sistema contable?					
5. ¿La empresa tiene procedimientos para la gestión de la seguridad de la información en los equipos informáticos y dispositivos?					
6. ¿Cuáles son los controles que la empresa aplica en los procesos informáticos?					
7. ¿Cómo es el proceso de comunicación que existe entre los departamentos que manejan el sistema informático?					
8. ¿Existe un manual de procedimientos para la gestión de la información?					
9. ¿La empresa maneja perfiles de usuarios para el sistema contable?					
10. ¿Cuáles son los procesos que considera medulares en cuanto a manejo de información?					
11. ¿Qué reportes genera el sistema actual y cómo se utilizan?					
12. ¿Los reportes que se emiten desde el sistema informático son correctos o tienen alguna deficiencia?					
13. ¿Con que frecuencia se da soporte y actualización al sistema informático?					
14. ¿Con que frecuencia se hacen correcciones a los registros en el sistema informatizado?					
15. ¿Se realiza una revisión frecuentemente a todos los equipos de cómputo con el fin de detectar si existe algún virus o software malicioso? ¿Cada que tiempo?					

Elaborado por: Vargas (2021)

2.1.5 Fases del desarrollo

Tabla No. 4 Fases del desarrollo

Objetivos específicos	Fase o etapas	Descripción
Identificar los activos de información que dispone la empresa para la detección de amenazas, vulnerabilidades y riesgos.	Preliminar o Diagnóstico	Esta fase tiene el fin de recabar y obtener información concisa y completa sobre los activos de información y qué factores internos podrían afectar a la empresa.
Delimitar el nivel de riesgo mediante la utilización de matrices aplicados a los procesos informatizados en las actividades de la empresa considerando los componentes y principios del COSO ERM 2017.	Administración del riesgo	En esta fase se aplicó una entrevista y un Check-lis para determinar y comprobar cómo evalúa los procesos informáticos mediante los componentes del COSO ERM 2017 y realizar matriz de riesgos para visibilizar de forma fácil cuales son

		los riesgos más relevantes en la empresa,
Emplear la metodología COBIT 2019 para la determinación del nivel de capacidad de los procesos informáticos alineados a los objetivos de gobierno y gestión de TI.	Ejecución de procesos informáticos	Se aplicaron directrices según la Metodología COBIT 2019 para evaluar el nivel de capacidad que la empresa tiene en cuanto a sus procesos informáticos.

Elaborado por: Vargas (2021)

Para el desarrollo de los objetivos planteados en el presente proyecto integrador, el cual tiene como propósito evaluar los procedimientos informáticos, para la Fase I se realizó un levantamiento al inventario de los activos de información para identificar las amenazas y vulnerabilidades que tienen estos activos dentro de la empresa.

Para dar cumplimiento a la Fase II, se analizó la información mediante una matriz de riesgos bajo los componentes dl COSO ERM 2017 a los procesos informáticos con el fin de determinar qué factores afectan o podrían afectar al sistema y controlar los riesgos que puedan efectuarse en cualquier proceso de la empresa, así mismo como apoyo se aplicó la técnica la entrevista y de la observación a través de una lista de chequeo (Check-list) para conocer cómo se evalúa los procesos informáticos, comprobar la fiabilidad de la información y conocer que amenazas, riesgos y vulnerabilidades que se han encontrado en el sistema.

Finalmente, en la Fase III para diagnosticar el nivel de capacidad de los procesos se aplicó las directrices según el marco de referencia COBIT 2019 como guía para las mejores prácticas en la ejecución del sistema informático y la alineación de los objetivos de la empresa con los objetivos de la TI.

CAPÍTULO III

DESARROLLO

3.1 Resultados y discusión

La gestión de la TI es un proceso de verificación, control y medidas de seguridad en el que la empresa debe enfocarse en cuatro elementos principales como:

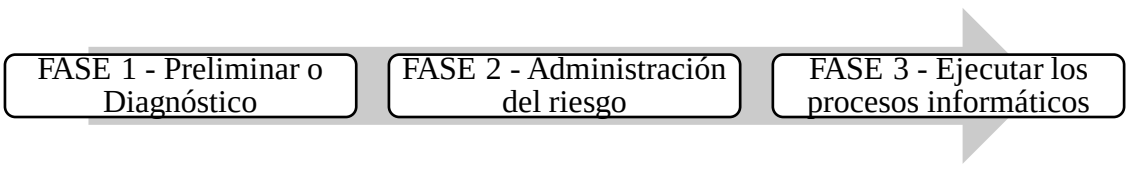
- Software
- Tecnología
- Procesos
- Personal

Para ello, es imprescindible ejecutar una evaluación para comprobar si existen medidas de seguridad informática y controles a los sistemas de información, puesto que se considera a una auditoría de sistemas como aquella que evalúa controles, técnicas o procesos, permitiendo detectar que fallas, riesgos o amenazas pueden existir en cada uno de los elementos mencionados anteriormente.

Por consiguiente, para la empresa D'Christian Maryuri es fundamental ejecutar los procesos informáticos, puesto que no existen controles por parte de la misma, con la evaluación del sistema como ayuda de control, monitoreo y revisión, los procesos y tecnologías de TI se utilizarán de manera más eficiente, lo que asegurara una mejor toma de decisiones.

Para ejecutar los procesos y cumplir con los objetivos del proyecto se implementó una serie de fases que ayudaron a realizar la aplicación práctica de manera ordenada y completa.

Gráfico No. 17 Fases del desarrollo



Elaborado por: Vargas (2021)

3.1.1 Fase 1: Preliminar o diagnostico

Se realiza el levantamiento de la información preliminar o de diagnóstico con el fin de obtener una base para iniciar el proyecto, además de identificar los activos de información esta fase se direcciona también a demostrar el funcionamiento que tiene cada activo para el desempeño de las operaciones de la empresa D´Christian Maryuri.

Como una herramienta para la organización de la empresa se desarrolló el inventario de los activos como necesidad para identificar que amenazas, vulnerabilidades y riesgos tienen cada uno estos. Es fundamental realizar el inventario para gestionar los riesgos de la seguridad de la información y poder establecer medidas o controles que ayuden a determinar que niveles de protección requieren.

.

A continuación, se presenta un inventario de los activos de información de las áreas de contabilidad, producto terminado, ventas y red en general, donde se definieron 19 activos.

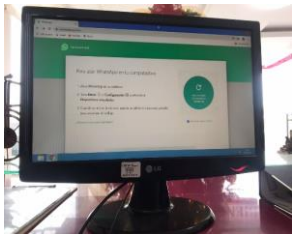
Tabla No. 5 Activos de información

ACTIVOS		FUNCIONAMIENTO	AMENAZAS	VULNERABILIDADES	RIESGOS
ELEMENTOS ESENCIALES					
BASE DE DATOS: INFORMACIÓN RELEVANTE	D´CHRISTIAN MARYURI	Almacena los datos sistemáticamente	Hackers, virus, gusanos, troyanos, ransomware.	-Errores en la gestión y asignación de permisos. -Desbordamiento de búfer. -Datos sensibles sin cifrar.	-Sustracción de información confidencial. -Auditorias débiles. -Exposición de los medios de almacenamiento. -Explotación de vulnerabilidades, bases de Datos mal configuradas.
SERVICIOS INTERNOS					
PÁGINA WEB	https://maryuriropainterior.com/ 	Brinda información sobre la empresa a los clientes.	Perdida de cuentas, robo de cuentas, hackeos, phishing.	Ataques a la base de datos, autenticación fraudulenta.	- Pérdida de autenticación. -Exposición a datos sensibles. -Mala configuración de la seguridad.

EQUIPAMIENTO INFORMÁTICO					
SISTEMA (SOFTWARE): Mikrotik RouterOS	MikroTik	Administrar los recursos que necesita el sistema operativo del computador para manejar los programas y aplicaciones, administra los activos en el sistema operativo mediante códigos.	Spam, malware, virus, datos erróneos.	-Errores en su código o configuración. -Errores de programación -Debilidad en el diseño de protocolos utilizados en las redes. -Políticas de seguridad deficientes e inexistentes.	-Amenazas e intrusiones a nivel de software. -Sabotaje Corporativo. -Ataques externos..
SISTEMA CONTABLE : FENIX	FENIX Sistema Administrativo Contable	Almacenar y procesar datos financieros y contables, automatizando tareas técnicas para mejores resultados.			-Modificación de información. -Suplantación de la entidad del usuario -Uso de claves compartidas
UPS ALMACENAMIENTO DE ENERGIA SMARTONLINE		Almacenar y proporcionar energía eléctrica cuando ocurren apagones.	Sobre cargas eléctricas, desastres naturales, desgaste.	Errores en el regulador de voltaje.	-Altas pérdidas rotacionales. -Problemas de congestión.

SERVER 2012 R2 INTEL XEON HP		Recibir, interpretar y entregar instrucciones.	Virus, gusanos, troyanos, ransomware.	Atacantes remotos pueden ejecutar códigos arbitrarios en el servidor.	-Caídas de la TI, interrupción de los procesos de negocio. -Pérdidas de datos y acceso limitado a los mismos. - Aplicaciones defectuosas o deshabilitadas (para los empleados). - Impedimentos en el acceso a los servicios (para los clientes).
ROUTER		Interconectar computadoras que funcionan en el marco de una red	Caídas, desastres naturales, cortocircuitos, golpes.	-Contraseñas débiles o sencillas. -Agujeros de seguridad. -Errores de configuración -Establecer un cifrado no existente (Wi-Fi sin cifrado) o deficiente (Wi-Fi con protocolo WEP craqueable)	- Secuestro de DNS. -Ataques de denegación de servicio (DoS). -Infección del router por una botnet.
MODEM CNT					-Manipulación de la configuración del equipo -No se cuenta con una red LAN No segmentada.

RELOJ BIOMETRICO BIOTECH			Utilizar huellas dactilares o rostros para realizar un seguimiento del tiempo y de las identidades.	Repudio, puenteo del sistema, daños, deterioro.	-Errores con el lector de huellas. -Fallos en el diseño del sistema. -Denegación del servicio.	-Violación de datos. -Destruccion de información mal intencionada.
ÁREA	**EQUIPO PARA EL PERSONAL (HARDWARE)**					
PRODUCTO TERMINADO	IMPRESORA EPSON		Captura y entrega documentos (copias), escanea.	Cortacircuitos, desastres naturales, golpes.	Errores en la utilización del equipo.	-Acceso y uso no autorizado. -Ser manipuladas por cualquier persona. -Documentos expuestos a ser recogidos.
-PRODUCTO TERMINADO -CONTABILIDAD	TELEFONO GRANDSTREAM		Recepción de llamadas, buzón de voz.	Descargas eléctricas, deterioro, golpes, daños.	Ausencia de políticas sobre el uso correcto del dispositivo.	Mal uso del dispositivo.

-PRODUCTO TERMINADO - VENTAS	COMPUTADOR DE MESA LG		Lleva a cabo procesos de datos en forma automática y a gran velocidad.	Robos, software deficiente, virus, desastres naturales, descargas eléctricas, posibles daños.	-Configuración inadecuada de los sistemas informáticos. -Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática. -Disponibilidad de herramientas que facilitan los ataques.	- Entrada de virus. -Sabotaje de software. -Robo de información. -Delitos informáticos. -Manipulación de la configuración del equipo.
CONTABILIDAD	LAPTOP LENOVO					
CONTABILIDAD	LAPTOP HP					
SOPORTES INFORMÁTICOS						
ALMACENAMIENTO EN LA NUBE			Protege la información relevante por medio de redes de servidores.	Robo de credenciales, ingresos de códigos maliciosos, accesos no autorizados.	Programas que los atacantes pueden usar para infiltrarse en el sistema y robar datos.	-Amenazas en la nube interna. -Fuga de información. -Suplantación identidad.

MEMORIA DE ALMACENAMIENTO DE 6T		Almacenar información relevante.	Robo, virus, perdida.	-Dispositivos que se hacen pasar por otros dispositivos del computador (BadUSB). -Programas que los atacantes pueden usar para infiltrarse en el sistema y robar datos.	-Robo de datos e información sensible (cuentas, contraseñas, emails, etc.). -Extender su red de dispositivos infectados (botnets). -Difusión de información sensible.
SERVICIOS CONTRATADOS A TERCEROS					
SERVICIO DE MANTENIMIENTO DE SOFTWARE		Corrección de errores, mejora el rendimiento, modificación del producto.	Personal inexperto.	Error en la instalación o actualización del sistema.	Problemas en su código o configuración.
MÉDICO PRIVADO		Brindar atención medica al personal de la empresa.	Datos erróneos, fallos en el sistema.	Finalización de contratos.	Inexistencia de controles, tardanza de pagos
PERSONAL					
USUARIOS (CONTADORES, EMPLEADOS, ANALISTAS, OPERADORES)		Llevan a cabo las tareas necesarias para conseguir que la institución funcione.	Hackers que se infiltran en las cuentas del personal	Poca capacitación en el área de trabajo	Pérdida de productividad por poca capacitación, daños en maquinas.

Elaborado por: Vargas (2021)

Considerando que los activos de información, amenazas, vulnerabilidades y riesgos ya están definidos, se procedió a identificar también que controles existen con el objeto de implementar procesos que ayuden a reducir o administrar los riesgos encontrados en cada activo.

Tabla No. 6 Controles de los activos de información

ACTIVO	ÁREA	RESPONSABLE	TIPO DE CONTROL	DESCRIPCIÓN DEL CONTROL
BASE DE DATOS	DATA CENTER	RED	PREVENTIVO	Evitar el acceso a personal no autorizado, para evitar errores o hechos fraudulentos
SISTEMA (SOFTWARE) MIKROTIK	GENERAL	RED	PREVENTIVO	Evitar la implementación de sistemas sin licencias
SISTEMA CONTABLE FENIX	GENERAL	GENERAL	DETECTIVO	Detectar intrusiones a través de un programa que detecta accesos no autorizados al sistema o red.
SERVER 2012 R2 INTEL XEON	DATA CENTER	RED	PREVENTIVO Y DETECTIVO	Realizar actualizaciones de los sistemas operativos frecuentemente
COMPUTADOR DE MESA LG	BODEGA PRODUCTO TERMINADO	ADRIANA CHANGO	PREVENTIVO	Monitorear los equipos con el objeto de identificar inmediatamente cualquier problema
COMPUTADOR DE MESA LG	BODEGA PRODUCTO TERMINADO	SUSANA RAURA	PREVENTIVO	Prevenir el uso y acceso no autorizado al ordenador
LAPTOP LENOVO	CONTABILIDAD	SAUL RUMIPAMBA	PREVENTIVO Y DETECTIVO	Monitorear las operaciones y transacciones, prevenir actos delictivos, evitar problemas potenciales
LAPTOP HP	CONTABILIDAD	JORGE AUCANSHALA		
ALMACENAMIENTO EN LA NUBE	GENERAL	GENERAL	PREVENTIVO	Restringir el acceso a la información aplicaciones, exploradores, autenticación y acceso a la web
USUARIOS (CONTADORES, EMPLEADOS, ANALISTAS, OPERADORES)	GENERAL	GENERAL	PREVENTIVO	Realizar capacitaciones para llevar un mejor control del sistema

Fuente: D´Christian Maryuri

Elaborado por: Vargas (2021)

3.1.1 Fase II: Administración del riesgo

La administración del riesgo se puede considerar como un proceso de ayuda para identificar y medir los riesgos existentes que pueden afectar directamente a los activos de información de la empresa, así como las ganancias, personal, servicios, entre otros. Hay que considerar que es inevitable la existencia de riesgos dentro de la empresa por lo que es inviable el tratar de eliminarlos completamente, pero si los podemos evaluar mediante una matriz de riesgos.

Para esta fase se recogió información mediante una entrevista y un Check list aplicados como instrumentos de recolección.

3.1.1.1 Entrevista

A continuación, se presenta el análisis de los resultados de la entrevista realizada a cada departamento.

Tabla No. 7 Matriz tabulación de datos entrevista

Pregunta	Entrevistado 1 Área Sistemas	Entrevistado 2 Área Producto terminado	Entrevistado 3 Área Ventas	Entrevistado 4 Área Contabilidad	Resumen Conclusión
1. ¿Cómo considera usted la forma en que actualmente se maneja la información en la empresa?	Actualmente se maneja de manera estructurada, en base a diversos dispositivos con los que cuenta la empresa.	Bien, correcta.	Buena	Regular por parte del sistema contable.	Consideran que la forma en que se maneja la información es buena y estructurada.
2. ¿Qué aspectos considera más vulnerables en el proceso informático que utiliza la empresa?	El acceso a la información mediante WIFI en el caso que no se actualice las bases de datos.	No opina	No opina	Cálculo de costos de Producción.	No opinan, mientras dos entrevistados sostienen que el acceso a la información y el cálculo de costos de Producción son los procesos más vulnerables en sus áreas

3. ¿La empresa ha implementado alguna metodología para la evaluación de procesos informáticos?	Por el momento no.	No	No	No	No
4. ¿Existen deficiencias o errores al momento de manejar los datos e incluirlos al sistema contable?	No	Si	Si	Si, por parte del usuario.	Si. Una de las entrevistas sostiene que no existen deficiencias en su área.
5. ¿La empresa tiene procedimientos para la gestión de la seguridad de la información en los equipos informáticos y dispositivos?	No	No	No	Ninguna	No
6. ¿Cuáles son los controles que la empresa aplica en los procesos informáticos?	Los procesos se realizan mediante un software llamado Mikrotik, ese es uno por que existen varios en la empresa.	No tienen controles	No opina	El almacén de datos en la nube es uno de ellos.	Un entrevistado sostiene que no existen controles, mientras que uno afirma que almacenar datos en la nube es uno de ellos. Los demás no opinan con relación a la pregunta.
7. ¿Cómo es el proceso de comunicación que existe entre los departamentos que manejan el sistema informático?	Mediante infraestructura de red.	Por correo o WhatsApp.	Buena	Por medio de e-mail, teléfono y WhatsApp.	Se considera que la comunicación es buena.
8. ¿Existe un manual de procedimientos para la gestión de la información?	Si	No	Si	No, no existe.	Varían las respuestas entre Si y No, por lo que se puede considera que el manual no ha sido dado a conocer o no existe.
9. ¿La empresa maneja perfiles de usuarios para el sistema contable?	Si	Si	Si	Si, para cada usuario del sistema.	Si.
10. ¿Cuáles son los procesos que considera medulares en cuanto a manejo de información?	Los más importantes serian usuarios, contraseñas tanto para el acceso del sistema.	No opina	Los pasos que debemos seguir.	El más importante es el respaldo de información.	Se considera que los más importante son los perfiles de usuarios y el respaldo de la información.

11. ¿Qué reportes genera el sistema actual y cómo se utilizan?		Reporte de inventarios	Reportes de ventas y compras, en esta área.	Información contable, reportes de carteras, inventarios y costos.	Cada reporte es diferente en cada área.
12. ¿Los reportes que se emiten desde el sistema informático son correctos o tienen alguna deficiencia?	Son correctos, pero depende el área.	Si tienen deficiencia	Si son correctos, en cuanto a ventas.	Depende del ingreso de información por los usuarios, pero por lo general son correctos.	Por lo general son correctos en tres áreas, pero una afirma que si tienen deficiencias.
13. ¿Con que frecuencia se da soporte y actualización al sistema informático?	Casi todos los días siempre se le monitorea, pero una vez a la semana.	Cada mes	Mensualmente o cuando nosotros necesitamos.	Depende a las actualizaciones generado desde la empresa proveedora del sistema.	Las respuestas varían, pero se considera que en cada área se realizan soporte.
14. ¿Con que frecuencia se hacen correcciones a los registros en el sistema informatizado?	Siempre	No realizan, solo cuando hay algún error.	No opina	Cada que se realiza una revisión de reportes.	Las respuestas varían.
15. ¿Se realiza una revisión frecuentemente a todos los equipos de cómputo con el fin de detectar si existe algún virus o software malicioso? ¿Cada que tiempo?	Cada tres meses o en el momento en el que los equipos necesitan alguna actualización, ese momento se lo realiza.	Si, cada tres meses	Si, cada tres meses o cuando el equipo necesita actualizaciones	Si, cada tres meses.	Todo de los entrevistados confirman que, si se realiza una revisión, pero en diferentes tiempos.

Fuente: D'Christian Maryuri

Elaborado por: Vargas (2021)

Es importante mencionar que la empresa no trabaja con ninguna metodología para evaluar los procesos informáticos, así mismo no existen controles o procesos para mantener la seguridad de la información, también existe personal que desconoce de varias actividades que debería implementar la empresa, puesto a que sus respuestas son cortas, no opinan o a su vez no responden en relación a la pregunta, se considera que no se tiene un óptimo funcionamiento por parte de la misma. Sin embargo,

podemos observar que la comunicación entre el personal que maneja el sistema es ágil, y que se realizan mantenimiento, soporte y revisión a los equipos periódicamente.

3.1.1.2 Check list

Para complementar la recolección de la información también se aplicó una lista de chequeo donde se obtuvo los siguientes resultados:

Tabla No. 8 Check list

CHECK LIST - COSO ERM 2017				
D´CHRISITAN MARYURI				
N°	**COMPONENTE: GOBIERNO Y CULTURA**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Supervisión de riesgos				
1	¿Se realizan reuniones con el fin de actualizar las prácticas de gestión de riesgos?	☐	☑	
2	¿Se revisan y actualizan periódicamente las decisiones y objetivos estratégicos de la entidad?	☑	☐	Se revisan cada semestre
3	¿Existe una asignación de responsabilidades para supervisión y control continuo de los procesos dentro de la empresa?	☑	☐	
4	¿Cuándo se toman decisiones dentro de la empresa existe un responsable que las notifique mediante procesos pertinentes?	☑	☐	
5	¿Existe un plan de acción para mitigar los riesgos de la infraestructura tecnológica de forma segura?	☑	☐	
PRINCIPIO: Establece estructuras operativas				
6	¿Existen normas, leyes y reglamentos que guíen los procesos dentro de la empresa?	☐	☑	
7	¿Existen políticas y procedimientos internos para los procesos dentro de la empresa?	☑	☐	
8	¿La entidad tiene prácticas de gestión de riesgos?	☐	☑	
9	¿El software que se utiliza cumple con los estándares de funcionalidad, requerimientos y necesidades de la empresa?	☑	☐	
10	¿La persona encargada de la supervisión y control de los procesos informáticos es independiente a la persona que los administra?	☐	☑	Se encarga la misma persona
11	¿Se realizan actividades de supervisión continuas sobre los riesgos existentes?	☐	☑	

12	¿La organización ha definido políticas de la seguridad de la información?	☐	☑	
13	¿Las políticas de seguridad están debidamente socializadas con el personal de la empresa?	☐	☑	No existen políticas
14	¿Existen normas de control interno donde se garantice la protección de los recursos para su disponibilidad e integridad?	☑	☐	
15	¿Existe un inventario de todos los activos asociados a las instalaciones de procesamiento de información?	☑	☐	
16	¿Se ha implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	☐	☑	
PRINCIPIO: Define la cultura deseada				
17	¿Se han establecido competencias habilidades y conocimientos necesarios para cada puesto de trabajo?	☑	☐	
18	¿Se han cumplido con los objetivos planteados en la empresa?	☑	☐	
PRINCIPIO: Demuestra compromiso con los valores claves				
19	¿Se realizan reuniones periódicas con todo el personal para identificar nuevos riesgos?	☐	☑	
20	¿Se definen indicadores para identificar situaciones y tendencias relacionadas a los estándares de conducta de la organización, incluyendo a los proveedores y clientes?	☐	☑	
21	¿Se cumple con los plazos acordados para cada uno de los procesos informáticos?	☑	☐	
22	¿Se toma en cuenta la opinión del personal para la toma de decisiones dentro de cada proceso?	☑	☐	
PRINCIPIO: Atrae, desarrolla y retiene individuos competentes.				
23	¿Existe algún responsable de orientar la ruta a seguir cuando existen dudas en los procesos informáticos?	☑	☐	
24	¿Se puede cometer algún error sin que incida en forma crítica dentro de los procesos?	☐	☑	
25	¿La cantidad de información que abarca cada uno de los procesos es razonable?	☑	☐	
26	¿Existe un responsable del control de los procesos informáticos?	☑	☐	
27	¿Se ha definido quien es el responsable de los activos de información?	☑	☐	
N°	**COMPONENTE: ESTRATEGIA Y OBJETIVOS**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Analiza el contexto empresarial				
28	¿La empresa cuenta con una misión dentro de su plan estratégico?	☑	☐	
29	¿Se ha definido la visión dentro de la empresa?	☑	☐	
30	¿La empresa ha definido valores institucionales?	☑	☐	

31	¿Existen canales de comunicación para informar sobre el plan estratégico que mantiene la empresa?	☑	☐	
PRINCIPIO: Define el apetito al riesgo				
32	¿Se tiene identificado los riesgos dentro de cada área que maneja procesos informáticos?	☐	☑	
PRINCIPIO: Evalúa estrategias alternativas				
33	¿Se han establecido alternativas para gestionar los riesgos?	☐	☑	
34	¿Se actualizan en forma periódica las estrategias establecidas?	☑	☐	
PRINCIPIO: Formula los objetivos empresariales				
35	¿Se han establecido estrategias alternativas para el logro de los objetivos?	☐	☑	
N°	**COMPONENTE: DESEMPEÑO**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Identifica riesgos				
36	¿La empresa cuenta con un procedimiento para identificar riesgos potenciales en los procesos informáticos que desarrollan?	☐	☑	
37	¿Se han encontrado errores en el sistema contable de la empresa? Especifique cuales en la casilla de observaciones	☐	☑	
PRINCIPIO: Evalúa la severidad de los riesgos				
38	¿Existen procedimientos establecidos que aseguren el cumplimiento de las leyes y regulaciones que conciernen al manejo de los recursos de la empresa?	☐	☑	
39	¿El riesgo de fraude o robo de datos es evaluado en los diferentes procesos de la empresa?	☐	☑	
40	¿Se detecta y previene la fuga de información, perdida de datos y las amenazas e intrusiones a nivel del software?	☑	☐	
41	¿Existen controles en el manejo del sistema contable para el ingreso de las transacciones en el sistema?	☑	☐	
42	¿Se realiza una evaluación de los riesgos que pueden afectar la infraestructura tecnológica mediante la utilización de una metodología?	☑	☐	
43	¿Se monitorea el plan de acción en contra de los riesgos de la infraestructura tecnológica?	☐	☑	
44	¿La empresa tiene medidas de protección física para prevenir desastres naturales, ataques maliciosos o accidentes?	☑	☐	
45	¿Existen controles preventivos como claves de acceso, etc.?	☑	☐	
46	¿Existe algún proceso para asegurar que los empleados y los contratistas hagan devolución de los activos de información de propiedad de la empresa a la terminación de su contrato laboral?	☐	☑	
PRINCIPIO: Prioriza los riesgos				
47	¿La empresa toma acciones para identificar factores críticos de riesgos potenciales en los procesos?	☐	☑	

PRINCIPIO: Implementar las respuestas al riesgo				
48	¿Se hace uso de una herramienta de gestión de autoevaluación para la identificación de riesgos?	☐	☑	
49	¿La empresa cuenta con procedimientos establecidos para mitigar riesgos identificados por fraude, robo datos, substracción de información confidencial con el fin de prevenirlos o detectarlos?	☑	☐	
50	¿Los procedimientos informáticos incluyen actividades de control para evaluar el desempeño?	☐	☑	
PRINCIPIO: Desarrollar un portafolio de riesgos				
51	¿En el área de contabilidad se monitorea nuevos riegos originados en los reportes financieros?	☑	☐	
52	¿El área de ventas cuenta con un sistema de información confiable para la obtención de reportes de ventas?	☑	☐	
53	¿El sistema de información genera reportes confiables en el área de producto terminado?		☑	Existen deficiencias en los inventarios
N°	**COMPONENTE: REVISIÓN**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Evalúa los cambios sustanciales				
54	¿Los procesos informáticos son evaluados para determinar su impacto en el cumplimiento de la estrategia de la gestión de riesgos?	☐	☑	
55	¿Se evalúan los cambios relevantes que se hayan producido en el procesamiento de la información?	☐	☑	
PRINCIPIO: Revisa los riesgos y el desempeño				
56	¿En los procedimientos informáticos de las áreas de contabilidad, producto terminado y ventas se han identificado riesgos?	☑	☐	
PRINCIPIO: Propone mejoras en la gestión de riesgos empresariales				
57	¿Para el seguimiento de las estrategias se evalúa el cumplimiento de los objetivos periódicamente?	☑	☐	
58	¿Se realizan auditorías en la empresa para medir la razonabilidad de la información en los diferentes procesos?	☑	☐	
N°	**COMPONENTE: INFORMACIÓN, COMUNICACIÓN Y REPORTE**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Aprovecha la información y la tecnología				
59	¿Existe un marco de referencia para la evaluación sistemática de los riesgos a los que está expuesta la infraestructura tecnológica de la institución?	☐	☑	

60	¿El sistema implementado en la empresa poseen información oportuna y confiable para evitar el doble registro de operaciones?	☑	☐	
61	¿La empresa maneja alguna app para la realización de ventas?	☐	☑	La empresa cuenta una app, pero no la utilizan
62	¿Realiza procesos de concientización con los empleados por mantener la seguridad de los activos?	☐	☑	
63	¿Los activos de información se codifican o etiquetan mediante algún programa?	☑	☐	
64	¿Se posee bitácoras de fallas detectadas en los equipos?	☐	☑	
65	¿Se realizan copias de seguridad de la base de datos?	☑	☐	
66	¿Los usuarios respaldan información en cada uno de sus equipos a cargo?	☑	☐	
67	¿Se tienen actualizados los inventarios de activos físico y lógicos de la red?	☑	☐	
68	¿La empresa trabaja con sistema en red?	☑	☐	
PRINCIPIO: Comunica los riesgos de información				
69	¿En el modo en que se establece nuevas políticas y procedimientos son estos comunicados?	☑	☐	
70	¿Se comunica oportunamente al gerente los riesgos identificados que afectan el cumplimiento de los objetivos empresariales?	☑	☐	
PRINCIPIO: Informes sobre riesgos, cultura y desempeño				
71	¿Los diferentes departamentos presentan informes sobre riesgos identificados y posibles medidas de mitigación?	☑	☐	Solo son avisos, no informes

Fuente: D´Christian Maryuri

Elaborado por: Vargas (2021)

En base a la información obtenida, la lista ha servido para comprobar que componentes del COSO ERM 2017 tienen un mayor riesgo en la empresa. Se realizó una evaluación específica para reconocer el nivel de riesgo y desempeño de cada componente y argumentar por qué se generan ciertas condiciones.

A continuación, se detalla cada componente:

Tabla No. 9 Evaluación específica del componte gobierno y cultura

	Evaluación específica			
	RESPUESTAS		CALIFIC.	
	SI	NO	PT	CT
	COMPONENTE: GOBIERNO Y CULTURA			
	PRINCIPIO: Supervisión de riesgos			
SUBTOTAL	4	1	5	4
	PRINCIPIO: Establece estructuras operativas			
SUBTOTAL	5	7	12	5
	PRINCIPIO: Define la cultura deseada			
SUBTOTAL	2	0	2	2
	PRINCIPIO: Demuestra compromiso con los valores claves			
SUBTOTAL	2	2	4	2
	PRINCIPIO: Atrae, desarrolla y retiene individuos competentes.			
SUBTOTAL	4	1	5	4
TOTAL	17	11	28	17

Elaborado por: Vargas (2021)

Donde se obtuvo lo siguiente:

MAPA DE RIESGO				RIESGO	ENFOQUE
GOBIERNO Y CULTURA				*MODERADO*	*MIXTO-DOBLE PROPÓSITO*
CT	17	NC RI	ENFOQUE	ARGUMENTO PARA EL RIESGO	
PT	28			El componente Gobierno y Cultura es moderado por que no existe un enfoque estructurado dentro de la empresa donde se evalúen, supervisen o tomen en consideración los riesgos existentes que puedan afectar a la empresa y su sistema.	
NC	61%	*MODERADO*			
RI	39%	*MODERADO*	*MIXTO-DOBLE PROPÓSITO*		
RESUMEN DE LA CONDICIÓN ENCONTRADA					
No existe un enfoque estructurado que ayude a identificar, analizar y evaluar los riesgos o amenazas dentro de la empresa.					

Tabla No. 10 Evaluación específica del componte estrategia y objetivos

	Evaluación específica			
	RESPUESTAS		CALIFIC.	
	SI	NO	PT	CT
	COMPONENTE: ESTRATEGIA Y OBJETIVOS			
	PRINCIPIO: Analiza el contexto empresarial			
SUBTOTAL	4	0	4	4
	PRINCIPIO: Define el apetito al riesgo			
SUBTOTAL	0	1	1	0
	PRINCIPIO: Evalúa estrategias alternativas			
SUBTOTAL	1	1	2	1
	PRINCIPIO: Formula los objetivos empresariales			
SUBTOTAL	0	1	1	0
TOTAL	5	3	8	5

Elaborado por: Vargas (2021)

Donde se obtuvo lo siguiente:

MAPA DE RIESGO				RIESGO	ENFOQUE
ESTRATEGIA Y OBJETIVOS				*MODERADO*	*MIXTO-DOBLE PROPÓSITO*
CT	**5**	**RIESGO**	**ENFOQUE**	**ARGUMENTO PARA EL RIESGO**	
PT	8			El componente Estrategia y Objetivos tiene un riesgo moderado debido a que no se identifican riesgos y por ende no se gestionan estos mismos, existen algunas actividades que la empresa no toma encuentra o no las emplea.	
NC	63%	*MODERADO*			
RI	38%	*MODERADO*	*MIXTO-DOBLE PROPÓSITO*		
RESUMEN DE LA CONDICIÓN ENCONTRADA					
No se identifican riesgos potenciales que pueden afectar directamente al funcionamiento de la empresa.					

Tabla No. 11 Evaluación específica del componte desempeño

	Evaluación específica			
	RESPUESTAS		**CALIFIC.**	
	SI	**NO**	**PT**	**CT**
	COMPONENTE: DESEMPEÑO			
	PRINCIPIO: Identifica riesgos			
SUBTOTAL	0	2	2	0
	PRINCIPIO: Evalúa la severidad de los riesgos			
SUBTOTAL	5	4	9	5
	PRINCIPIO: Prioriza los riesgos			
SUBTOTAL	0	1	1	0
	PRINCIPIO: Implementa las respuestas al riesgo			
SUBTOTAL	1	2	3	1
	PRINCIPIO: Desarrollar un portafolio de riesgos			
SUBTOTAL	2	1	3	2
TOTAL	8	10	18	8

Elaborado por: Vargas (2021)

Donde se obtuvo lo siguiente:

MAPA DE RIESGO				RIESGO	ENFOQUE
DESEMPEÑO				*ALTO*	*SUSTANTIVO*
CT	**8**	**RIESGO**	**ENFOQUE**	**ARGUMENTO PARA EL RIESGO**	
PT	18			El componente Desempeño tiene un riesgo alto debido a que existen varios procesos que no son relevantes para la empresa por consiguiente no puede implementar o establecer estrategias sin conocer que riesgos existen.	
NC	44%	*BAJO*			
RI	56%	*ALTO*	*SUSTANTIVO*		
RESUMEN DE LA CONDICIÓN ENCONTRADA					
No se realizan procesos para identificar, evaluar y priorizar riesgos.					

Tabla No. 12 Evaluación específica del componte revisión

	Evaluación específica			
	RESPUESTAS		CALIFIC.	
	SI	NO	PT	CT
	COMPONENTE: REVISIÓN			
	PRINCIPIO: Evalúa los cambios sustanciales			
SUBTOTAL	0	2	2	0
	PRINCIPIO: Revisa los riesgos y el desempeño			
SUBTOTAL	1	0	1	1
	PRINCIPIO: Propone mejoras en la gestión de riesgos empresariales			
SUBTOTAL	2	0	2	2
TOTAL	3	2	5	3

Elaborado por: Vargas (2021)

Donde se obtuvo lo siguiente:

MAPA DE RIESGO				RIESGO	ENFOQUE
REVISIÓN				*MODERADO*	*MIXTO-DOBLE PROPÓSITO*
CT	3	RIESGO	ENFOQUE	ARGUMENTO PARA EL RIESGO	
PT	5			EL componente Revisión tiene un riesgo Moderado debido a que no se evalúan los procesos y cambios importantes que hayan producido al momento de procesar la información.	
NC	60%	*MODERADO*			
RI	40%	*MODERADO*	*MIXTO-DOBLE PROPÓSITO*		
RESUMEN DE LA CONDICIÓN ENCONTRADA					
No se evalúan los cambios sustanciales.					

Tabla No. 13 Evaluación específica del componte información, comunicación y reporte

	Evaluación específica			
	RESPUESTAS		CALIFIC.	
	SI	NO	PT	CT
	COMPONENTE: Información, comunicación y reporte			
	PRINCIPIO: Aprovecha la información y la tecnología			
SUBTOTAL	6	3	9	6
	PRINCIPIO: Comunica los riesgos de información			
SUBTOTAL	2	0	2	2
	PRINCIPIO: Informes sobre riesgos, cultura y desempeño			
SUBTOTAL	1	0	1	1
TOTAL	9	3	12	9

Elaborado por: Vargas (2021)

Donde se obtuvo lo siguiente:

MAPA DE RIESGO				RIESGO	ENFOQUE
INFORMACIÓN, COMUNICACIÓN Y REPORTE				*MODERADO*	*MIXTO-DOBLE PROPÓSITO*
CT	**9**	**RIESGO**	**ENFOQUE**	**ARGUMENTO PARA EL RIESGO**	
PT	12			El componente Información, comunicación y reporte es moderado debido a que la empresa no aprovecha la tecnología al limite y no se implementan marcos de control para la evaluación de riesgos o fallos encontrados en el sistema.	
NC	75%	*MODERADO*			
RI	25%	*MODERADO*	*MIXTO-DOBLE PROPÓSITO*		
RESUMEN DE LA CONDICIÓN ENCONTRADA					
No se aprovecha la información y la tecnología.					

Mediante la ejecución de esta evaluación se observó que todos componentes del COSO ERM 2017 tienen un riesgo moderado a excepción del componte Desempeño el cual su riesgo se considera alto, ya que al analizarlo no se implementa y aplican varias actividades o procesos que contribuyan a prevenir riesgos internos, lo que limita el alcance del sistema al no proporcionar un desempeño para el cumplimiento de los objetivos. Por tanto, se podría decir que no hay una eficiencia empresarial en cuanto a la identificación y gestión de riesgos, ya que al considerar los demás componentes no existe uno que se mantenga bajo.

3.1.1.2.1 Evaluación nivel de confianza y riesgo

1. **Valoración**

$$\mathbf{CP=}\frac{CT}{PT}x100$$

Ponderación Total (P.T.) = 71

Calificación Total (C.T.) = 42

Nivel de Confianza **NC=** CT/PT x 100 = 59,15%

Nivel de Riesgo **R=** 100% - NC% = 40,85%

2. **Determinación de los niveles de riesgo**

NIVEL DE CONFIANZA		
BAJO	MODERADO	ALTO
15%-50%	51% - 75%	76% - 95%
85%-50%	49% - 25%	24% - 5%
ALTO	MODERADO	BAJO
NIVEL DE RIESGO (100-NC)		

3. **Resultado de la evaluación**

Nivel de confianza	MODERADA
Nivel de riesgo	**MODERADO**

Una vez aplicado el Check list a cada componente se obtuvo como resultado que existe un nivel de confianza moderado de 59,15% y un nivel de riesgo moderado de 40,85%, por tanto, se deduce que la empresa D'Christian Maryuri mantiene un control moderado en el desarrollo de sus actividades, cabe recalcar que existen varias disposiciones que no se cumplen en función a los principios que solicita el COSO ERM 2017, por lo que se recomienda cumplir con dichas disposiciones e implementar medidas preventivas para reducir el riesgo, con el fin de mejorar los procesos y que a futuro se puedan evitar daños o consecuencias graves a la empresa.

3.1.2 Matriz de riesgo

La matriz de riesgo como una herramienta de gestión, ayuda a identificar y evaluar los factores de riesgo permitiendo una correcta aplicación de medidas que ayuden a controlarlos.

A continuación, se presenta las escalas utilizadas para evaluar riesgos de los componentes del COSO ERM 2017:

Tabla No. 14 Escala de probabilidad

	PROBABILIDAD	GUÍA
5	Muy alta	La probabilidad de ocurrencia de forma continua y permanente
4	Alta	La probabilidad ocurrencia: una vez al mes
3	Moderada	La probabilidad de ocurrencia: con cierta frecuencia
2	Baja	Insignificante posibilidad de ocurrencia existe casos muy aislados
1	Muy baja	La probabilidad de ocurrencia es excepcional no se conocen de casos similares

Fuente: Yessenia (2021)

Elaborado por: Vargas (2022)

Tabla No. 15 Escala de impacto

	IMPACTO	DESCRIPCIÓN	INTERPRETACIÓN
5	CATASTROFICO	CONSECUENCIAS EMINENTES	Requiere medidas preventivas urgentes. El proyecto no se debe iniciar sin la aplicar medidas de prevención necesarias.
4	IMPACTO MAYOR	DE SUCEDER HABRIAN ALTAS CONSCUENCIAS	Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo.
3	MODERADO	EL EVENTO TRENDIA CONSECUENCIAS PARCIALES	Tomar precauciones mediante la inclusión preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
2	MENOR	SI SUCEDIERA EL ENVENTO EL IMPACTO SERIA BAJO	Existe un impacto bajo, la empresa puede continuar operando, pero posiblemente tenga un impacto en algún proceso, retraso en actividades o errores
1	SIGNIFICANTE	MÍNIMO NO TRENDAN MAYORES CONSECUENCIAS	Se vigilará, aunque no requiere medidas preventivas.

Elaborado por: Vargas (2022)

Tabla No. 16 Escala de riesgo

	RIESGO	DESCRIPCIÓN
5	Extremo	Se exige respuesta y atención inmediata.
4	Alto	Debe presentar la atención apropiada.
3	Medio	Evaluar el riesgo y determinar si las medidas de control implementadas son adecuadas y efectivas
2	Bajo	Administrar mediante procedimientos rutinarios; notificar, supervisar y revisar localmente según sea necesario
1	Leve	Monitoreo constante a las actividades diarias

Fuente: Yessenia (2021)

Elaborado por: Vargas (2022)

Tabla No. 17 Matriz de riesgos

MATRIZ DE RISGOS														
N°	COMPONENTE	PRINCIPIO	ACTIVOS DE INFORMACIÓN VULNERABLES	DESCRIPCIÓN DEL RIESGO	ANÁLISIS					ADM. DE RIESGO			DESCRIPCIÓN DE CONTROL	RESPONSABLE	FRECUENCIA
					PROBABILIDAD	IMPACTO	RIESGO TOTAL	RIESGO ESCALA	NIVEL DE RIESGO	ASUMIDO	ELIMINACION	MITIGACION			
R1	Gobierno y Cultura	Supervisión de riesgos	Usuarios	No se realizan reuniones con el fin de actualizar las prácticas de gestión de riesgos	3	4	12	4	Alto	X			Aplicar prácticas de gestión de riesgos	Jefe de cada departamento	Permanente
R2		Establece estructuras operativas		No se implementan normas, leyes y reglamentos que guíen los procesos dentro de la empresa	4	5	20	5	Extremo	X			Ejecutar los procesos mediante leyes y normas reglamentarias	Gerente General /Administración / Jefe de cada departamento	Permanente
R3				No existen prácticas de gestión de riesgos	4	5	20	5	Extremo	X			Aplicar prácticas de gestión de riesgos	Jefe de cada departamento	Permanente
R4				La persona encargada de la supervisión y control de los procesos informáticos es la misma persona que los administra	2	2	4	2	Bajo		X		Designar a otro usuario la administración de los procesos informáticos	Gerente General	Periódicamente
R5				La organización no ha definido políticas de la seguridad de la información	4	5	20	5	Extremo	X			Establecer políticas de seguridad de la información	Gerente general /Administración	Anual

R6				No se socializan las políticas de seguridad porque no existen	4	5	20	5	Extremo	X			Establecer políticas de seguridad	Gerente general /Administración	Anual
R7				No se ha implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal	3	3	9	3	Medio			X			
R8		Demuestra compromiso con los valores claves		No se realizan reuniones periódicas con todo el personal para identificar nuevos riesgos	3	4	12	2	Bajo			X	Realizar reuniones periódicas con el personal para la identificación de riesgos	Gerente General	Periódicamente
R9				No hay indicadores para identificar situaciones y tendencias relacionadas a los estándares de conducta de la organización, incluyendo a los proveedores y clientes	3	2	6	2	Bajo	X			Definir indicadores que ayuden a identificar estándares de conducta de la organización	Gerente General	Permanente
R10	Estrategia y objetivos	Define el apetito al riesgo	-Usuarios -Almacenamiento en la nube -Base de datos -Software	No se identifica los riesgos dentro de cada área que maneja procesos informáticos	4	5	20	5	Extremo	X			Implementar procesos para la identificación de riesgos en cada una de las áreas que manejan procesos informáticos	Gerente General /Administración / Jefe de cada departamento	Periódicamente
R11		Evalúa estrategias alternativas		No se establecen alternativas para gestionar riesgos	4	5	20	5	Extremo	X			Establecer alternativas o estrategias para gestionar riesgos	Gerente General	Permanente
R12		Formula los objetivos empresariales		No se establecen estrategias alternativas para el logro de los objetivos	4	5	20	5	Extremo	X			Determinar estrategias para alcanzar los objetivos institucionales	Gerente General	Anual
R13	Desempeño	Identifica riesgos	'-Software -Hardware (computador, laptop, server) -Sistemas	La empresa no cuenta con un procedimiento para identificar riesgos potenciales en los procesos informáticos que desarrollan	4	5	20	5	Extremo			X	Establecer procedimientos para identificar riesgos potenciales en los procesos informáticos que lleva toda la empresa	Gerente General	Permanente
R14		Evalúa la severidad de los riesgos		No hay procedimientos establecidos que aseguren el cumplimiento de las leyes y regulaciones que conciernen al manejo de los recursos de la empresa	4	5	20	4	Alto	X			Implementar procedimientos que aseguren el cumplimiento y empleo de leyes y regulaciones competen al manejo de los recursos de la empresa	Gerente General /Administración / Jefe de cada departamento	Permanente

R15				El riesgo de fraude o robo de datos no es evaluado en los diferentes procesos de la empresa	3	5	15	4	Alto			X	Evaluar en todos los procesos riesgos de fraude o robo para mitigarlos	Gerente General	Mensual
R16				No existe un plan de acción en contra de los riesgos de la infraestructura tecnológica	3	4	12	4	Alto	X			Adoptar un plan de acción	Gerente General	Anual
R17				No existen procesos para asegurar que los empleados y los contratistas hagan devolución de los activos de información de propiedad de la empresa a la terminación de su contrato laboral	4	5	20	3	Medio	X			Establecer una política que asegure la devolución de los activos de información	Gerente General	Anual
R18		Prioriza los riesgos		La empresa no toma acciones para identificar factores críticos de riesgos potenciales en los procesos	4	5	20	5	Extremo			X	Tomar acciones para identificar factores críticos en riesgos potenciales	Gerente general /Administración	Periódicamente
R19		Implementa las respuestas al riesgo		No se usan herramientas de gestión de autoevaluación para la identificación de riesgos	4	5	20	5	Extremo			X	Adoptar herramientas de gestión para evaluar riesgos	Jefe de cada departamento	Permanente
R20				No se emplean actividades de control para evaluar el desempeño de los procedimientos informáticos	3	4	12	4	Alto	X			Determinar actividades que ayuden a evaluar el desempeño de los procedimientos informáticos	Gerente general /Administración	Permanente
R21		Desarrollar un portafolio de riesgos		El sistema de información genera reportes inconsistentes en el área de producto terminado	3	4	12	4	Alto			X	Cambiar el sistema por uno que sea seguro y confiable y que se adapte a las necesidades de la empresa	Sistemas	Anual
R22	Revisión	Evalúa los cambios sustanciales	-Base de datos	Los procesos informáticos no son evaluados para determinar su impacto en el cumplimiento de la estrategia de la gestión de riesgos	4	5	20	4	Alto			X	Aplicar prácticas de gestión de riesgos	Gerente general /Administración	Permanente
R23				No se evalúan cambios relevantes que se producen en el procesamiento de la información	3	4	12	3	Medio			X	Identificar y evaluar los cambios que se producen en el procesamiento de la información	Jefe de cada departamento	Periódicamente

R24	Información, comunicación y reporte	Aprovecha la información y la tecnología	-Hardware (computador, laptop, server)	No se cuenta con un marco de referencia para la evaluación sistemática de los riesgos a los que está expuesta la infraestructura tecnológica de la institución	2	2	4	3	Medio	**X**			Aplicar un marco de referencia como una herramienta para la evaluación de riesgos	Gerente general /Administración	Permanente
R25				La empresa cuenta con una app para la realización de venta sin embargo no la utiliza	3	2	6	2	Bajo		**X**		Aprovechar la tecnología y utilizar la app con la que cuenta la empresa	Ventas	Permanente
R26				No se realizan procesos de concientización con los empleados por mantener la seguridad de los activos	3	4	12	3	Medio	**X**			Realizar reuniones o pláticas con los empleados para concientizar sobre el uso de los activos y su seguridad	Gerente general	Trimestral
R27				No se realizan bitácoras de fallas detectadas en los equipos	3	3	9	3	Medio			**X**	Presentar bitácoras sobre fallas detectadas en los equipos por parte de cada departamento	Jefe de cada departamento	Periódicamente

Fuente: Empresa D'Christian Maryuri

Elaborado por: Vargas (2021)

Además de los riesgos en la matriz presentada también se tomó en cuenta los activos de información con el fin de conocer cuáles de estos son los más vulnerables en cada principio, cabe recalcar que estos ya fueron identificados en la primera fase. Como resultado de la matriz podemos observar que de acuerdo a las escalas ya definidas existen riesgos extremos, altos, medianos y bajos.

Con relación a lo anterior, el objetivo de esta evaluación de riesgos es apoyar a la toma de decisiones, en sobre qué riesgos son necesarios tratar y dar prioridad, evaluar los riesgos implica realizar una comparación del nivel de impacto y la probabilidad de ocurrencia de dicho riesgo con el fin de analizar la necesidad del tratamiento.

A continuación, se presenta un mapa de calor donde se identifican los riesgos según su nivel.

Gráfico No. 18 Mapa de calor

MAPA DE CALOR					
PROBABILIDAD	SUPERIOR (5)				
	MAYOR (4)				R2 R3 R5 R6 R10 R11 R12 R13 R14 R 17 R18 R19 R22
	IMPORTANTE (3)		R9 R25	R1 R8 R16 R20 R21 R23 R26	R15
	MENOR (2)		R4 R24		
	INFERIOR (1)				
		SIGNIFICANTE (1)	MENOR (2)	IMPACTO MAYOR (4)	CATASTROFICO (5)
		IMPACTO			

Elaborado por: Vargas (2022)

A través del mapa de calor se identifica los riesgos que tienen mayor impacto de afectación a los procesos y funcionamiento de la empresa. Este mapa se apoya en cinco niveles tanto para la probabilidad de ocurrencia, como para el impacto que pude generar, y están representados por un código de color, en donde el rojo representa un riesgo extremo.

En efecto como se puede observar en el mapa, se han identificado los riesgos con mayor impacto **R2, R3, R5, R6, R10, R11, R12, R13, R14, R17, R18, R19, y R22** (**Tabla No. 16 Matriz de riesgos**), puesto que la mayoría corresponden al componente desempeño se realizó, una comparación con la evaluación específica del mismo dando como resultado que este componente tiene el riesgo más elevado entre todos debido a que, existen varias actividades que no se han aplicado e implementado, por lo que es necesario tomar en cuenta los controles establecidos en la matriz, así como también lo demuestra la entrevista, en donde se observó que el personal no tiene conocimientos de muchas actividades y que no se ha adoptado completamente una cultura de concientización y responsabilidad sobre la importancia de los procesos informáticos en la operatividad de la empresa.

Se recomienda dar prioridad a los riesgos extremos y con mayor impacto, así mismo administrar, gestionar y analizar estos riesgos, con el fin de tomar acciones que ayuden a controlarlos, asumirlos, eliminarlos o mitigarlos según las necesidades de gestión de los riesgos que requiera la empresa.

3.1.3 FASE III: Ejecución de procesos informáticos

Para construir un marco efectivo de gobierno y administración se deben unir lo principios en un enfoque integral que habilite y permite optimizar la tecnología de la información y obtener beneficios de todas las partes interesadas de la organización.

Cabe recalcar que COBIT establece 17 objetivos corporativos para la empresa de COBIT y metas para la TI, que mediante un mapeo entre estas se indica que objetivos son principales y cuales son un apoyo secundario.

Se identifica a “P” como una relación fundamental o principal entre los objetivos y metas.
Se identifica “S” como una relación secundaria, de soporte o apoyo entre las mismas

Tabla No. 18 Objetivos de la empresa de COBIT

OBJETIVOS DE LA EMPRESA DE COBIT				
Dimension del CMI	Objetivo de la Empresa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las Partes Interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Fuente: ISACA, Marco de referencia COBIT 5: Objetivos de la empresa de COBIT (2012)

Elaborado por: Vargas (2022)

Tabla No. 19 Metas de las TI

Metas de las TI		
Dimension del CMI	Objetivo de Información y Tecnología relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio.
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.
	04	Riesgos de negocio relacionados con las TI gestionados.
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.
Cliente	06	Transparencia de los costes, beneficios y riesgos de las TI Cliente.
	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio.
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas Interna.
	09	Agilidad de las TI.
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.
Interna	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y relevante para la toma de decisiones.
	15	Cumplimiento de las políticas internas por parte de las TI Aprendizaje y Crecimiento.
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado.
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio.

Fuente: ISACA, Marco de referencia COBIT 5: Metas de las TI (2012)

Elaborado por: Vargas (2022)

A continuación, se presenta el mapeo de los objetivos corporativos de COBIT con los objetivos de TI:

Tabla No. 20 Mapeo de los objetivos corporativos de COBIT con los objetivos de TI

Mapeando los objetivos corporativos de COBIT con los objetivos de TI																			
			Valor para las Partes Interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Objetivo Relativo a TI			Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01	Alineamiento de TI y estrategia de negocio.	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.				S	P										P		
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.	P	S	S				S	S			S		P			S	S
	04	Riesgos de negocio relacionados con las TI gestionados.			P	S		P	S		S				S		S	S	
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	P	P				S		S		S	S	P		S			S
	06	Transparencia de los costes, beneficios y riesgos de las TI Cliente.	S		S		P				S	P		P					
Objetivo	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas Interna.	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidad de las TI.	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.		P	P				P								P		
	11	Optimización de activos, recursos y capacidades de las TI.	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones.	S	S	S				P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI Aprendizaje y Crecimiento.		S	S												P		
Aprendizaje y Crecimi	16	Personal del negocio y de las TI competente y motivado.	S	S	P			S		S						P			S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio.	S	P				S		P	S		S		S				P

Fuente: ISACA, Marco de referencia COBIT 5: Mapeo de los objetivos de COBIT con los objetivos de TI (2012)
Elaborado por: Vargas (2022)

Este marco define una serie de procesos de gobierno y gestión, en el dónde los procesos de gobierno se enfocan en actividades encaminadas a evaluar, orientar y supervisar opciones estratégicas y optimizar riesgos y recursos. En cambio, los procesos de gestión abarcan prácticas y actividades que cubren varias áreas de la empresa y la TI. Por lo que es necesario presentar un mapeo entre los objetivos relacionados con TI con procesos COBIT.

Tabla No. 21 Mapeo entre los objetivos relacionados con TI en procesos COBIT

Mapeo entre Objetivos relacionados con TI en COBIT 5 con procesos																				
			Objetivos Relacionados con TI																	
			Alineamiento de TI y estrategia de negocio.	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con	Riesgos de negocio relacionados con las TI gestionados.	Realización de beneficios del portafolio de	Transparencia de los costes, beneficios y riesgos	Entrega de servicios de TI de acuerdo a los	Uso adecuado de aplicaciones, información y	Agilidad de las TI.	Seguridad de la información, infraestructura de	Optimización de activos, recursos y capacidades de las	Capacitación y soporte de procesos de	Entrega de Programas que proporcionen	Disponibilidad de información útil y relevante para la	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y	Conocimiento, experiencia e iniciativas para la
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			**Financiera**						**Cliente**		**Interna**							**Aprendizaje y Crecimiento**		
Evaluar, Orientar y Monitorear	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
Alinear, Planificar y Organizar	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			
Construir, Adquirir e Implementar	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		

Fuente: ISACA, Marco de referencia COBIT 5: Mapeo entre los Objetivos relacionados con TI en procesos COBIT (2012)

Elaborado por: Vargas (2022)

Para ejecutar los procesos informáticos y evaluar a cada de una de las actividades de COBIT se estableció un criterio de evaluación donde se definen brechas para cada nivel con el fin de medir estas actividades, así mismo se estableció niveles de capacidad para determinar qué grado de aptitud tiene cada actividad y practica de gobierno.

Tabla No. 22 Criterio de evaluación

CRITERIO DE EVALUACIÓN Y BRECHA				
NIVEL OBSERVADO NO			NIVEL MINIMO ACEPTABLE (NMA)	DEFINICIÓN DE BRECHA
0	INCOMPLETO	EL PROCESO NO ESTA INPLEMENTADO O NO ALCANZA SU PROPOSITO, HAY MUY POCA O NINGUNA EVIDENCIA DEL PROCESO SISTEMATICO.	3	SI NMA - NO = 3 ; BRECHA SIGNIFICATIVA
1	EJECUTADO	EL PROCESO IMPLEMENTADO ALCANZA SU PROPOSITO.	3	SI NMA - NO = 2 ; BRECHA MODERADA
2	ADMINISTRADO	EL PROCESO EJECUTADO DESCRITO ESTA IMPLEMENTADO DE FORMA GESTIONADA (PLANIFICADO, SUPERVISADO, AJUSTADO Y SUS RESULTADOS ESTAN ESTABLECIDOS CONTROLADOS Y MANTENIDOS DE FORMA APROPIADA)	3	SI NMA -NO = 1 ; BRECHA MINIMA
3	ESTABLECIDO	EL PROCESO GESTIONADO ESTA AHORA IMPLEMENTADO UTILIZANDO UN PROCESO DEFINIDO QUE ES CAPAZ DE ALCANZAR SUS RESULTADOS.	3	SI NMA <= 0 : BRECHA MINIMA
4	PREDECIBLE	EL PROCESO ESTABLECIDO AHORA SE EJECUTA DENTRO DE LOS LIMITES DEFINIDOS PARA ALCANZAR SUS OBJETIVOS	3	SI NMA <= 0 : BRECHA MINIMA
5	OPTIMIZADO	EL PROCESO PREDECIBLE ES MEJORADO CONTINUAMENTE PARA CUMPLIR CON LAS METAS EMPRESARIALES PRESENTES Y FUTURAS	3	SI NMA <= 0 : BRECHA MINIMA

Fuente: ISACA, Marco de referencia COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa (2012)
Elaborado por: Vargas (2021)

A continuación, se presenta la evaluación realizada a cada proceso con sus respectivas prácticas de gobierno, estas tablas tienen el objetivo de detectar las actividades que generan brechas significativas, para así poder implementar soportes que ayuden a gestionarlas y beneficien al cumplimiento de los objetivos o metas de la entidad.

Cabe mencionar que se determinó un nivel de capacidad objetivo al que quiere llegar la empresa siendo este 3. Al determinarlo todas las actividades tiene una meta “F”, para lo cual se establecido un nivel de cumplimiento a cada actividad de las prácticas de gobierno permitiendo identificar si dicha meta se cumple o no considerando que aquellas que tengan un porcentaje mayor al 85% ayudaran a su cumplimiento, mientras

que las actividades que tengan un porcentaje menor o igual al 85% no permitirán cumplir la meta y se deberá establecer prioridades para referenciar el nivel de impacto que tiene sobre el proceso evaluado.

Al final se presentará una tabla que resume los promedios obtenidos en cada dominio enfocados a los niveles de capacidad conseguidos en los procesos.

Tabla No. 23 Niveles de capacidad de los procesos

NIVEL DE CAPACIDAD DE PROCESOS		
SIGLAS	**DESCRIPCIÓN**	**VALORACIÓN DE PORCENTAJES**
F	COMPLETAMENTE	> 85%
L	EN GRAN MEDIDA	> 50% AL 85%
P	PARCIALMENTE	> 15% AL 50%
N	NO CUMPLE	0% AL 15%

Elaborado por: Vargas (2021)

3.1.3.1 Evaluar, orientar y supervisar (EDM)

Tabla No. 24 Asegurar la optimización del riesgo

EDM.03	**Asegurar la Optimización del Riesgo**	
Descripción del Proceso Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.		
Declaración del Propósito del Proceso Asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.		
PRACTICAS DE GOBIERNO		
EDM.03.01	Evaluar la gestión de riesgos	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.
EDM.03.02	Orientar la gestión de riesgos	Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo
EDM.03.03	Supervisar la gestión de riesgos	Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	
06 Transparencia de los costes, beneficios y riesgos de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI	

10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías

Fuente: ISACA, Marco de referencia COBIT 5: Asegurar la Optimización del Riesgo EDM03 (2012)

Elaborado por: Vargas (2022)

Tabla No. 25 Evaluación a las actividades del proceso EDM03

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
EDM.03.01 Evaluar la gestión de riesgos	3	0	3,00	BRECHA SIGNIFICATIVA	14,0	F	NO CUMPLE
EDM.03.02 Orientar la gestión de riesgos	3	0,17	2,83	BRECHA SIGNIFICATIVA	20,0	F	NO CUMPLE
EDM.03.03 Supervisar la gestión de riesgos	3	0,50	2,50	BRECHA SIGNIFICATIVA	32,0	F	NO CUMPLE
VALOR PROMEDIO DE EDM03	**3**	**0,22**	**2,78**	BRECHA SIGNIFICATIVA	**22,0**	F	NO CUMPLE

Elaborado por: Vargas (2021)

3.1.3.2 Alinear, planificar y organizar (APO)

Tabla No. 26 Gestionar el riesgo

APO.12	**Gestionar el Riesgo**	
Descripción del Proceso Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.		
Declaración del Propósito del Proceso Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.		
PRÁCTICAS DE GESTIÓN		
APO.12.01	Recopilar datos	Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.
APO.12.02	Analizar el riesgo	Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.
APO.12.03	Supervisar y revisar el SGSI	Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados
APO.12.04	Mantener un perfil de riesgo	Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.
APO.12.05	Definir un portafolio de acciones para la gestión de riesgos	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.
APO.12.06	Responder al riesgo	Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
02 Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de reputación • Número de asuntos de incumplimiento relacionados con TI reportados a la junta que llegan a ser de dominio público o que provocan situaciones de escándalo • Número de asuntos de incumplimiento relacionados con acuerdos contractuales con proveedores de servicio TI • Cobertura de la evaluación del cumplimiento	
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	

06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Número de programas que necesitan ser revisados significativamente debido a defectos de calidad • Coste del mantenimiento de aplicaciones respecto al coste total de TI

Fuente: ISACA, Marco de referencia COBIT 5: Gestionar el Riesgo APO12 (2012)

Elaborado por: Vargas (2022)

Tabla No. 27 Evaluación a las actividades del proceso APO12

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
APO.12.01 Recopilar datos	3	0	2,71	BRECHA SIGNIFICATIVA	24,29	F	NO CUMPLE
APO.12.02 Analizar el riesgo	3	0,43	2,57	BRECHA SIGNIFICATIVA	26,43	F	NO CUMPLE
APO.12.03 Supervisar y revisar el SGSI	3	0,57	2,43	BRECHA MODERADA	28,57	F	NO CUMPLE
APO.12.04 Mantener un perfil de riesgo	3	0,40	2,60	BRECHA SIGNIFICATIVA	24,20	F	NO CUMPLE
APO.12.05 Definir un portafolio de acciones para la gestión de riesgos	3	0,67	2,33	BRECHA MODERADA	38,00	F	NO CUMPLE
APO.12.06 Responder al riesgo	3	1,00	2,00	BRECHA MODERADA	44,75	F	NO CUMPLE
VALOR PROMEDIO DE APO12	**3**	**2**	**2**	BRECHA MODERADA	**31,04**	F	NO CUMPLE

Elaborado por: Vargas (2022)

Tabla No. 28 Gestionar la seguridad

APO.13	**Gestionar la Seguridad**	
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.		
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.		
PRÁCTICAS DE GESTIÓN		
APO.13.01	Establecer y mantener un SGSI	Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa
APO.13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.
APO.13.03	Supervisar y revisar el SGSI	Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad	
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	

06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de casos de inversión de negocio, que tienen claramente definidos y aprobados los costes y beneficios esperados relacionados con TI • Porcentaje de servicios de TI que tienen claramente definidos y aprobados los costes operacionales y los beneficios esperados • Encuestas de satisfacción dirigidas a los principales accionistas en relación al nivel de transparencia, entendimiento y precisión de la información financiera de TI
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
14 Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión • Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa

Fuente: ISACA, Marco de referencia COBIT 5: Gestionar la Seguridad APO13 (2012)

Elaborado por: Vargas (2022)

Tabla No. 29 Evaluación a las actividades del proceso APO13

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
APO.13.01 Establecer y mantener un SGSI	3	1	2,14	BRECHA MODERADA	35,14	F	NO CUMPLE
APO.13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	3	0,43	2,57	BRECHA SIGNIFICATIVA	26,43	F	NO CUMPLE
APO.13.03 Supervisar y revisar el SGSI	3	0,60	2,40	BRECHA MODERADA	35,60	F	NO CUMPLE
VALOR PROMEDIO DE APO13	**3**	**1**	**2,4**	BRECHA MODERADA	**32,39**	F	NO CUMPLE

Elaborado por: Vargas (2022)

3.1.3.3 Construir, adquirir e implementar (BAI)

Tabla No. 30 Gestionar los cambios

BAI.06	**Gestionar los Cambios**	
Descripción del Proceso Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación		
Declaración del Propósito del Proceso Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.		
		PRÁCTICAS DE GESTIÓN
BAI.06.01	Evaluar, priorizar y autorizar peticiones de cambio.	Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.
BAI.06.02	Gestionar cambios de emergencia	Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.
BAI.06.03	Hacer seguimiento e informar de cambios de estado	Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.
BAI.06.04	Cerrar y documentar los cambios	Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados	

10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías

Fuente: ISACA, Marco de referencia COBIT 5: Gestionar los Cambios BAI06 (2012)

Elaborado por: Vargas (2022)

Tabla No. 31 Evaluación a las actividades del proceso BAI06

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
BAI.06.01 Evaluar, priorizar y autorizar peticiones de cambio.	3	1	2,29	BRECHA MODERADA	36,71	F	NO CUMPLE
BAI.06.02 Gestionar cambios de emergencia	3	1,25	1,75	BRECHA MÍNIMA	47,25	F	NO CUMPLE
BAI.06.03 Hacer seguimiento e informar de cambios de estado	3	1,50	1,50	BRECHA MÍNIMA	52,25	F	NO CUMPLE
BAI.06.04 Cerrar y documentar los cambios	3	2,00	2,00	BRECHA MODERADA	34,33	F	NO CUMPLE
VALOR PROMEDIO DE BAI06	**3**	**1**	**1,9**	BRECHA MÍNIMA	42,64	F	NO CUMPLE

Elaborado por: Vargas (2022)

Tabla No. 32 Gestionar los activos

BAI.09	**Gestionar los Activos**	
Descripción del Proceso Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.		
Declaración del Propósito del Proceso Contabilización de todos los activos de TI y optimización del valor proporcionado por estos activos.		
PRÁCTICAS DE GESTIÓN		
BAI.09.01	Identificar y registrar activos actuales	Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera
BAI.09.02	Gestionar activos críticos	Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.
BAI.09.03	Gestionar el ciclo de vida de los activos.	Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente
BAI.09.04	Optimizar el coste de los activos	Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.
BAI.09.05	Administrar licencias.	Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.	

11 Optimización de activos, recursos y capacidades de TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI

Fuente: ISACA, Marco de referencia COBIT 5: Gestionar los Activos BAI09 (2012)

Elaborado por: Vargas (2022)

Tabla No. 33 Evaluación a las actividades del proceso BAI09

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
BAI.09.01 Identificar y registrar activos actuales	3	2,50	0,50	BRECHA MÍNIMA	70,00	F	NO CUMPLE
BAI.09.02 Gestionar activos críticos	3	2,33	0,67	BRECHA MÍNIMA	67,22	F	NO CUMPLE
BAI.09.03 Gestionar el ciclo de vida de los activos.	3	3,00	0,00	BRECHA MÍNIMA	75,00	F	NO CUMPLE
BAI.09.04 Optimizar el coste de los activos	3	2,50	0,50	BRECHA MÍNIMA	70,00	F	NO CUMPLE
BAI.09.05 Administrar licencias.	3	2,33	0,67	BRECHA MÍNIMA	63,17	F	NO CUMPLE
VALOR PROMEDIO DE BAI09	**3**	**3**	**0,5**	BRECHA MÍNIMA	69,08	F	NO CUMPLE

Elaborado por: Vargas (2022)

3.1 Entrega, servicio y soporte (DSS)

Tabla No. 34 Gestionar las operaciones

DSS.01	**Gestionar las Operaciones**	
Descripción del Proceso Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.		
Declaración del Propósito del Proceso Entregar los resultados del servicio operativo de TI, según lo planificado.		
PRÁCTICAS DE GESTIÓN		
DSS.01.01	Ejecutar procedimientos operativos	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
DSS.01.02	Gestionar servicios externalizados de TI	Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.
DSS.01.03	Supervisar la infraestructura de TI	Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.
DSS.01.04	Gestionar el entorno	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.
DSS.01.05	Gestionar las instalaciones	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	

07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
11 Optimización de activos recursos y capacidades de TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI

Fuente: ISACA, Marco de referencia COBIT 5: Gestionar las Operaciones DSS01 (2012)

Elaborado por: Vargas (2022)

Tabla No. 35 Evaluación a las actividades del proceso DSS01

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
DSS.01.01 Ejecutar procedimientos operativos	3	2	1,00	BRECHA MÍNIMA	57,80	F	NO CUMPLE
DSS.01.02 Gestionar servicios externalizados de TI	3	1,75	1,25	BRECHA MÍNIMA	54,75	F	NO CUMPLE
DSS.01.03 Supervisar la infraestructura de TI	3	0,17	2,83	BRECHA SIGNIFICATIVA	20,00	F	NO CUMPLE
DSS.01.04 Gestionar el entorno	3	2,88	0,13	BRECHA MÍNIMA	73,75	F	NO CUMPLE
DSS.01.05 Gestionar las instalaciones	3	2,91	0,09	BRECHA MÍNIMA	74,09	F	NO CUMPLE
VALOR PROMEDIO DE DSS01	**3**	**1,94**	**1,1**	BRECHA MÍNIMA	56,08	F	NO CUMPLE

Elaborado por: Vargas (2022)

Tabla No. 36 Gestionar servicios de seguridad

DSS.05	**Gestionar Servicios de Seguridad**	
Descripción del Proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.		
Declaración del Propósito del Proceso Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.		
PRÁCTICAS DE GESTIÓN		
DSS.05.01	Proteger contra software malicioso (malware).	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).
DSS.05.02	Gestionar la seguridad de la red y las conexiones	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
DSS.05.03	Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.
DSS.05.04	Gestionar la identidad del usuario y el acceso lógico.	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio
DSS.05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.
DSS.05.06	Gestionar documentos sensibles y dispositivos de salida.	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.
DSS.05.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochornos públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocios habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías

Fuente: ISACA, Marco de referencia COBIT 5: Gestionar Servicios de Seguridad DSS05 (2012)

Elaborado por: Vargas (2022)

Tabla No. 37 Evaluación a las actividades del proceso DSS05

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
DSS.05.01 Proteger contra software malicioso (malware).	3	1,00	2,00	BRECHA MODERADA	43,00	F	NO CUMPLE
DSS.05.02 Gestionar la seguridad de la red y las conexiones	3	0,78	2,22	BRECHA MODERADA	35,00	F	NO CUMPLE
DSS.05.03 Gestionar la seguridad de los puestos de usuario final.	3	1,78	1,22	BRECHA MÍNIMA	59,33	F	NO CUMPLE
DSS.05.04 Gestionar la identidad del usuario y el acceso lógico.	3	0,75	2,25	BRECHA MODERADA	35,75	F	NO CUMPLE
DSS.05.05 Gestionar el acceso físico a los activos de TI.	3	1,29	1,71	BRECHA MÍNIMA	44,57	F	NO CUMPLE
DSS.05.06 Gestionar documentos sensibles y dispositivos de salida.	3	1,40	1,40	BRECHA MÍNIMA	54,80	F	NO CUMPLE
DSS.05.07 Supervisar la infraestructura para detectar eventos relacionados con la	3	0,00	3,00	RECHA SIGNIFICATIV	14,00	F	NO CUMPLE
VALOR PROMEDIO DE DSS05	**3**	**1**	**2,0**	BRECHA MÍNIMA	40,92	F	NO CUMPLE

Elaborado por: Vargas (2022)

3.1.3.5 Supervisar, evaluar y valorar (MEA)

Tabla No. 38 Supervisar, evaluar y valorar rendimiento y conformidad

MEA.01	**Supervisar, Evaluar y Valorar Rendimiento y Conformidad**	
Descripción del Proceso Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada		
Declaración del Propósito del Proceso Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.		
PRÁCTICAS DE GESTIÓN		
MEA.01.01	Establecer un enfoque de la supervisión	Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.
MEA.01.02	Establecer los objetivos de cumplimiento y rendimiento.	Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.
MEA.01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.
MEA.01.04	Analizar e informar sobre el rendimiento	Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión
MEA.01.05	Asegurar la implantación de medidas correctivas	Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.
El proceso apoya la consecución de un conjunto de principales metas TI:		
Meta TI	**Métricas Relacionadas**	
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	
07 Entrega de servicios TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI Entregados	

11 Optimización de activos, recursos y capacidades de TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI
15 Cumplimiento de las políticas internas por parte de TI	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de partes interesadas que comprenden las políticas • Porcentaje de políticas soportadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de las políticas

Fuente: ISACA, Marco de referencia COBIT 5: Supervisar, Evaluar y Valorar Rendimiento y Conformidad MEA01 (2012)

Elaborado por: Vargas (2022)

Tabla No. 39 Evaluación a las actividades del proceso MEA01

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
MEA.01.01 Establecer un enfoque de la supervisión	3	3	0	BRECHA MÍNIMA	75,00	F	NO CUMPLE
MEA.01.02 Establecer los objetivos de cumplimiento y rendimiento.	3	2,25	0,75	BRECHA MÍNIMA	66,25	F	NO CUMPLE
MEA.01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.	3	2,20	0,8	BRECHA MÍNIMA	67,00	F	NO CUMPLE
MEA.01.04 Analizar e informar sobre el rendimiento	3	2,17	0,83	BRECHA MÍNIMA	65,83	F	NO CUMPLE
MEA.01.05 Asegurar la implantación de medidas correctivas	3	2,25	0,75	BRECHA MÍNIMA	67,50	F	NO CUMPLE
VALOR PROMEDIO DE MEA01	**3**	**2,37**	**0,6**	BRECHA MÍNIMA	68,32	F	NO CUMPLE

Elaborado por: Vargas (2022)

Tabla No. 40 Supervisar, evaluar y valorar el sistema de control interno

MEA.02	**Supervisar, Evaluar y Valorar el Sistema de Control Interno**	
Descripción del Proceso Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.		
Declaración del Propósito del Proceso Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.		
PRÁCTICAS DE GESTIÓN		
MEA.02.01	Supervisar el control interno.	Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.
MEA.02.02	Revisar la efectividad de los controles sobre los procesos de negocio	Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias
MEA.02.03	Realizar autoevaluaciones de control.	Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.
MEA.02.04	Identificar y comunicar las deficiencias de control.	Identificar deficiencias de control y analizar e identificar las causas raíz subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.
MEA.02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.
MEA.02.06	Planificar iniciativas de aseguramiento.	Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.
MEA.02.07	Estudiar las iniciativas de aseguramiento.	Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.
MEA.02.08	Ejecutar las iniciativas de aseguramiento.	Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.
El proceso apoya la consecución de un conjunto de principales metas TI:		

Meta TI	Métricas Relacionadas
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
15 Cumplimiento de las políticas internas por parte de TI	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de partes interesadas que comprenden las políticas • Porcentaje de políticas soportadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de las políticas

Fuente: ISACA, Marco de referencia COBIT 5: Supervisar, Evaluar y Valorar el Sistema de Control Interno MEA02 (2012)

Elaborado por: Vargas (2022)

Tabla No. 41 Evaluación a las actividades del proceso MEA02

Práctica clave de Gobierno	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD		
	Nivel mínimo aceptable	Nivel Observado (NO)	Definición de brecha		Valor	Nivel alcanzado	Observación
MEA.02.01 Supervisar el control interno.	3	1	2,43	BRECHA MODERADA	27,86	F	NO CUMPLE
MEA.02.02 Revisar la efectividad de los controles sobre los procesos de negocio	3	1,40	1,60	BRECHA MÍNIMA	56,00	F	NO CUMPLE
MEA.02.03 Realizar autoevaluaciones de control.	3	0,71	2,29	BRECHA MODERADA	33,71	F	NO CUMPLE
MEA.02.04 Identificar y comunicar las deficiencias de control.	3	1,67	1,33	BRECHA MÍNIMA	59,17	F	NO CUMPLE
MEA.02.05 Garantizar que los proveedores de aseguramiento son independientes	3	3,00	0,00	BRECHA MÍNIMA	75,00	F	NO CUMPLE
MEA.02.06 Planificar iniciativas de aseguramiento.	3	0,00	3,00	RECHA SIGNIFICATIV	14,00	F	NO CUMPLE
MEA.02.07 Estudiar las iniciativas de aseguramiento.	3	0,20	2,80	RECHA SIGNIFICATIV	21,20	F	NO CUMPLE
MEA.02.08 Ejecutar las iniciativas de aseguramiento.	3	0,75	2,25	BRECHA MODERADA	35,13	F	NO CUMPLE
VALOR PROMEDIO DE MEA02	**3**	**1,04**	**1,96**	BRECHA MÍNIMA	40,26	F	NO CUMPLE

Elaborado por: Vargas (2022)

Tabla No. 42 Promedios obtenidos en cada proceso

DOMINIO	CÓDIGO	PROCESO	CÓDIGO	PRÁCTICAS	DETALLE	NIVEL DE CAPACIDAD			
						F	L	P	N
Evaluar, Orientar y Supervisar (EDM)	EDM.03	Asegurar la Optimización del Riesgo	EDM.03.01	**Evaluar la gestión de riesgos**	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.				14,00
			EDM.03.02	**Orientar la gestión de riesgos**	Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo			20,00	
			EDM.03.03	**Supervisar la gestión de riesgos**	Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.			32,00	
Alinear, Planificar y Organizar (APO)	APO 12	Gestionar el Riesgo	APO.12.01	**Recopilar datos**	Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.			24,29	
			APO.12.02	**Analizar el riesgo**	Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.			26,43	
			APO.12.03	**Supervisar y revisar el SGSI**	Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados			28,57	
			APO.12.04	**Mantener un perfil de riesgo**	Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.			24,20	
			APO.12.05	**Definir un portafolio de acciones para la gestión de riesgos**	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.			38,00	
			APO.12.06	**Responder al riesgo**	Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.			44,75	

Alinear, Planificar y Organizar (APO)	APO.13	**Gestionar la Seguridad**	APO 13.01	**Establecer y mantener un SGSI**	Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa			35,14	
			APO 13.02	**Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.**	Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.			26,43	
			APO 13.03	**Supervisar y revisar el SGSI**	Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua			35,60	
Construir, adquirir e implementar (BAI)	BAI.06	**Gestionar los Cambios**	BAI.06.01	**Evaluar, priorizar y autorizar peticiones de cambio.**	Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.			36,71	
			BAI.06.02	**Gestionar cambios de emergencia**	Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.			47,25	
			BAI.06.03	**Hacer seguimiento e informar de cambios de estado**	Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.		52,25		
			BAI.06.04	**Cerrar y documentar los cambios**	Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.			34,33	

Construir, adquirir e implementar (BAI)	BAI.09	**Gestionar los Activos**	BAI.09.01	**Identificar y registrar activos actuales**	Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.		70,00		
			BAI.09.02	**Gestionar activos críticos**	Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.		67,22		
			BAI.09.03	**Gestionar el ciclo de vida de los activos.**	Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente.		75,00		
			BAI.09.04	**Optimizar el coste de los activos**	Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.		70,00		
			BAI.09.05	**Administrar licencias.**	Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.		63,17		
Entrega, Servicio y Soporte (DSS)	DSS.01	**Gestionar las Operaciones**	DSS.01.01	**Ejecutar procedimientos operativos**	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.		57,80		
			DSS.01.02	**Gestionar servicios externalizados de TI**	Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.		54,75		
			DSS.01.03	**Supervisar la infraestructura de TI**	Supervisar las infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.			20,00	
			DSS.01.04	**Gestionar el entorno**	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.		73,75		
			DSS.01.05	**Gestionar las instalaciones**	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo		74,09		

Entrega, Servicio y Soporte (DSS)	DSS.05	**Gestionar Servicios de Seguridad**	DSS.05.01	**Proteger contra software malicioso (malware).**	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).			43,00	
			DSS.05.02	**Gestionar la seguridad de la red y las conexiones**	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.			35,00	
			DSS.05.03	**Gestionar la seguridad de los puestos de usuario final.**	Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.		59,33		
			DSS.05.04	**Gestionar la identidad del usuario y el acceso lógico.**	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.			35,75	
			DSS.05.05	**Gestionar el acceso físico a los activos de TI.**	Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.			44,57	
			DSS.05.06	**Gestionar documentos sensibles y dispositivos de salida.**	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.		54,80		
			DSS.05.07	**Supervisar la infraestructura para detectar eventos relacionados con la seguridad.**	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.				14,00

Supervisar, Evaluar y Valorar (MEA)	MEA.01	**Supervisar, Evaluar y Valorar Rendimiento y Conformidad**	MEA.01.01	**Establecer un enfoque de la supervisión**	Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.		75,00		
			MEA.01.02	**Establecer los objetivos de cumplimiento y rendimiento.**	Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.		66,25		
			MEA.01.03	**Recopilar y procesar los datos de cumplimiento y rendimiento.**	Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.		67,00		
			MEA.01.04	**Analizar e informar sobre el rendimiento**	Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.		65,83		
			MEA.01.05	**Asegurar la implantación de medidas correctivas**	Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.		67,50		
	MEA.02	**Supervisar, Evaluar y Valorar el Sistema de Control Interno**	MEA.02.01	**Supervisar el control interno.**	Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.			27,86	
			MEA.02.02	**Revisar la efectividad de los controles sobre los procesos de negocio**	Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias		56,00		
			MEA.02.03	**Realizar autoevaluaciones de control.**	Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.			33,71	

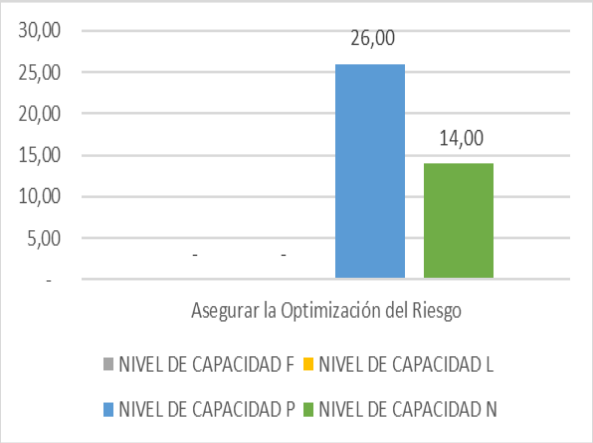
Supervisar, Evaluar y Valorar (MEA)	MEA.02	**Supervisar, Evaluar y Valorar el Sistema de Control Interno**	MEA.02.04	**Identificar y comunicar las deficiencias de control.**	Identificar deficiencias de control y analizar e identificar las causas raíz subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.		59,17		
			MEA.02.05	**Garantizar que los proveedores de aseguramiento son independientes y están cualificados.**	Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.		75,00		
			MEA.02.06	**Planificar iniciativas de aseguramiento.**	Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.				14,00
			MEA.02.07	**Estudiar las iniciativas de aseguramiento.**	Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.			21,20	
			MEA.02.08	**Ejecutar las iniciativas de aseguramiento.**	Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.			35,13	

Fuente: Evaluación de los niveles de capacidad de procesos de la empresa D'Christian Maryuri; ISACA, Marco de referencia COBIT 5: Dominios (2012)

Elaborado por: Vargas (2022)

Una vez identificado los promedios se realizaron los gráficos correspondientes a cada dominio. Al analizar estos gráficos se encontraron hallazgos potenciales los cuales se especifican al final.

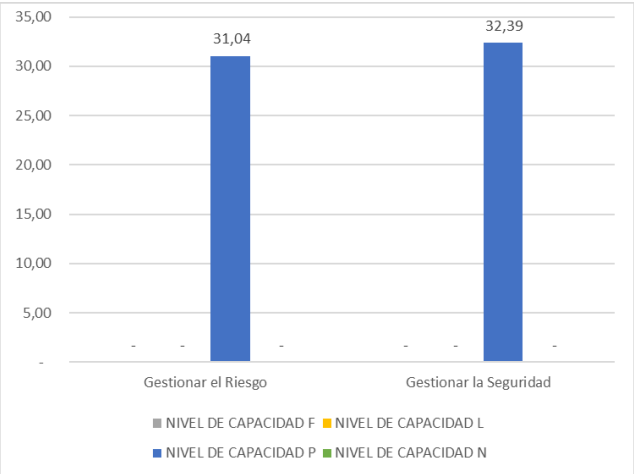
Gráfico No. 19 Promedio obtenido en el dominio evaluar, orientar y supervisar (EDM)



Elaborado por: Vargas (2022)

Análisis: Al analizar el dominio EDM mediante un promedio general arrojó los siguientes resultados, en el proceso Asegurar la Optimización del Riesgo el 26% corresponde a aquellos procesos que tiene un nivel de capacidad "P" es decir que las actividades se cumplen parcialmente y un 14% como nivel de capacidad "N" dando a entender que la empresa no cumple con varias actividades de las prácticas de gestión.

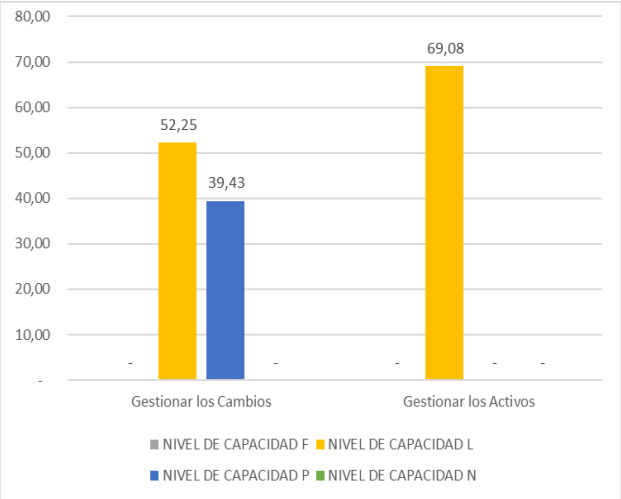
Gráfico No. 20 Promedio obtenido en el dominio alinear, planificar y organizar (APO)



Elaborado por: Vargas (2022)

Análisis: En el dominio APO se sostiene que en los dos procesos analizados se ha desarrollado con las actividades de manera parcial "P", sin embargo, en el proceso Gestionar el Riesgo las actividades se ejecutan con un 31,04% mientras que en el proceso Gestionar la Seguridad se realizan con un 32,39% siendo estos un promedio general del dominio.

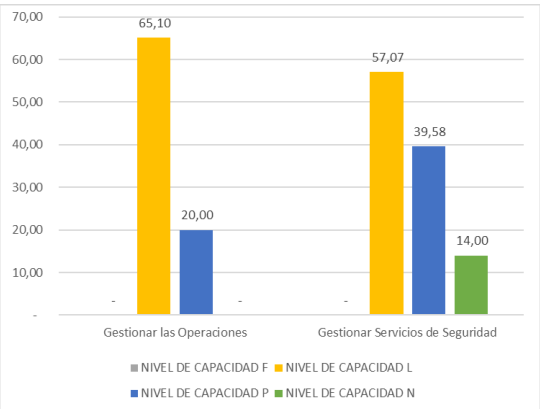
Gráfico No. 21 Promedio obtenido en el dominio construir, adquirir e implementar (BAI)



Elaborado por: Vargas (2022)

Análisis: Mediante el análisis del dominio BAI se obtuvo los siguientes resultados, en el proceso Gestionar los Cambios se determinó que se cumple en gran medida "L" un 52,25% de las actividades y un 39,43% parcialmente "P", mientras que en el proceso Gestionar los Activos se obtuvo como promedio general que el 69,08% de las actividades se cumplen en gran medida.

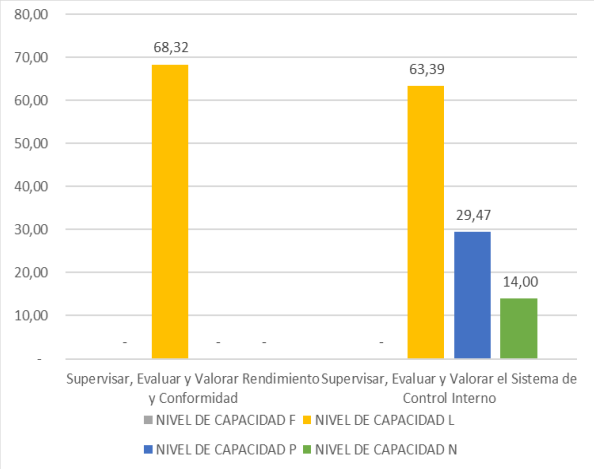
Gráfico No. 22 Promedio obtenido en el dominio entrega, servicio y soporte (DSS)



Elaborado por: Vargas (2022)

Análisis: Al analizar el dominio DSS en el proceso Gestionar las Operaciones el 65, 10% corresponde a un nivel de capacidad en gran medida “L” y el 20% corresponde a un nivel de capacidad parcial, mientras que en el proceso Gestionar Servicios de Seguridad se obtuvo tres niveles que corresponden a el 57,07% en gran medida, el 39,58% parcialmente y el 14% que señala que no se cumple con varias de las actividades.

Gráfico No. 23 Promedio obtenido en el dominio supervisar, evaluar y valorar (MEA)



Elaborado por: Vargas (2022)

Análisis: En el dominio MEA se analizaron dos procesos, en Supervisar, Evaluar y Valorar Rendimiento y Conformidad se obtuvo que el 68,32% de las actividades se cumplieron en gran medida “L”, mientras que en el proceso Supervisar, Evaluar y Valorar el Sistema de Control Interno los niveles de capacidad fueron el 63,39% en gran medida, el 29,47% parcialmente y el 14% no se cumplen con varias actividades.

Tabla No. 43 Hallazgos encontrados en la evaluación

DOMINIO	HALLAZGO	CONDICIÓN	CAUSA	EFECTO	RECOMENDACIÓN
Evaluar, Orientar y Supervisar (EDM)	**1**	No se reconoce la necesidad de identificar riesgos, por ende, no existe un análisis, ni se conoce el apetito y la tolerancia que pueden tener estos riesgos.	Inexistencia de políticas, prácticas de gestión, procedimientos para la identificación y control de riesgos potenciales relacionados con la TI.	Mayor probabilidad de afectación a los procesos, pérdidas económicas, paros en la producción, la rentabilidad disminuye o toma de decisiones inadecuadas.	Dirigido a: Gerente Implementar prácticas de gestión.
Alinear, Planificar y Organizar (APO)	**2**	Ausencia de procesos para identificar y analizar riesgos empresariales relacionados con la TI, estos riesgos no son gestionados, así mismo no se definen, operan y supervisan procesos para la seguridad de la información	No existe un SGSI definido, ni se establecen niveles de tolerancia de riesgos.	Mayor probabilidad de aumentar riesgos de incidentes de seguridad, ocasionando consigo pérdidas financieras, robo de información sensible, perdida de prestigio.	Dirigido a: Dirección ejecutiva Implementar un SGSI y aplicar políticas de seguridad de la información de acuerdo a los estatutos, normas y leyes vigentes.
Construir, adquirir e implementar (BAI)	**3**	Falta de adaptación a cambios, no se identifican todas las copias de software instalado con licencia.	No existen procesos y políticas estructuradas para gestionar cambios y peticiones, no se realizan auditorías en sistemas.	Personal no preparado para cambios en el entorno del trabajo, modificaciones o errores en las copias de software.	Dirigido a: Gerente Administrar cambios e incluir cambios estándar y de emergencia que estén relacionados con los procesos de negocio, aplicaciones e infraestructura.
Entrega, Servicio y Soporte (DSS)	**4**	Ausencia de revisiones periódicas y supervisión a varias actividades de TI, puede que los empleados no concienticen sobre softwares maliciosos que pueden entrar al sistema.	Inexistencia de políticas para la seguridad de la información, no se implementan reglas ni se establecen procedimientos para supervisar la infraestructura de TI, descuido por parte de la directiva en revisiones, falta de implementación de procesos para concientizar a los empleados sobre softwares maliciosos.	Mayor probabilidad de generarse posibles nuevas amenazas, entradas de virus, riesgos de robo o hackeo, eventos potenciales, incidentes de seguridad.	Dirigido a: Gerente y Área de Sistemas Implementar controles internos, establecer políticas de seguridad con el fin de proteger la información y sobre todo realizar auditorías de sistemas cada año.
Supervisar, Evaluar y Valorar (MEA)	**5**	Inadecuado sistema de control.	Inexistencia de procesos que ayuden a la evaluación del control interno y a localizar deficiencias o riesgos.	Dificultad para cumplir o lograr con los objetivos o metas de la empresa.	Dirigido a: Gerente Implementar un marco de control interno que se adapte a las necesidades de la empresa y contribuya al establecimiento de normas y responsabilidades para un sistema de control interno efectivo.

Elaborado por: Vargas (2022)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Una vez finalizado el proyecto integrador se obtuvieron las siguientes conclusiones:

- Al realizar de forma preliminar el levantamiento del inventario de los activos de información de la empresa D'Christian Maryuri. Se evidencia que existen activos de información que son mayormente expuestos a vulnerabilidades como: la base de datos, el sistema contable, hardware (computadores, equipos informáticos) y usuarios del sistema informático. Estos al no ser gestionados de forma correcta o al no aplicar controles de forma tanto preventiva como detectiva o correctiva, da paso a que las amenazas exploten esas vulnerabilidades y puedan provocar un daño a la empresa con un impacto negativo.

- Mediante la aplicación de una evaluación especifica realizada a los componentes del COSO ERM 2017 se constata que la mayoría de las actividades tiene un riesgo moderado. No obstante, existe actividades con riesgos altos que pueden generar impactos considerables para la empresa, estos riesgos se evalúan mediante una matriz donde se evidencia que existen riesgos extremos que exigen respuesta y atención inmediata por parte de la institución, debido a que estos riesgos a futuro podrían traer repercusiones tanto financieras como operativas.

- Al considerar el Marco de Referencia COBIT 2019 como un apoyo para alinear los objetivos del negocio con los objetivos de TI y evaluar los procesos informático. Se evidencia que en la empresa D'Christian Maryuri varios dominios se encuentran en un nivel de capacidad razonable equivalente a 3 como un nivel mínimo aceptable; es decir, un nivel establecido de los procesos de gobierno y gestión de las TI. Sin embargo, existen varios procesos que no logran un nivel óptimo debido a que algunas actividades se encuentran en un

nivel observado cero, dando como consecuencia brechas significativas en varias actividades que no permiten el cumplimiento adecuado de los objetivos y metas de la institución y de las prácticas claves.

4.2 Recomendaciones

Una vez finalizado el proyecto integrador se obtuvieron las siguientes recomendaciones:

- Poner mayor atención a aquellos activos identificados como más vulnerables expuestos a amenazas y riesgos gestionando controles, políticas y procedimientos que permitan salvaguardar dichos activos de manera adecuada y eficiente. De igual manera se debe concientizar sobre la responsabilidad en el mantenimiento y conservación de dichos activos a todos los usuarios que los administran, en vista de que estos constituyen un elemento importante dentro de la institución. Y por último nombrar a una persona que se encargue de gestionar la seguridad y control de los activos de información e implemente junto al Gerente procesos y políticas que garanticen la devolución de los mismo al terminar un contrato laboral.

- Realizar una vez al año un monitoreo de gestión de los riesgos, aquellos que fueron considerados altos para que a través de mecanismos se puede dar una mejor respuesta. Priorizar controles y frecuencias evaluativas que permitan establecer acciones de mejora e implementar un mapa de riesgos que posibilite identificar y supervisar continuamente los riesgos detectados.

- Se recomienda aplicar planes de acción como una hoja de ruta que permita focalizar cada una de las actividades dando como prioridad aquellas encontradas en el transcurso de la evaluación con brechas significativas. También se debe establecer políticas que permitan tener un mayor control de los procesos y sus actividades, y sobre todo supervisarlas mensualmente hasta que las mismas puedan alcanzar el nivel de capacidad deseado por la empresa. Y para complementar se debe realizar una auditoría informática anualmente

con el objeto de examinar y controlar el nivel de los procesos ya evaluados en comparación a una nueva evaluación donde se identifiquen nuevas brechas.

BIBLIOGRAFÍA

Arias, A. H. (2010). Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs). *Compendium*, *13*(25), 3-4. URL: https://www.redalyc.org/articulo.oa?id=88019355001

Armendáriz, D. N. L. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica-ESPOL*, *30*(1). URL: http://200.10.150.204/index.php/tecnologica/article/view/581/356

Ballesteros, H., Verde, J., Costabel, M., Sangiovanni, R., Dutra, I., Rundie, D., Cavaleri, F., & Bazán, L. (2010). Análisis FODA: Fortalezas, Oportunidades, Debilidades y Amenazas. *Revista Uruguaya de enfermería*, *5*(2). URL: http://rue.fenf.edu.uy/index.php/rue/article/view/85/83

Biler, S. A. (2017). Auditoría. Elementos esenciales. *Dominio de las Ciencias*, *3*(1), DOI: 138-151. http://dx.doi.org/10.23857/dc.v3i1.379

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

Comas, R., Nogueira, D., & Medina, A. (2014). El control de gestión y los sistemas de información: Propuesta de herramientas de apoyo. *Ingeniería Industrial*, *35*(2), 214-228. URL: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=s1815-59362014000200009

Cruz, M. A., Pozo, M. A., Aushay, H. R., & Arias, A. D. (2019). Las Tecnologías de la Información y de la Comunicación (TIC) como forma investigativa interdisciplinaria con un enfoque intercultural para el proceso de formación estudiantil. *e-Ciencias de la Información*, *9*(1), 44-59. DOI: http://dx.doi.org/10.15517/eci.v1i1.33052

Díaz, J., Pérez, A., & Florido, R. (2011). Impacto de las tecnologías de la información y las comunicaciones (TIC) para disminuir la brecha digital en la sociedad actual. *Cultivos tropicales*, *32*(1), 81-90. URL: http://scielo.sld.cu/scielo.php?pid=S0258-59362011000100009&script=sci_arttext&tlng=pt

Díaz, Y., Pérez, Y., & Proenza, D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Ciencias Holguín*, *20*(2), 1-14. URL: https://www.redalyc.org/articulo.oa?id=181531232002

Fernández, D. A. A., & Casas, X. C. (2017). Auditoría informática: Un enfoque efectivo. *Dominio de las Ciencias*, *3*(3), 157-173. URL: https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Figueroa, J. A., Rodríguez, R. F., Bone, C. C., & Saltos, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del conocimiento*, *2*(12), 145-155. URL: https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

García, J. B., & Gavilanes, M. A. (2015). *Análisis y propuesta de implementación de las mejores prácticas de itil en el departamento de sistemas de la universidad Politécnica Salesiana Sede Guayaquil.* [Trabajo de grado, Ingeniería de Sistemas]. Universidad Politécnica Salesiana. Repositorio Institucional de la Universidad Politécnica Salesiana. RIUPS https://dspace.ups.edu.ec/bitstream/123456789/10305/1/UPS-GT001202.pdf

Grajales, T. (2000). *Tipos de investigación.* https://cmapspublic2.ihmc.us/rid=1RM1F0L42-VZ46F4-319H/871.pdf

Guzmán, A., & Taborda, C. A. (2015). *Diseño de un sistema de gestión de la seguridad informática–SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá DC, a través de la auditoría*. [Trabajo de grado, Seguridad Informática]. Universidad Nacional Abierta y a Distancia. Repositorio Institucional de la Universidad Nacional Abierta y a Distancia. RIUNAD. https://repository.unad.edu.co/handle/10596/3448

Hernández, H. M., Cantero, L. G. Z., Vidal, D. M. R., & Villadiego, L. R. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia*, *2*, 528-541.URL: https://www.redalyc.org/jatsRepo/290/29063446029/29063446029.pdf

ISACA, C. (2012a). *Procesos Catalizadores*.

ISACA, C. (2012b). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.

ISACA, C. (2018). *COBIT® 2019 Framework: Introduction and Methodology*.

López, P. A. (2010). *Seguridad informática*. Editex.

Martínez, J. V., & Peralta, M. A. C. (2014). La calidad en los procesos informáticos de las Universidades Ecuatorianas. *Ciencia Unemi*, *7*(12), 58-68. DOI. https://doi.org/10.29076/issn.2528-7737vol7iss12.2014pp58-68p

Martínez, Y. A., Alfonso, B. B., & Marichal, L. L. (2012). Auditoría con informática a sistemas contables. *Revista Arquitectura e Ingeniería*, *6*(2), 4-14. URL. https://www.redalyc.org/pdf/1939/193924743004.pdf

Montilla, O. de J., & Herrera, L. G. (2006). El deber ser de la auditoría. *Estudios gerenciales*, *22*(98), 83-110. URL: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=s0123-59232006000100004

Naranjo, A. (2009). *Conceptos de la Auditoría de sistemas*. El Cid Editor.

Ortiz, P. P. (2011). Las tecnologías de hoy en un mundo globalizado. *Todays technologies in a globalized world*, 210-215. URL: https://www.usbcali.edu.co/sites/default/files/9_tecnologiashoy.pdf

Pesado, P. M., Bertone, R., Esponda, S., Pasini, A., Boracchia, M., Martorelli, S., & Swaels, M. (2013). Mejora de procesos en el desarrollo de sistemas de software y en procesos de gestión. *Workshop de Investigadores en Ciencias de la Computación (WICC)*, *15*. URL: https://digital.cic.gba.gob.ar/handle/11746/2335

Prieto, V., Quiñones, I., Ramírez, G., Fuentes, Z., Labrada, T., Pérez, O., & Montero, M. (2011). Impacto de las tecnologías de la información y las comunicaciones en la educación y nuevos paradigmas del enfoque educativo. *Educación médica superior*, *25*(1), 95-102. URL: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21412011000100009

Ramírez, G., & Álvarez, E. (2003). Auditoría a la Gestión de las Tecnologías y Sistemas de Información. *Industrial Data*, *6*(1), 99-102. URL: https://www.redalyc.org/pdf/816/81606114.pdf

Roa, M., Mejía, G., & Rubio, C. (2017). COSO ERM 2017 y la Generación de Valor. *Deloitte Touche Tohmatsu Limited.*, *202017*, 20. URL: https://www2. deloitte. com/content/dam/Deloitte/co/Documents/risk/Presenta ci% C3% B3n% 20COSO% 20ERM

Rodríguez, N., & Martínez, W. (1998). P*lanificación y evaluación de proyectos informáticos.* Editorial Universidad Estatal a Distancia, 11.

Rodríguez, Ó. J. S. (2004). La Auditoría de Sistemas de Información como elemento de control. *Cuadernos de administración*, *20*(31), 121-136. URL: https://dialnet.unirioja.es/servlet/articulo?codigo=5006406

Rodriguez, E. G. (2018). *Propuesta de un sistema de control interno informático para los laboratorios de computación de la UACE de la UTMACH.* [Trabajo de grado, Contabilidad y Auditoría]. Universidad Técnica de Machala Repositorio Digital UTMACH. http://repositorio.utmachala.edu.ec/handle/48000/12848

Salazar, J. B., & Campos, P. G. (2009). Modelo para Seguridad de la Información en TIC. *CEUR Workshop Proceedings*, *488*, 234-253. URL: https://www.academia.edu/download/46380698/paper13.pdf

Sánchez, E. (2008). Las tecnologías de información y comunicación (TIC) desde una perspectiva social. *Revista Electrónica Educare*, *12*, 155-162. DOI: https://doi.org/10.15359/ree.12-Ext.13

Sánchez, L. (2015). COSO ERM y la gestión de riesgos. *Quipukamayoc*, *23*(44), 43-50. URL: https://core.ac.uk/download/pdf/304895479.pdf

Serna, J. R. (2007). *El nuevo sistema de información de marketing*. Madrid: ESIC.

Suñagua, D., & Félix, Á. (2013). Auditoría de seguridad de información. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, *6*(6), 19-30. URL: http://www.scielo.org.bo/scielo.php?pid=S2071-081X2013000100004&script=sci_arttext

Tamayo, A. (1999). Teoría general de sistemas. *Facultad de Ingeniería y Arquitectura*. URL: https://repositorio.unal.edu.co/handle/unal/60006

Tarazona, T., & Cesar, H. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*, *28*, 137. URL. https://dialnet.unirioja.es/descarga/articulo/3311853.pdf

Torres, C. F. (2017). *Plan estratégico informático para el Área de Tecnologías de la Información de la Empresa Impofreico SA* [Trabajo de grado, Ingeniería en Sistemas]. Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas. Repositorio Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/handle/123456789/25194

Trasobares, A. H. (2003). Los sistemas de información: Evolución y desarrollo. *Proyecto social: Revista de relaciones laborales*, *10*, 149-165. URL: https://dialnet.unirioja.es/servlet/articulo?codigo=793097

Veiga, J., & Zimmermann Verdejo, M. (2008). Modelos de estudios en investigación aplicada: Conceptos y criterios para el diseño. *Medicina y seguridad del trabajo*, *54*(210), 81-88. URL: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0465-546X2008000100011

Voutssas, M. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*, *24*(50), 127-155. URL: http://www.scielo.org.mx/scielo.php?pid=S0187-358X2010000100008&script=sci_abstract&tlng=pt

Yessenia, S. (2021). *Control interno y la optimización de la gestión del riesgo en la Cooperativa de Ahorro y Crédito Alli Trpuk Ltda, 2018* [Trabajo de grado, Ingeniería en Contabilidad y Auditoría]. Universidad Nacional de Chimborazo. Repositorio Digital UNACH. http://dspace.unach.edu.ec/handle/51000/7526

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: Consideraciones. *Dominio de las Ciencias*, *3*(3), 676-688. URL: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Zubenko, Y., Cataldi, Z., & Lage, F. J. (2001). Aplicación de la teoría general de sistemas al análisis de los sistemas informáticos. *III Workshop de Investigadores en Ciencias de la Computación*. URL: http://sedici.unlp.edu.ar/handle/10915/21719

ANEXOS

Anexo 1

ENTREVISTA

OBJETIVO: Comprobar la fiabilidad de la información y conocer que amenazas, riesgos y vulnerabilidades se ha encontrado en el sistema contable.

TEMA: AMBIENTE DE CONTROL

1. ¿Cómo considera usted la forma en que actualmente se maneja la información en la empresa?
2. ¿Qué aspectos considera más vulnerables en el proceso informático que utiliza la empresa?

TEMA: EVALUACIÓN DE RIESGOS

3. ¿La empresa ha implementado alguna metodología para la evaluación de procesos informáticos?
4. ¿Existen deficiencias o errores al momento de manejar los datos e incluirlos al sistema contable?

TEMA: ACTIVIDADES DE CONTROL

5. ¿La empresa tiene procedimientos para la gestión de la seguridad de la información en los equipos informáticos y dispositivos?
6. ¿Cuáles son los controles que la empresa aplica en los procesos informáticos?
7. ¿Cómo es el proceso de comunicación que existe entre los departamentos que manejan el sistema informático?
8. ¿Existe un manual de procedimientos para la gestión de la información?
9. ¿La empresa maneja perfiles de usuarios para el sistema contable?

TEMA: INFORMACIÓN Y COMUNICACIÓN

10. ¿Cuáles son los procesos que considera medulares en cuanto a manejo de información?
11. ¿Qué reportes genera el sistema actual y cómo se utilizan?
12. ¿Los reportes que se emiten desde el sistema informático son correctos o tienen alguna deficiencia?

TEMA: SOPORTE Y MANTENIMIENTO

13. ¿Con que frecuencia se da soporte y actualización al sistema informático?

14. ¿Con que frecuencia se hacen correcciones a los registros en el sistema informatizado?
15. ¿Se realiza una revisión frecuentemente a todos los equipos de cómputo con el fin de detectar si existe algún virus o software malicioso? ¿Cada que tiempo?

Anexo 2

Evaluación especifica de todos los componentes del COSO ERM 2017

CHECK LIST PARA EL CONTROL INTERNO SEGÚN EL COSO ERM 2017				
D´CHRISITAN MARYURI				
N°	**COMPONENTE: GOBIERNO Y CULTURA**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Supervisión de riesgos				
1	¿Se realizan reuniones con el fin de actualizar las prácticas de gestión de riesgos?	☐	☑	
2	¿Se revisan y actualizan periódicamente las decisiones y objetivos estratégicos de la entidad?	☑	☐	Se revisan cada semestre
3	¿Existe una asignación de responsabilidades para supervisión y control continuo de los procesos dentro de la empresa?	☑	☐	
4	¿Cuándo se toman decisiones dentro de la empresa existe un responsable que las notifique mediante procesos pertinentes?	☑	☐	
5	¿Existe un plan de acción para mitigar los riesgos de la infraestructura tecnológica de forma segura?	☑	☐	
PRINCIPIO: Establece estructuras operativas				
6	¿Existen normas, leyes y reglamentos que guíen los procesos dentro de la empresa?	☐	☑	
7	¿Existen políticas y procedimientos internos para los procesos dentro de la empresa?	☑	☐	
8	¿La entidad tiene prácticas de gestión de riesgos?	☐	☑	
9	¿El software que se utiliza cumple con los estándares de funcionalidad, requerimientos y necesidades de la empresa?	☑	☐	
10	¿La persona encargada de la supervisión y control de los procesos informáticos es independiente a la persona que los administra?	☐	☑	Se encarga la misma persona
11	¿Se realizan actividades de supervisión continuas sobre los riesgos existentes?	☑	☐	
12	¿La organización ha definido políticas de la seguridad de la información?	☐	☑	
13	¿Las políticas de seguridad están debidamente socializadas con el personal de la empresa?	☐	☑	No existen políticas
14	¿Existen normas de control interno donde se garantice la protección de los recursos para su disponibilidad e integridad?	☑	☐	
15	¿Existe un inventario de todos los activos asociados a las instalaciones de procesamiento de información?	☑	☐	
16	¿Se ha implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	☐	☑	

PRINCIPIO: Define la cultura deseada				
17	¿Se han establecido competencias habilidades y conocimientos necesarios	☑	☐	
18	¿Se han cumplido con los objetivos planteados en la empresa?	☑	☐	
PRINCIPIO: Demuestra compromiso con los valores claves				
19	¿Se realizan reuniones periódicas con todo el personal para identificar nuevos riesgos?	☐	☑	
20	¿Se definen indicadores para identificar situaciones y tendencias relacionadas a los estándares de conducta de la organización, incluyendo a los proveedores y clientes?	☐	☑	
21	¿Se cumple con los plazos acordados para cada uno de los procesos	☑	☐	
22	¿Se toma en cuenta la opinión del personal para la toma de decisiones dentro	☑	☐	
PRINCIPIO: Atrae, desarrolla y retiene individuos competentes.				
23	¿Existe algún responsable de orientar la ruta a seguir cuando existen dudas en los	☑	☐	
24	¿Se puede cometer algún error sin que incida en forma crítica dentro de los procesos?	☐	☑	
25	¿La cantidad de información que abarca cada uno de los procesos es razonable?	☑	☐	
26	¿Existe un responsable del control de los procesos informáticos?	☑	☐	
27	¿Se ha definido quien es el responsable de los activos de informacion?	☑	☐	
N°	**COMPONENTE: ESTRATEGIA Y OBJETIVOS**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Analiza el contexto empresarial				
28	¿La empresa cuenta con una misión dentro de su plan estratégico?	☑	☐	
29	¿Se ha definido la visión dentro de la empresa?	☑	☐	
30	¿La empresa ha definido valores institucionales?	☑	☐	
31	estratégico que mantiene la empresa?	☑	☐	
PRINCIPIO: Define el apetito al riesgo				
32	¿Se tiene identificado los riesgos dentro de cada área que maneja procesos informáticos?	☐	☑	
PRINCIPIO: Evalúa estrategias alternativas				
33	¿Se han establecido alternativas para gestionar los riesgos?	☐	☑	
34	¿Se actualizan en forma periódica las estrategias establecidas?	☑	☐	
PRINCIPIO: Formula los objetivos empresariales				
35	¿Se han establecido estrategias alternativas para el logro de los objetivos?	☐	☑	
N°	**COMPONENTE: DESEMPEÑO**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Identifica riesgos				
36	¿La empresa cuenta con un procedimiento para identificar riesgos potenciales en los procesos informáticos que desarrollan?	☐	☑	
37	¿Se han encontrado errores en el sistema contable de la empresa? Especifique cuales en la casilla de observaciones	☐	☑	

PRINCIPIO: Evalúa la severidad de los riesgos				
38	¿Existen procedimientos establecidos que aseguren el cumplimiento de las leyes y regulaciones que conciernen al manejo de los recursos de la empresa?	☐	☑	
39	¿El riesgo de fraude o robo de datos es evaluado en los diferentes procesos de la empresa?	☐	☑	
40	¿Se detecta y previene la fuga de información, perdida de datos y las amenazas e intrusiones a nivel del software?	☑	☐	
41	¿Existen controles en el manejo del sistema contable para el ingreso de las transacciones en el sistema?	☑	☐	
42	¿Se realiza una evaluación de los riesgos que pueden afectar la infraestructura tecnológica mediante la utilización de una metodología?	☑	☐	
43	¿Se monitorea el plan de acción en contra de los riesgos de la infraestructura tecnológica?	☐	☑	
44	¿La empresa tiene medidas de protección física para prevenir desastres naturales, ataques maliciosos o accidentes?	☑	☐	
45	¿Existen controles preventivos como claves de acceso, etc?	☑	☐	
46	¿Existe algún proceso para asegurar que los empleados y los contratistas hagan devolución de los activos de información de propiedad de la empresa a la terminación de su contrato laboral?	☐	☑	
PRINCIPIO: Prioriza los riesgos				
47	¿La empresa toma acciones para identificar factores críticos de riesgos potenciales en los procesos?	☐	☑	
PRINCIPIO: Implementa las respuestas al riesgo				
48	¿Se hace uso de una herramienta de gestión de autoevaluación para la	☐	☑	
49	¿La empresa cuenta con procedimientos establecidos para mitigar riesgos identificados por fraude, robo datos, substracción de información confidencial con el fin de prevenirlos o detectarlos?	☑	☐	
50	¿Los procedimientos informáticos incluyen actividades de control para evaluar el desempeño?	☐	☑	
PRINCIPIO: Desarrollar un portafolio de riesgos				
51	¿En el área de contabilidad se monitorea nuevos riegos originados en los reportes financieros?	☑	☐	
52	¿El área de ventas cuenta con un sistema de información confiable para la obtención de reportes de ventas?	☑	☐	
53	¿El sistema de información genera reportes confiables en el área de producto terminado?		☑	Existen deficiencias en los inventarios
N°	**COMPONENTE: REVISIÓN**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Evalúa los cambios sustanciales				
54	¿Los procesos informáticos son evaluados para determinar su impacto en el cumplimiento de la estrategia de la gestión de riesgos?	☐	☑	
55	¿Se evaluan los cambios relevantes que se hayan producido en el procesamiento de la información?	☐	☑	

PRINCIPIO: Revisa los riesgos y el desempeño				
56	¿En los procedimientos informaticos de las áreas de contabilidad, producto terminado y ventas se han identificado riesgos?	☑	☐	
PRINCIPIO: Propone mejoras en la gestión de riesgos empresariales				
57	¿Para el seguimiento de las estrategias se evalua el cumplimiento de los objetivos periódicamente?	☑	☐	
58	¿Se realizan auditorías en la empresa para medir la razonabilidad de la información en los diferentes procesos?	☑	☐	
N°	**COMPONENTE: Información, comunicación y reporte**	**SI**	**NO**	**OBSERVACIÓN**
PRINCIPIO: Aprovecha la información y la tecnología				
59	¿Existe un marco de referencia para la evaluación sistemática de los riesgos a los que está expuesta la infraestructura tecnológica de la institución?	☐	☑	
60	¿El sistema implementado en la empresa poseen información oportuna y confiable para evitar el doble registro de operaciones?	☑	☐	
61	¿La empresa maneja alguna app para la realizacion de ventas?	☐	☑	La empresa cuenta una app pero no la utilizan
62	¿Realiza procesos de concientización con los empleados por mantener la seguridad de los activos?	☐	☑	
63	¿Los activos de información se codifican o etiquetan mediante algún programa?	☑	☐	
64	¿Se posee bitácoras de fallas detectadas en los equipos?	☐	☑	
65	¿Se realizan copias de seguridad de la base de datos?	☑	☐	
66	¿Los usuarios respaldan informacion en cada uno de sus equipos a cargo?	☑	☐	
67	¿Se tienen actualizados los inventarios de activos físico y lógicos de la red?	☑	☐	
68	¿La empresa trabaja con sistema en red?	☑	☐	
PRINCIPIO: Comunica los riesgos de información				
69	¿En el modo en que se establece nuevas políticas y procedimientos son estos comunicados?	☑	☐	
70	¿Se comunica oportunamente al gerente los riesgos identificados que afectan el cumplimiento de los objetivos empresariales?	☑	☐	
PRINCIPIO: Informes sobre riesgos, cultura y desempeño				
71	¿Los diferentes departamentos presentan informes sobre riesgos identificados y posibles medidas de mitigación?	☑	☐	Solo son avisos, no informes

Anexo 3

Tablas de la Evaluación de los procesos informáticos de COBIT 2019

Dominio: Evaluar, Orientar y Monitorear

Asegurar la Optimización del Riesgo EDM03

	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
ACTIVIDADES	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo)	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
ACTIVIDADES	NIVEL MÍNIMO ACEPTABLE	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE

Dominio: Alinear, Planificar y Organizar

Gestionar el Riesgo APO12

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ capturar. Proponer la respuesta al riesgo óptima.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE

Gestionar la Seguridad APO13

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
7. Comunicar el enfoque de SGSI	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Recomendar programas de formación y concienciación en seguridad de la información.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
2. Realizar auditorías internas al SGSI a intervalos planificados	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

Dominio: Construir, Adquirir e Implementar

Gestionar los Cambios BAI06

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Categorizar todas las peticiones de cambio (ej. procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software externo adquirido) y relacionarlas con los elementos de configuración afectados.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados. Evaluar la probabilidad de que afecten negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, legales, contractuales, y de cumplimiento normativo del cambio solicitado. Considerar además todas las inter-dependencias entre cambios. Involucrar a los propietarios de procesos de negocio en el proceso de evaluación, de forma apropiada.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
6. Planificar y programar todos los cambios aprobados.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
7. Considerar el impacto en los proveedores de servicios contratados (ej. procesamiento de negocio externalizado, infraestructuras, desarrollo de aplicaciones y servicios compartidos) en el proceso de gestión del cambio, incluyendo la integración de la gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y ANSs	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE

	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
ACTIVIDADES	**NIVEL MÍNIMO ACEPTABLE (NMA)**	**NIVEL OBSERVADO (NO)**	**BRECHA**		**F**	**L**	**P**	**N**	**VALOR**	**METAS**	**OBSERVACIÓN**
1. Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar elcambio de emergencia.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
3. Supervisar todos los cambios de emergencia y realizar revisiones post-implantación involucrando a todas las partes interesadas. La revisión debería considerar e iniciar acciones correctivas basadas en causas raíz tales como problemas en los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales e integridad de datos	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Definir qué constituye un cambio de emergencia	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE

	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
ACTIVIDADES	**NIVEL MÍNIMO ACEPTABLE (NMA)**	**NIVEL OBSERVADO (NO)**	**BRECHA**		**F**	**L**	**P**	**N**	**VALOR**	**METAS**	**OBSERVACIÓN**
1. Categorizar las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados pero aún no iniciados, aprobados y en proceso y cerrados).	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
4. Mantener un sistema de seguimiento e informe para todas las peticiones de cambio	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
ACTIVIDADES	**NIVEL MÍNIMO ACEPTABLE (NMA)**	**NIVEL OBSERVADO (NO)**	**BRECHA**		**F**	**L**	**P**	**N**	**VALOR**	**METAS**	**OBSERVACIÓN**
1. Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio como parte integral del cambio	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación de usuario.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Someter a la documentación a la misma revisión que al cambio en sí mismo.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

Gestionar los Activos BAI09

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Identificar todos los activos en propiedad en un registro que indique el estado actual. Mantener su alineación con los procesos de gestión de cambios y de la configuración, el sistema de gestión de la configuración y los registros contables financieros.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Verificar la existencia de todos los activos en propiedad mediante la realización periódica de controles de inventario físicos y lógicos y su conciliación, incluyendo la utilización de herramientas software de descubrimiento.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Comprobar que los activos se adecuan a sus objetivos (p.ej., están en condiciones útiles).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6. Asegurar la contabilización de todos los activos.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSEERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Identificar los activos que son críticos en la provisión de la capacidad del servicio refiriéndose a los requisitos en las definiciones de servicio, ANSs y el sistema de gestión de la configuración	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes y, en caso necesario, tomar medidas para reparar o reemplazar	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. De forma regular, considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
4. Mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, de supervisión del rendimiento y, si fuera necesario, proporcionando alternativas y/o activos adicionales para reducir la probabilidad de fallo.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Establecer un plan de mantenimiento preventivo para todo el hardware, considerando un análisis coste-beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. Establecer contratos de mantenimiento que impliquen el acceso de terceros a las instalaciones de TI de la organización para actividades in situ y fuera del sitio (p. ej. externalización). Establecer contratos formales de servicio que contengan o se refieran a todas las condiciones de seguridad necesarias, incluidos los procedimientos de autorización de acceso, para garantizar el cumplimiento de las políticas y estándares de seguridad de la organización.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
7. Comunicar a los clientes y los usuarios afectados el impacto esperado (p. ej., las restricciones de rendimiento) de las actividades de mantenimiento	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
8. Asegurar que los servicios de acceso remoto y perfiles de usuario (u otros medios utilizados para el mantenimiento o diagnóstico) están activos sólo cuando sea necesario	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
9. Incorporar el tiempo de inactividad previsto en general en el calendario de producción, y programar las actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico, si fuera necesario.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por contrato.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Asignar activos a los usuarios, con aceptación y firma de responsabilidades, según corresponda.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. Reasignar los activos siempre que sea posible cuando ya no sean necesarios debido a un cambio de función de rol del usuario, redundancia dentro de un servicio o finalización de un servicio.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
7. Eliminar los activos cuando no sirvan a ningún propósito útil debido a la finalización de todos los servicios relacionados, tecnología obsoleta o falta de usuarios.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
8. Eliminar los activos de forma segura, teniendo en cuenta, por ejemplo, la eliminación permanente de los datos registrados en dispositivos y posibles daños al medio ambiente.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
9. Planificar, autorizar y realizar las actividades relacionadas con la finalización de uso, manteniendo los registros apropiados para satisfacer las necesidades regulatorias y cambiantes del negocio	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Revisar la base general de activos de forma regular, teniendo en cuenta si está alineada con los requerimientos del negocio.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor coste, incluyendo, cuando sea necesario, el reemplazo con nuevas alternativas	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Revisar las garantías y considerar la relación calidad-precio y estrategias de reemplazo para determinar opciones de menor coste.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Revisar la base general para identificar oportunidades de normalización, abastecimiento único y otras estrategias que pueden disminuir los costes de adquisición, soporte y mantenimiento	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
5. Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6. Revisar el estado general para identificar las oportunidades para aprovechar tecnologías emergentes o estrategias de aprovisionamiento alternativas para reducir los costes o incrementar el valor del dinero.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. De forma regular, llevar a cabo una auditoría para identificar a todos las copias de software instalado con licencia.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Comparar el número de copias de software instalado con el número de licencias en propiedad.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Cuando las copias sean inferiores al número en propiedad, decidir si existe una necesidad de mantener o cancelar licencias, considerando el potencial de ahorrar en mantenimiento innecesario, formación y otros gastos.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5 Cuando las copias sean superiores al número en propiedad, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas, y después, si es necesario, adquirir licencias adicionales para cumplir con los acuerdos de licencia.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. De forma regular, considerar si se puede obtenerse un mejor valor mediante la actualización de productos y licencias asociadas.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

Dominio: Entregar, dar Servicio y Soporte

Gestionar las Operaciones DSS01

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4. Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs con terceros que alojan o proveen servicios.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
4. Planificar la realización de auditorías y aseguramientos independiente de los entonos operativos de los proveedores de externalización (outsourcing) 51:56para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
3. Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no estén sobrecargados con información innecesaria.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
6. Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, está protegido contra las amenazas del entorno. Asegurar que la política limite o impida comer, beber y fumar en áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio en los centros de procesamiento de datos.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
4. Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados. Atender a los puntos de no-conformidad de manera oportuna.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
7. Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p.ej. robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servidores de producción y de desarrollo alejados entre sí).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
8. Mantener en todo momento a los sitios de TI y las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSEERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Examinar los requerimientos de las instalaciones de TI respecto de la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación ininterrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad del negocio.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Probar periódicamente los mecanismos del sistema de alimentación ininterrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en conductos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado. Proteger adecuadamente al cableado contra el daño causado por fuego, humo, agua, interceptación e interferencia.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Asegurar que el cableado y el patching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p.ej. plano del edificio y diagramas de cableado).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
7. Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
8. Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo. Capacitar al personal en simulacros de incendio y rescate para asegurar el adecuado conocimiento y las acciones apropiadas a tomar en caso de incendio o incidentes similares.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
9. Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición informes sobre incidentes en instalaciones donde la legislación y las regulaciones requieran su divulgación.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
10. Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
11. Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p.ej. daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de continuidad de negocio y de gestión de edificios.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE

Gestionar Servicios de Seguridad DSS05

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3.Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
4.Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5.Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6.Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1.Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2.Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Cifrar la información en tránsito de acuerdo con su clasificación.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6.Configurar los equipamientos de red de forma segura.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
8.Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
9.Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSEERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Configurar los sistemas operativos de forma segura.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Implementar mecanismos de bloqueo de los dispositivos.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Cifrar la información almacenada de acuerdo a su clasificación.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Gestionar el acceso y control remoto.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
5. Gestionar la configuración de la red de forma segura.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
7. Proteger la integridad del sistema.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
8. Proveer de protección física a los dispositivos de usuario final.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
9. Deshacerse de los dispositivos de usuario final de forma segura.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5.Segregar y gestionar cuentas de usuario privilegiadas.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6.Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
8.Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
7. Realizar regularmente formación de concienciación de seguridad física.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3.. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
4.Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE
5.Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	3	0	3	BRECHA SIGNIFICATIVA				14	14	F	NO CUMPLE

Dominio: Supervisar, Evaluar y Valorar

Supervisar, Evaluar y Valorar Rendimiento y Conformidad MEA01

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Identificar las partes interesadas (p. ej. dirección, propietarios de procesos o usuarios).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
2. Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes (p. ej. glosario corporativo, metadatos y taxonomías), líneas de referencia y estudios comparativos (benchmarking).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía así como las herramientas utilizadas para la obtención de datos y presentación de informes corporativos (p. ej. aplicaciones de inteligencia de negocio).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Acordar los objetivos y métricas (p. ej., cumplimiento, rendimiento, valor, riesgo), taxonomía (clasificación y relación entre objetivos y métricas) y la retención de datos (evidencias).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Acordar un proceso de control de cambios y de gestión del ciclo de vida de la supervisión y la presentación de informes. Incluir oportunidades de mejora para la presentación de la información, métricas, enfoque, líneas de referencia y estudios comparativos	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
6. Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
7. Validar periódicamente el enfoque utilizado e identificar los nuevos o cambiantes grupos de interés, requisitos y recursos.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Definir y revisar periódicamente los objetivos y métricas con las partes interesadas para identificar cualquier detalle significativo omitido y definir la razonabilidad de metas y tolerancias.	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
2. Comunicar los cambios propuestos en las metas y tolerancias de rendimiento y cumplimiento (referidos a las métricas) con las partes interesadas clave con la debida diligencia (p. ej., legal, auditoría, RR.HH., ética, cumplimiento y financiero).	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
3. Hacer público a los usuarios de la información los cambios en metas y tolerancias	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Evaluar si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Diseñar informes de rendimiento de procesos que sean concisos, fáciles de entender y ajustados a las diferentes necesidades de gestión y audiencias. Facilitar la toma efectiva y oportuna de decisiones (p. ej., cuadros de mando, informes con semáforos) y asegurar que la causa y el efecto entre objetivos y métricas se comunican de una forma comprensible.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Comparar los valores de rendimiento con metas y estudios comparativos internos (benchmarks) y, cuando sea posible, con estudios comparativos externos (tanto del sector, como respecto a competidores clave).	3	1	2	BRECHA MODERADA			50		50	F	NO CUMPLE
3. Recomendar cambios a los objetivos y métricas, cuando sea procedente.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
4. Distribuir los informes a las partes interesadas relevantes.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE
5. Analizar la causa de las desviaciones respecto a las metas, iniciar acciones correctivas, asignar responsabilidades para la remediación y realizar su seguimiento. En el momento oportuno, revisar todas las desviaciones y buscar causas raíz cuando sea necesario. Documentar las incidencias para contar con guía adicional si el problema vuelve a aparecer. Documentar los resultados.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
6. Cuando sea factible, enlazar el cumplimiento de objetivos de desempeño con el sistema de compensación y gratificación de la organización.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE

ACTIVIDADES	NIVEL DE MADUREZ				NIVEL DE CAPACIDAD DE PROCESOS				NIVEL DE CUMPLIMIENTO		
	NIVEL MÍNIMO ACEPTABLE (NMA)	NIVEL OBSERVADO (NO)	BRECHA		F	L	P	N	VALOR	METAS	OBSERVACIÓN
1. Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
2. Asegurar que se mantiene la asignación de responsabilidades en las acciones correctivas.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
3. Hacer seguimiento de los resultados de las acciones comprometidas.	3	2	1	BRECHA MÍNIMA		65			65	F	NO CUMPLE
4. Informar de los resultados a las partes interesadas.	3	3	0	BRECHA MÍNIMA		75			75	F	NO CUMPLE