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:

"Sistema de control interno a los procesos informáticos de la empresa "La Bahía" de la ciudad de Ambato"

Autora: Cepeda Cruz, Eliana Carolina

Tutora: Ing. Sánchez Herrera, Bertha Jeaneth

Ambato – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Ing. Bertha Jeaneth Sánchez Herrera con cédula de identidad No. 180373657-6, en calidad de Tutora del proyecto integrador sobre el tema: "**SISTEMA DE CONTROL INTERNO A LOS PROCESOS INFORMÁTICOS DE LA EMPRESA "LA BAHÍA" DE LA CIUDAD DE AMBATO**", desarrollado por Eliana Carolina Cepeda Cruz, 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, junio 2022

TUTORA

Ing. Bertha Jeaneth Sánchez Herrera

C.I. 180373657-6

DECLARACIÓN DE AUTORÍA

Yo, Eliana Carolina Cepeda Cruz con cédula de identidad No.1804392882, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: **"SISTEMA DE CONTROL INTERNO A LOS PROCESOS INFORMÁTICOS DE LA EMPRESA "LA BAHÍA" 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, junio 2022

AUTORA

Eliana Carolina Cepeda Cruz
C.I. 1804392882

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 primordiales 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, junio 2022

AUTORA

Eliana Carolina Cepeda Cruz
C.I. 1804392882

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema: **"SISTEMA DE CONTROL INTERNO A LOS PROCESOS INFORMÁTICOS DE LA EMPRESA "LA BAHÍA" DE LA CIUDAD DE AMBATO"**, elaborado por Eliana Carolina Cepeda Cruz, 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, junio 2022

Dra. Mg. Tatiana Valle

PRESIDENTE

Dr. Guido Tobar

MIEMBRO CALIFICADOR

Dr. Edisson Coba

MIEMBRO CALIFICADOR

DEDICATORIA

Cada esfuerzo, cada sacrificio que hice para lograr mi meta, se la dedico primeramente a Dios por haberme dado mucha salud y conocimiento para seguir adelante, también dedico a mis padres Martha y Enrique que fueron mi pilar fundamental para cumplir mis sueños, además quiero dedicar a mis segundos padres Felipe y Elena que fueron mi guía y apoyo, también dedico a toda mi familia por siempre apoyarme y no dejarme.

A mis dos angelitos del cielo mis abuelitos Ángel y Romelia, que desde su partida me han enseñado a ser fuerte y guerrera, son y serán mi inspiración toda mi vida.

Quiero también dedicar mi trabajo a mi novio Cristian Remache por siempre apoyarme y enseñarme a cada momento.

A mis dos mascotas Boby y Pelusita por siempre ser mi felicidad.

Eliana Carolina Cepeda Cruz

AGRADECIMIENTO

Quiero agradecer a Dios por permitirme cumplir mi sueño tan anhelado y agradécele por la oportunidad de seguir luchando mis sueños, a la vez agradecer a mis padres Martha y Enrique por siempre estar a mi lado en las buenas y en las malas, a mis abuelitos Felipe y Elena por ser mis segundos padres quienes me han guiado para cumplir mi sueño.

A mis angelitos del cielo Ángel y Romelia quienes fueron mi apoyo espiritual desde su partida.

A toda mi familia quienes me supieron dar una mano en cualquier momento. También quiero agradecer a todos mis docentes que fueron mi guía en mi vida universitaria y en especial a mi querida docente Ing. Berthita Sánchez quien desde el inicio de mi carrera me supo enseñar y valorar el esfuerzo que debemos dar para cumplir el sueño tan anhelado que tengo.

A mi novio Cristian Remache por siempre estar a mi lado en todo momento y a todos mis amigos.

Eliana Carolina Cepeda Cruz

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "SISTEMA DE CONTROL INTERNO A LOS PROCESOS INFORMÁTICOS DE LA EMPRESA "LA BAHÍA" DE LA CIUDAD DE AMBATO"

AUTORA: Eliana Carolina Cepeda Cruz

TUTORA: Ing. Bertha Jeaneth Sánchez Herrera

FECHA: Junio 2022

RESUMEN EJECUTIVO

Analizando la situación que está pasando la empresa en cuanto a los procesos informáticos en los tres procesos que son ventas, compras y contabilidad se procede al diseño del Sistema de Control Interno a los procesos informáticos en la empresa "La Bahía" de la ciudad de Ambato teniendo como objetivo principal el cumplimiento de metas corporativas. Es por ello, que para el diseño se realizó un diagnóstico de información de la situación actual de la empresa con relación a los procesos y activos informáticos que poseen. Además, se realizó entrevistas a la Gerente y contadora con el fin de conocer todos los problemas que han ocurrido. También se ocupó la metodología COBIT 5 con sus cinco componentes y sus principios, los cuales fueron la base para identificar los problemas. De acuerdo con los problemas encontrados en base a la aplicación de la metodología se diseñó el Sistema de Control Interno, el cual contiene políticas, controles y procedimientos en base a cada problema que tienen como objetivo solucionarlos de manera eficiente y a la vez concientizando la importancia del manejo correcto de los activos informáticos.

PALABRAS DESCRIPTORAS: SISTEMA DE CONTROL INTERNO, ACTIVOS INFORMÁTICOS, COBIT 5, PROCESOS, PROCESOS INFORMÁTICOS.

TECHNICAL UNIVERSITY OF AMBATO

FACULTY OF ACCOUNTING AND AUDITING

ACCOUNTING AND AUDITING CAREER

TOPIC: "INTERNAL CONTROL SYSTEM FOR THE COMPUTER PROCESSES OF THE "LA BAHÍA" COMPANY OF THE CITY OF AMBATO"

AUTHOR: Eliana Carolina Cepeda Cruz

TUTOR: Ing. Bertha Jeaneth Sánchez Herrera

DATE: June 2022

ABSTRACT

Analyzing the situation that the company is going through in terms of computer processes in the three processes that are sales, purchases and accounting, we proceed to the design of the Internal Control System for the computer processes in the company "La Bahia" in the city of Ambato having as main objective the fulfillment of corporate goals. That is why, for the design, an information diagnosis was made of the current situation of the company in relation to the processes and computer assets they possess. In addition, interviews were conducted with the Manager and accountant in order to learn about all the problems that have occurred. The COBIT 5 methodology was also dealt with with its five components and its principles, which were the basis for identifying problems. According to the problems found based on the application of the methodology, the Internal Control System was designed, which contains policies, controls and procedures based on each problem that aim to solve them efficiently and at the same time raising awareness of the importance of proper management of computer assets.

KEYWORDS: INTERNAL CONTROL SYSTEM, IT ASSETS, COBIT 5, PROCESSES, IT PROCESSES.

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

PÁGINAS PRELIMINARES

ÍNDICE DE ILUSTRACIONES

CONTENIDO **PÁGINA**

ÍNDICE DE GRÁFICOS

CONTENIDO **PÁGINA**

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

CAPÍTULO I

MARCO TEÓRICO

1.1 Introducción

1.1.1 Antecedentes del proyecto integrador

El 9 de enero del 2002 en la ciudad de Ambato la Sra. Rosa Benigna Torres Rodríguez creó la empresa “La Bahía”, con su respectivo RUC # 1705424271001 acompañado de su eslogan en donde describe dos palabras importantes para sus clientes que es la tranquilidad y la economía, teniendo en cuenta que el consumidor es el punto clave para el crecimiento de la empresa.

La empresa lidera en la ciudad de Ambato por su actividad económica, que es la venta al por menor de electrodomésticos como: refrigeradoras, cocinas, microondas, lavadoras, entre otros.

Lo que le diferencia del resto de las empresas es su stock, su imagen corporativa, que hacen que el cliente sienta confianza y pueda encontrar todo lo que necesita en un solo lugar.

El edificio principal se encuentra ubicado en la ciudad de Ambato en la Av. Atahualpa diagonal al Comercial KYWI S.A. y la sucursal en el centro de la ciudad en las calles Juan Benigno Vela y Joaquín Lalama.

Ilustración 1. Ubicación de la empresa “La Bahía”

Fuente: Google Maps

A continuación, se presenta los pilares fundamentales que la empresa posee:

MISIÓN

Ofrecer a nuestros clientes electrodomésticos de calidad a un precio económico, dándoles la mayor tranquilidad para que puedan solventar sus necesidades.

VISIÓN

Ser la empresa líder a nivel nacional en la venta de electrodomésticos, superando las expectativas de nuestros clientes e ir mejorando nuestra propuesta de negocio.

VALORES EMPRESARIALES

Los valores más importantes de la empresa son el respeto, la equidad, integridad, puntualidad, responsabilidad, eficiencia, lealtad, liderazgo, integridad y el trabajo en equipo que es muy indispensable en el crecimiento empresarial.

ORGANIGRAMA EMPRESARIAL

La empresa “La Bahía” de la ciudad de Ambato tiene el siguiente organigrama:

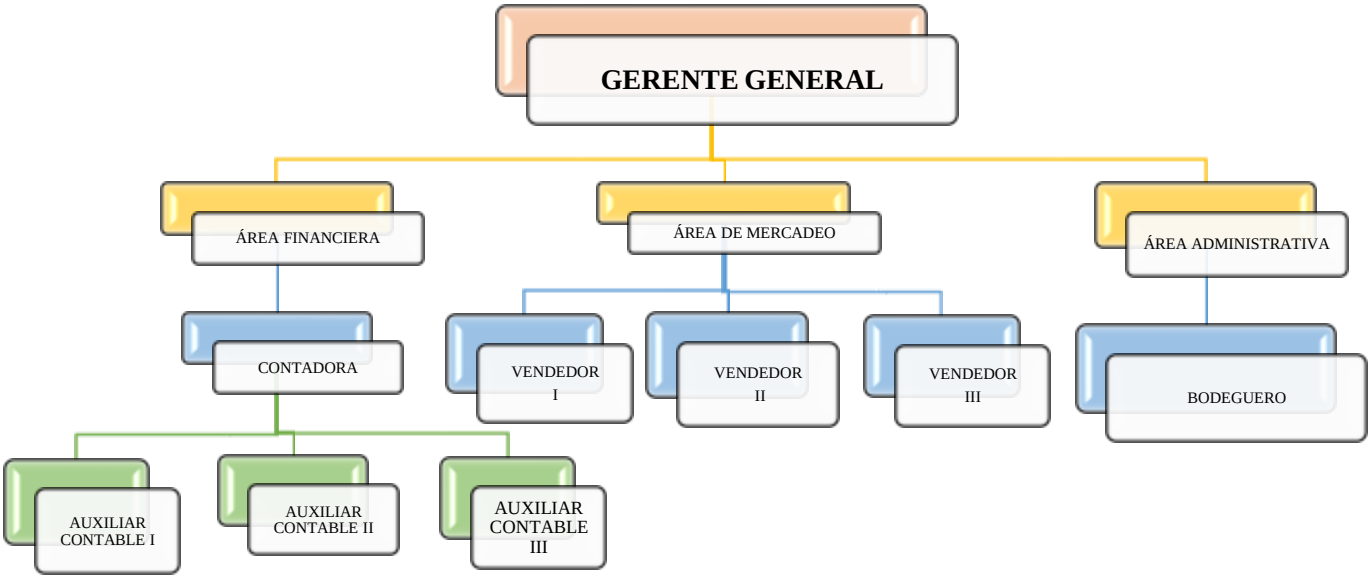


Gráfico 1. Organigrama “La Bahía”
Fuente: Elaboración propia

FUNCIONES

- **GERENTE GENERAL**
    - Planificar todas las actividades que deben ser desarrolladas en la empresa.
    - Solucionar los problemas de manera rápida y eficiente.
    - Supervisar y controlar a los empleados.
    - Gestionar y administrar los presupuestos de la empresa.
    - Mantener y buscar proveedores potenciales.
    - Dirige todas las actividades a cumplir en la empresa.
- **CONTADORA**
    - Dirigir a sus auxiliares contables.
    - Establecer actividades a cada una de sus auxiliares.
    - Identificar los errores de manera más rápida y eficaz.
    - Elaboración de los estados financieros.
    - Analizar e identificar la situación económica de la empresa.
    - Elaborar las declaraciones y demás asuntos tributarios.
    - Mantener toda la información al día de todos los soportes en el software contable.
    - Asesorar financiera y tributariamente al gerente.
    - Administrar los recursos financieros.
    - Gestionar la nómina de la empresa.
    - Analizar las ganancias y los gastos.
- **AUXILIAR CONTABLE No. 1**
    - Se encarga de las compras.
    - Revisión del inventario.
    - Revisar a los clientes potenciales mensualmente.
    - Controla las ventas.
    - Control de los proveedores.
    - Otras actividades que requieren el departamento contable.
- **AUXILIAR CONTABLE No. 2**
    - Se encarda de la cartera de clientes
    - Control de las tarjetas de crédito

- Control de los inventarios.
- Control de los proveedores.
- Otras actividades que requieren el departamento contable.

- **AUXILIAR CONTABLE No. 3**
  - Responsable de los pagos a proveedores.
  - Control de los proveedores.
  - Otras actividades que requieren el departamento contable.
  - Controla los inventarios.
  - Control de las tarjetas de crédito.
  - Realiza presupuestos financieros.
- **VENDEDORES**
  - Asignación de los precios en los productos.
  - Resuelven y responden a todas las consultas o dudas que tenga el cliente ante un producto.
  - Capta a los clientes potenciales.
  - Asesora de manera personalizada a cada cliente.
  - Explicar a los clientes las características y cualidades de los productos.
  - Tener un conocimiento de todos los productos y características que posee la empresa.
- **BODEGUERO**
  - Encargado de recibir toda la mercadería.
  - Lleva un control de la mercadería que tenga en bodega.
  - Mantener la bodega limpia y ordenada.
  - Encargo de distribuir la mercadería a los diferentes locales.
  - Organizar todos los movimientos de mercadería dentro de la bodega.

SISTEMAS INFORMÁTICO

En la empresa utilizan el sistema contable llamado **MICROPLUS** en donde guarda toda la información de la empresa, el mismo que está conectado a varios computadores mediante red.

Ilustración 2. Sistema contable Microplus SQL Profesional

Fuente: Empresa" La Bahía"

FODA

En la empresa "LA BAHÍA" podemos encontrar sus debilidades, amenazas, fortalezas y lo más relevante las oportunidades, que se presentan a continuación mediante un gráfico:

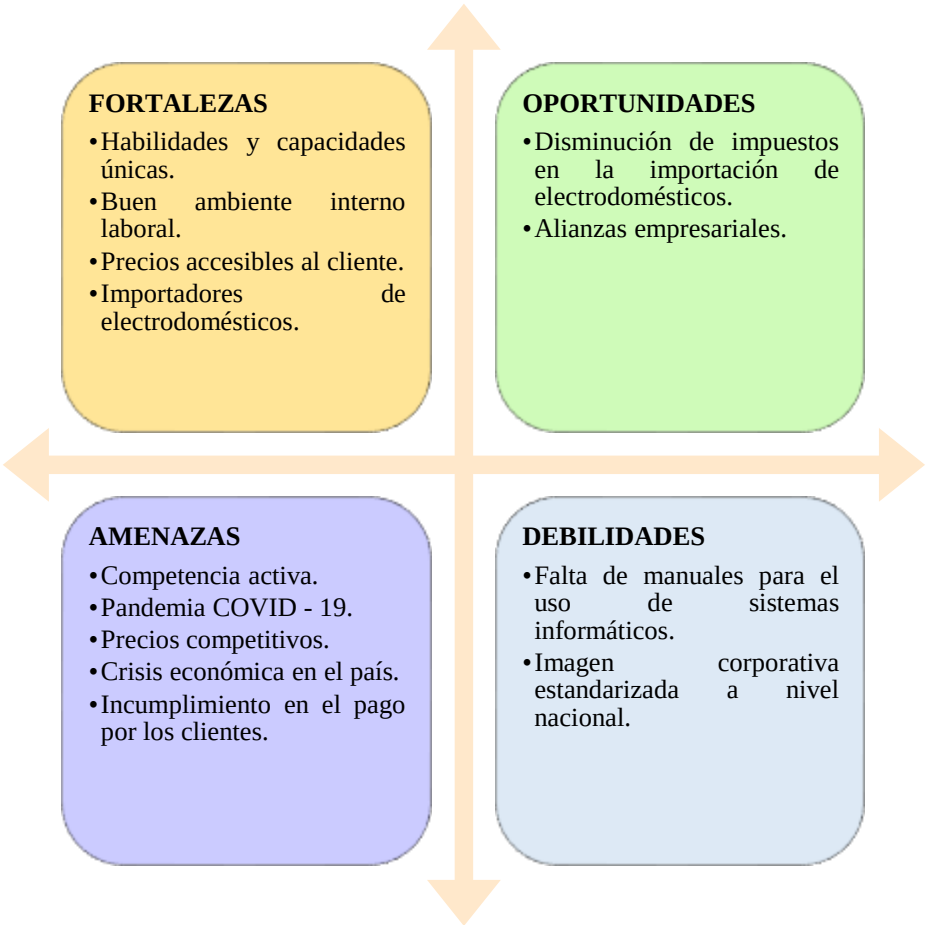


Gráfico 2. Análisis FODA
Fuente: Empresa "La Bahía"

1.1.2 Descripción del entorno

En el mundo actual el control interno es uno de los pilares fundamentales en todas las organizaciones empresariales, el cual permite observar claramente la eficacia y eficiencia de las empresas, se puede identificar en la confiabilidad de los registros y el cumplimiento de todas las normas, leyes y regulaciones que se apliquen en cada proceso productivo (Mendoza-Walter, Delgado-María y Ponce-Tania, 2018).

Así mismo, cabe resaltar que todas las empresas latinoamericanas han aplicado controles internos en sus operaciones, lo cual les ha ayudado a conocer la seguridad real, en donde aprendieron la importancia de la planificación para que puedan verificar cada uno de los controles cumplan su función, para darle una mejor versión sobre la gestión , además es claramente indispensable tener un buen sistema de control interno en las empresas (Mendoza-Walter et. al. ,2018).

Por lo tanto, como menciona Cabrera y Ortega (2013):

> La importancia de tener un buen sistema de control interno en las organizaciones se ha incrementado en los últimos años, debido a lo práctico que resulta medir la eficiencia y la productividad en el momento de implantarlos; en especial si se centra en las actividades básicas que ellas realizan, pues de ello dependen para mantenerse en el mercado (p. 2).

Además, el control interno es aquel que se perfila como un mecanismo correcto para contribuir en cada uno de los esfuerzos que realiza la empresa, por ende, garantiza razonablemente los principios que posee (Gamboa-Jinsop, Puente-Silvia y Vera-Piedad, 2016).

Es decir, que el sistema de control interno ha sido muy utilizado en los últimos años, debido a lo práctico que resulta medir la eficiencia y la productividad al momento de implantarlos, en especial si se lo hace en las actividades que tienen, para así poder mantenernos en el mercado (Cabrera y Ortega, 2013).

Sin embargo, como afirma Cabrera y Ortega (2013):

> El control interno en una entidad está orientado a prevenir o detectar errores e irregularidades, las diferencias entre estos dos es la intencionalidad del hecho; el término error se refiere a omisiones no intencionales, y el término irregular se refiere a errores intencionales (p. 2).

Es por ello, que las empresas ecuatorianas ocupan el control interno por el impacto positivo dentro de la organización, cada avance tecnológico induce a la empresa a disponer de información cada vez más certera , oportuna y especializada en descubrir los escándalos contables como financieros que estén dentro de la empresa (Lopez y Cañizares, 2018).

Por ende, las empresas ameritan poseer un sistema de control interno, en donde el representante legal que es el gerente general pueda visualizar los defectos que la empresa posee, es por eso que la misión del control interno es encontrar las deficiencias y oportunidades, para poder tomar decisiones oportunas, manteniendo así en el mercado a la organización.

Por lo tanto, se realizó una visita a la empresa “LA BAHÍA”, en donde se detectó algunos inconvenientes en cuanto a la seguridad de los procesos informáticos que posee la organización, dando como resultado una deficiencia en el proceso en donde puede existir un hallazgo, y amerite investigación en cada uno de los procesos.

En base a lo anteriormente mencionado se le realizó una propuesta sobre la implementación de un sistema de control interno en los procesos informáticos de la empresa, para que dé está manera la organización pueda operar de manera eficiente en los procesos y así poderse mantener en el mercado sin ninguna novedad, es por ello que se dará recomendaciones en base al estudio realizado con el fin que puedan aplicarlas.

1.1.3 Justificación

1.1.3.1 Justificación teórica

El control interno se ejecuta en absolutamente todos los niveles que la organización tenga, en diferentes etapas de los procesos, también se puede decir en el cumplimiento de normas y a la vez en la seguridad en el uso de todas las tecnologías, en donde sirven

como mecanismos que aseguran el cumplimiento de los objetivos, visión y misión. (Villa-César, Samaniego-Florípes y Ulloa-Diana ,2017).

A medida que ha pasado el tiempo los problemas de corrupción y los fraudes detectados en cada entidad inclusive las entidades internacionales, vieron la necesidad de implementar el control interno en diferentes países, por ende, el control interno es la base principal en la auditoría.

Además, como menciona Villa et al. (2017):

> El control interno se convierte en una función inherente a la administración, integrada al funcionamiento organizacional y a la dirección institucional y deja así, de ser una función que se asignaba a un área específica de una empresa (p. 2).

Dentro del marco de auditoría, el control interno es una herramienta indispensable para una gestión contable y financiera, la cual nos ayuda a estudiar la eficiencia de los procedimientos establecidos.

Por lo tanto, como manifiesta Mantilla (2013):

> El control interno comprende el plan de la organización y todos los métodos y medidas coordinados que se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y la confiabilidad de sus datos contables, promover la eficiencia operacional y fomentar la adherencia a las políticas escritas (p. 22).

La empresa necesita el apoyo fundamental del control interno, el mismo que ayuda a la administración para que puedan planear, analizar y dirigir correctamente el desempeño de las acciones que dan seguridad para cumplir todos los objetivos, que ayuden a salvaguardar los activos logrando un uso económico eficiente de los recursos (Mantilla, 2013).

Es por ello, que Blanco Encinosa (2008) menciona que:

> En la actualidad la auditoría ha pasado a ser un patrimonio de toda una serie de actividades humanas como medicina, la economía, el control medioambiental, etc. La esencia del término "auditoría" es sinónimo de revisión, análisis, control, examen, búsqueda, etc. (p. 16).

La importancia y la necesidad del control interno cada día se resalta más en el mundo actual, llevando así que cada empresa pueda tener un plan de organización, con cada uno de los métodos y medidas que puedan ser adaptados de acuerdo a sus negocios.

Por consiguiente (Blanco Encinosa, 2008) menciona a la auditoría utilizando sistemas informáticos como un:

> Conjunto de técnicas y procedimientos que ayudan a una empresa a evaluar el grado que cumple la observancia de todos los controles interno que posee el Sistema Informático, teniendo en cuenta que determina el grado de protección de los activos y recurso informáticos, que nos ayuda a verificar sus actividades que podrán desarrollarse de manera eficiente.

Se puede mencionar que toda medida, acción, plan al sistema que tenga la empresa, y su cumplimiento de sus objeticos es una fortaleza para el control interno, y al no cumplirla es una debilidad en vista de que es una herramienta que identifica los factores de riesgo en ciertas áreas logrando un objetivo.

Siendo así, Mendoza-Walter, Delgado-María y Ponce-Tania (2018) manifiesta que:

> El Control Interno bien aplicado contribuye fuertemente a obtener una gestión óptima, toda vez que genera beneficios a la administración de la entidad, en todos los niveles, así como en todos los procesos, subprocesos y actividades en donde se implemente.

Se puede desarrollar un control interno adecuado a cada tipo de organización, que nos permitirá optimizar la utilización de recursos con calidad para alcanzar una adecuada gestión financiera y administrativa, logrando así mejores niveles de productividad (Mendoza-Walter, Delgado-María, Ponce-Tania, 2018).

De igual forma como menciona Mendoza-Walter, Delgado-María y Ponce-Tania (2018):

> Es una herramienta surgida de la imperiosa necesidad de accionar proactivamente a los efectos de suprimir y/o disminuir significativamente la multitud de riesgos a las cuales se hayan afectadas los distintos tipos de organizaciones, sean estos privados o públicos, con o sin fines de lucro, siendo la base donde descansan las actividades y operaciones de una entidad; es decir, que las actividades de producción, distribución, financiamiento, administración, entre otras, son regidas por el Control Interno; además, es un instrumento de eficiencia y no un plan que proporciona un reglamento tipo policíaco o de carácter tiránico (p. 10).

Finalmente, podemos decir que el control interno se adecúa a las necesidades de la empresa, buscando proteger los recursos de la entidad previniendo y detectando fraudes, errores dentro de los diferentes procesos que posee la empresa.

1.1.3.2 Justificación Práctica

Los sistemas informáticos de la empresa serán evaluados mediante la metodología COBIT, en donde se amplíen los conocimientos sobre su aplicación, por ende, se pueda identificar claramente los problemas que posee la empresa para corregir de la manera más eficiente y eficaz. Adicionalmente les permitirá crear y aplicar algunos controles internos que fortalezcan los sistemas informáticos, logrando así una mayor productividad en la gestión empresarial.

El presente proyecto tendrá un impacto positivo en donde la institución conocerá que al utilizar está metodología COBIT se podrá identificar la importancia de manejar correctamente los modelos de madurez. A la vez le ayudará a tomar las decisiones correctas, eso quiere decir que incrementará sus utilidades en un porcentaje mínimo, pero con el pasar del tiempo se incrementará hasta en un 50%, en vista de que sus procesos tecnológicos operarán de manera eficiente.

Finalmente, en la empresa los procesos de tecnología de información deben operar de manera correcta, para lo cual se debe aplicar políticas, procedimientos, normas de

control y ser evaluados mediante la metodología COBIT, que permitirá identificar los riesgos que dificultan el normal funcionamiento de la organización en la parte tecnológica y la gestión de procesos.

1.1.4 Objetivos

1.1.4.1 Objetivo general

Diseñar un sistema de control interno a los procesos informáticos en la empresa "LA BAHÍA" de la ciudad de Ambato.

1.1.4.2 Objetivos específicos

- Diagnosticar los procesos informáticos que se aplican a la empresa para la identificación de fortalezas y debilidades.
- Aplicar la metodología COBIT en los procesos informáticos que desarrolla la empresa para la determinación de los puntos y riesgos de control.
- Presentar las políticas y procedimientos del sistema de control interno a los procesos informáticos para la gestión eficiente de las actividades informáticas.

1.2 Revisión de la literatura

1.2.1 Auditoría

1.2.1.1 Concepto

La auditoría es una gran herramienta de control y a la vez de supervisión, en donde ayuda a la creación de una cultura con disciplina organizacional, que permite descubrir los errores o falles en las estructuras organizacionales (Villardefrancos Alvarez y Rivera, 2006).

Además, como menciona Panchi Arias (2021):

> La auditoría en el ámbito educativo es muy importante, porque la administración sin práctica de auditoría no puede garantizar completamente que los datos económicos registrados sean verdaderos y confiables. La auditoría también evalúa el grado de eficiencia y efectividad de la realización

de las tareas administrativas y el grado de cumplimiento de los planes y lineamientos de gestión (p. 1).

Es por ello, que la auditoría es definida como un examen y a la vez controla todas las situaciones que tenga la empresa principalmente se podría decir lo económico, para que se pueda identificar las cosas incorrectas, por lo cual podrían mejorar a través de un punto clave.

De igual manera, como afirma Grimaldo (2017):

> La Auditoria se ha convertido en una de las técnicas utilizadas, más importantes dentro de las organizaciones, gracias a su implementación y desarrollo, la alta dirección encuentra un mecanismo de control que permite conocer el estado actual del sus procesos y la veracidad de la información, para determinar la eficacia y eficiencia con la cual se están ejecutando y así, poder tomar a tiempo las acciones necesarias para su correcto cumplimiento de objetivos y metas (p.7).

1.2.1.2 Importancia

La importancia que tiene la auditoría en las entidades financieras es muy fundamental puesto que gracias a la auditoría se puede identificar los aspectos negativos que no permitan desarrollarse a la empresa de mejor manera.

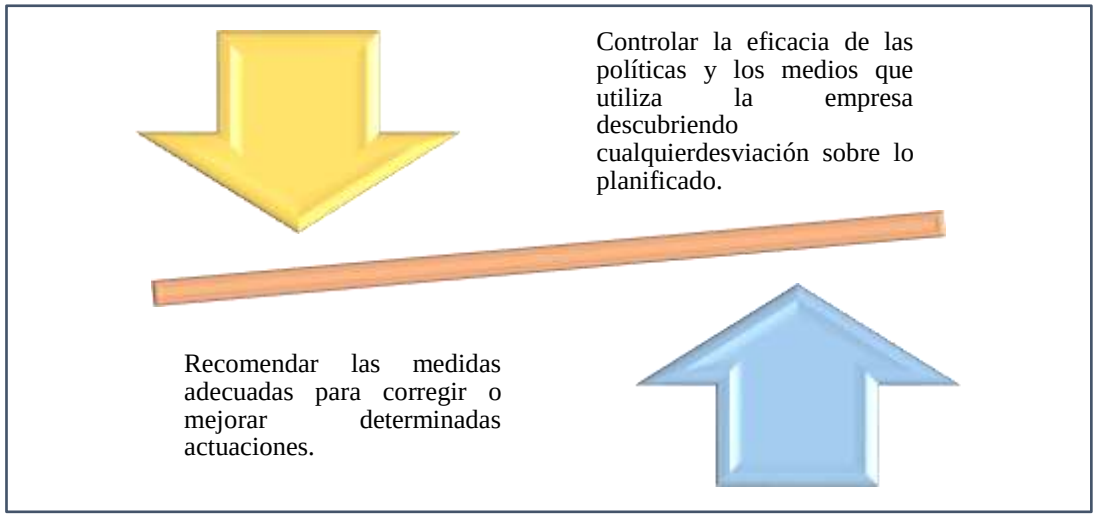


Gráfico 3. Importancia de la Auditoría
Fuente: (Villardefrancos Alvarez y Rivera, 2006)

1.2.2 Control interno

1.2.2.1 Concepto

El control interno según Gamboa Poveda, Puente Tituaña, Vera Franco (2016) menciona que se "perfila como un mecanismo idóneo para apoyar los esfuerzos de las entidades públicas con miras a garantizar razonablemente los principios constitucionales y la adecuada rendición de cuentas".

Por lo tanto, que (Coopers & Lybrand, 1997) define al control interno como:

> Un procedimiento, realizado por el personal de una empresa, diseñado para conseguir unos objetivos específicos. La definición es amplia y cubre todos los aspectos de control de un negocio, pero al mismo tiempo permite centrarse en los objetivos específicos. El control interno consta de cinco componentes relacionados entre sí que son inherentes al estilo de la operación de la entidad. Estos componentes están vinculados entre sí y sirven como criterios para determinar si el sistema es eficaz (p. 26).

Además (Mantilla, 2013) afirma que:

> El control interno comprende el plan de la organización y todos los métodos y medidas coordinadas que se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y la confiabilidad de sus datos contables, promover la eficiencia operacional y fomentar la adherencia a las políticas prescritas (p. 7).

Cabe recalcar que el control interno también son las acciones que debe tomar la administración en donde se planea, organiza y dirige el desempeño de cada una de todas las acciones necesarias que aporten a una seguridad razonable que cumpla los objetivos (Mantilla, 2013).

1.2.2.2 Objetivos

Los objetivos del control interno son muy claros respecto a que la empresa debe comprender los mismos, para que tenga un examen real de la situación de su empresa.

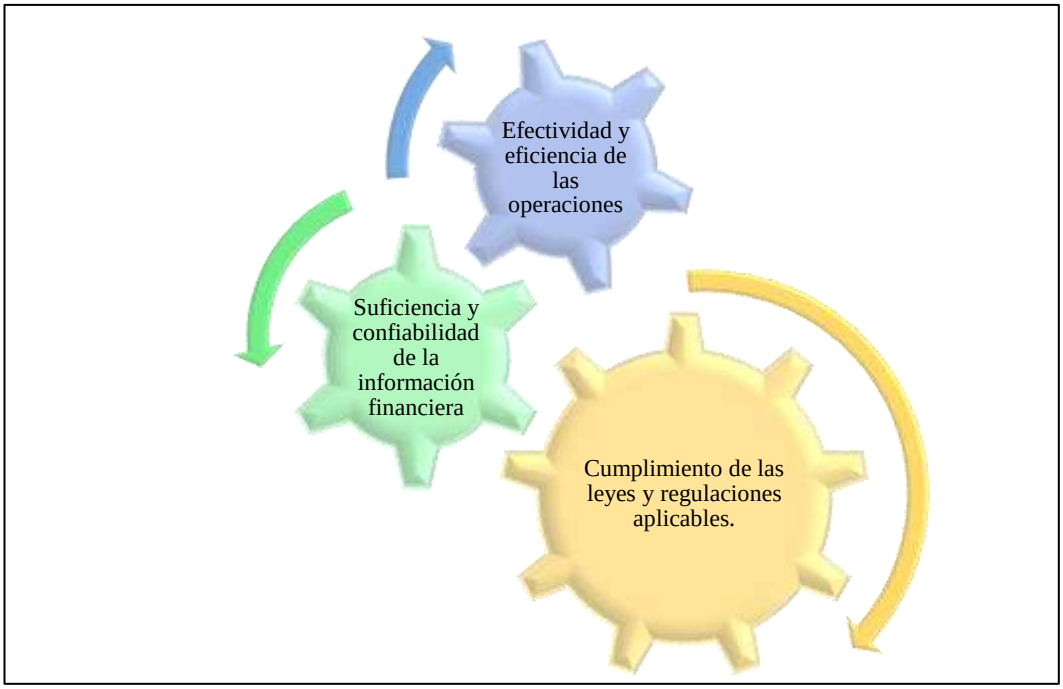


Gráfico 4. Objetivos del control interno
Fuente: (Estupiñan Rodrigo, 2015)

1.2.2.3 Beneficios

Se puede describir que los beneficios del control interno son notorios, por lo que la empresa podrá encontrar los errores y falencias que tenga la organización, algunos de los beneficios los describimos a continuación:

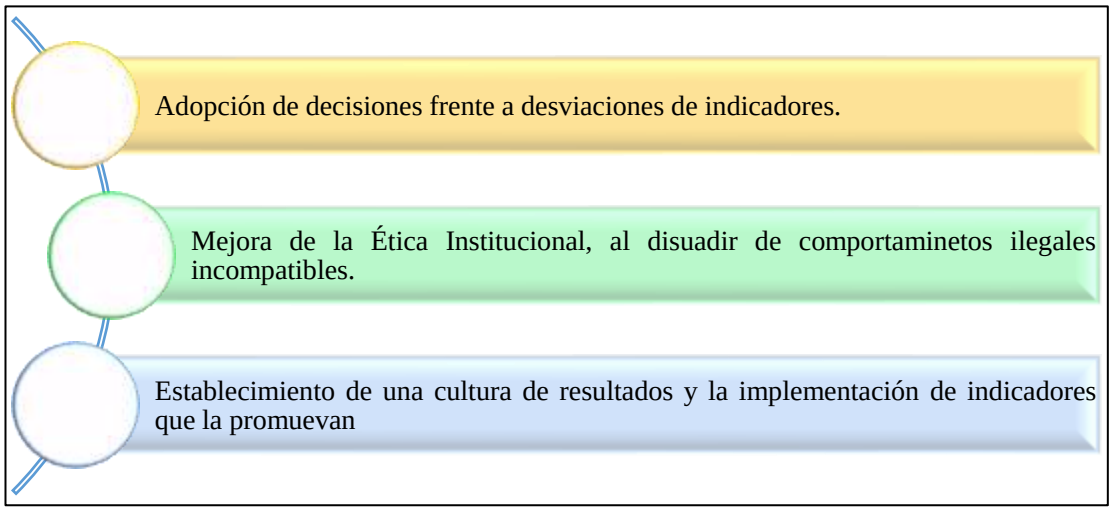


Gráfico 5. Beneficios del control interno
Fuente: (Mendoza-Walter, Delgado-María, Ponce-Tania, 2018)

1.2.2.4 Principios

El control interno tiene sus principios por lo que es un asunto prioritario, en vista de que es necesario conocer cuáles son los objetivos que se están buscando.

Tabla 1. Principios del Control Interno

PRINCIPIOS DEL CONTROL INTERNO	
Segregación de funciones	Segregación de las funciones relacionadas con los distintos roles vinculados con el control interno. Por niveles
Autocontrol	No hay controles internos que sean externos, es por ello que la dirección, gestión, supervisión y evaluación del control interno son resorte de la administración principal (alta gerencia).
Desde arriba - hacia-abajo	El control interno es una 'presión' o 'influencia' ejercida por los máximos niveles administrativos (alta gerencia), desde arriba hacia abajo.
Costo menor que beneficio	Afianza el hecho de que el control interno genera valor para la organización (generación de valor para el cliente y agregación de valor para el accionista).
Eficacia	Depende directamente del logro de los objetivos de negocio que tiene el sistema: eficacia y eficiencia de las operaciones, confiabilidad del proceso de presentación de reportes financieros, cumplimiento de normas y obligaciones, salvaguarda de activos, direccionamiento estratégico
Confiabilidad	Es la relación que existe entre la efectividad del diseño y operación del sistema de control interno y la extensión de la documentación, conciencia y monitoreo del control interno.
Documentación	Debe estar debidamente documentada, de manera tal que pueda ser analizada por cualquier Interesado, ya se trate de la administración (para efectos de su propia valoración), de los auditores (para efectos de su evaluación o de su dictamen) o de los reguladores (para efectos derivados de las acciones de supervisión, inspección, vigilancia y control).

Fuente: (Mantilla, 2018)

1.2.2.5 Componente del sistema de control interno

El sistema de control interno posee sus componentes los cuales permiten que sean más fáciles de entender por lo que la empresa pueda evaluar si el principio se encuentra presente y funciona correctamente con el sistema de control interno(Villa César, Samaniego Florípes, Vargas Diana, 2017).

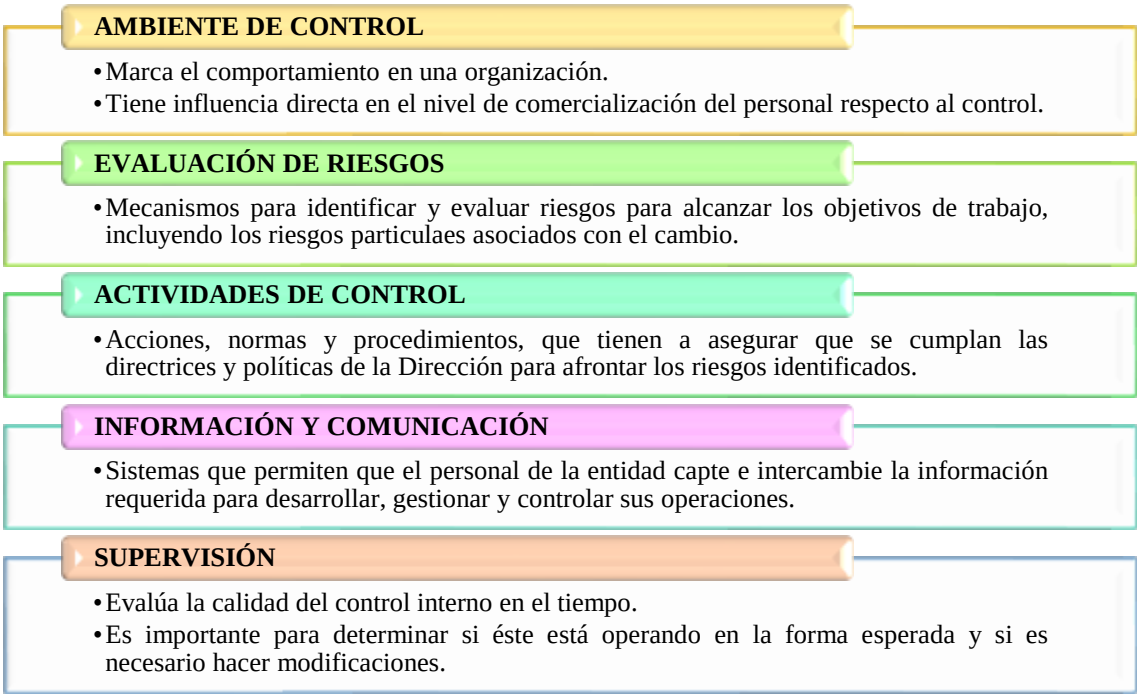


Gráfico 6. Componentes del control interno
Fuente: (Villa et al., 2017)

1.2.2.6 Procesos

El control interno debe cumplir con un proceso que tiene un fin de determinar su calidad, y nivel de confianza en los resultados obtenidos con su aplicación utilizando una metodología (Jiménez, 2011).

Tabla 2. Procesos del Control Interno

PROCESOS DEL CONTROL INTERNO	
PLANEACIÓN	La evaluación puede abarcar a la totalidad del sistema o a partes o actividades específicas, según sea el interés o requerimiento de la administración, el evaluador requiere tener una comprensión adecuada del negocio de la entidad o empresa, de su entorno y de los componentes del control interno existente, de manera de poder identificar y dar un criterio o valoración de los riesgos que podrían impedir el cumplimiento de los objetivos que se ha planteado la administración.
PRUEBAS DE CUMPLIMIENTO DE CONTROLES	En función del requerimiento o interés de la administración, en una auditoría de control interno se puede dar los siguientes enfoques al trabajo a realizar: • Una evaluación total que comprenda todos los componentes del control interno existentes en una organización o de algún

	componente en particular. • Evaluar los controles relacionados con una o más de las categorías de objetivos de control. • Evaluar los controles relacionados a ciertas actividades (Ventas, compras, cartera, etc.)
COMUNICACIÓN DE RESULTADOS	La comunicación de resultados de una evaluación de control interno, que en definitiva significa el producto que el auditor o evaluador debe entregar a la administración, significa una tarea muy importante ya que debe contemplar varios aspectos como son: la oportunidad de reporte de novedades, calidad y claridad de la redacción, contendidos de interés, selección adecuada de destinatarios del reporte, y formas de presentación de estos reportes.

Fuente: (Jiménez, 2011)

1.2.2.7 Tipos

Existen tres tipos de control interno como menciona Cajiao María, García María y Jimbo Monica (2016):

> La administración puede implantar controles antes de que comience una actividad, mientras ésta se desarrolla, o después de que ésta se termina. Al primer tipo se le llama control previo; al segundo se le nombra control concurrente; y el tercero es control posterior (p. 18).

1.2.2.8 Métodos de evaluación

Como mencionan Quinaluisa Morán Nancy, Ponce Verónica, Muñoz Sandra, Ortega Xavier y Pérez Jazmín (2018) que:

> A partir de la década de los 90, los nuevos modelos desarrollados en el campo del control definen una nueva corriente de pensamiento con una amplia concepción de la organización a nivel mundial, lo cual provoca una mayor participación de la dirección, los gerentes y el personal en general (p. 4).

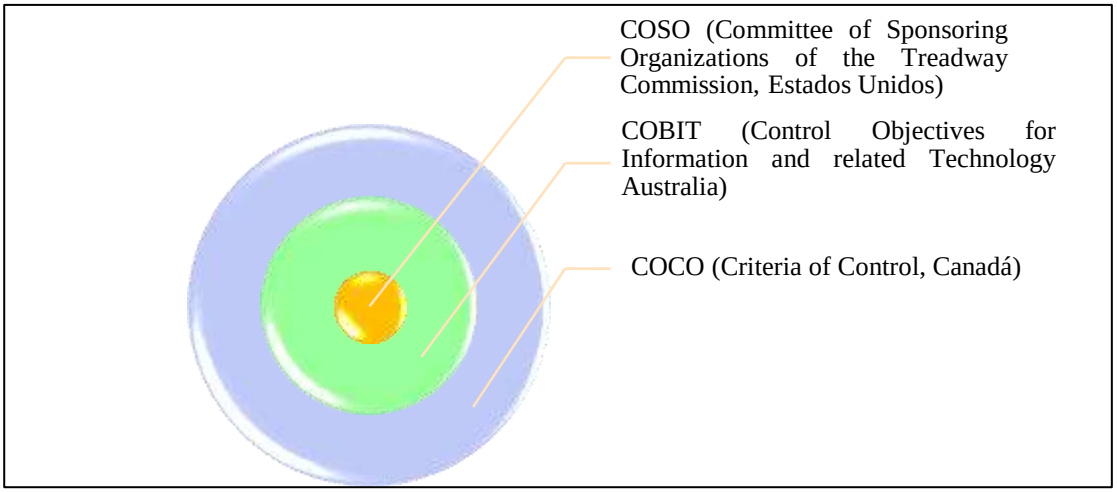


Gráfico 7. Métodos de evaluación del control interno
Fuente: (Quinaluisa Morán et al., 2018)

Con lo anteriormente mencionado, sobre los métodos de evaluación del control interno se podrá explicar de mejor manera que significa cada una de ellas a continuación.

Tabla 3. Concepto de los métodos de evaluación del control interno

MÉTODOS DE LA EVALUACIÓN DEL CONTROL INTERNO	SIGNIFICADO DE SUS SIGLAS	CONCEPTO
COSO	Committee of Sponsoring Organizations of the Treadway Commission - **Estados Unidos**	Consta de cinco categorías o componentes que la administración diseña y aplica para proporcionar la seguridad razonable de que sus objetivos de control se llevarán a cabo adecuadamente.
COBIT	Control Objectives for Information and related Technology - **Australia**	Simplificación de los conceptos y el lenguaje para hacer posible una discusión sobre el alcance total del control, con la misma facilidad, en cualquier nivel de la organización.
COCO	Criteria of Control - **Canadá**	Estructura que provee una herramienta para que los propietarios de los procesos del negocio descarguen eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos

Fuente: (Quinaluisa Morán et al., 2018)

1.2.3 Riesgo

1.2.3.1 Marco de apetito al riesgo

El Marco de Apetito al Riesgo que es una herramienta fundamental que ayuda a fortalecer la cultura del riesgo de las empresas (Conejos Merita, 2018).

1.2.3.2 Gestión de riesgo

La gestión de riesgos según Conejos Merita (2018) menciona que:

> Es un pilar estratégico de la organización que fomenta la creación de valor y el desarrollo del negocio de acuerdo con los niveles de apetito y tolerancia a los riesgos determinados por los órganos de gobierno (p. 20).

1.2.4 Sistemas informáticos

1.2.4.1 Concepto

Desde el punto de vista de Laudon y Laudon (2012) le conceptualiza a un sistema de información como:

> Un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores del conocimiento a analizar problemas, visualizar temas complejos y crear nuevos productos (p. 47).

Cabe recalcar que un sistema de información según Purificación Aguilera López (2010) está constituido por:

> Un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos…) y con frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y el hardware) (p. 10).

1.2.4.2 Actividad que realiza un sistema de información

Con base a lo mencionado según Purificación Aguilera López (2010):

> Un sistema de informático es un conjunto del sistema de información, pero debemos tomar en cuenta que un sistema de información no tiene por qué contener elementos informáticos, aunque es difícil imaginar que la actividad humana no utilice la informática (p. 10).

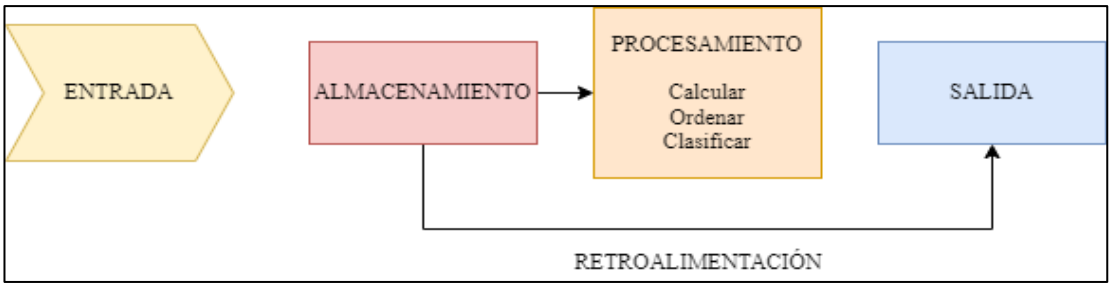


Gráfico 8. Actividad que realiza un sistema de información
Fuente: (Purificación Aguilera López, 2010)

1.2.4.3 Importancia

Como mencionan Laudon y Laudon (2012) los sistemas informáticos son una parte muy importante para la organización, a continuación, se las detalla:

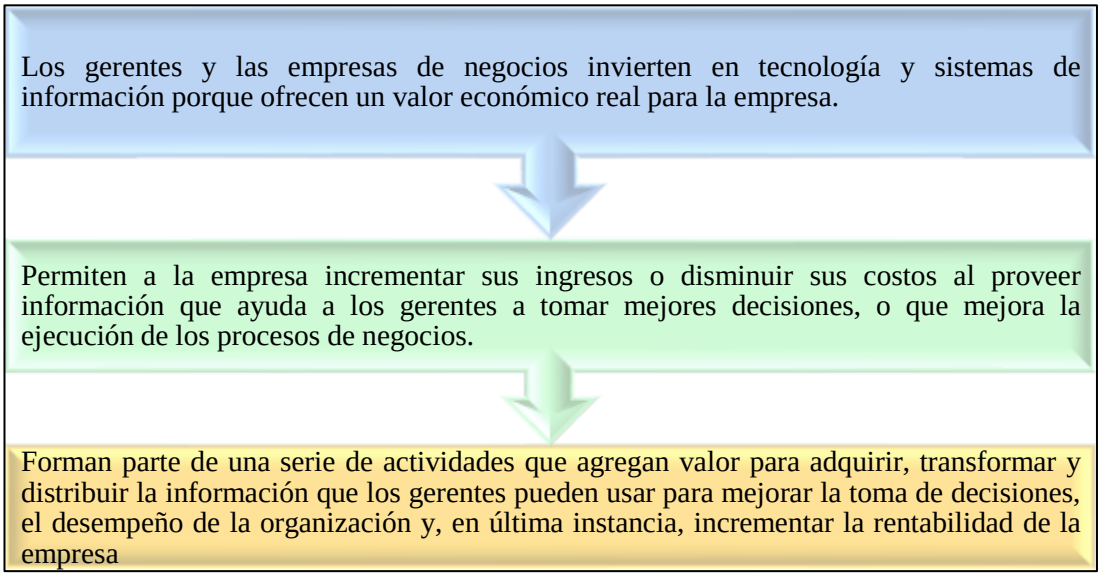


Gráfico 9. Importancia de los sistemas informáticos
Fuente: (Laudon y Laudon, 2012)

1.2.4.4 Clasificación

A la hora de clasificar los Sistemas de Información, existe una gran variedad de criterios, podemos ver algunas de las principales tipologías de sistema de información (Hernández Trasobares, 2003).

Tabla 4. Clasificación de los sistemas informáticos

TIPO DE SISTEMA DE INFORMACIÓN	TIPOS
GRADO DE FORMALIDAD	• Formales • Informales
AUTOMATIZACIÓN	• Manuales • Informáticos
RELACIÓN CON LA TOMA DE DECISIONES	• Estratégicos (alta dirección) • Gerencial (nivel intermedio) • Operativos (control operativo)
FUNCIONALIDAD	• Gestión comercial • Gestión contable • Gestión financiera • Gestión de Recursos Humanos • Gestión de la Producción
GRADO ESPECIALIZACIÓN	• Específicos • Generales

Fuente: (Hernández Trasobares, 2003)

1.2.5 Tecnologías de información (TI)

1.2.5.1 Herramientas

Las tecnologías de información están compuestas por un kit de herramientas, conteniendo una variedad de recursos tales como:

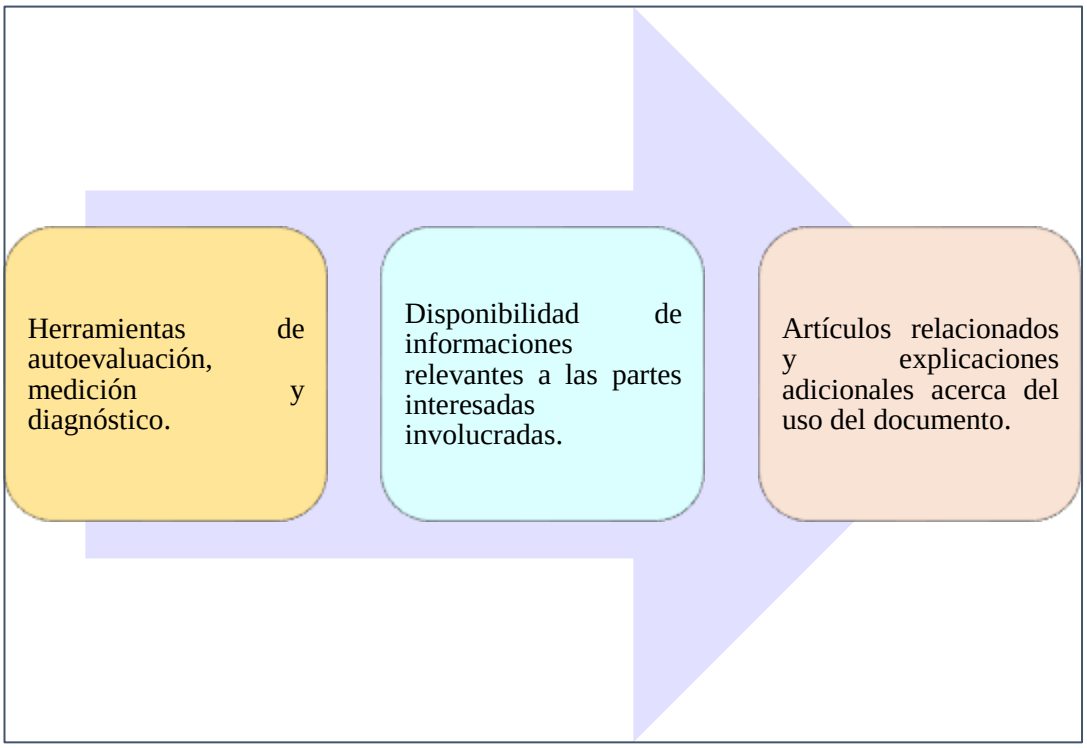


Gráfico 10. Herramientas de las tecnologías de información (TI)
Fuente:(Espino, 2014)

1.2.5.2 Gobernanza

Las tecnologías de información (TI) según lo menciona (Diogo-Reis, 2015) que tiene como objetivo principal atender absolutamente todas las estrategias y necesidades que posee el negocio, teniendo en cuenta que su conformidad hace relación a las leyes, reglamentos y normas internas y externas, los cuales son requisitos legales para el negocio, los mismo que varían de acuerdo a su finalidad, tipo, exigencias regulatorias de todas las entidades.

1.2.6 Seguridad informática

1.2.6.1 Concepto

Debemos tener en cuenta que (Diogo-Reis, 2015) manifiesta que la seguridad de la

información consiste en el establecimiento de cada una de las directrices, políticas y acciones, que son referentes a la seguridad de la infraestructura, los datos, aplicaciones, informaciones, con socios corporativos y proveedores en relación de negocios.

Cabe recalcar que según (Bertolin Areitio, 2008) menciona que:

> La seguridad es un proceso continuo multidimensional, que debe tener en cuenta en la definición, gestión y en la reingeniería de empresas y procesos de negocios, la misma que es una disciplina en continua evolución, la meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando los sistemas (p. 4).

1.2.6.2 Características que define a la seguridad de la información

Debemos tener en cuenta que cada una de las características son muy importantes, y su prioridad depende de la empresa (Daltabuit Enrique, Hernández Leobardo, Mallén Guillermo y Vázquez José de Jesús 2007).

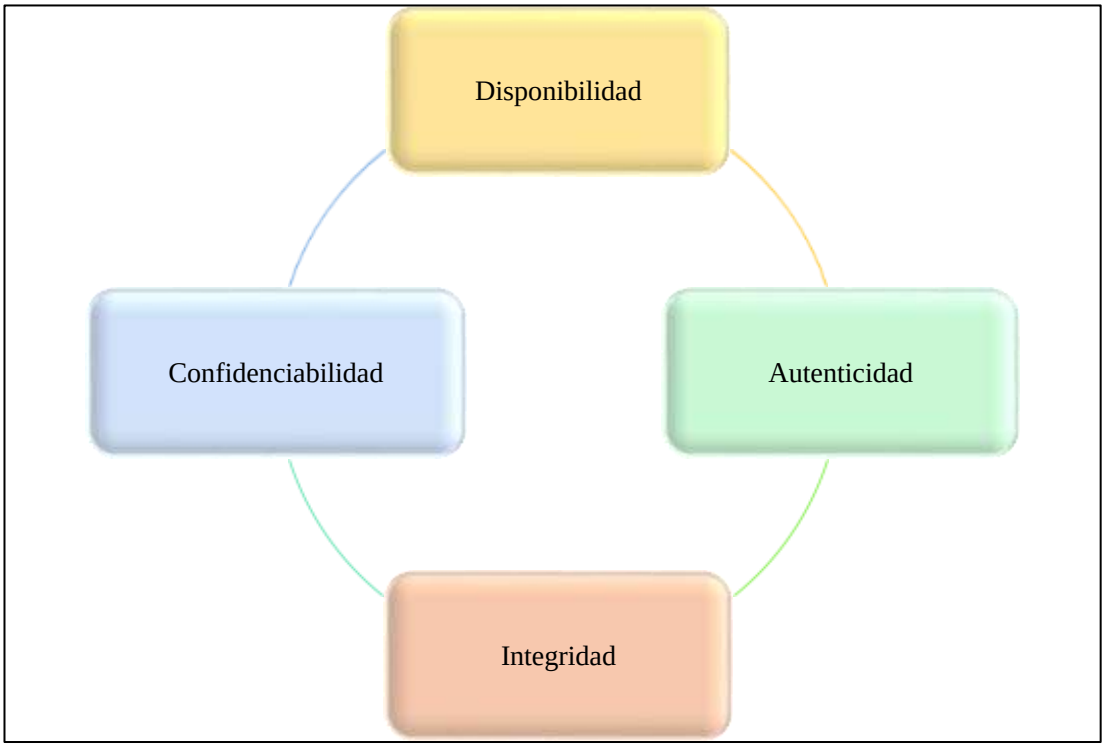


Gráfico 11. Características que define a la seguridad de la información
Fuente: (Daltabuit et al., 2007)

1.2.6.3 Tipos

Existen dos tipos de seguridad de la información que se pueden encontrar en una organización.

Tabla 5. Tipos de seguridad de la información

TIPOS	CONCEPTOS	EJEMPLO
ACTIVA	Comprende el conjunto de medidas o defensas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.	Impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas.
PASIVA	Está formada por las medidas que se implantan para, una vez producido incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema.	Teniendo siempre al día copias de seguridad de los datos.

Fuente: (Purificación Aguilera López, 2010)

1.2.6.4 Modelos

Es necesario conocer que Purificación Aguilera López (2010) identifica a los modelos de seguridad informática como:

> Un modelo de seguridad es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información, Al decir formal queremos expresar que estará redactado fundamentalmente en términos técnicos y matemáticos (p. 24).

1.2.6.5 Clasificación de los modelos de seguridad informática

Los modelos de seguridad informática se clasificarán en relación con las operaciones o funciones que necesite mayor control.

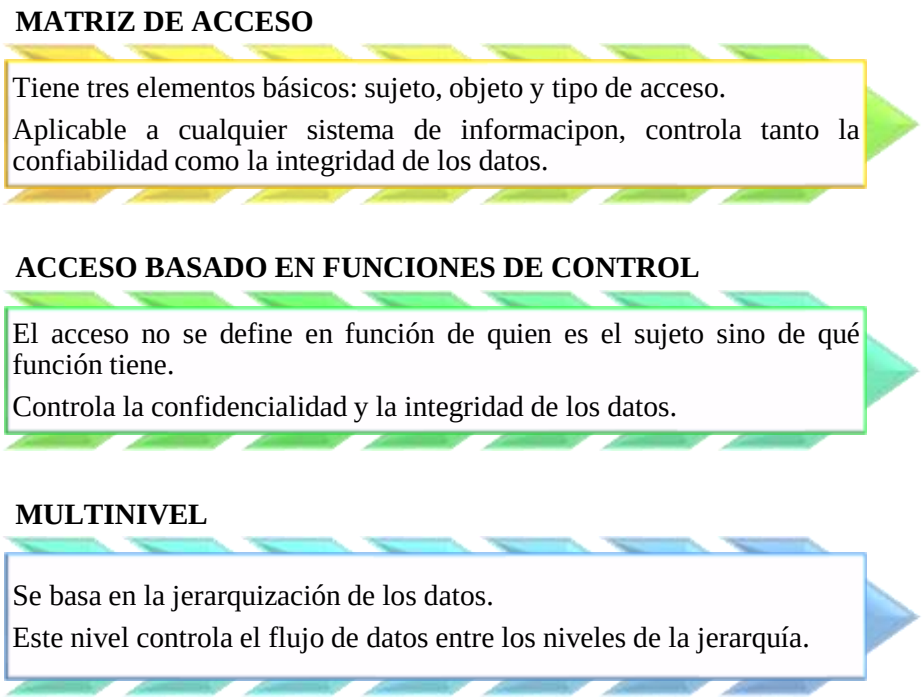


Gráfico 12. Clasificación de los modelos de seguridad informática
Fuente: (Purificación Aguilera López, 2010)

1.2.6.6 Motivos para proteger la información

Tengamos en cuenta que nuestra vida es digital y debemos protegerla de una u otra manera, la información que tengamos en todos los dispositivos electrónicos como las tabletas, laptops y móviles, deben tener un usuario y contraseña, existen tres motivos para que protejamos nuestra información (Purificación Aguilera López, 2010).

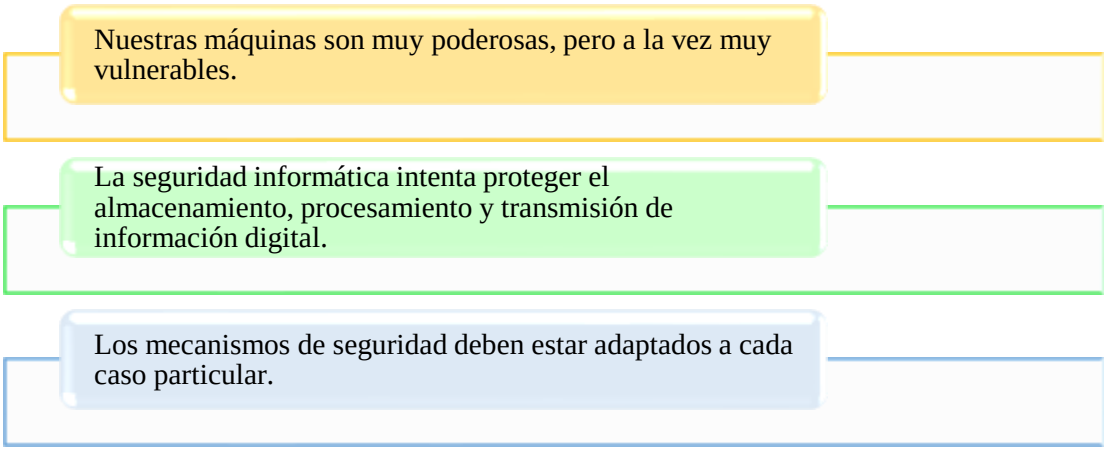


Gráfico 13. Motivos para proteger la información
Fuente: (Purificación Aguilera López, 2010)

1.2.7 Activos informáticos

1.2.7.1 Concepto

Los activos de información son herramientas esenciales que son utilizadas dentro del sistema de gestión de seguridad de la información, para que las empresas puedan cumplir cada objetivo propuesto por la alta dirección de la empresa (Arévalo, 2020).

1.2.7.2 Etapas para documentar

Las etapas para documentar correctamente los activos de información, están relacionados directa e indirectamente con amenazas, impactos, vulnerabilidades y riesgos internos y externos, a continuación se describe las etapas (Arévalo, 2020) .

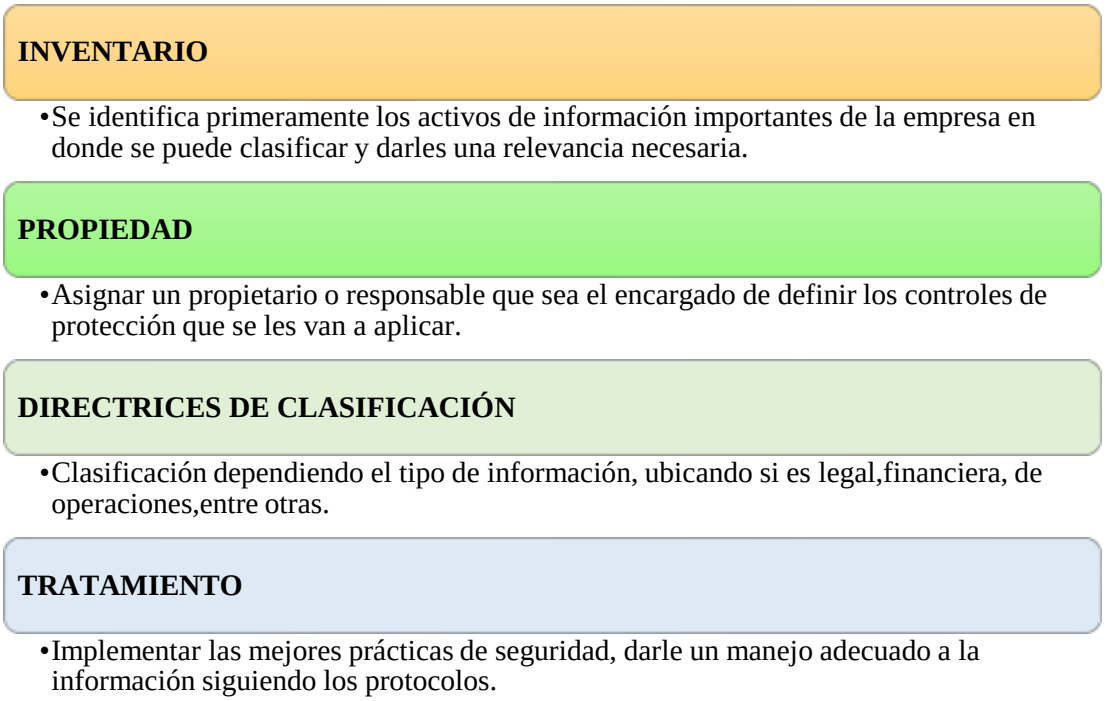


Gráfico 14. Etapas para documentar los activos de información
Fuente: (Arévalo, 2020)

1.2.7.3 Tipos

Los activos de información poseen una clasificación según menciona Industria y Comercio Superintendencia (2018) que se menciona a continuación:

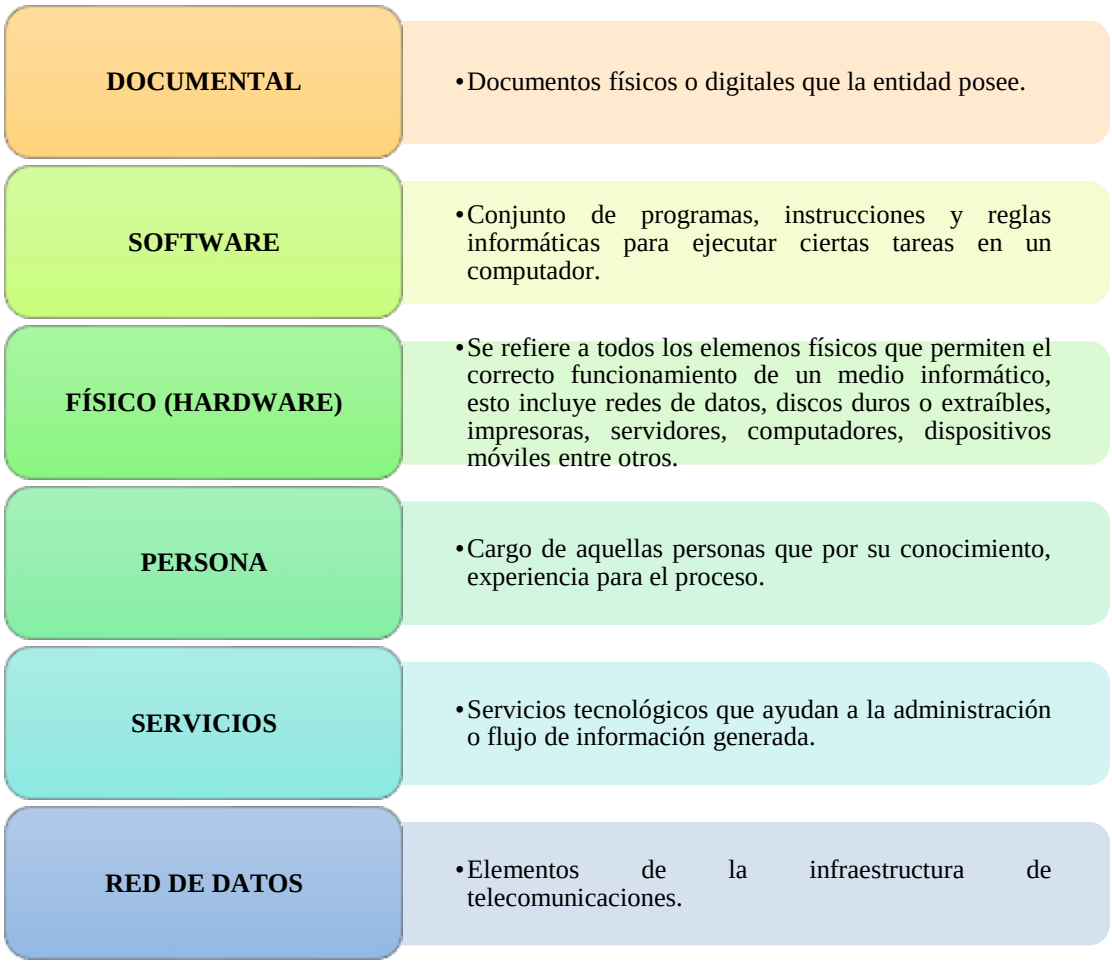


Gráfico 15. Tipos de activos de información
Fuente: (Industria y Comercio Superintendencia, 2018)

En el siguiente cuadro, se presentan las propiedades de seguridad aplicables, que según el tipo de activo de información.

Tabla 6. Propiedades de los tipos de activos de información

CATEGORÍA DEL ACTIVO	PROPIEDADES APLICABLES		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Físico			X
Documental	X	X	X
Personal			X
Servicio			X
Software			X
Red			X
Otros	X	X	X

Fuente: (Industria y Comercio Superintendencia, 2018)

1.2.8 Concepto de MySQL

El MySQL según Robledano (2019) "es un sistema de gestión de bases de datos que cuenta con una doble licencia. Por una parte, es de código abierto, pero por otra, cuenta con una versión comercial gestionada por la compañía Oracle":

1.2.9 Concepto de sistema de punto de red final

Un sistema de punto final como manifiesta IBM (2010) "es cualquier sistema o partición lógica de la red IP que pueda elegirse para gestionarlo a través del sistema central".

1.2.10 Concepto de cortafuegos

Como menciona Yustas (2015) el cortafuegos es "un sistema de control que se sitúa entre una red corporativa e Internet y la función principal del cortafuegos es constituir un punto de paso para el intercambio de información entre ambas redes; por lo que en este dispositivo determinará cuáles son los protocolos, es decir los servicios, que pueden atravesarlo y en qué condiciones":

1.2.11 Metodología COBIT

1.2.11.1 Antecedentes

El sistema COBIT cuando inició estaba basado en los Objetivos de Control de la Fundación de Auditoría y Control de Sistemas de Información (ISACF) como manifiesta Santacruz Espinoza et al. (2017) que al pasar el tiempo cada día se han realizado mejoras al sistema, es por ello que en la actualidad el sistema cuenta con estándares internacionales a diferentes niveles como técnico, profesional, específico y regulatorio dentro de la industria.

Podemos decir que, el sistema COBIT se ha desarrollado en varias ediciones, su primera edición se publicó en el año 1996, su segunda edición se publicó a los dos años después de haber publicado la primera edición, eso quiere decir que se realizó en el año 1998, su tercera edición en el año 2000, teniendo en cuenta que estuvo disponible en el internet en el año 2003 y la cuarta edición en diciembre del 2005, es por ello que se publicó la versión 4.1 desde el mes de mayo del 2007, la versión online

de COBIT 5 ya está disponible para nosotros.

1.2.11.2 Concepto

Santacruz Espinoza, Vega Abad,Pinos Castillo, Cárdenas Villavicencio (2017) define al método COBIT una guía para realizar auditorías de la gestión y control de los sistemas de información y tecnología, dirigido al área informática de una empresa, es decir a los auditores implicados en el procedimiento.

1.2.11.3 Significado de las siglas COBIT

Según Gómez, Pérez, Donoso y Herrera (2010) el significado de las siglas COBIT es "Control Objectives for Information and related Technology – Objetivos de control para tecnología de información y tecnologías"

1.2.11.4 Propósito

Menciona Santacruz-Espinoza, Vega-Abad, Pinos-Castillo, Cárdenas-Villavicencio (2017) que el propósito del método COBIT es proporcionar y colaborar a las empresas para que puedan alcanzar el valor inmemorable de las TI manteniendo el equilibrio entre la ejecución de los beneficios, la administración de recursos y las fases de riesgo tomados.

1.2.11.5 Principios

En base a Velásquez-Pérez, Puentes-Velásquez y Pérez-Pérez (2015) los principios que se utilizan en el método COBIT son:

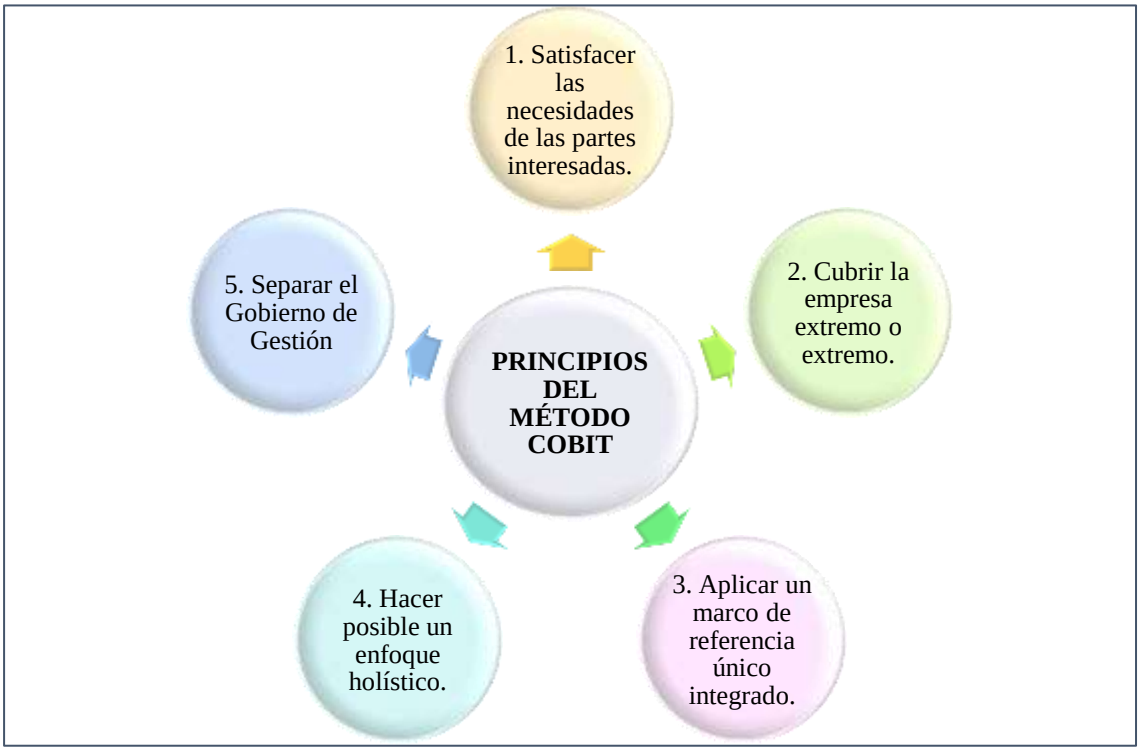


Gráfico 16. Principios del método COBIT
Fuente: (Velásquez Pérez et al., 2015)

Además, cada uno de los principios comprender algunos puntos clave que posee la empresa, mediante ello pueda operar de mejor manera.

Tabla 7. Características de los principios del método COBIT

PRINCIPIOS	CARACTERÍSTICAS
Cumplir las necesidades de las partes interesadas.	Permite la creación de valor del negocio mediante el uso de las tecnologías de información (TI), con el apoyo de las herramientas propias.
Cubrir la entidad en su totalidad.	Resguardar todos los procesos de la empresa, incluyendo todas las áreas funcionales de las tecnologías de información, personal interno y externo, que sea relevante para la gestión de las TI.
Emplear un marco de referencia único completo.	Se emplea un marco de referencia único integrando estándares, marcos de trabajo y buenas prácticas que sean relacionados con las tecnologías de información.

Crear un posible enfoque holístico.	Define diferentes herramientas para colaborar con la ejecución de un sistema de gobierno y gestión para las tecnologías de la información de la entidad, basados en principios, políticas, procesos, estructuras organizativas, cultura, ética, comportamiento, habilidades y competencias.
Apartar el Gobierno de Gestión	Dividir claramente al gobierno y gestión por lo que cada uno involucra diferentes estructuras y propósitos organizacionales diferentes.

Fuente: (Vivar Gualsaquí, 2013)

1.2.11.6 Adaptación

Manifiesta Velásquez Pérez et al. (2015) que éste método COBIT "es general y se puede adaptar en todo tipo de empresas, desde el sector comercial, productivo, con o sin ánimo de lucro, empresas públicas o privadas" (p. 166).

De este modo Santacruz Espinoza et al. (2017) comenta que:

> La orientación al negocio que realiza COBIT consiste en ´ vincular las metas del negocio con las metas de TI, brindando métricas y modelos de madurez para medir los logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI (p. 3).

De todos modos, la metodología COBIT tiene como principal objetivo evaluar la adecuación de los controles internos que se han establecido, para detectar algunas debilidades y riesgos en el funcionamiento del mismo. Se puede decir que capacidad de realizar un análisis exhaustivo de los objetivos de control son necesarios para avalar el correcto funcionamiento, la operatividad y calidad de los resultados (Almanza - Gomez, 2012).

Así mismo, Santacruz Espinoza et al. (2017) indica que la metodología COBIT es:

> Empleado en todo el mundo por colaboradores, quienes tienen como encargo principal los procedimientos del negocio y la tecnología, por lo cual los colaboradores son quienes dependen de la tecnología y la información confiable, además son los mismos quienes proveen información eficiente.

Finalmente Almanza - Gomez (2012) testifica lo siguiente:

> Es recomendable que la gerencia implante una política de evaluación del funcionamiento de los recursos Tics, a fin de definir programas y planes operativos de fortalecimiento y modernización de la plataforma informática, incluyendo mejoramiento del nivel servicio para los clientes internos, planes de contingencia y mitigación de riesgos (p. 15).

1.2.11.7 Habilitadores

Los habilitadores del COBIT según Santacruz Espinoza et al. (2017) son siete y son los siguientes:

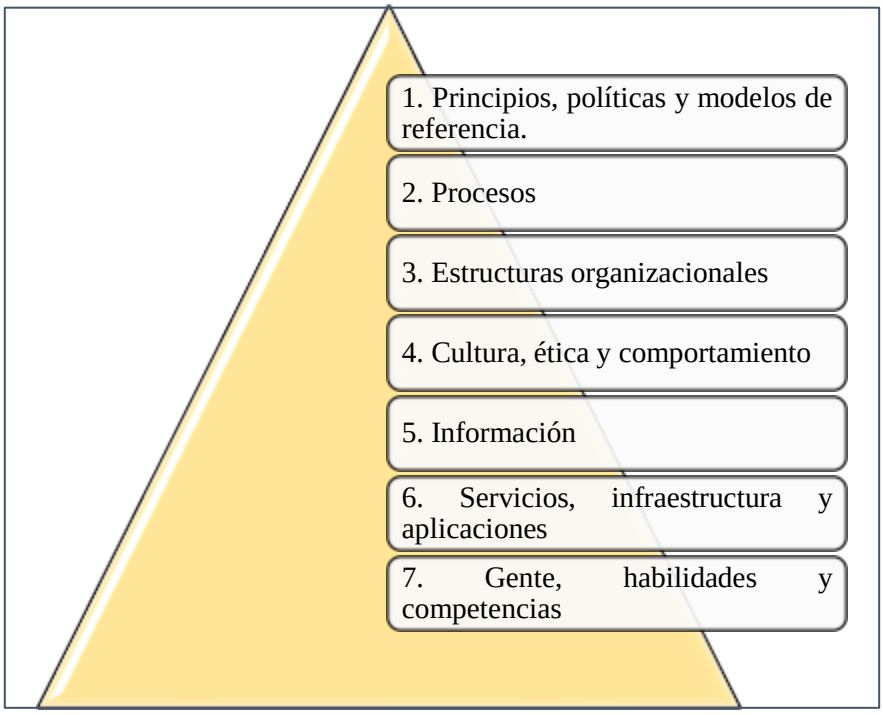


Gráfico 17. Habilitadores del COBIT
Fuente:(Santacruz Espinoza et al., 2017)

1.2.11.8 Componentes

La metodología COBIT tiene cinco componentes según Instituto de Auditores Internos (2017) que ayudarán a evaluar, direccionar a la organización para que se pueda gestionar los riesgos de mejor manera, y son los siguientes:

Ilustración 3 Componentes de la Metodología COBIT 5

Fuente: (Instituto de Auditores Internos, 2017)

Ilustración 4. Descripción de los componentes de la Metodología COBIT

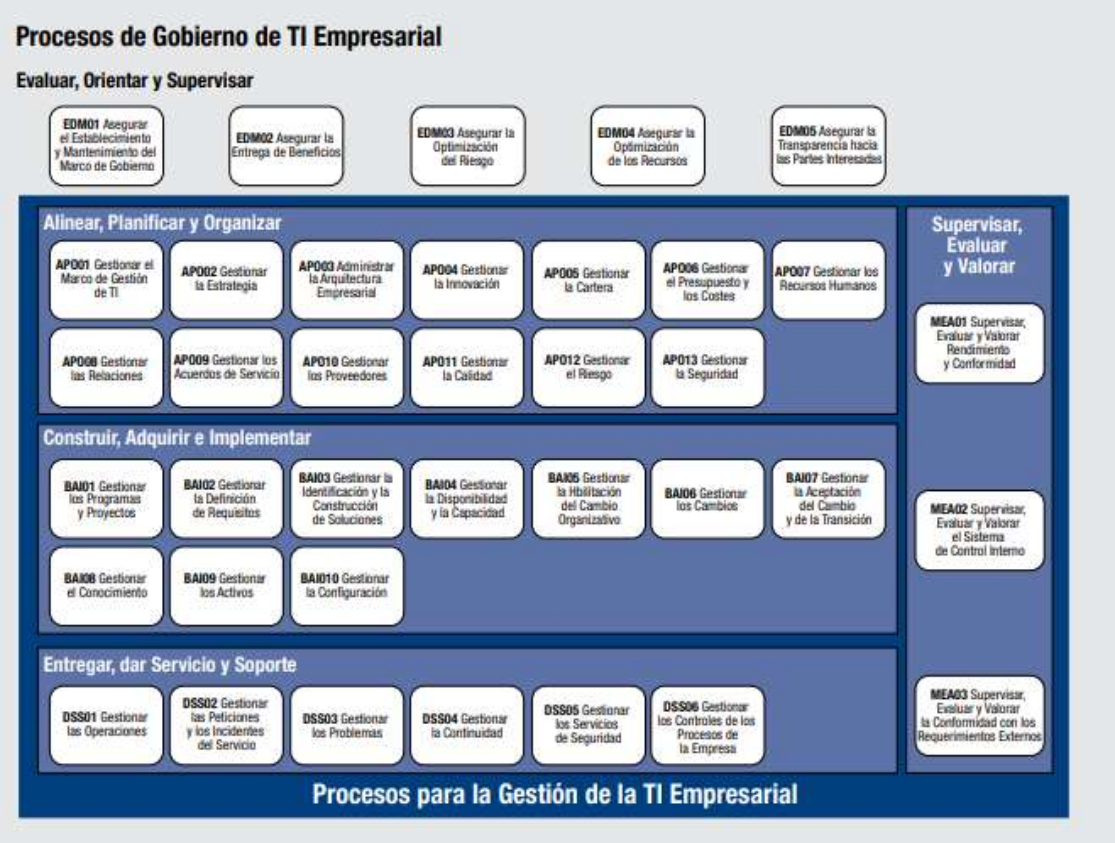
Gobierno y Cultura	El gobierno establece el tono de la organización, reforzando la importancia de, y estableciendo responsabilidades de supervisión, para la gestión de riesgos empresariales. La cultura se refiere a valores éticos, comportamientos deseados y comprensión del riesgo en la entidad.
Estrategia y objetivos	Gestión de riesgos empresariales, estrategia y objetivos trabajan juntos en el proceso de planeación estratégica. El apetito al riesgo es definido y alineado con la estrategia; los objetivos de negocio ponen la estrategia en practica mientras sirve para identificar, evaluar y responder a los riesgos.
Desempeño	Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados. Riesgos son priorizados por severidad y en el contexto del apetito al riesgo. La organización selecciona las respuestas al riesgo y toma el riesgo que ha asumido.
Revisión	Para revisar el desempeño de la entidad, una organización puede considerar qué tan bien funcionan los componentes de gestión de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y qué revisiones se necesitan.
Información, comunicación y reporte	La gestión de riesgos empresariales requiere un proceso continuo para obtener y compartir información necesaria, de fuentes internas y externas, que fluya en todas las direcciones y a través de toda la organización.

Fuente: (Instituto de Auditores Internos, 2017)

1.2.11.9 Modelo de referencia de procesos de COBIT

En la metodología COBIT incluye un modelo de referencia de procesos los cuales definen y describen varios procesos de gestión y de gobierno, los mismo que ayudarán a la identificación de las tecnologías de información (TI). Por lo tanto ISACA (2012) menciona que "El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica".

Ilustración 5. Modelo de referencia de procesos de COBIT



Fuente: (ISACA, 2012b)

1.2.11.10 Marco de referencia

El marco de referencia de COBIT según menciona Mora Julio, León Joffre,Huilcapi Magdalena y Escobar Diana (2017) clasifica a cada proceso de las unidades de las TI de las organizaciones en cuatro dominios principales.

1. Planificación y organización	• Abarca las estrategias y tácticas, además identifica la forma rn que la tecnología puede mejorar al logro de los objetivos del negocio.
2. Adquisición e implementación	• Cubre los cambios y mantenimiento realizados a sistemas existentes para asegurar que el ciclo de vida es continuo para esos sistemas.
3. Entrega y soporte	• Entrega o distribución de los servicios requeridos que abarcan diferentes operaciones tradicionales hasta el entrenamiento.
4. Monitoreo	• Su objetivo es verificar la calidad y la suficiencia en cuanto a los requerimientos de control.

Gráfico 18. Dominios del COBIT 5

Fuente: (Mora et al., 2017) (Comité Directivo de COBIT y IT Governance Institute, 2000)

1.2.11.11 Cuadro comparativo del sistema COBIT con otros sistemas como (COSO)

Se puede identificar las diferencias que posee cada uno de los sistemas que se presentan a continuación:

Tabla 8. Cuadro comparativo del sistema COBIT con otros sistemas como (COSO)

	COBIT	COSO
CARACTERÍSTICAS	• Esta, basado en la filosofía de que los recursos de TI necesitan ser agrupados. • Diseñado como un estándar aceptado y ajustable a las buenas prácticas de seguridad y control en TIC. • Es practica y simple. • Ayuda a la gerencia a comprender y asociar los riesgos administrados, con TIC.	• Ambiente de control • Evaluación de riesgos • Actividades de control • Información y comunicación • Supervisión
VENTAJAS	• Mejora la calidad y medición de las TI. • Ayuda a implementar un sistema de control. • Presenta las actividades en una estructura manejable y lógica.	• Tener una visión global de algunos riesgos, los cuales a su vez ayudarían de manera correcta a los planes de gestión. • Ayudan a poder tomar decisiones más seguras y adecuadas. • Fomenta a la gestión de riesgos como un pilar fundamental dentro de la empresa.
DESVENTAJAS	• Las buenas prácticas de COBIT están enfocadas en el control y no en la ejecución. • El marco de referencia mejora las áreas TI desde el punto de vista del gobierno corporativo.	• Se manifiesta que el control interno no debe costar más de lo que recibe mediante sus beneficios. • El control interno solamente está dirigido a las cuestiones rutinarias más no a las situaciones globales.

CICLO DE VIDA	• Dominio • Procesos • Actividades	
OBJETIVOS	• Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio para asegurar sus logros futuros.	• Orientar a la gestión ejecutiva y a todas las entidades gubernamentales el establecimiento de operaciones de negocio más eficientes, eficaces y éticas en un ámbito global.

Fuente: (Santacruz Espinoza et al., 2017)

1.2.11.12 Niveles de capacidad según el marco de referencia COBIT 2019

Los niveles de capacidad según ISACA (2012) se dividen como se describe a continuación:

Tabla 9. Niveles de capacidad según el Marco de Referencia COBIT 5

NIVELES	DESCRIPCIÓN
NIVEL 0 (Proceso incompleto)	El proceso no alcanza su objetivo, es por ello que existe poca posibilidad de tener una evidencia de ningún logro sistemático del objetivo del procedimiento.
NIVEL 1 (Proceso ejecutado)	La técnica implementada alcanza su meta.
NIVEL 2 (Proceso gestionado)	El procedimiento ya está gestionado (planificado, supervisado y ajustado) y los resultados están determinados, inspeccionados y cuidados de forma adecuada.
NIVEL 3 (Proceso establecido)	Se utiliza un procedimiento establecido que ayude en el cumplimiento de los resultados propuestos.
NIVEL 4 (Proceso predecible)	Procedimiento elaborado dentro de los parámetros establecidos para alcanzar sus efectos de este.
NIVEL 5 (Proceso optimizado)	El método es mejorado de manera inmediata que ayuda al desempeño de los objetivos empresariales.

Fuente:(ISACA, 2012)

Elaborado por: (Cepeda, 2022)

1.2.12 Criterios de evaluación según la ISO 15504

Los criterios de evaluación según Alarcón-Andrea, González -Juan y Rodríquez -Sandra, (2011) se describe a continuación:

Tabla 10. Criterios de evaluación según la ISO 15504

SIGLA	DESCRIPCIÓN	VALORACIÓN %
F	Completamente Alcanzado	>86 <=100
L	Alcanzado en gran manera	>50 <=85
P	Parcialmente Alcanzado	>15 <=50
N	No cumple (no alcanzado)	0<=15

Fuente:(Alarcón et al., 2011)

1.2.13 Concepto de gobierno

El Gobierno asevera que se deben valorar todas las condiciones, necesidades y puntos de vista que den las partes interesadas para lograr las metas empresariales, estableciendo una dirección que puede ser a través de la toma de decisiones y la priorización, además, se podrá calcular el rendimiento y el cumplimiento (Vivar Gualsaquí, 2013).

1.2.14 Concepto de gestión

La gestión es aquella que planifica, construye, ejecuta y controla cada una de las actividades con la dirección que se establece para que pueda alcanzar las metas empresariales (Vivar Gualsaquí, 2013).

1.2.15 Concepto del modelo de madurez

El modelo de madurez del sistema de control interno por lo general al realizarlo son muy costosos y no disponen de procedimientos para su implementación, teniendo que es una herramienta de diagnóstico que permitirá una administración activa para conocer el estado del sistema de control interno, por lo que es un insumo muy importante para la autoevaluación del mismo sistema (Pérez-Mergarejo Elizabeth, Vergara Ilena y Rodríguez Yordán, 2014).

En este sentido Pérez-Rojas Aurora, Medina-Marin Joselito, Corona-Armenta José Ramón y Montaño-Arango Oscar (2010) entiende al modelo de madurez como:

> Modelo que reúne y organiza en niveles de madurez un conjunto de criterios de gestión con el fin de orientar las actuaciones. Donde los niveles sirven de base para el aprendizaje, asimilar prácticas y como metas a conseguir por parte de las organizaciones (p. 392).

1.2.16 Concepto del nivel de madurez

Como menciona Pérez-Rojas et al. (2010) al nivel de madurez como:

> Escala para medir las capacidades de la organización para llevar a cabo sus procesos e implementarlos, o sea ponerlos en práctica, que se puedan traducir en Buenas Prácticas en el camino de la excelencia y, a su vez, sirvan de plataforma en el camino para conseguir una mejora. Cada nivel de madurez considera un conjunto de objetivos que una vez satisfechos caracterizan a la organización (p. 392).

1.2.17 Características del modelo de madurez

Entre las características que un modelo de madurez para empresas debe presentar siguientes las características citadas por Pérez-Rojas et al. (2010):

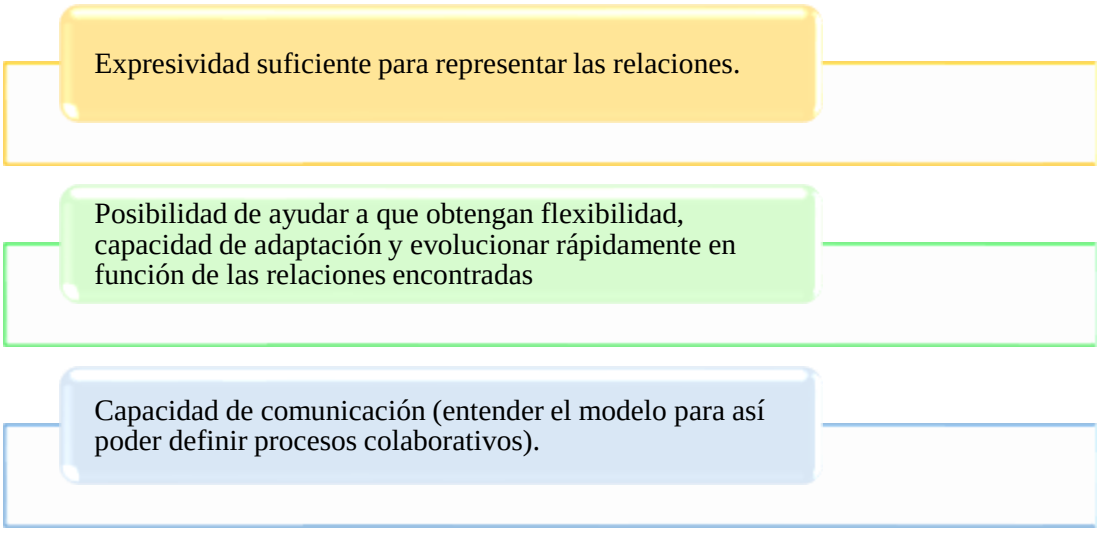


Gráfico 19. Características del modelo de madurez
Fuente: (Pérez-Rojas et al., 2010)

1.2.18 Clasificación de actividades de control

Pueden clasificar Serrano-Carrión, Señalin-Morales, Vega Jaramillo, Herrera Peña (2018) a las actividades de control en:

> Preventivos, detectivos y correctivos, además pueden incluirse controles a los manuales de usuario, de tecnología de información y controles administrativos. Básicamente las actividades de control deben encontrarse relacionadas con el tipo de empresa y con el personal y las funciones que realiza dentro de ella (p. 4).

CAPÍTULO II

METODOLOGÍA

2.1 Descripción de la metodología

2.1.1 Población

Para Lind-Douglas, Wathen-Samuel y Marchal-William (2012) “Es el conjunto de individuos u objetos de interés o medidas que se obtienen a partir de todos los individuos u objetos de interés”. La población de estudio serán todos los procesos tecnológicos llevados a cabo por la empresa “LA BAHÍA”, por ende, no tiene muestra está investigación.

2.1.2 Unidad de análisis

Desde el punto de vista de Picón y Melian (2014) la unidad de análisis es el conjunto de elementos que van hacer investigados, los mismos que formarán parte de la investigación.

Para el presente proyecto integrador se ha considerado como unidad de análisis a la empresa “La Bahía”, su edificio principal se encuentra ubicado en la ciudad de Ambato en la Av. Atahualpa diagonal al Comercial KYWI S.A. y la sucursal en el centro en las calles Juan Benigno Vela y Joaquín Lalama. La empresa lidera en la ciudad de Ambato por su actividad económica, que es la venta al por menor de electrodomésticos como: refrigeradoras, cocinas, microondas, lavadoras, entre otros. Además, lo que le diferencia del resto de las empresas es su stock, la imagen corporativa que hacen que el cliente sienta confianza y pueda encontrar todo lo que necesita en un solo lugar, es por ello que su eslogan describe dos palabras importantes para sus clientes, que es la tranquilidad y la economía, teniendo en cuenta que el consumidor es el punto clave para el crecimiento de la empresa.

En la actualidad la empresa ha ido creciendo e innovando su imagen corporativa y a la vez dando descuentos a todos sus clientes por la confianza y la fidelidad. Dicha empresa es muy reconocida en nuestra ciudad, por el trato al cliente y los cómodos precios de los electrodomésticos que garantiza al consumidor tener un producto de

calidad en su hogar.

2.1.3 Métodos, procedimientos y técnicas

2.1.3.1 Método

El método es un procedimiento que tiene un orden que debe ser respetado, el cual establece el significado de los fenómenos y hechos que son dirigidos hacia la investigación para demostrar, encontrar, refutar, describir y aportar conocimiento (Muñoz-Razo, 2011). En este proyecto integrador utilizaremos la metodología COBIT que evalúa las tecnologías de información **(TI)** de la empresa, el cual tiene como objetivo diseñar un sistema de control interno a los procesos informáticos.

2.1.3.2 Procedimientos y técnicas

El primer objetivo de la investigación es diagnosticar los procesos informáticos que se aplican a la empresa para la identificación de fortalezas y debilidades, el mismo que tiene una fuente primaria en donde se ocupará la técnica de la observación, que ayudará a plantear y efectuar el procedimiento adecuado del problema, investigando las diferentes ventajas que posee permitiendo continuar con el proceso, integrando programas, planes y métodos, también se utilizará la técnica de la entrevista que nos ayudará a conocer la situación de la empresa por medio del diálogo con el gerente empresarial, en conjunto con la ficha de observación que será el instrumento utilizado para cumplir el procedimiento, teniendo como producto un FODA reestructurado.

Para el mismo objetivo tiene como procedimientos los siguientes:

Tabla 11. Procedimiento del Objetivo I

PLANIFICACIÓN
Visita previa en la empresa.
Entrevista con el gerente de la empresa.
Revisión de cada parte consultada.
Identificación de las fortalezas y debilidades que poseen los procesos informáticos.

Fuente: (Cepeda Carolina, 2022)

Además, el siguiente objetivo es aplicar la metodología COBIT en los procesos informáticos que desarrolla la empresa, para la determinación de los puntos y riesgos

de control, teniendo como fuente primaria la encuesta, que es la técnica que más se ocupa en los equipos de auditoría, la misma que debe ser preparada con anterioridad, utilizando los cuestionarios con preguntas reestructuradas de control interno empleando la metodología COBIT, por lo tanto el producto sería un informe de los puntos y riesgos de control.

Es por ello, que para efectuar este objetivo debemos cumplir el siguiente proceso:

Tabla 12. Procedimiento del Objetivo II

PROCEDIMIENTO
Agendar una visita previa en la empresa.
Aplicación del cuestionario de control interno
Corroborar cada una de las respuestas del cuestionario.
Evaluar los riesgos y la calidad de las TI.
Aplicar principios de la metodología COBIT.
Redactar los puntos y riesgos de control.

Fuente: (Cepeda Carolina, 2022)

Finalmente, el último objetivo es presentar las políticas y procedimientos del sistema de control interno a los procesos informáticos para la gestión eficiente de las actividades informáticas, por ende se ocupará la fuente primaria, en donde se utiliza la técnica de la observación, que ayuda a corroborar lo que plasmamos en el informe con la realidad, la entrevista también se utilizará para informar al gerente de la empresa de lo que hemos encontrado, por lo tanto el producto es un Manual de políticas y procedimientos de control interno para los procesos informáticos.

Por consecuente, tenemos que efectuar el siguiente procedimiento:

Tabla 13. Procedimiento del Objetivo III

PROCEDIMIENTO
Describir el motivo de la elaboración del manual de políticas y procedimientos de control interno para la gestión adecuada de los procesos informáticos.
Establecer las políticas y procedimientos de control para los procesos informáticos
Elaborar el manual de políticas y procedimientos bajo la metodología COBIT.

Fuente: (Cepeda Carolina, 2022)

CAPÍTULO III

DESARROLLO

En esté capitulo se va a desarrollar la evaluación de control interno en la empresa “La Bahía”, por lo que se iniciará con una visita a la empresa para obtener información acerca de sus procesos informáticos que ocupen dentro de la institución e información relevante que nos ayuden en la investigación.

En el presente capítulo la información que se presenta a continuación, fueron recolectadas por fuente primaria, identificando todo el ámbito empresarial que posee, continuamos con la ejecución del cuestionario de control interno a los procesos informáticos y activos de información ocupando la metodología COBIT, la misma que evaluará los componentes Gobierno y Cultura, Estrategia y Objetivos, Desempeño, Revisión e Información y Comunicación y Reporte, el cual fue respondido por la gerente de la institución, posteriormente continuamos con el siguiente proceso.

Por consiguiente, corroboró sus activos de información utilizando un cuadro de procesos de información, el mismo que nos ayuda a la identificación de las fortalezas y debilidades que tienen los procesos y activos de información, dando como resultado un FODA de los procesos informáticos, luego se procede a la determinación de los puntos y riesgos de control.

Finalmente, como producto de la investigación se realizará un manual de las políticas y procedimientos del sistema de control interno aplicadas a los procesos informáticos de la empresa del sector de línea blanca, para una mejor gestión eficiente de las actividades informáticas que tenga la empresa, con ello podrán mejorar y cumplir todas sus expectativas.

DIAGNÓSTICO DE LOS PROCESOS INFORMÁTICOS

3.1 Diagnóstico de la empresa

INFORMACIÓN DE LA EMPRESA	
NOMBRE DE LA EMPRESA:	LA BAHÍA
TIPO DE AUDITORÍA:	Evaluación de procesos informáticos
PERÍODO AUDITADO:	Del 1 de enero al 31 de diciembre de 2021

ÍNDICE		
DIAGNÓSTICO DE LOS PROCESOS INFORMÁTICOS	**REF. /PT.**	**DESCRIPCIÓN**
	G.V. P	Guía de Visita Previa
	I.A. I	Identificación de los activos informáticos que tiene la empresa.
	P.D.E.	Procedimientos dentro de la empresa
	F.O.D.A	FODA de los procesos informáticos.

EQUIPO DE AUDITORÍA			
Nombre	**Iniciales**	**Cargos**	**% Participación**
Bertha Jeaneth Sánchez Herrera	**B.J.S.H**	Supervisora	50%
Eliana Carolina Cepeda Cruz	**E.C.C.C**	Senior	100%

	INICIALES	**FECHA**
ELABORADO POR	E.C.C.C	19/01/2022
REVISADO POR	B.J.S.H	26/01/2022

GUÍA DE VISITA PREVIA

1. INFORMACIÓN GENERAL	
1.1. Nombre de la entidad	Empresa “La Bahía”
1.2. Número de Ruc	1705424271001
1.3. Dirección	Ambato - Av. Atahualpa diagonal al Comercial KYWI S.A.
1.4. Correo electrónico de la empresa	contabilidadlabahia2020@gmail.com
1.5. Fecha de la visita	Ambato, 02 de febrero de 2022
1.6. Responsable de contestar la entrevista: Nombre y Cargo	Sra. Rosa Benigna Torres Rodríguez **GERENTE GENERAL**
1.7. Entrevistador: Nombre y Cargo	Srta. Eliana Carolina Cepeda Cruz **SENIOR**

2. INFORMACIÓN AMBIENTE INTERNO

La empresa “La Bahía”, fue creada el 9 de enero del 2002 en el Ecuador en la ciudad de Ambato, iniciando su actividad comercial con el siguiente número de RUC 1705424271001, es por ello que hoy en día tiene un edificio principal que se encuentra ubicado en la ciudad de Ambato en la Av. Atahualpa diagonal al Comercial KYWI S.A. y la sucursal en el centro de la ciudad, en las calles Juan Benigno Vela y Joaquín Lalama. La empresa lidera en la ciudad de Ambato por su actividad económica, que es la venta al por menor de electrodomésticos como: refrigeradoras, cocinas, microondas, lavadoras, entre otros. Además, lo que le diferencia del resto de las empresas es su stock, la imagen corporativa que hacen que el cliente sienta confianza y pueda encontrar todo lo que necesita en un solo lugar, es por ello que su eslogan describe dos palabras importantes para sus clientes, que es la tranquilidad y la economía, teniendo en cuenta que el consumidor es el punto clave para el crecimiento de la empresa. En la actualidad la empresa ha ido creciendo e innovando su imagen corporativa y a la vez dando descuentos a todos sus clientes por la confianza y la fidelidad. La Gerente General y propietaria de la empresa es la Sra. Rosa Benigna Torres Rodríguez y sus colaboradores que están

distribuidos en tres áreas, así como el Área Financiera en donde se encuentra la Contadora y sus tres auxiliares contables, en el Área de Mercadeo está constituida por tres vendedores y finalmente está el Área Administrativa con el Bodeguero. Dicha empresa es muy reconocida en nuestra ciudad, por el trato al cliente y los cómodos precios de los electrodomésticos que garantiza al consumidor tener un producto de calidad en su hogar.

Tabla 14. Cuestionario de los procedimientos y activos de información

No.	PREGUNTAS	SI	NO	OBSERVACIÓN
GOBIERNO Y CULTURA				
1	¿La empresa tiene detallada la actividad económica a la que se dedica?	X		
2	¿La empresa cuenta con una lista de clientes?	X		
3	¿La empresa cuenta con una lista de sus proveedores?	X		
4	¿La empresa se encuentra sujeta a entidades de control?	X		
5	¿Indique cuáles son los procedimientos dentro de la empresa?	X		**Ver P/T P.D.E.**
6	¿La empresa cuenta con un Software Contable?	X		
7	¿La Gerencia toma alguna decisión para proteger los activos informáticos?	X		
8	¿El departamento de Contabilidad trabajan mediante red?	X		
9	¿La empresa posee una red de internet propia?	X		
10	¿Toda la información de la empresa tiene algún respaldo de información?	X		
ESTRATEGIA Y OBJETIVOS				
1	¿Están los usuarios finales satisfechos con la calidad del servicio de TI?	X		Conocimiento del mercado y su trayectoria.
2	¿Se tarda en la toma de decisiones importantes de las TI?	X		
3	¿Los clientes utilizan algún activo de información?	X		El reporte solamente se le puede entregar a los clientes mayoristas.
4	¿La empresa está consciente de que se necesita un análisis sobre las tecnologías existentes?	X		
5	¿La entidad posee cámaras de seguridad y vigilancia?	X		
6	¿Posee un responsable de la vigilancia de las cámaras de seguridad?	X		
DESEMPEÑO				
1	¿El Software Contable cuenta con claves de acceso?	X		
2	¿Existe un responsable de los activos informáticos?		X	
3	¿Se cuenta con un proceso de monitoreo para verificar el		X	

	cumplimiento de las políticas de TI?			
4	¿Los activos informáticos tienen un mantenimiento oportuno?	X		
5	¿Existe obligaciones para monitorear el marco legal, y regulatorio sobre TI?	X		
6	¿Posee una nómina de activos informáticos que posee la empresa?		X	
7	¿Cada departamento cuenta con equipos informáticos?	X		
8	¿Existe constante capacitación acerca de la utilización correcta de los activos informáticos?		X	
REVISIÓN				
1	¿Se aseguran que el personal contratado sea calificado para la administración de TI cumpla con las políticas organizacionales de protección de los activos de información?	X		
2	¿Se revisan periódicamente los registros de acceso a los sistemas?	X		
3	¿Se dan soluciones tecnológicas oportunas para todas las áreas de la empresa?	X		
4	¿Los equipos de información tienen claves de seguridad?	X		
INFORMACIÓN, COMUNICACIÓN Y REPORTE				
1	¿Se mantiene un control de la salida de activos informáticos por parte de terceros?		X	La mayoría de veces lo realizan en la empresa.
2	¿Se emite un informe a la Administración sobre el desempeño de los servicios ofrecidos?		X	
3	¿Se mide el cumplimiento del correcto uso de las TI?		X	
4	¿Se realiza un correcto mantenimiento a los activos informáticos?	X		

Fuente: (Cepeda Carolina, 2022)

3. INFORMACIÓN AMBIENTE EXTERNO

En el sector de la línea blanca en donde se comercializa todo tipo de electrodomésticos sus ventas fueron exitosas y tenían una gran utilidad, en el año 2019 ocurrió la emergencia sanitaria por Covid-19, en donde el sector fue afectado en sus ventas los primeros meses, por lo que los clientes no tenían ingresos económicos para comprar, es por ello que también no podían salir de sus casas en donde cada empresa realiza una estrategia de vender de manera online incluyendo el valor del envío en sus hogares, además gracias aquella estrategia lograron culminar el año 2020 con satisfacción. Además, como manifiesta **Leonardo Otatti**, director de la **Cámara Ecuatoriana de Comercio Electrónico** (CECE), señala que este año habrá un 45% más de comercios que entrarán a la ola digital. “Existirá una gran competencia porque los almacenes y

emprendimientos que no aprovecharon el 2020 para vender por Internet, este año apostarán por estrategias más agresivas", es por ello que las empresas del sector de línea blanca lograron cumplir todas las expectativas planteadas (Alvarado, 2021).

3.1. ASPECTO ECONÓMICO, LEGAL Y POLÍTICO

Como menciona el Ministerio de Industrias y Productividad (MIPRO) el sector de línea blanca en China y Latinoamérica son los mercados que más crecen, siendo así, Latinoamérica representa el 10% del total de las ventas, teniendo en cuenta que en Ecuador los productos que más se comercializan son los refrigeradores, lavadoras y las cocinas, por lo que la producción ecuatoriana posee dos productores mayores que representan el 90% de la producción. Por consiguiente, nuestro país Ecuador exporta $130 millones de dólares siendo uno de los mayores exportadores de la región, en donde las cocinas es el electrodoméstico más exportado (Ministerio de Industrias y Productividad, 2015).

Las exportaciones ecuatorianas poseen una amenaza principal que es la reducción de costos para mantener competitivo el sector y a la vez tener un tener un mercado externo más adverso.

Por otro lado, Andrés Mata, director ejecutivo de la Asociación de Almacenes de Electrodomésticos del Ecuador (Asadelec), manifestó que en esta temporada se ha demandado televisores, aires acondicionados, refrigeradoras, cocinas y lavadoras, teniendo en cuenta que las tiendas han optado por brindar a los clientes mayores facilidades de pago y ofertas, lo que en otras empresas realizaron ajustes en la nómina.

Los almacenes que venden electrodomésticos se han apoyado en las ventas en línea para mantenerse. Pero en ese este sector hubo también una baja del 28% entre enero y mayo del 2020 (Nación, 2020).

Finalmente, en la industria de la línea blanca la fábrica Ecoline con su Gerente General Diego Malo expresó, que los meses más fatales para la economía del sector fue marzo y abril, por lo que a inicios del mes de mayo reabrieron la planta con la previa autorización del Comité de Operaciones Emergentes (COE), aplicando todos los protocolos de bioseguridad con sus empleados, aunque los números aún no reflejen la

utilidad de la industria de línea blanca, se empezó a mostrar un leve crecimiento en sus ventas (El Universo, 2020).

3.2. ASPECTO TECNOLÓGICO

En el sector de los electrodomésticos la implementación de la tecnología es un aporte para el cambio en el sector, por lo que estás nuevas tecnologías han ayudado a cerrar una venta por medio de la red social WhatsApp o por otras redes, de esta manera han logrado que los clientes tengan una relación más cercana digitalmente con la empresa. A medida de que la tecnología se vaya innovando permite que el cliente empiece a valorar más la experiencia que puede tener al momento de realizar la compra, que algún otro beneficio, sin olvidarnos que está gran oportunidad de ocupar la tecnología nos permite fidelizar a los clientes (Avilés, 2020).

Además, la inversión de una nueva tecnología nos ayuda a llevar acabo nuevos procesos productivos que requieren la incorporación de nuevas líneas y productos para el consumidor, en los últimos años el sector industrial de línea blanca en el Ecuador ha tenido un dinamismo, que es producto de la innovación de productos, nuevas marcas, y también ofertas de nuevos precios en los productos que presenten eficiencia para el cliente (Centro de Investigaciones Económicas y de la Micro, 2011).

3.3. ASPECTO DE COMPETENCIA

La empresa LA BAHÍA no posee competencias dentro de la provincia de Tungurahua, en vista de que no existe otra empresa que ofrezca lo mismo, por lo que la empresa tiene todo lo necesario para amoblar un hogar, de tal manera que sus precios son económicos y de esta manera los clientes pueden comprar todo lo necesario.

Sra. Rosa Benigna Torres Rodríguez	Srta. Eliana Carolina Cepeda Cruz
Gerente General	**Senior Auditoría**
EMPRESA "LA BAHÍA"	**AUDITORÍA LIDER**

IDENTIFICACIÓN DE LOS ACTIVOS INFORMÁTICOS QUE POSEE LA EMPRESA

Tabla 15. Identificación de los activos informáticos que posee la empresa

No.	ACTIVOS INFORMÁTICOS	SI	NO	OBSERVACIÓN
DOCUMENTAL				
1	Actas		**X**	
2	Acuerdos		**X**	
3	Circulares	**X**		
4	Informes		**X**	
5	Manuales y planes		**X**	
SOFTWARE				
1	Cliente	**X**		
2	Planificación de recursos empresariales		**X**	
3	Herramientas de bases de datos (MSQL)	**X**		
4	Aplicaciones de comercio electrónico		**X**	
FÍSICO (HARDWARE)				
1	Dispositivos de almacenamiento	**X**		
2	Ordenadores de mesa	**X**		
3	Estaciones de trabajo	**X**		
4	Tablet	**X**		
5	Equipos de mano	**X**		
6	Servidores	**X**		
7	Módems	**X**		
8	Líneas de terminación de red (Punto de red final)	**X**		
9	Dispositivos de comunicaciones	**X**		
10	Equipos multifunción	**X**		
11	Cámaras de seguridad	**X**		
PERSONAL				
1	Personal	**X**		
2	Operadores	**X**		
3	Abogados		**X**	
4	Asesores externos	**X**		
5	Proveedores	**X**		
SERVICIO				
1	Servicios de autenticación de usuario	**X**		Windows Server
2	Cortafuegos	**X**		

3	Servicios de red	**X**		
4	Servicios inalámbricos	**X**		
5	Anti-spam (mensajes)	**X**		
6	Virus	**X**		
7	Servicios web	**X**		
8	Teletrabajo		**X**	Por el momento NO
9	Seguridad		**X**	
10	Correo electrónico	**X**		
11	Mensajería instantánea		**X**	
12	Contratos de soporte		**X**	
13	Mantenimiento del software	**X**		
RED DE DATOS				
1	Servidores	**X**		
2	Dispositivos de red	**X**		

Fuente: (Cepeda Carolina, 2022)

PROCEDIMIENTOS DENTRO DE LA EMPRESA DEL SISTEMA INFORMÁTICO

EMPRESA: "LA BAHÍA"

PROCESO A: COMPRAS

PROCEDIMIENTO	RESPONSABLE
1. Se realiza un pedido de compra de inventario.	Vendedores
2. Se autoriza el pedido de compra de inventario.	Gerente General
3. Se procede a facturar la compra del inventario.	Proveedor
4. La factura de compra se ingresa al sistema contable a los diferentes módulos	Auxiliar Contable
5. Se analiza la forma de pago, el mismo que será dirigido a sus respectivos módulos	Auxiliar Contable

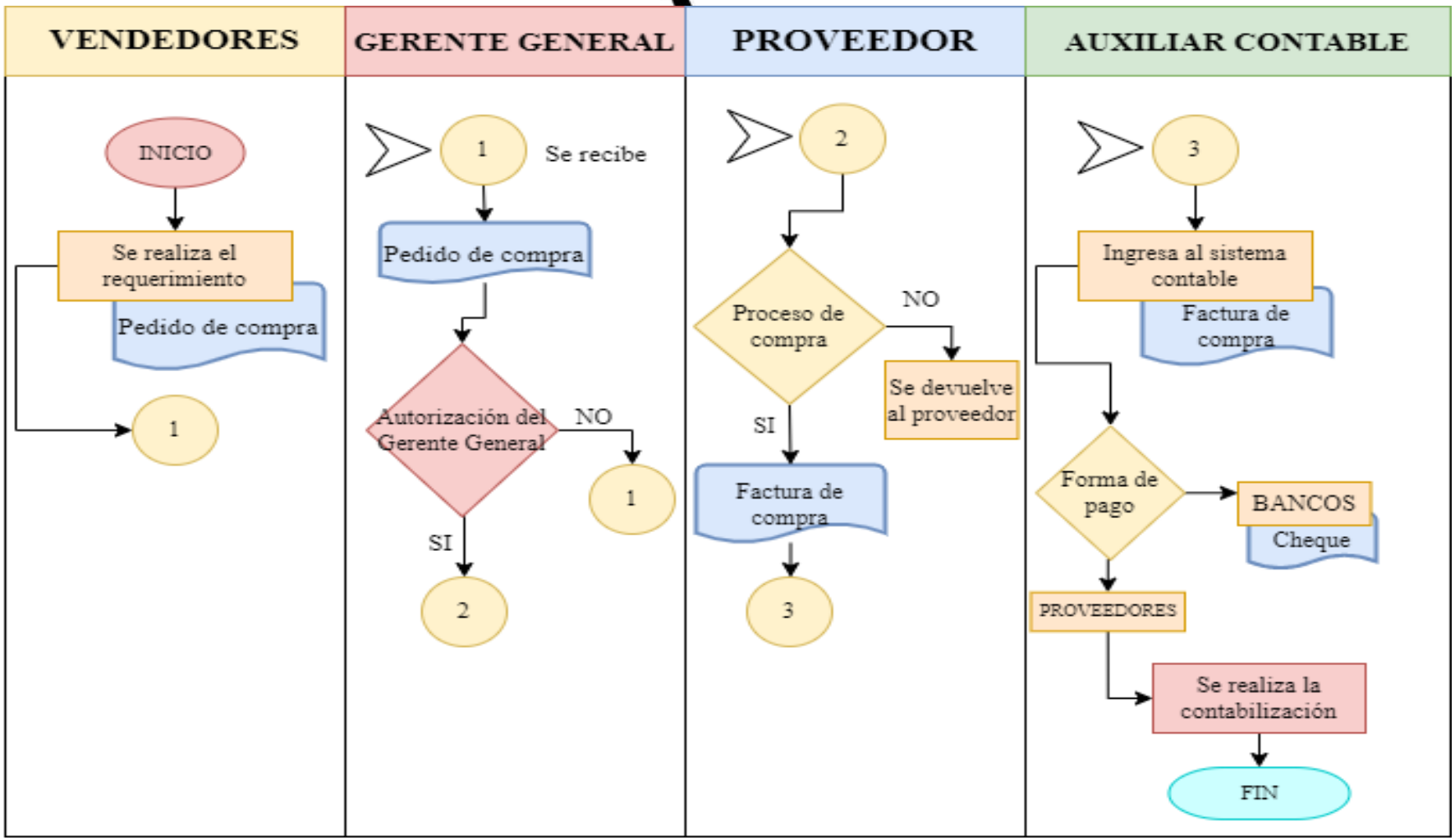


Gráfico 20. Diagrama del proceso A de la empresa "La Bahía"
Fuente: (Cepeda, 2022)

EMPRESA: "LA BAHÍA"

PROCESO B: VENTAS

PROCEDIMIENTO	RESPONSABLE
1. Se busca al cliente en el sistema contable para realizar la venta.	VENDEDOR
2. Buscar el nombre del producto que se va a vender	VENDEDOR
3. Escoger en la lista de precios a cual corresponde el cliente.	VENDEDOR
4. Elegir la forma de pago que pueden ser efectivo, cheque y tarjeta de crédito	VENDEDOR
5. Se realiza la facturación electrónica.	VENDEDOR
6. Verifica la autorización automática del sistema.	AUXILIAR CONTABLE
7. En una hora en específico se envía para la respectiva autorización de la factura.	AUXILIAR CONTABLE
8. Se realiza el respectivo registro contable.	AUXILIAR CONTABLE

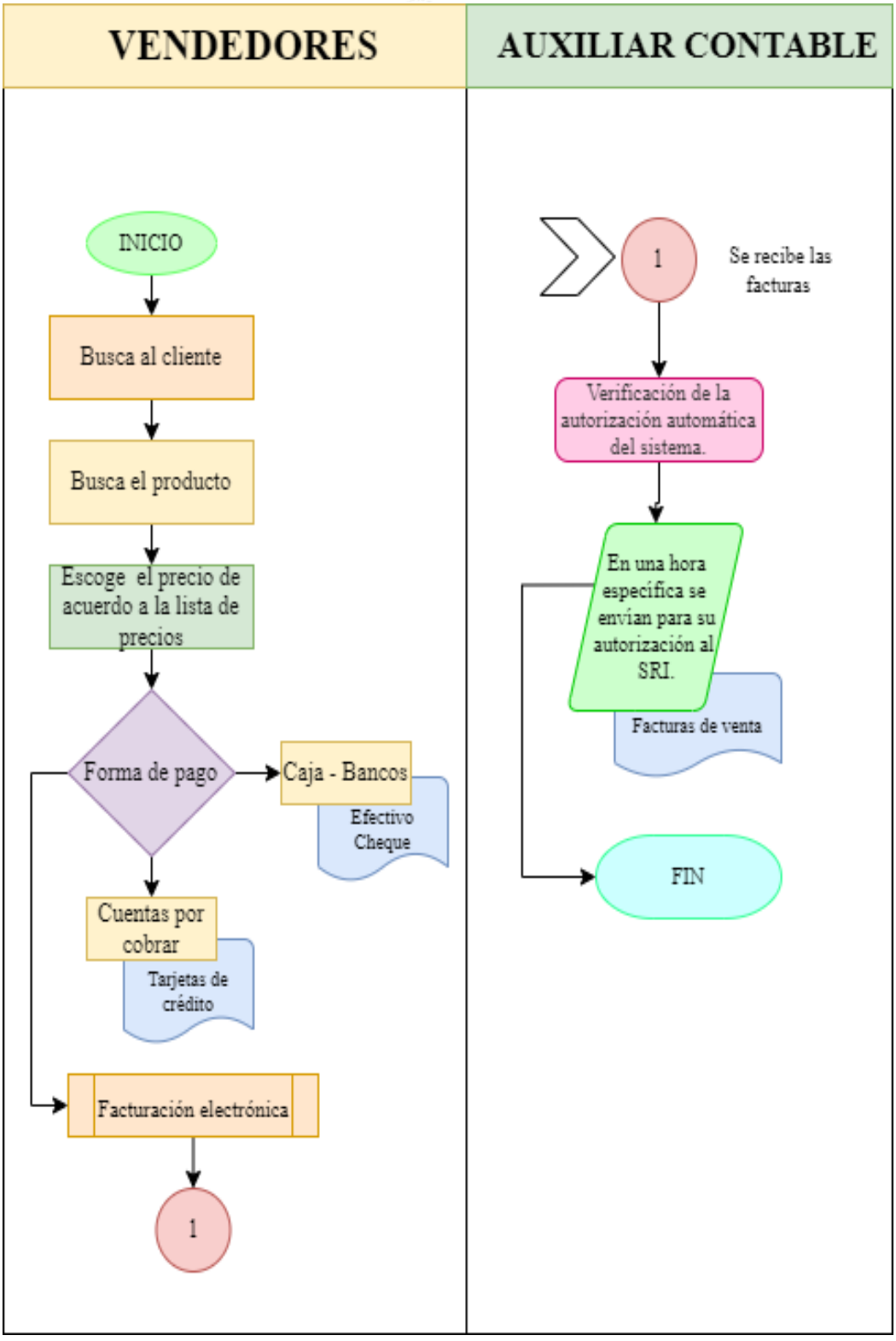


Gráfico 21. Diagrama del proceso B de la empresa “La Bahía”
Fuente: (Cepeda, 2022)

EMPRESA: "LA BAHÍA"

PROCESO C: CONTABILIDAD

PROCEDIMIENTO	RESPONSABLE
1. Ingresa la factura de venta.	AUXILIAR CONTABLE
2. Se revisa la factura de venta.	AUXILIAR CONTABLE
3. Se procede a verificar la forma de pago.	AUXILIAR CONTABLE
4. Continúa con el proceso de contabilización	AUXILIAR CONTABLE

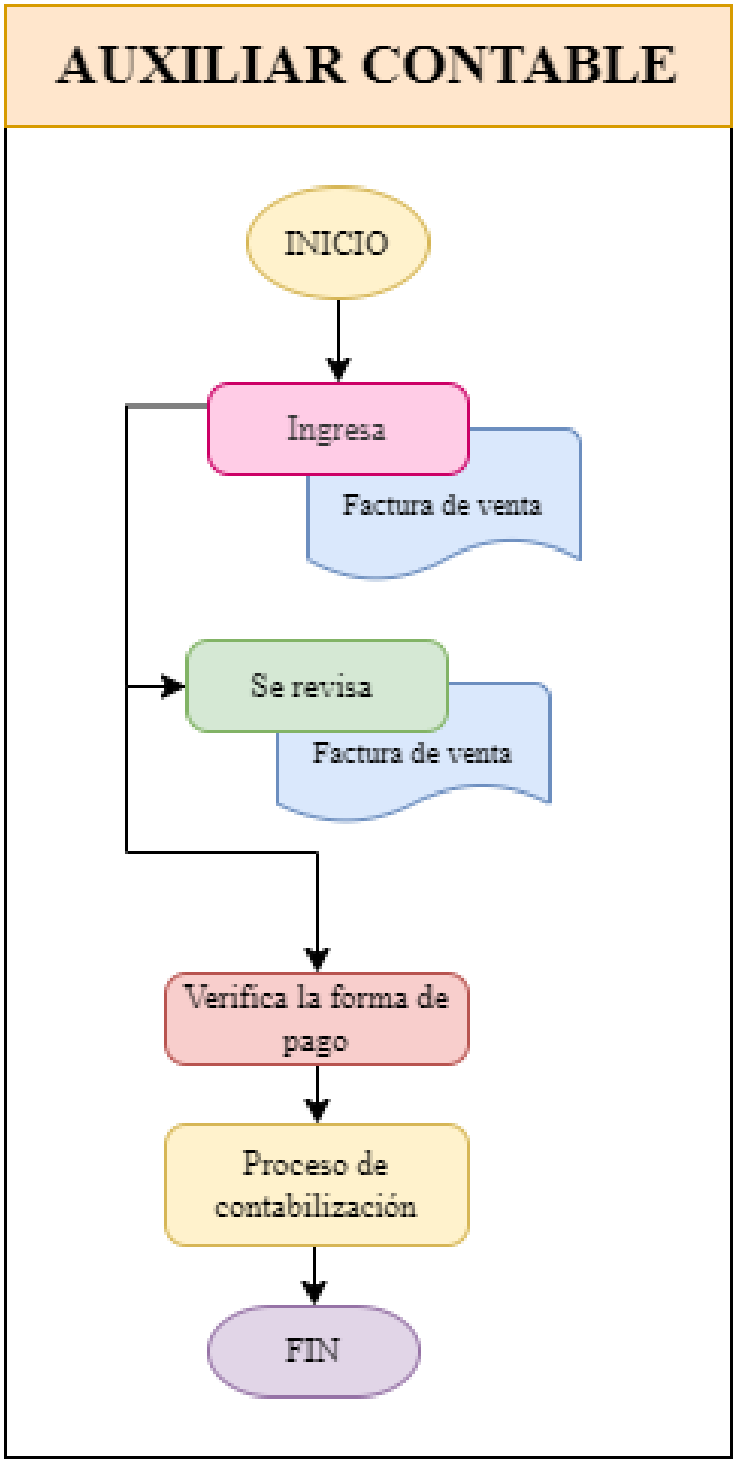


Gráfico 22. Diagrama del proceso C de la empresa "La Bahía"
Fuente: (Cepeda, 2022)

FODA DE LOS PROCESOS INFORMÁTICOS

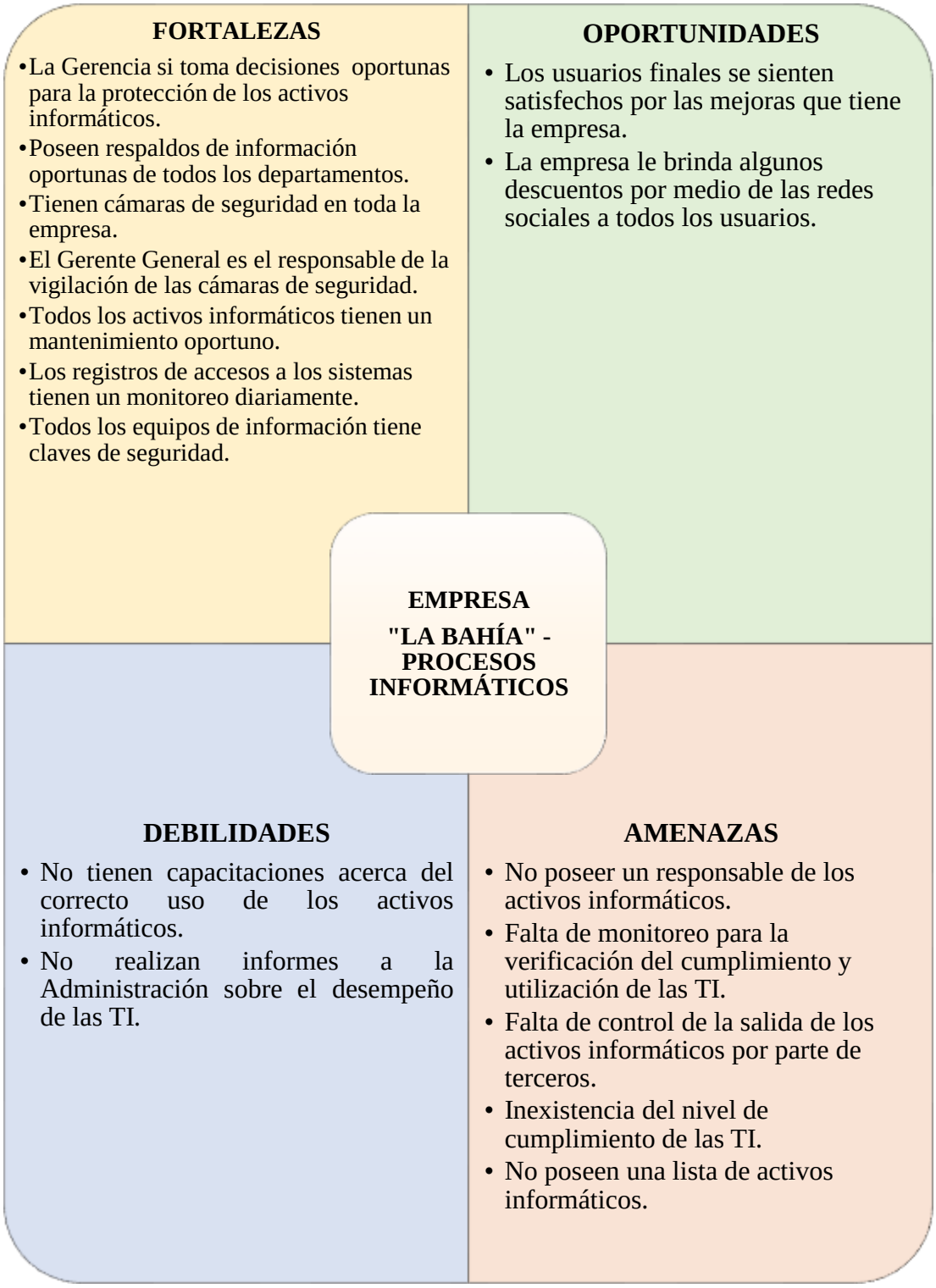


Gráfico 23. FODA de los procesos informáticos

Fuente: (Cepeda Carolina, 2022)

APLICACIÓN DE LA METODOLOGÍA COBIT

3.2 Aplicación de la metodología Cobit

INFORMACIÓN DE LA EMPRESA	
NOMBRE DE LA EMPRESA:	LA BAHÍA
TIPO DE AUDITORÍA:	Evaluación de procesos informáticos
PERÍODO AUDITADO:	Del 1 de enero al 31 de diciembre de 2021

ÍNDICE		
	REF. /PT.	**DESCRIPCIÓN**
APLICACIÓN DE LA METODOLOGÍA COBIT	**A.A.M**	Antecedentes para la aplicación de la Metodología COBIT
	E.D.M.	Evaluar, orientar y supervisar
	A.P.O.	Alinear, planificar y organizar
	B.A.I.	Construir, adquirir e implementar
	D.S.S.	Entrega, servicio y soporte
	M.E.A.	Supervisar, evaluar y valorar
	H.H.	Hoja de hallazgos

EQUIPO DE AUDITORÍA			
Nombre	**Iniciales**	**Cargos**	**% Participación**
Bertha Jeaneth Sánchez Herrera	**B.J.S.H**	Supervisora	50%
Eliana Carolina Cepeda Cruz	**E.C.C.C**	Senior	100%

	INICIALES	**FECHA**
ELABORADO POR	E.C.C.C	19/01/2022
REVISADO POR	B.J.S.H	26/01/2022

ANTECEDENTES PARA LA APLICACIÓN DE LA METODOLOGÍA COBIT 5 EN LA EMPRESA

Antes de iniciar la aplicación de la metodología COBIT 5 iniciamos con las respectivas valoraciones para proceder con la metodología en cada uno de los procesos de las TI definidos en el marco referencial, a continuación, las tablas que se va a utilizar para la aplicación:

Tabla 16. Niveles de capacidad para ocupar en la empresa

NIVELES	DESCRIPCIÓN
NIVEL 0 (Proceso incompleto)	El proceso no alcanza su objetivo, es por ello que existe poca posibilidad de tener una evidencia de ningún logro sistemático del objetivo del procedimiento.
NIVEL 1 (Proceso ejecutado)	La técnica implementada alcanza su meta.
NIVEL 2 (Proceso gestionado)	El procedimiento ya está gestionado (planificado, supervisado y ajustado) y los resultados están determinados, inspeccionados y cuidados de forma adecuada.
NIVEL 3 (Proceso establecido)	Se utiliza un procedimiento establecido que ayude en el cumplimiento de los resultados propuestos.
NIVEL 4 (Proceso predecible)	Procedimiento elaborado dentro de los parámetros establecidos para alcanzar sus efectos de este.
NIVEL 5 (Proceso optimizado)	El método es mejorado de manera inmediata que ayuda al desempeño de los objetivos empresariales.

Fuente:(ISACA, 2012)

Además, en este proceso debemos ocupar otra tabla en donde se mencione los criterios de evaluación en cuanto al cumplimiento que debe tener la empresa por cada actividad.

Tabla 17. Criterios de evaluación para ocupar en la empresa según la ISO 15504

SIGLA	DESCRIPCIÓN	VALORACIÓN %
F	Completamente Alcanzado	>86 ≤ 100
L	Alcanzado en gran manera	>50 ≤ 85
P	Parcialmente Alcanzado	>15 ≤ 50
N	No cumple (no alcanzado)	0 ≤ 15

Fuente:(Alarcón et al., 2011)

MATRICES PARA LA APLICACIÓN DE LA METODOLOGÍA COBIT 5 EN LA EMPRESA

En la empresa "La Bahía" se aplicó la metodología COBIT 5, en donde no se ocuparon todos los catalizadores por el tamaño de la empresa, es por ello que a continuación se detalla las matrices utilizadas.

Tabla 18. EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
Descripción del Proceso Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.	
Declaración del Propósito del Proceso Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas relacionadas**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI • Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados • Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	• Porcentaje de los roles de la gestión ejecutiva con responsabilidades claramente definidas para las decisiones de TI • Número de ocasiones en que TI de forma proactiva está en la agenda del Consejo de Administración • Frecuencia de las reuniones del Comité (Ejecutivo) de TI. • Ratio de ejecución de las decisiones ejecutivas relativas a TI
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
Metas y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas.	• Tiempo de ciclo actual vs objetivo para las decisiones clave • Nivel de satisfacción mediante encuestas de las personas interesadas
2. Garantizar que el sistema de gobierno para TI está incorporado al gobierno corporativo.	• Número de roles, responsabilidades y autoridades que están definidas, asignadas y aceptadas a gestores para una gestión del negocio y de las TI apropiados. • Grado en que los principios de gobierno acordados para las TI están evidenciados en procesos y prácticas (porcentaje de procesos y prácticas con clara trazabilidad a los principios) • Número de casos de no-cumplimiento con las directrices de comportamiento ético y profesional
3. Obtener garantías de que el sistema de gobierno para TI está operando de manera efectiva.	• Frecuencia de revisiones independientes del gobierno de TI • Frecuencia del reporte del gobierno de TI al Comité Ejecutivo y a la dirección • Número de aspectos de gobierno de TI notificados

MATRIZ RACI EDM01

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero(CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Director de Recursos Humanos	Cumplimiento Normativo	Auditoría	Director de Informática (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Director de Privacidad de la Información
EDM01.01 Evaluar el sistema de	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Orientar el sistema de	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Supervisar el sistema de	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

EDM01 Prácticas, actividades y entradas/salidas del Proceso				
Práctica de gobierno	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	MEA03.02	Comunicaciones de los requerimientos de cumplimiento modificados.	Principios directrices del gobierno de la empresa	Todo EDM APO01.01 APO01.03
			Modelo de toma de decisiones	Todo EDM APO01.01
	Fuera del Ámbito de COBIT	• Tendencias en el entorno del negocio • Regulaciones • Gobierno/modelo de toma de decisiones • Constitución/normas/ estatutos de la organización	Niveles de autoridad	Todo EDM APO01.02

Actividades	Nivel de capacidad
1. Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno.	3
2. Determinar la relevancia de TI y su papel con respecto al negocio.	3
3. Considerar las regulaciones externas, obligaciones legales y contractuales y determinar cómo deben ser aplicadas en del gobierno de TI de la empresa.	3
4. Alinear el uso y el procesamiento ético de la información y su impacto en la sociedad, en el entorno natural y en los intereses de las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa.	4
5. Determinar las implicaciones del entorno de control conjunto de la empresa con respecto a TI.	3
6. Articular los principios que guiarán el diseño de la toma de decisiones sobre el gobierno de TI.	3
7.Comprender la cultura empresarial de la toma de decisiones y determinar un modelo óptimo en la toma de decisiones para TI.	4
8. Determinar los niveles apropiados para la delegación de autoridad, incluyendo reglas de umbrales, para las decisiones de TI.	4

Nivel de capacidad objetivo

3

			87,13	**Nivel de cumplimiento**	**Nivel de cumplimiento objetivo**	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
		80		80	F	No se cumple
			90	90	F	Cumplida
			88	88	F	Cumplida
			90	90		Cumplida
			87	87	F	Cumplida
			86	86	F	Cumplida
			90	90		Cumplida
			86	86		Cumplida

EDM01 Prácticas, actividades y entradas/salidas del Proceso (cont.)				
Prácticas de Gobierno	**Entradas**		**Salidas**	
EDM01.02 Orientar el sistema de gobierno. Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.	**De**	**Descripción**	**Descripción**	**A**
			Comunicaciones del gobierno de la empresa	Todo EDM APO01.04
			Enfoque de sistema de recompensa	APO07.03 APO07.04

Actividades	**Nivel de capacidad**
1. Comunicar los principios del gobierno de TI y acordar con el gestor ejecutivo la manera de establecer un liderazgo informado y comprometido.	4
2. Establecer o delegar el establecimiento de las estructuras, procesos y prácticas del gobierno en línea con los principios de diseño acordados.	3
3. Asignar responsabilidad, autoridad y la responsabilidad de que se apliquen los principios de diseños de gobierno, los modelos de toma de decisión y de delegación acordados.	4
4. Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos con la responsabilidad de la supervisión y toma de decisiones.	4
5. Orientar al personal para que siga las directrices relevantes para un comportamiento ético y profesional y garantizar que las consecuencias del no cumplimiento se conocen y se respetan.	4
6. Orientar el establecimiento de un sistema de recompensa para promover el cambio cultural deseable.	4

			87,67	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			88	88		Cumplida
			87	87	F	Cumplida
			86	86		Cumplida
			89	89		Cumplida
			90	90		Cumplida
			86	86		Cumplida

Práctica de Gobierno	Entradas		Salidas	
	De	Descripción	Descripción	A
EDM01.03 Supervisar el sistema de gobierno. Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	MEA01.04	Informes de rendimiento	Retroalimentación sobre el rendimiento y efectividad del gobierno	Todo EDM APO01.07
	MEA01.05	Estado y resultados de las acciones		
	MEA02.01	• Resultados de estudios comparativos y otras evaluaciones. • Resultado de la monitorización y revisiones de control interno		
	MEA02.03	Resultados de las revisiones de las autoevaluaciones		
	MEA02.06	Planes de aseguramiento		
	MEA03.03	Confirmaciones de cumplimiento		
	MEA03.04	• Informes sobre aspectos de no cumplimiento y el origen de sus causas • Informes de aseguramiento del cumplimiento		
	Fuera del Ámbito de COBIT	• Obligaciones • Informes de auditoría	Acciones para mejorar la entrega de valor	EDM05.01 APO05.04 APO06.02 BAI01.01

Actividades	Nivel de capacidad
1. Evaluar la efectividad y rendimiento de las partes interesadas en las que se ha delegado responsabilidad y autoridad para el gobierno de TI de la empresa.	4
2. Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.	4
3. Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.	4
4. Mantener la supervisión sobre el punto hasta el que TI satisface las obligaciones (regulatorias, legislación, leyes comunes, contractuales), políticas internas, estándares y directrices profesionales.	4
5. Proporcionar supervisión de la efectividad de, y el cumplimiento, con el sistema de control de la empresa.	4
6. Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.	4

			87,80	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			86	86		Cumplida
			88	88		Cumplida
			89	89		Cumplida
			90	90		Cumplida
			86	86		Cumplida
			87	87		Cumplida

MARCA	DESCRIPCIÓN
	En la aplicación de la metodología COBIT en la actividad Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno, se obtuvo un nivel de capacidad de 4 y su nivel de cumplimiento alcanzable del 85%, que no está dentro de los parámetros establecidos, es decir existe un desconocimiento de la legislación que regula las TI por parte de la empresa. **HH (1)**

Tabla 19. EDM03 Asegurar la Optimización del Riesgo

EDM03 Asegurar la Optimización del Riesgo	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
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.	
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
15 Cumplimiento de las políticas internas por parte de las 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
Metas y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	• Nivel de alineamiento entre riesgo TI y riesgo de negocio • Número de potenciales riesgos TI identificados y gestionados • Frecuencia de refresco de la evaluación de los factores de riesgo
2. La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	• Porcentaje de proyectos de la empresa que consideran el riesgo TI • Porcentaje de planes de acción de riesgo TI ejecutados en tiempo • Porcentaje de riesgos críticos que han sido eficazmente mitigados
3. Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado.	• Nivel de impacto empresarial inesperado • Porcentaje de riesgos TI que exceden el riesgo empresarial tolerado

EDM03 RACI Chart

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
EDM03.01 Evaluar la gestión de riesgos.	A	R	C	C	R	C	R			I	R	C		I	C	C	C	R	C							C
EDM03.02 Orientar la gestión de	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I	I	I
EDM03.03 Supervisar la gestión de	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	I	I	C

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gobierno		**Entradas**	**Salidas**	
	De	**Descripción**	**Descripción**	**A**
EDM03.01 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.	APO12.01	Factores y problemas de riesgos emergentes	Guías de apetito de riesgo	APO12.03
			Niveles de tolerancia de riesgo aprobados	APO12.03
	Fuera del Ámbito de COBIT	Principios de la gestión de riesgos de la empresa	Evaluación de las actividades de gestión de riesgo	APO12.01

Actividades	Nivel de capacidad
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
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
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.	4
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.	4
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
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

Nivel de capacidad objetivo

3

			86,67
N	**P**	**L**	**F**
			86
		85	
			87
			89
			86
			87

Nivel de cumplimiento
Valor
86
85
87
89
86
87

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	No se cumple
	Cumplida
	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gobierno	Entradas		Salidas	
	De	Descripción	Descripción	A
EDM03.02 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.	APO12.03	Perfil de riesgo agregado incluyendo el estado de las acciones de gestión del riesgo	Políticas de gestión de riesgos	APO12.01
			Objetivos claves a ser monitorizados por la gestión de riesgos	APO12.01
	Fuera del Ámbito de COBIT	Perfiles y planes de mitigación de la Gestión del Riesgo de la Empresa (ERM)	Proceso aprobado para la medición de la gestión de riesgos	APO12.01

Actividades	Nivel de capacidad
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.	4
2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.	4
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.	4
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
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
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

Nivel de capacidad objetivo
3

			87,83
N	P	L	F
			86
			88
			89
			87
			90
			87

Nivel de cumplimiento
Valor
86
88
89
87
90
87

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gobierno	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
EDM03.03 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.	APO12.02	Resultados del análisis de riesgos	Acciones correctivas para tratar las desviaciones en la gestión del riesgo	APO12.06
	APO12.04	• Oportunidades para la aceptación de un mayor riesgo • Resultados de las evaluaciones de riesgos de terceras partes • Análisis de riesgos e informes de perfil de riesgos para las partes interesadas	Problemas de la gestión de riesgos para la Dirección	EDM05.01

Actividades	Nivel de capacidad
1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.	3
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
3. Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.	3
4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.	4

Nivel de capacidad objetivo

			87,00
N	**P**	**L**	**F**
			86
			87
			88
			87

Nivel de cumplimiento
Valor
86
87
88
87

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida

MARCA	DESCRIPCIÓN
	En la metodología COBIT en la actividad Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa, la misma que tiene un nivel de capacidad 3 y nivel de cumplimiento alcanzable del 85% , dando como resultado que no dispone de una guía en donde se establezcan los parámetros de las TI. HH (2)

Tabla 20. EDM04 Asegurar la Optimización de Recursos

EDM04 Asegurar la Optimización de Recursos	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar"**
Descripción del Proceso Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	
Declaración del Propósito del Proceso Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
09 Agilidad de las TI	• Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos • Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas • Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada
11 Optimización de los activos, recursos y capacidades de las 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
16 Personal del negocio y de las TI competente y motivado	• Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función • Porcentaje del personal satisfecho con su función TI • Número de horas de aprendizaje/prácticas por trabajador
Metas y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Las necesidades de recursos de la empresa son cubiertos con capacidades óptimas.	• Nivel de realimentación de las partes interesadas sobre la optimización de los recursos • Serie de beneficios (p.ej., ahorro de costes) que se logran a través de la utilización óptima de los recursos • Número de desviaciones del plan de recursos y las estrategias de arquitectura empresarial
2. Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones.	• Número de desviaciones (y excepciones) de los principios de gestión de recursos • Porcentaje de proyectos con asignación de recursos adecuados
3. El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico.	• Porcentaje de reutilización de componentes de la arquitectura • Porcentaje de proyectos y programas con un estado de riesgo medio o alto debido a los problemas en la gestión de recursos • Número de metas de rendimiento de la gestión de recursos alcanzadas

Matriz RACI EDM04

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
EDM04.01 Evaluar la gestión de recursos.	A	R	C	C	R		R			I	C	C	C	C	C	C	C	R	C	C	C					
EDM04.02 Orientar la gestión de recursos.	A	R	C	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM04.03 Supervisar la gestión de	A	R	C	C	R	I	R	I	I	I	C	C	C	C	C	C	C	R	C	C	C	I	I	I	I	I

EDM04 Asegurar la Optimización de Recursos				
Práctica de Gobierno	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
EDM04.01 Evaluar la gestión de recursos. Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa	APO02.04	Brechas y cambios necesarios para hacer realidad los objetivos de capacidad	Principios rectores para la asignación de recursos y capacidades	APO02.01 APO07.01 BAI03.11
	APO07.03	Planes de desarrollo de competencias	Principios rectores de la arquitectura de la empresa	APO03.01
	APO10.02	Decisiones sobre los resultados de evaluación de proveedores	Plan de recursos aprobado	APO02.05 APO07.01 APO09.02

Actividades	Nivel de capacidad
1. Examinar y evaluar la estrategia actual y futura, las opciones de aprovisionamiento de recursos TI y desarrollar capacidades para cubrir las necesidades actuales y futuras (incluyendo alternativas de aprovisionamiento).	4
2. Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI puedan satisfacer las necesidades de la empresa, con la habilidad y capacidad requerida de acuerdo a las prioridades acordadas y las limitaciones presupuestarias.	4
3. Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la empresa para la entrega de valor y la mitigación de riesgos con los recursos asignados.	3
4. Comprender los requisitos para alinear la gestión de recursos con la planificación de recursos empresariales financieros y humanos.	4
5. Definir los principios para la gestión y el control de la arquitectura de la empresa.	4

			87,20
N	**P**	**L**	**F**
			86
			87
			88
			89
			86

Nivel de cumplimiento
Valor
86
87
88
89
86

Nivel de capacidad objetivo

3

Nivel de cumplimiento objetivo	
Meta	**Observación**
	Cumplida
	Cumplida
F	Cumplida
	Cumplida
	Cumplida

Práctica de Gobierno	Entradas		Salidas	
EDM04.02 Orientar la gestión de recursos.	**De**	**Descripción**	**Descripción**	**A**
Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica.			Comunicación de las estrategias de reasignación de recursos	APO02.06 APO07.05 APO09.02
			Responsabilidades asignadas para la gestión de los recursos	APO01.02 DSS06.03
			Principios para la protección de recursos	APO01.04

Actividades	Nivel de capacidad
1. Comunicar e impulsar la adopción de estrategias de gestión de recursos, principios y el plan de recursos y las estrategias de arquitectura de empresa acordados.	4
2. Asignar responsabilidades para la ejecución de la gestión de recursos.	4
3. Definir los objetivos, medidas y métricas clave para la gestión de los recursos.	4
4. Establecer los principios relacionados con la protección de recursos.	4
5. Alinear la gestión de recursos con la planificación de RRHH y financiera de la empresa.	4

			87,60
N	**P**	**L**	**F**
			87
			88
			89
			86
			88

Nivel de cumplimiento
Valor
87
88
89
86
88

Nivel de capacidad objetivo

3

Nivel de cumplimiento objetivo	
Meta	**Observación**
	Cumplida
	Cumplida
	Cumplida
	Cumplida
	Cumplida

Práctica de Gobierno	Entradas		Salidas	
EDM04.03 Supervisar la gestión de recursos.	**De**	**Descripción**	**Descripción**	**A**
Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.			Comentarios sobre la asignación y la eficacia de los recursos y capacidades	EDM05.01 APO02.05 APO07.05 APO09.05
			Acciones correctivas para hacer frente a las desviaciones de gestión de recursos	APO02.05 APO07.01 APO07.03 APO09.04

Actividades	Nivel de capacidad
1. Supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la empresa mediante objetivos y métricas acordados.	4
2. Supervisar las estrategias de aprovisionamiento TI y de arquitectura de la empresa y los recursos y capacidades TI para garantizar que las necesidades actuales y futuras de la empresa puedan ser satisfechas.	4
3. Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes.	4

Nivel de capacidad objetivo

3

			85,67
N	P	L	F
			86
			86
		85	

Nivel de cumplimiento
Valor
86
86
85

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
	Cumplida
	No se cumple

MARCA	DESCRIPCIÓN
	En la actividad de la metodología COBIT Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes se tiene un nivel de capacidad 4 y su nivel de cumplimiento alcanzable del 85%, por lo cual se les dificulta el reconocimiento al rendimiento de los recursos informáticos. **HH (3)**

Tabla 21. EDM05 Asegurar la Transparencia hacia las Partes Interesadas

EDM05 Asegurar la Transparencia hacia las Partes Interesadas	**Área: Gobierno**
	Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso	
Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	
Declaración del Propósito del Proceso	
Asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	• Porcentaje de roles de dirección ejecutiva con responsabilidades claramente definidas en cuanto a decisiones de TI
	• Número de veces que TI está de forma proactiva como tema en la agenda del Consejo de Administración
	• Frecuencia de las reuniones del comité (ejecutivo) de estrategia de TI
	• Cuota de ejecución de decisiones ejecutivas relacionadas con TI
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.
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
Metas y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Los informes para las partes interesadas se ajustan a sus requisitos.	• Fecha de la última revisión de los requisitos de elaboración de informes
	• Porcentaje de interesados incluidos en los requisitos de elaboración de informes
2. La elaboración de informes es completa, oportuna y precisa.	• Porcentaje de informes no presentados a tiempo
	• Porcentaje de informes que contienen imprecisiones
3. La comunicación es eficaz y las partes interesadas están satisfechas.	• Nivel de satisfacción de las partes interesadas con respecto a la elaboración de informes
	• Número de veces que no se han cumplido los requisitos obligatorios en cuanto a elaboración de informes

Matriz RACI EDM05																										
Práctica Clave de Gobierno	Consejo de administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Dueños del proceso de negocio	Comité Ejecutivo de estrategia	Comité directivo (de programas/proyectos)	Oficina de Gestión de Proyectos	Oficina de gestión de valor	Director de gestión del riesgo	Director de seguridad de la información	Comité de arquitectura	Comité de riesgo empresarial	Jefe de Recursos Humanos	Conformidad	Auditoría	Director de informática (CIO)	Arquitecto jefe	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Administrador de servicio	Administrador de seguridad de la	Administrador de continuidad del negocio	Director de privacidad
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.	A	R	C	C	C	I										C	C	R	I			I				
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.	A	R	C	C	C	I										C	C	R	I			I				
EDM05.03 Supervisar la comunicación con las partes interesadas.	A	R	C	C	C	I										C	C	R	I			I				

EDM05 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gobierno	**Entradas**		**Salidas**	
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.	**De**	**Descripción**	**Descripción**	**A**
Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación	EDM02.03	Acciones dirigidas a mejorar la entrega de valor	Evaluación de los requisitos corporativos de elaboración de informes	MEA01.01
	EDM03.03	Cuestiones de gestión del riesgo a tratar por el Consejo de Administración	Principios de elaboración de informes y de comunicación	MEA01.01
	EDM04.03	Retroalimentación sobre la asignación y la eficacia		
		de los recursos y las capacidades		
	MEA02.08	Ámbito de aplicación refinado		

Actividades	Nivel de capacidad
1. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes respecto al uso de TI dentro de la empresa (regulación, legislación, leyes generales, requisitos contractuales), incluyendo alcance y frecuencia.	3
2. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes para otros interesados respecto al uso de TI dentro de la empresa, incluyendo alcance y condiciones.	3
3. Mantener los principios de comunicación con interesados externos e internos, incluyendo formatos y canales de comunicación y los principios de aceptación y aprobación de los informes por parte de las partes interesadas.	3

			87,00
N	**P**	**L**	**F**
			87
			88
			86

Nivel de cumplimiento
Valor
87
88
86

Nivel de capacidad objetivo

3

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gobierno	Entradas		Salidas	
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.	**De**	**Descripción**	**Descripción**	**A**
Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.	APO12.04	Informes de análisis de riesgos y de perfil de riesgos para las partes interesadas	Reglas de validación y aprobación de informes obligatorios	MEA01.01
				MEA03.04
			Directrices de escalado	MEA01.05

Actividades	Nivel de capacidad
1. Orientar el establecimiento de la estrategia de comunicación para interesados externos e internos.	3
2. Orientar la implementación de mecanismos para garantizar que la información cumple todos los criterios de los requisitos corporativos obligatorios en cuanto a elaboración de informes de TI.	3
3. Establecer mecanismos de validación y aprobación de la elaboración obligatoria de informes.	3
4. Establecer mecanismos de escalado en la elaboración de informes.	3

			89,00
N	**P**	**L**	**F**
			88
			87
			90
			91

Nivel de cumplimiento
Valor
88
87
90
91

Nivel de capacidad objetivo	
3	
Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de gobierno	Entradas		Salidas	
EDM05.03 Supervisar la comunicación con las partes interesadas.	**De**	**Descripción**	**Descripción**	**A**
Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.	MEA02.08	• Informe de la revisión de aseguramiento	Evaluación de la eficacia de la elaboración de informes	MEA01.01
		• Resultados de la revisión de aseguramiento		MEA03.04

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad
1. Evaluar periódicamente la eficacia de los mecanismos para asegurar la precisión y la fiabilidad de la elaboración obligatoria de informes.	3
2. Evaluar periódicamente la eficacia de los mecanismos y las salidas de la comunicación con interesados externos e internos.	3
3. Determinar si se están cumpliendo los requisitos de los diferentes interesados.	3

			90,67
N	P	L	F
			90
			92
			90

Nivel de cumplimiento
Valor
90
92
90

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida

Tabla 22. APO01 Gestionar el Marco de Gestión de TI

APO01 Gestionar el Marco de Gestión de TI	**Área: Gestión**
	Dominio: Alinear, Planificar y Organizar
Descripción del Proceso	
Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	
Declaración del Propósito del Proceso	
Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI
	• Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados
	• Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
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
09 Agilidad de las TI	• Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos
	• Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas
	• Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada
11 Optimización de activos, recursos y capacidades de las 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 las 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
16 Personal del negocio y de las TI competente y motivado	• Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función
	• Porcentaje del personal satisfecho con su función TI
	• Número de horas de aprendizaje/prácticas por trabajador
17 Conocimiento, experiencia e iniciativas para la innovación de negocio	• Nivel de concienciación y comprensión de las posibilidades de innovación de TI del negocio ejecutivo.
	• Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas de la innovación TI.
	• Número de iniciativas aprobadas resultantes de ideas innovadoras de TI.
Objetivos y Métricas de Procesos	
Meta del Proceso	**Métricas Relacionadas**
1. Se ha definido y se mantiene un conjunto eficaz de políticas.	• Porcentaje de políticas, estándares y otros elementos catalizadores activos documentados y actualizados
	• Fecha de las últimas actualizaciones del marco de trabajo y de los elementos catalizadores
	• Número de exposiciones a riesgos debidas a la inadecuación del diseño del entorno de control
2. Todos tienen conocimiento de las políticas y de cómo deberían implementarse.	• Número de empleados que asistieron a sesiones de formación o de sensibilización
	• Porcentaje de proveedores indirectos con contratos en los que se definen requisitos de control

Matriz RACI APO01																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de Negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática / Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO01.01 Definir la estructura organizativa.		C	C	C	C		I		C						R	I	I	A	C	C	C	R	C	C	C	
APO01.02 Establecer roles y responsabilidades.					I	C			C						C	C	C	A	C	C	C	R	C	C	C	C
APO01.03 Mantener los elementos catalizadores del sistema de gestión.	C	A	C	R	C	C	I				C	C	C	C		C	C	R				R				
APO01.04 Comunicar los objetivos y la dirección de gestión.		A	R	R	R	I	R	I	I	I	R	R	I	I	I	I	I	R	I	I	I	I	I	I	I	I
APO01.05 Optimizar la ubicación de la función de TI.		C	C	C	C		A		C						C	C	C	R	C	C	C	R	C	C	C	
APO01.06 Definir la propiedad de la información (datos) y del sistema.		I	I	C	A	R									C	C	C	C	C						C	C
APO01.07 Gestionar la mejora continua de los procesos.				A		R			R				C		I	C	C	R	R	R	R	R	R	R	R	
APO01.08 Mantener el cumplimiento con las políticas y		A				R			R				R		R	C	I	R	R	R	R	R	R	R	R	

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión		**Entradas**	**Salidas**	
APO01.01 Definir la estructura organizativa.	**De**	**Descripción**	**Descripción**	**A**
Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.	EDM01.01	• Modelo de toma de decisiones	Definición de estructura y funciones organizativas	APO03.02
		• Principios rectores del gobierno corporativo		
	APO03.02	Modelo de arquitectura de procesos	Directrices operativas de la organización	APO03.02
			Reglas básicas de comunicación	Todo APO
				Todo BAI
				Todo DSS
				Todo MEA

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*	
Actividades APO01.01 Definir la estructura organizativa.	**Nivel de capacidad**
1. Definir el alcance, las funciones internas y externas, los roles internos y externos, y las capacidades y los derechos de decisión requeridos, incluidas actividades de TI realizadas por terceras partes.	3
2. Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la gestión y ejecución de servicios de TI.	4
3. Establecer la implicación de las partes interesadas críticas para la toma de decisiones (quiénes rendirán cuentas, quiénes son responsables, quiénes deben ser consultados y quiénes informados).	3
4. Alinear la organización relativa a TI con los modelos organizativos de arquitectura corporativa.	3
5. Definir el enfoque, los roles y las responsabilidades de cada función dentro de la estructura organizativa relativa a TI.	4
6. Definir las estructuras y relaciones de gestión para contribuir a las funciones y roles de gestión y ejecución, en consonancia con la dirección de gobierno establecida.	3
7. Establecer un Comité Estratégico de TI (o equivalente) a nivel del Consejo de Administración. Este comité debería asegurarse de que el gobierno de TI, como parte del gobierno corporativo, está contemplado de forma adecuada, debe aconsejar sobre la dirección estratégica y revisar las inversiones principales, en representación del consejo de administración al completo.	3
8. Establecer un comité directivo de TI (o equivalente) compuesto por la dirección ejecutiva, de negocio y de TI para determinar las prioridades de los programas de inversión de TI de acuerdo con la estrategia y prioridades de negocio de la empresa; realizar un seguimiento del estado de los proyectos y resolver los conflictos de recursos; y supervisar los niveles de servicio y las mejoras en el servicio.	4
9. Proporcionar directrices para cada estructura de gestión (incluyendo órdenes, objetivos, asistentes a reuniones, marco temporal, seguimiento, supervisión y vigilancia), así como las entradas requeridas y las salidas esperadas en cuanto a las reuniones.	3
10. Definir reglas básicas de comunicación mediante la identificación de las necesidades comunicativas y la implementación de planes basados en dichas necesidades, teniendo en cuenta la comunicación de arriba hacia abajo, de abajo hacia arriba y horizontal.	3
11. Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre el negocio y las funciones de TI dentro de la empresa y con entidades no pertenecientes a la empresa.	3
12. Verificar regularmente la adecuación y la eficacia de la estructura organizativa.	4

			92,33
N	**P**	**L**	**F**
			90
			87
			92
			90
			86
			95
			96
			95
			95
			92
			95
			95

Nivel de cumplimiento
Valor
90
87
92
90
86
95
96
95
95
92
95
95

Nivel de capacidad objetivo

3

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
APO01.02 Establecer roles y responsabilidades.	**De**	**Descripción**	**Descripción**	**A**
Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.	EDM01.01	Niveles de autoridad	Definición de roles y responsabilidades relativos a TI	DSS05.04
	EDM04.02	Responsabilidades asignadas para la gestión de recursos	Definición de prácticas de supervisión	APO07.01
	APO07.03	• Planes de desarrollo de habilidades		
		• Matriz de habilidades y competencias		
	APO11.01	Roles, responsabilidades y derechos de decisión dentro del sistema de gestión de la calidad (SGC)		
	APO13.01	Declaración de alcance del sistema de gestión de seguridad de la información (SGSI)		
	DSS06.03	• Niveles de autoridad asignados		
		•Roles y responsabilidades asignados		

Actividades	Nivel de capacidad
1. Establecer, acordar y comunicar roles y responsabilidades relativos a TI para todo el personal de la empresa, de acuerdo con las necesidades y los objetivos del negocio. Delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones.	3
2. Tener en cuenta los requisitos desde la empresa y la continuidad del servicio de TI a la hora de definir los roles, incluyendo el respaldo por parte de la plantilla y los requisitos de formación interdisciplinar.	3
3. Contribuir al proceso de continuidad del servicio de TI manteniendo actualizada la información de contacto y las descripciones de roles de la empresa.	4
4. Incluir en las descripciones de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales.	3
5. Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. El nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas.	3
6. Asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades.	4
7. Estructurar los roles y las responsabilidades para reducir las posibilidades de que un solo rol pueda comprometer un proceso crítico.	3

			88,86	Nivel de cumplimiento		Nivel de cumplimiento objetivo	
N	P	L	F	Valor		Meta	Observación
			90	90		F	Cumplida
		85		85	✈	F	No se cumple
			92	92			Cumplida
			90	90		F	Cumplida
		80		80	⊖	F	No se cumple
			95	95			Cumplida
			90	90		F	Cumplida

.

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
APO01.03 Mantener los elementos catalizadores del sistema de gestión.	**De**	**Descripción**	**Descripción**	**A**
Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos).				
	EDM01.01	Principios rectores del gobierno corporativo	Políticas relativas a TI	Todo APO
				Todo BAI
				Todo DSS
				Todo MEA
	APO02.05	Hoja de ruta estratégica		
	APO12.01	Problemas y factores de riesgo emergentes		
	APO12.02	Resultados del análisis de riesgos		

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad	N	P	L	F	Nivel de cumplimiento – Valor	Nivel de cumplimiento objetivo – Meta	Nivel de cumplimiento objetivo – Observación
					91,89			
1. Adquirir comprensión de la visión, la dirección y la estrategia corporativas.	3				90	90	F	Cumplida
2. Tener en cuenta el entorno interno de la empresa, incluyendo la cultura y la filosofía de gestión, la tolerancia al riesgo, la seguridad, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de integridad en la gestión.	3				88	88	F	Cumplida
3. Inferir e integrar los principios de TI con los principios de negocio.	3				92	92	F	Cumplida
4. Alinear el entorno de control de TI con el entorno de políticas de TI, con los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control. Evaluar las buenas prácticas o los requisitos específicos del sector (p. ej., normativa específica del sector) e integrarlos donde corresponda.	3				90	90	F	Cumplida
5. Alinearse con todos los estándares y códigos de práctica de gobierno y gestión aplicables a nivel nacional e internacional y evaluar buenas prácticas disponibles, como el Marco de Trabajo Integrado para Control Interno de COSO y el Marco de Trabajo Integrado para Gestión Empresarial del Riesgo de COSO.	3				86	86	F	Cumplida
6. Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.	4				95	95		Cumplida
7. Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativo o de negocio.	4				96	96		Cumplida
8. Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.	3				95	95	F	Cumplida
9. Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.	3				95	95	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
APO01.04 Comunicar los objetivos y la dirección de gestión.	**De**	**Descripción**	**Descripción**	**A**
Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa.	EDM01.02	Comunicación de gobierno corporativo	Comunicación de objetivos de TI	Todo APO Todo BAI Todo MEA
	EDM04.02	Principios de protección de recursos		
	APO12.06	Comunicación de impactos de riesgo		
	BAI08.01	Comunicación sobre valor del conocimiento		
	DSS04.01	Política y objetivos de continuidad empresarial		
	DSS05.01	Política de prevención de software malintencionado		
	DSS05.02	Política de seguridad de la conectividad		
	DSS05.03	Políticas de seguridad sobre terminales		

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad	N	P	L	F	Nivel de cumplimiento – Valor	Nivel de cumplimiento objetivo – Meta	Nivel de cumplimiento objetivo – Observación
					89,67			
1. Comunicar continuamente los objetivos y la dirección de TI. Asegurar que las comunicaciones reciban apoyo de la dirección ejecutiva, tanto de palabra como mediante acciones, empleando todos los canales disponibles.	3				90	90	F	Cumplida
2. Garantizar que la información comunicada engloba una clara articulación de la misión, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código ético/de conducta, las políticas y procedimientos, los roles y las responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado para cada respectiva audiencia dentro de la empresa.	3				87	87	F	Cumplida
3. Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo.	3				92	92	F	Cumplida

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
APO01.05 Optimizar la ubicación de la función de TI.	**De**	**Descripción**	**Descripción**	**A**
Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte del CIO debe ser proporcional a la importancia de las TI en la empresa.	Fuera del Ámbito de COBIT	• Modelo operativo empresarial	Evaluación de las opciones para la organización de TI	APO03.02
		• Estrategia del negocio	Definir la función operacional de las funciones de TI	APO03.02

Actividades	Nivel de capacidad
1. Entender el contexto de la función de TI, incluyendo una evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, híbrido), importancia de TI, la situación y opciones para la provisión.	3
2. Identificar, evaluar y priorizar las opciones para la ubicación en la organización, los modelos operativos y de aprovisionamiento.	4
3. Definir la ubicación de las funciones de TI y obtener aprobación.	3

			92,33
N	**P**	**L**	**F**
			90
			95
			92

Nivel de cumplimiento
Valor
90
95
92

Nivel de capacidad objetivo
3

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
APO01.06 Definir la propiedad de la información (datos) y del sistema.	**De**	**Descripción**	**Descripción**	**A**
Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.			Directrices para la clasificación de datos	APO03.02 BAI02.01
				DSS05.02
				DSS06.01
			Directrices para el control y seguridad de datos	BAI02.01
			Procedimientos de integridad de datos	BAI02.01 DSS06.01

Actividades	Nivel de capacidad
1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa.	3
2. Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario.	4
3. Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.	4
4. Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (*data warehouses*) y archivos de datos.	3

Nivel de capacidad objetivo

3

			91,75
N	**P**	**L**	**F**
			90
			95
			92
			90

Nivel de cumplimiento
Valor
90
95
92
90

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
APO01.07 Gestionar la mejora continua de los procesos.	**De**	**Descripción**	**Descripción**	**A**
Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso.	EDM01.03	Realimentación de la efectividad y funcionamiento del gobierno	Evaluaciones de la capacidad de los procesos	MEA01.03
	MEA03.02	Actualización de políticas, principios, procedimientos y estándares	Oportunidades de mejoras de proceso	Todo APO Todo BAI Todo DSS Todo MEA
			Objetivos y métricas de rendimiento para el seguimiento de la mejora de procesos	MEA01.02

Actividades	Nivel de capacidad
1. Identificar los procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora. Analizar las diferencias en la capacidad y control del proceso. Identificar las opciones de mejora y rediseño de procesos. Priorizar iniciativas para la mejora de procesos basadas en el potencial coste-beneficio.	3
2. Implementar las mejoras acordadas, funcionando como una práctica normal del negocio y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.	3
3. Considerar las maneras de mejorar la eficiencia y eficacia (p. ej., mediante formación, documentación, estandarización y automatización de procesos).	4
4. Aplicar prácticas de gestión de calidad para la actualización de procesos.	4
5. Retirar procesos, componentes o catalizadores desactualizados.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			90,60			
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			88	88	F	Cumplida
			92	92		Cumplida
			90	90		Cumplida
			93	93	F	Cumplida

Nivel de capacidad objetivo

3

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
APO01.08 Mantener el cumplimiento con las políticas y procedimientos.	**De**	**Descripción**	**Descripción**	**A**
Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control.	DSS01.04	Políticas del entorno	Acciones de remediación por no cumplimiento	MEA01.05
	MEA03.02	Actualización de políticas, principios, procedimientos y estándares		

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad	N	P	L	F	Nivel de cumplimiento Valor	Nivel de cumplimiento objetivo Meta	Observación
					90,20			
1. Hacer un seguimiento del cumplimiento con políticas y procedimientos.	3				95	88	F	Cumplida
2. Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir el cambio de requerimientos).	3				86	86	F	Cumplida
3. Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.	3				91	91	F	Cumplida
4. Evaluar periódicamente el desempeño de los catalizadores del marco de referencia y adoptar las acciones necesarias.	3				89	89	F	Cumplida
5. Analizar las tendencias en el funcionamiento y cumplimiento y adoptar las acciones apropiadas.	3				90	90	F	Cumplida

MARCA	DESCRIPCIÓN
	En la aplicación de la metodología COBIT en la actividad Tener en cuenta los requisitos desde la empresa y la continuidad del servicio de TI a la hora de definir los roles, incluyendo el respaldo por parte de la plantilla y los requisitos de formación interdisciplinar, se menciona que tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, es decir que los empleados no poseen un conocimiento amplio acerca de las TI. **HH(4)**
	La metodología COBIT analiza la actividad Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. Además, el nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas, por lo cual está actividad tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 80%, es por ello que la empresa no dispone de un supervisor de recursos y responsabilidades de los activos informáticos. **HH(5)**

Tabla 23. APO07 Gestionar los Recursos Humanos

APO07 Gestionar los Recursos Humanos	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción del Proceso Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	
Declaración del Propósito del Proceso Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas:**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI • Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados • Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
11 Optimización de activos, recursos y capacidades de las 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
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
16 Personal del negocio y de las TI competente y motivado	• Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función • Porcentaje del personal satisfecho con su función TI • Número de horas de aprendizaje/prácticas por trabajador
17 Conocimiento, experiencia e iniciativas para la innovación de negocio	• Nivel de sensibilización y comprensión de las posibilidades de innovación de TI por parte de los Ejecutivos de negocio • Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas en innovación de las TI • Número de iniciativas aprobadas procedentes de ideas innovadoras de TI
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil.	• Número de definiciones de servicio y catálogos de servicio •Nivel de satisfacción de los ejecutivos con la toma de decisiones de la gerencia • Número de decisiones que no pudieron resolverse dentro de las estructuras de gestión y se escalaron a las estructuras de gobierno
4. Los recursos humanos son gestionados eficaz y eficientemente.	• Porcentaje de rotación del personal • Duración media de las vacantes • Porcentaje de puestos de TI vacantes

APO07 Gestionar los Recursos Humanos																									
Práctica Clave de Gobierno	Consejo de Administración	**Director General (CEO)**	**Director General Financiero (CFO)**	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	**Comité Estratégico**	**Oficina de Gestión de Proyectos**	**Oficina de Gestión del Valor**	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	**Director de Informática/Sistemas (CIO)**	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de Negocio**	**Gestor de Privacidad de la información**
APO07.01 Mantener la dotación de personal suficiente y adecuada.									R		I				R			A	R	R	R	R	R	R	R	
APO07.02 Identificar personal clave de TI.									R						R			A	R	R	R	R	R	R	R	
APO07.03 Mantener las habilidades y competencias del personal.									R						R			A	R	R	R	R	R	R	R	
APO07.04 Evaluar el desempeño laboral de los empleados.									R						R			A	R	R	R	R	R	R	R	
APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.					R	C	A	R	R						I			R	R	R	R	R	R	R	R	
APO07.06 Gestionar el personal contratado.									R						R			A	R	R	R	R	R	R	R	

APO07 Prácticas, Entradas/Salidas y Actividades del Proceso				
Practica de Gestión	**Entradas**		**Salidas**	
APO07.01 Mantener la dotación de personal suficiente y adecuada.	**De**	**Descripción**	**Descripción**	**A**
Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.	EDM04.01	• Plan de recursos aprobado • Principios rectores para la asignación de recursos y capacidades	Evaluaciones de requisitos de personal	Interno
	EDM04.03	Acciones correctivas para hacer frente a las desviaciones de gestión de recursos	Planes de desarrollo de carrera y de competencias	Interno
	APO01.02	Definición de las prácticas de supervisión	Planes de aprovisionamiento de personal	Interno
	APO06.03	• Comunicaciones del presupuesto • Plan y presupuesto de TI.		
	Fuera del Ámbito de COBIT	• Metas y objetivos empresariales • Políticas empresariales y procedimientos de RRHH		

Actividades	Nivel de capacidad
1. Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar que: • La función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos empresariales. • La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI.	4
2. Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa.	3
3. Incluir controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores. El alcance y la frecuencia de estos controles depende de la sensibilidad y/o criticidad de la función.	3
4. Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias, contratistas externos y acuerdos de servicio con terceras partes.	3
5. Asegurarse de que el entrenamiento cruzado se lleva a cabo y que hay respaldo para el personal clave para reducir la dependencia de una sola persona.	3

Nivel de capacidad objetivo

3

			93,40
N	**P**	**L**	**F**
			95
			95
			95
			95
			87

Nivel de cumplimiento
Valor
95
95
95
95
87

Nivel de cumplimiento objetivo	
Meta	**Observación**
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Practica de Gestión	Entradas		Salidas	
APO07.02 Identificar personal clave de TI.	**De**	**Descripción**	**Descripción**	**A**
Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal.				

Actividades	Nivel de capacidad	N	P	L	F	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
		0	0	0	93,75			
		N	P	L	F	Valor	Meta	Observación
1. Minimizar la dependencia en una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión, el respaldo (backup) del personal, el entrenamiento cruzado e iniciativas de rotación de puestos.	3				88	88	F	Cumplida
2. Como medida de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que deben tomar los individuos clave.	4				97	97		Cumplida
3. Tomar acciones expeditivas con respecto a cambios laborales, especialmente despidos.	4				100	100		Cumplida
4. Probar regularmente los planes de respaldo (*backup*) del personal.	3				90	90	F	Cumplida

Practica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO07.03 Mantener las habilidades y competencias del personal. Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.	EDM01.02	Enfoque del sistema de recompensas	Matriz de habilidades y competencias	APO01.02 BAI01.02 BAI01.04
	EDM04.03	Acciones correctivas para hacer frente a las desviaciones en la gestión de recursos	Planes de desarrollo de habilidades	EDM04.01 APO01.02
	BAI08.03	Publicar repositorios de conocimiento	Revisión de informes	Interno
	BAI08.04	Concienciación del conocimiento y esquemas de formación		
	DSS04.06	• Seguimiento de resultados en habilidades y competencias • Requisitos de formación		
	Fuera del Ámbito de COBIT	Metas y objetivos de la empresa		

Actividades	Nivel de capacidad
1. Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos.	4
2. Proporcionar una planificación formal de la carrera y desarrollo profesional para fomentar el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave.	4
3. Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias.	3
4. Identificar las diferencias entre las habilidades necesarias y las disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva, tales como formación (técnica y en habilidades de comportamiento), contratación, redistribución y cambios en las estrategias de contratación.	3
5. Desarrollar y ejecutar programas de formación basados en los requisitos organizativos y de procesos, incluidos los requisitos sobre conocimiento empresarial, control interno, conducta ética y seguridad.	3
6. Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Revisar la planificación de la sucesión.	3
7. Revisar los materiales y programas de formación de manera regular para asegurarse su adecuación a los requisitos empresariales cambiantes y su impacto en los conocimientos, aptitudes y habilidades necesarias.	4

			92,43	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			96	96		Cumplida
			92	92		Cumplida
			90	90	F	Cumplida
			95	95	F	Cumplida
			90	90	F	Cumplida
			88	88	F	Cumplida
			96	96		Cumplida

Practica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO07.04 Evaluar el desempeño laboral de los empleados. Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado.	EDM01.02	Enfoque de sistema de recompensas	Metas personales	Interno
	APO04.01	Programa de reconocimiento y recompensa	Evaluaciones de desempeño	Interno
	BAI05.04	Objetivos de desempeño de RRHH alineados	Planes de mejora	Interno
	BAI05.06	Resultados de la revisión de desempeño de RRHH		
	DSS06.03	Derechos de acceso asignados		
	Fuera del Ámbito de COBIT	Metas y objetivos empresariales		

Actividades	Nivel de capacidad
1. Considerar los objetivos funcionales/de empresa como el contexto para establecer las metas individuales.	4
2. Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales. Basar las metas en objetivos SMART (específicos, medibles, realizables, pertinentes y de duración determinada) que reflejen las competencias básicas, los valores empresariales y las habilidades necesarias para la(s) función(es).	3
3. Recopilar los resultados de la evaluación de desempeño de 360 grados.	3
4. Implementar y comunicar un proceso disciplinario.	3
5. Proporcionar instrucciones específicas para el uso y almacenamiento de información personal en el proceso de evaluación, de conformidad con la legislación laboral y sobre datos personales aplicables	3
6. Proporcionar retroalimentación oportuna sobre el desempeño frente a las metas del individuo.	4
7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, el desarrollo de competencias y el logro exitoso de los objetivos de desempeño. Asegurar que el proceso se aplica de forma coherente y en consonancia con las políticas de la organización.	3
8. Desarrollar planes de mejora del desempeño basados en los resultados del proceso de evaluación y los requisitos de capacitación y desarrollo de competencias identificados.	4

			91,63	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			100	100		Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida
			95	95		Cumplida
			88	88	F	Cumplida
			90	90		Cumplida

Practica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio. Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.	EDM04.02	Comunicación de las estrategias de aprovisionamiento de recursos	Inventario de recursos humanos del negocio y de TI	BAI01.04
	EDM04.03	Comentarios sobre la asignación y eficacia de recursos y capacidades	Análisis de deficiencias en la obtención de recursos	BAI01.06
	APO06.02	Asignaciones presupuestarias	Registros de utilización de recursos	BAI01.06
	BAI01.04	Requisitos y funciones de recursos		
	BAI01.12	Requisitos de recursos de proyecto		
	Organización corporativa	Carteras actuales y futuras		
	Fuera del Ámbito de COBIT	Estructura organizativa de la empresa		

Actividades	Nivel de capacidad
1. Crear y mantener un inventario de recursos humanos de negocio y TI.	3
2. Entender la demanda actual y futura de recursos humanos para apoyar el logro de los objetivos de TI y ofrecer servicios y soluciones basados en la cartera de las iniciativas actuales relacionadas con las TI, la cartera de inversiones futuras y las necesidades operativas del día a día.	3
3. Identificar las carencias y proporcionar datos de entrada a planes de aprovisionamiento, así como a los procesos de contratación de la empresa y de TI. Crear y revisar el plan de personal, haciendo seguimiento del uso real.	3
4. Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos.	4

			91,25
N	P	L	F
			87
			92
			90
			96

Nivel de cumplimiento
Valor
87
92
90
96

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida

Practica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO07.06 Gestionar el personal contratado. Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización, así como los requisitos contractuales previamente acordados.	BAI01.04	Requisitos y funciones de recursos	Políticas de contratación de personal	Interno
	BAI01.12	Requisitos de recursos de proyecto	Acuerdos contractuales	Interno
	BAI01.14	Comunicación del retiro del programa y responsabilidades en curso	Revisiones de acuerdos contractuales	Interno

Actividades	Nivel de capacidad
1. Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización y el marco de control de TI.	4
2. Obtener un acuerdo formal por parte de los contratistas en el inicio del contrato en cuanto a que están obligados a cumplir con el marco de control de TI de la empresa, tal como políticas de control de seguridad, control de acceso físico y lógico, uso de las instalaciones, requisitos de confidencialidad de la información y los acuerdos de confidencialidad.	4
3. Advertir a los contratistas de que la gerencia se reserva el derecho de supervisar e inspeccionar todo uso de los recursos de TI, incluyendo correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.	5
4. Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades como parte de sus contratos, incluidos requisitos explícitos para documentar su trabajo en base a normas y formatos previamente acordados.	3
5. Revisar el trabajo de los contratistas y basar la aprobación de los pagos en los resultados.	4
6. Definir todo el trabajo a realizar por terceras partes en contratos formales y sin ambigüedades.	3
7. Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios.	4
8. Llevar a cabo revisiones periódicas para asegurarse de que las funciones de los contratistas y sus derechos de acceso son adecuadas y en línea con los acuerdos.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			93,50			
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			95	95		Cumplida
			95	95		Cumplida
			100	100		Cumplida
			90	90	F	Cumplida
			90	90		Cumplida
			96	96	F	Cumplida
			90	90		Cumplida
			92	92	F	Cumplida

Tabla 24. APO12 Gestionar el Riesgo

APO12 Gestionar el Riesgo	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
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.	
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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El riesgo relacionado con TI está identificado, analizado, gestionado y reportado.	• Grado de visibilidad y reconocimiento en el entorno actual • Número de eventos de pérdida con características clave, capturados en repositorios • Porcentaje de auditorías, eventos y tendencias capturados en repositorios
2. Existe un perfil de riesgo actual y completo.	• Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo • Completitud de atributos y valores en el perfil de riesgo
3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	• Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado • Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos
4. Las acciones de gestión de riesgos están efectivamente implementadas.	• Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados • Número de medidas que no reducen el riesgo residual

Matriz RACI APO12

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO12.01 Recopilar datos.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analizar el riesgo.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Mantener un perfil de riesgo.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Expresar el riesgo.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Definir un portafolio de acciones para la gestión de		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Responder al riesgo.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	EDM03.01	Evaluación de actividades de gestión de riesgos	Datos en el entorno de operación relacionados con el riesgo	Interno
	EDM03.02	• Procesos aprobados para medir la gestión de riesgos • Objetivos clave a ser monitorizados por la gestión de riesgos • Políticas de gestión de riesgos	Datos en eventos de riesgo y en factores contribuyentes	Interno
	APO02.02	Brechas y riesgos relacionados con capacidades actuales	Elementos y factores de riesgo emergentes	EDM03.01 APO01.03 APO02.02
	APO02.05	Evaluación del riesgo		
	APO10.04	Riesgo de entrega de proveedores identificado		
	DSS02.07	Estado de incidentes e informe de tendencias		

Nivel de capacidad objetivo

3

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

APO12.01 Actividades	**Nivel de capacidad**					**Nivel de cumplimiento**	**Nivel de cumplimiento objetivo**	
					90,43			
		N	**P**	**L**	**F**	**Valor**	**Meta**	**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				92	92	F	Cumplida
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				90	90	F	Cumplida
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				92	92	F	Cumplida
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				86	86	F	Cumplida
5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.	4				87	87		Cumplida
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				90	90	F	Cumplida
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.	4				96	96		Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO12.02 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.	DSS04.02	Análisis de impacto en el negocio	Alcance de los esfuerzos de análisis de riesgos	Interno
	DSS05.01	Evaluaciones de amenazas potenciales	Escenarios de riesgo de TI	Interno
	Fuera del Ámbito de COBIT	Avisos de amenaza	Resultados de análisis de riesgos	EDM03.03 APO01.03 APO02.02 BAI01.10

Actividades	Nivel de capacidad
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
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
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
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.	3
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.	4
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.	4
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

Nivel de capacidad

3

			90,43
N	**P**	**L**	**F**
			90
			91
			89
			88
			92
			93
			90

Nivel de cumplimiento
Valor
90
91
89
88
92
93
90

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO12.03 Mantener un perfil de riesgo. 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.	EDM03.01	• Niveles aprobados de tolerancia el riesgo • Guía de apetito al riesgo	Escenarios de riesgo documentados por línea de negocio y función	Interno
	APO10.04	Riesgo de entrega de proveedores identificado	Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo	EDM03.02 APO02.02
	DSS05.01	Evaluaciones de amenazas potenciales		

Actividades	Nivel de capacidad
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. 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
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.	3
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.	3
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.	4
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
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

Nivel de capacidad

3

			91,14
N	**P**	**L**	**F**
			90
			90
			92
			90
			90
			90
			90
			96

Nivel de cumplimiento
Valor
90
90
92
90
90
90
90
96

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO12.04 Expresar el 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.			Análisis de riesgos e informes del perfil de riesgos para las partes interesadas	EDM03.03 EDM05.02 APO10.04 MEA02.08
			Revisión de resultados de evaluaciones de riesgos de terceras partes	EDM03.03 APO10.04 MEA02.01
			Oportunidades para la aceptación de un riesgo mayor	EDM03.03

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad
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.	4
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
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
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
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

			90,40
N	P	L	F
			90
			90
			92
			90
			90

Nivel de cumplimiento
Valor
90
90
92
90
90

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.			Propuestas de proyecto para reducir el riesgo	APO02.02 APO13.02

Actividades	Nivel de capacidad
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
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
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

			91,33
N	P	L	F
			90
			92
			92

Nivel de cumplimiento
Valor
90
92
92

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida

Nivel de capacidad objetivo

3

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	EDM03.03	Acciones correctoras para tratar las desviaciones de gestión de riesgos	Planes de respuesta para incidentes relacionados con el riesgo	DSS02.05
			Comunicaciones del impacto del riesgo	APO01.04 APO08.04 DSS04.02
			Causas raíz relacionadas con el riesgo	DSS02.03 DSS04.02 MEA02.04 MEA02.07 DSS03.01 MEA02.08 DSS03.02

Actividades	Nivel de capacidad
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.	4
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
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.	3
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

				90,00
N	P	L	F	
			90	
			90	
			90	
			90	

Nivel de cumplimiento
Valor
90
90
90
90

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Nivel de capacidad objetivo

3

Tabla 25. APO13 Gestionar la Seguridad

APO13 Gestionar la Seguridad	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
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.	
El proceso contribuye al logro de un conjunto de objetivos principales relacionados con TI:	
Metas 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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos •Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

Matriz RACI APO13

Práctica Clave de Gobierno	Consejo de Administración	**Director General Ejecutivo (CEO)**	**Director General Financiero (CFO)**	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	**Comité Estratégico**	**Oficina de Gestión de Proyectos**	**Oficina de Gestión del Valor**	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	**Director de Informática/ Sistemas (CIO)**	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de Negocio**	**Gestor de Privacidad de la información**
APO13.01 Establecer y mantener un		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Supervisar y revisar el SGSI.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO13.01 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.	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	APO01.02 DSS06.03

Actividades	Nivel de capacidad
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
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.	3
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.	4
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.	4
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	4
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.	4
7. Comunicar el enfoque de SGSI.	4

Nivel de capacidad objetivo

3

			88,14	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			86	86		Cumplida
			87	87		Cumplida
			88	88	F	Cumplida
			91	91	F	Cumplida
			90	90	F	Cumplida
			87	87	F	Cumplida
			88	88	F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO13.02 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.	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Plan de tratamiento de riesgos de seguridad de la información	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	APO03.02	Descripciones de dominios de partida y definición de arquitectura	Casos de negocio de seguridad de información	APO02.05
	APO12.05	Propuestas de proyectos para reducir el riesgo		

Actividades	Nivel de capacidad
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
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.	4
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.	4
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.	4
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.	4
6. Recomendar programas de formación y concienciación en seguridad de la información.	4
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.	4

Nivel de capacidad objetivo

3

			89,29	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90		Cumplida
			86	86	F	Cumplida
			87	87	F	Cumplida
			88	88	F	Cumplida
			90	90	F	Cumplida
			91	91	F	Cumplida
			93	93	F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
APO13.03 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.	DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI	MEA02.01
			Recomendaciones para mejorar el SGSI	Interno

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad
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
2. Realizar auditorías internas al SGSI a intervalos planificados.	4
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.	4
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.	4
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			89,20			
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90		Cumplida
			92	92	F	Cumplida
			86	86	F	Cumplida
			88	88	F	Cumplida
			90	90		Cumplida

Tabla 26. BAI02 Gestionar la Definición de Requisitos

BAI02 Gestionar la Definición de Requisitos	**Área: Gestión** **Dominio: Construir, Adquirir e Implementar**
Descripción del Proceso Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.	
Declaración del Propósito del Proceso Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
01 Alineamiento de TI y estrategia de negocio	• Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI • Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados • Porcentaje de los facilitadores de valor de TI mapeados con facilitadores de valor del negocio
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
12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	• Número de incidentes en los procesos de negocio debidos a errores de integración tecnológica • Número de cambios en los procesos de negocio que necesitan ser retrasados o modificados debido a problemas de integración tecnológica. • Número de procesos de negocio habilitados por TI que se retrasan o incurren en un mayor coste debido a asuntos de integración tecnológica • Número de aplicaciones o infraestructuras críticas operando en silos sin integración
Objetivos y Métricas del Proceso	
Objetivos del Proceso	**Métricas Relacionadas**
1. Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización.	• Porcentaje de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización • Nivel de satisfacción de las partes interesadas con los requerimientos
2. La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio.	• Porcentaje de requerimientos satisfechos por la solución propuesta
3. El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta.	• Números de incidentes no identificados como riesgo • Porcentaje de riesgos no mitigado exitosamente
4. Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables).	• Porcentaje de los objetivos del caso de negocio alcanzados por la solución propuesta • Porcentaje de partes interesadas que no aprueban la solución con relación al caso de negocio

Matriz RACI BAI02

Práctica Clave de Gobierno	Consejo de Administración	**Director General Ejecutivo (CEO)**	**Director General Financiero (CFO)**	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	**Comité Estratégico**	**Oficina de Gestión de Proyectos**	**Oficina de Gestión del Valor**	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	**Director de Informática/Sistemas (CIO)**	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de Negocio**	**Gestor de Privacidad de la información**
BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.					I	R		A	R		C					C	C	C	R	R	C		C	C	C	C
BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.					R	R		A	R							C	C	C	C	R	C		C	C	C	C
BAI02.03 Gestionar los riesgos de los requerimientos.					R	R		A	R		R					C	C	R	C	R	R		C	C	C	C
BAI02.04 Obtener la aprobación de los requerimientos y soluciones.					R	R		A	R							C	C	C	C	C	C		C	C	C	C

BAI02 Prácticas, Entradas/Salidas y Actividades del Proceso				
Prácticas de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**Hacia**
BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio. Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información de negocio, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio de TI propuesta.	APO01.06	• Procedimientos de integridad de datos • Guías de control y seguridad de los datos • Guías de clasificación de datos	Repositorio de definición de requerimientos	BAI03.01 BAI03.02 BAI04.01 BAI05.01
	APO03.01	Principios de arquitectura	Confirmación de los criterios de aceptación de las partes interesadas	BAI03.01 BAI03.02 BAI04.03 BAI05.01 BAI05.02
	APO03.02	• Modelo de arquitectura de la información • Descripciones de los dominios de referencia y definición de arquitectura	Registro de las peticiones de cambios de los requerimientos	BAI03.09
	APO03.05	Guía de desarrollo de la solución		
	APO10.02	RFIs y RFPs de proveedores		
	APO11.03	Criterios de aceptación		

BAI02.01 Actividades	Nivel de capacidad
1. Definir e implementar la definición de requerimientos y el procedimiento de mantenimiento y un repositorio de requisitos acorde al tamaño, complejidad, objetivos y riesgos de la iniciativa que la empresa está considerando acometer.	4
2. Expresar los requerimientos de la empresa en términos de cómo la diferencia entre las capacidades de negocio existentes y deseadas son tratadas y como cada rol interactuará con la solución y la utilizará.	4
3. Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para las partes interesadas, patrocinadores de negocio y personal de la implementación técnica, reconociendo que los requerimientos pueden cambiar y llegar a ser más detallados según se implementen.	3
4. Especificar y priorizar la información, los requerimientos técnicos y funcionales basados en los requerimientos de las partes interesadas. Incluir requerimientos de control de la información en los procesos de negocio, procesos automatizados y entornos de TI para hacer frente a los riesgos de la información y cumplimiento con regulaciones, leyes y contratos comerciales.	4
5. Validar todos los requerimientos mediante aproximaciones tales como revisión por iguales, validación del modelo o prototipo operativo.	3
6. Confirmar la aceptación de aspectos clave de los requerimientos, incluyendo reglas de negocio, controles de información, continuidad de negocio, cumplimiento legal y regulatorio, 'auditabilidad', ergonomía, operatividad y usabilidad, seguridad y soporte documental.	4
7. Hacer seguimiento y controlar el alcance, los requerimientos y los cambios a lo largo del ciclo de vida de la solución durante el proyecto según evolucione la comprensión de la solución.	3
8. Considerar los requerimientos relativos a políticas y estándares empresariales, arquitectura empresarial, planes TI estratégicos y tácticos, procesos de TI internos y externalizados, requerimientos de seguridad, requerimientos regulatorios, competencias del personal, estructura organizativa, caso de negocio y tecnologías catalizadoras.	4

			87,63
N	P	L	F
			86
			87
			88
			89
			90
			88
			87
			86

Nivel de cumplimiento
Valor
86
87
88
89
90
88
87
86

Nivel de capacidad objetivo
3

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas. Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida. Si se considera, implementar la opción seleccionada como un piloto para determinar posibles mejoras.	APO03.05	Guía de desarrollo de la solución	Informe de estudio de viabilidad	BAI03.02 BAI03.03
	APO10.01	Catálogo de proveedores	Plan de alto nivel de adquisiciones/desarrollo	APO10.02 BAI03.01
	APO10.02	• Resultados de decisión de las evaluaciones de proveedores • Evaluaciones de RFI y RFP • RFIs y RFPs de proveedores		
	APO11.03	Criterios de aceptación		

Nivel de capacidad objetivo
3

Actividades	Nivel de capacidad
1. Definir y ejecutar un estudio de viabilidad, piloto o solución básica funcional que clara y concisamente describa las soluciones alternativas que satisfarán los requerimientos funcionales y de negocio. Incluir una evaluación de su viabilidad técnica y económica.	3
2. Identificar las acciones requeridas para la adquisición o desarrollo de la solución, basada en la arquitectura de la empresa y tener en cuenta el alcance y/o tiempo y/o limitaciones de presupuesto.	3
3. Revisar las soluciones alternativas con todas las partes interesadas y seleccionar la más apropiada basada en criterios de viabilidad, incluyendo costes y riesgos.	3
4. Traducir la línea de acción preferida a un plan de alto de nivel de adquisición/desarrollo identificando recursos a utilizar y fases que requieran decisiones de continuar/no continuar.	4

			88,50
N	P	L	F
			87
			88
			89
			90

Nivel de cumplimiento
Valor
87
88
89
90

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	Desde	**Descripción**	**Descripción**	**Para**
BAI02.03 Gestionar los riesgos de los requerimientos. Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta.			Registro de riesgos de los requerimientos	BAI01.10 BAI03.02 BAI04.01 BAI05.01
			Acciones de mitigación de riesgos	BAI01.10 BAI03.02 BAI05.01

Actividades	Nivel de capacidad
1. Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información (debido por ejemplo a falta de involucración de los usuarios, expectativas irreales, desarrolladores añadiendo funcionalidad innecesaria).	3
2. Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto. Si aplica, determinar los impactos en coste y tiempo.	3
3. Identificar modos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de prioridad.	3

			90,00
N	**P**	**L**	**F**
			88
			90
			92

Nivel de cumplimiento
Valor
88
90
92

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**Hacia**
BAI02.04 Obtener la aprobación de los requerimientos y soluciones. Coordinar la realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas, obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas.	BAI01.09	Plan de gestión de calidad	Aprobaciones del patrocinador de los requerimientos y soluciones propuestas	BAI03.02 BAI03.03 BAI03.04
			Aprobación de las revisiones de calidad	APO11.02

Actividades	Nivel de capacidad
1. Asegurar que el patrocinador de negocio o propietario del producto toman la decisión final con respecto a la elección de la solución, enfoque de adquisición y diseño de alto nivel acorde al caso de negocio. Coordinar la realimentación de las partes interesadas afectadas y obtener el cierre por parte de las autoridades apropiadas tanto técnicas como de negocio (por ejemplo, dueño del proceso, arquitecto de empresa, gestor de operaciones, seguridad) para el enfoque propuesto.	4
2. Obtener revisiones de calidad completas y de cada fase clave del proyecto, iteración o versión comparando los resultados obtenidos contra los criterios originales de aceptación. Disponer de la firma del patrocinador y otros interesados en cada revisión de calidad.	3

			86,50
N	**P**	**L**	**F**
			88
		85	

Nivel de cumplimiento
Valor
88
85

Nivel de cumplimiento objetivo	
Meta	**Observación**
	Cumplida
F	No se cumple

MARCA	DESCRIPCIÓN
	En la metodología COBIT en la actividad analizada dice Obtener revisiones de calidad completas y de cada fase clave del proyecto, iteración o versión comparando los resultados obtenidos contra los criterios originales de aceptación, por lo tanto, disponer de la firma del patrocinador y otros interesados en cada revisión de calidad. Dando como resultado que posee un nivel de capacidad 3 y un nivel de cumplimiento alcanzable del 85%, por lo cual la empresa no realiza periódicamente controles de calidad de las TI. HH (6)

B**AI04 Gestionar la Disponibilidad y la Capacidad**	**Área: Gestión** **Dominio: Construir, Adquirir e Implementar**
Descripción del Proceso Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.	
Declaración del Propósito del Proceso Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
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
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
Objetivos y Métricas de Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El plan de disponibilidad anticipa la expectativa del negocio en cuanto a requerimientos críticos de capacidad	• Número de actualizaciones de capacidad, rendimiento o disponibilidad no planificada
2. Cumplimiento de requerimientos de capacidad, rendimiento y disponibilidad	• Número de picos de transacciones donde se excede la meta de rendimiento • Número de incidentes de disponibilidad • Número de eventos donde la capacidad ha excedido los límites planificados
3. Cuestiones de disponibilidad, rendimiento y capacidad identificados y resueltos de manera rutinaria	• Número y porcentaje de cuestiones de disponibilidad, rendimiento y capacidad no resueltos

Matriz RACI BAI04

Práctica Clave de Gobierno	Consejo de Administración	**Director General Ejecutivo (CEO)**	**Director General Financiero (CFO)**	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	**Comité Estratégico**	**Oficina de Gestión de Proyectos**	**Oficina de Gestión del Valor**	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	**Director de Informática / Sistemas (CIO)**	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de Negocio**	**Gestor de Privacidad de la información**
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.						I												C		C	A		R	C	C	
BAI04.02 Evaluar el impacto en el negocio.						A												C		C	R		R	C	C	
BAI04.03 Planificar requisitos de servicio nuevos o modificados.						R												C		C	A		R	C	C	
BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.						R												C		C	A		R	C	C	
BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.					I	R												I	R	C	A		R	I	I	

BAI04 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los ANSs. Crear líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.	BAI02.01	Repositorio de definición de requisitos	Opciones de financiación	APO02.05
	BAI02.03	Registro de requisitos de riesgo	Expectativas de retorno de inversión	EDM02.01 APO02.04 APO06.02 BAI01.06

Actividades	Nivel de capacidad
1. Considerar en la evaluación (actual o prevista) de disponibilidad, rendimiento y capacidad de servicios y recursos lo siguiente: Requisitos del cliente, prioridades de negocio, objetivos de negocio, impacto en el presupuesto, utilización de recursos, capacidades de TI y tendencias de la industria.	3
2. Supervisar el rendimiento y la utilización de la capacidad reales frente a los umbrales definidos, con el apoyo cuando sea necesario de software automatizado.	3
3. Identificar y dar seguimiento a todos los incidentes causados por un rendimiento o una capacidad inadecuados.	3
4. Evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento (la demanda del negocio, capacidad de servicio y capacidad de los recursos) mediante la comparación con las tendencias y los ANSs, teniendo en cuenta los cambios en el entorno.	3

				Nivel de cumplimiento	Nivel de capacidad objetivo	
			89,50		3	
N	P	L	F	Valor	Meta	Observación
			88	88	F	Cumplida
			89	89	F	Cumplida
			90	90	F	Cumplida
			91	91	F	Cumplida

BAI04 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
BAI04.02 Evaluar el impacto en el negocio. Identificar los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias del negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos.	BAI03.02	ANSs internos y externos	Escenarios de disponibilidad, rendimiento y capacidad	Interno
			Evaluaciones de impacto en el negocio de disponibilidad, rendimiento y capacidad	Interno

Nivel de capacidad objetivo

3

Actividades	Nivel de capacidad
1. Identificar solamente aquellas soluciones o servicios que son críticas para los procesos de gestión de la disponibilidad y la capacidad.	4
2. Realizar un mapa de las soluciones o servicios seleccionados con la(s) aplicación(es) e infraestructura (TI y de instalaciones) de los que dependen, para permitir un enfoque en los recursos críticos para la planificación de la disponibilidad.	3
3. Recolectar datos de patrones de disponibilidad de los registros de fallos pasados y de la monitorización del rendimiento. Utilizar herramientas de modelado que ayuden a predecir fallos basados en tendencias de utilización en el pasado y expectativas de la dirección sobre nuevos entornos o condiciones de los usuarios.	3
4. Crear escenarios basados en datos recolectados, describiendo situaciones de disponibilidad futura para ilustrar varios niveles de capacidad potenciales necesarios para alcanzar el objetivo de rendimiento de la disponibilidad.	4
5. Determinar la probabilidad de que el objetivo del rendimiento de la disponibilidad no será alcanzado basado en los escenarios.	3
6. Determinar el impacto de los escenarios en las medidas de rendimiento del negocio (ej. Ingresos, beneficios, servicios a clientes). Involucrar a la línea de negocio, líderes funcionales (especialmente finanzas) y regionales para comprender su evaluación de impacto.	3
7. Asegurar que los propietarios de procesos de negocio comprenden completamente y están de acuerdo con los resultados del análisis. Obtener una lista de escenarios de riesgo inaceptables de los propietarios de negocio que requieran una respuesta para reducir el riesgo a niveles aceptables.	4

		85,00	90,43
N	**P**	**L**	**F**
			92
		85	
			90
			92
		85	
			92
			97

Nivel de cumplimiento
Valor
92
85
90
92
85
92
97

Nivel de cumplimiento	
Meta	**Observación**
	Cumplida
F	No se cumple
F	Cumplida
	Cumplida
F	No se cumple
F	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
BAI04.03 Planificar requisitos de servicios nuevos o modificados. Planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio	BAI02.01	Criterios de aceptación confirmados de las partes interesadas	Mejoras priorizadas	APO02.02
	BAI03.01	Especificaciones de diseño de alto nivel aprobadas	Planes de capacidad y rendimiento	APO02.02
	BAI03.02	Especificaciones de diseño detallado aprobadas		
	BAI03.03	Componentes de la solución documentados		

Actividades	Nivel de capacidad
1. Revisar las implicaciones en la disponibilidad y la capacidad del análisis de tendencias del servicio.	3
2. Identificar las implicaciones en la disponibilidad y la capacidad de cambios en las necesidades del negocio y oportunidades de mejora. Utilizar técnicas de modelado para validar los planes de disponibilidad, rendimiento y capacidad.	3
3. Priorizar las necesidades de mejora y crear planes de disponibilidad y capacidad justificables en costes.	3
4. Ajustar los planes de rendimiento y capacidad y los ANSs sobre la base de los procesos de negocio y servicios que los soportan realistas, nuevos, propuestos o proyectados, sobre cambios a las aplicaciones y la infraestructura, así como revisiones del rendimiento y uso de la capacidad actual, incluyendo niveles de carga de trabajo.	3
5. Asegurar que la dirección lleva a cabo comparaciones de la demanda actual de recursos con la demanda y suministro previstos para evaluar las técnicas de previsión actuales y realizar mejoras donde sea posible.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			88	88	F	Cumplida
			89	89	F	Cumplida
			90	90	F	Cumplida
			91	91	F	Cumplida
			89	89	F	Cumplida

BAI04 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**Hacia**
BAI04.04 Supervisar y revisar la disponibilidad y la capacidad. Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a las líneas de referencia establecidas. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.			Informes de disponibilidad y rendimiento	MEA01.03

Actividades	Nivel de capacidad
1. Establecer un proceso de recolección de datos para proporcionar a la dirección información de seguimiento e informes de la carga de trabajo de disponibilidad, rendimiento y capacidad de todos los recursos relacionados con la información.	3
2. Proporcionar información periódica de los resultados en una forma apropiada para su revisión por las TI y la gestión del negocio y comunicar a la dirección empresarial.	3
3. Integrar las actividades de supervisión e información en las actividades iterativas de gestión de la capacidad (supervisión, análisis, ajuste e implementaciones).	3
4. Proveer informes de capacidad para los procesos de presupuesto.	3

			89,50
N	**P**	**L**	**F**
			88
			89
			90
			91

Nivel de cumplimiento	**Nivel de cumplimiento objetivo**	
Valor	**Meta**	**Observación**
88	F	Cumplida
89	F	Cumplida
90	F	Cumplida
91	F	Cumplida

Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad. Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.			Brechas de rendimiento y capacidad	Interno
			Acciones correctivas	APO02.02
			Procedimiento de escalado ante emergencias	DSS02.02

Actividades	Nivel de capacidad
1. Obtener la orientación de manuales de productos de proveedores para garantizar un nivel adecuado de rendimiento de disponibilidad para picos de procesamiento y cargas de trabajo.	3
2. Identificar brechas de rendimiento y capacidad sobre la base de la monitorización del rendimiento actual y previsto. Utilizar las especificaciones de disponibilidad, continuidad y recuperación conocidas para clasificar los recursos y permitir la priorización.	3
3. Definir acciones correctivas (ej. cambiando la carga de trabajo, dando prioridad a las tareas o la adición de recursos, cuando se identifican los problemas de rendimiento y capacidad).	3
4. Integrar las acciones correctivas requeridas dentro de los procesos apropiados de planificación y gestión de cambios.	3
5. Definir un procedimiento de escalado para la resolución rápida en emergencias en caso de problemas de capacidad y rendimiento.	3

			90,00
N	**P**	**L**	**F**
			88
			89
			90
			91
			92

Nivel de cumplimiento	**Nivel de cumplimiento objetivo**	
Valor	**Meta**	**Observación**
88	F	Cumplida
89	F	Cumplida
90	F	Cumplida
91	F	Cumplida
92	F	Cumplida

Tabla 27. BAI08 Gestionar el Conocimiento

BAI08 Gestionar el Conocimiento	**Área: Gestión** **Dominio: Construir, Adquirir e Implementar**
Descripción del Proceso Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.	
Declaración del Propósito del Proceso Proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
09 Agilidad de las TI	• Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos • Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas • Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada
17 Conocimiento, experiencia e iniciativas para la innovación de negocio	• Nivel de concienciación y comprensión de las posibilidades de innovación de TI del negocio ejecutivo • Nivel de satisfacción de las partes interesadas con los niveles de experiencia e ideas de la innovación TI • Número de iniciativas aprobadas resultantes de ideas innovadoras de TI
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Las fuentes de información son identificadas y clasificadas.	• Porcentaje cubierto de categorías de información • Volumen de información clasificado • Porcentaje de información categorizada que ha sido validada
2. El conocimiento es utilizado y compartido.	• Porcentaje de conocimiento disponible utilizado realmente • Número de usuarios formados en el uso y compartición de conocimiento
3. La compartición de conocimiento está integrada en la cultura de la empresa.	• Nivel de satisfacción de los usuarios • Porcentaje del repositorio de conocimiento utilizado
4. El conocimiento es actualizado y mejorado para dar soporte a los requisitos.	• Frecuencia de actualización

Matriz RACI BAI08

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos.					A	R										R	R	R	R	R	R	R	R	R	R	R
BAI08.02 Identificar y clasificar las fuentes de información.					A	R									C	C	C	R		R	R		R			
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.						C									C	I	I	A		R	R	R				
BAI08.04 Utilizar y compartir el conocimiento.						A										R	R	R	C	C	C	R	C	C	C	C
BAI08.05 Evaluar y retirar la información.						A										C	C	R	R	R	R	R	R	R	R	R

BAI08 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos. Concebir e implantar un esquema para cultivar y facilitar una cultura de intercambio de conocimientos.	**De**	**Descripción**	**Descripción**	**A**
			Comunicaciones sobre el valor del conocimiento	APO01.04

Actividades	**Nivel de capacidad**
1. Comunicar proactivamente el valor del conocimiento para impulsar la creación, uso, reutilización y compartición de conocimiento.	4
2. Impulsar la compartición y transferencia de conocimiento mediante la identificación de factores que influyan en la motivación.	4
3. Crear un entorno, herramientas y elementos que den soporte a la compartición y transferencia de conocimientos.	4
4. Integrar prácticas de gestión del conocimiento en otros procesos de TI.	4
5. Establecer expectativas de la Dirección y demostrar la actitud adecuada acerca de la utilidad del conocimiento y la necesidad de compartir el conocimiento corporativo.	4

			90,60	**Nivel de cumplimiento**	**Nivel de capacidad objetivo** 3 / **Nivel de cumplimiento objetivo**	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90		Cumplida
			94	94		Cumplida
			95	95		Cumplida
			86	86		Cumplida
			88	88		Cumplida

Práctica de Gestión	**Entradas**		**Salidas**	
BAI08.02 Identificar y clasificar las fuentes de información. Identificar, validar y clasificar las diversas fuentes de información interna y externa necesarias para posibilitar el uso y la operación efectivas de los procesos de negocio y los servicios de TI.	**De**	**Descripción**	**Descripción**	**A**
	Fuera del Ámbito de COBIT	Requisitos y fuentes de conocimiento	Clasificación de fuentes de información	Interno

Actividades	**Nivel de capacidad**
1. Identificar usuarios potenciales de conocimiento, incluyendo propietarios de información que pueden necesitar contribuir y aprobar conocimiento. Obtener requisitos de conocimiento y fuentes de información de los usuarios identificados.	3
2. Considerar tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), elementos (documentos, registros, vídeo, voz) e información estructurada y no estructurada (expertos, medios de comunicación social, correo electrónico, buzones de voz, fuentes RSS).	3
3. Clasificar las fuentes de información basándose en un esquema de clasificación de contenido (ej. modelo de arquitectura de información). Trazar un mapa de fuentes de información con el esquema de clasificación.	3
4. Recoger, poner en orden y validar las fuentes de información basándose en criterios de validación de la información (ej. facilidad de comprensión, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, actualidad y fiabilidad).	4

			90,25	**Nivel de cumplimiento**	**Nivel de cumplimiento objetivo**	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90	F	Cumplida
			86	86	F	Cumplida
			90	90	F	Cumplida
			95	95		Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento. Organizar la información basándose en criterios de clasificación. Identificar y crear relaciones significativas entre elementos de información y facilitar el uso de la información. Identificar propietarios y definir e implementar niveles de acceso a los recursos de información.	BAI03.03	Compontes documentados de la solución	Repositorios de información publicada	APO07.03
	BAI05.07	Planes de transferencia de conocimiento		

Actividades	Nivel de capacidad
1. Identificar atributos compartidos y casar fuentes de información, creando relaciones entre conjuntos de información (etiquetado de información).	3
2. Crear vistas para conjuntos de datos relacionados, considerando requisitos organizativos y de las partes interesadas.	3
3. Concebir e implantar un esquema para gestionar la información no estructurada que no esté disponible a partir de fuentes formales (ej. conocimiento experto).	3
4. Publicar y hacer accesible el conocimiento a las partes interesadas relevantes basándose en roles y mecanismos de acceso.	3

			89,50	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90	F	Cumplida
			86	86	F	Cumplida
			87	87	F	Cumplida
			95	95	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
BAI08.04 Utilizar y compartir el conocimiento. Difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).	BAI03.03	Compontes documentados de la solución	Base de datos de usuarios de conocimiento	Interno
	BAI05.05	Plan de uso y operaciones	Esquemas de concienciación y formación de conocimiento	APO07.03
	BAI05.07	Planes de transferencia de conocimiento		

Actividades	Nivel de capacidad
1. Identificar usuarios potenciales de conocimiento mediante la clasificación de la información.	4
2. Transferir el conocimiento a los usuarios de conocimientos basándose en un análisis de necesidades, técnicas de aprendizaje efectivas y herramientas de acceso.	3
3. Educar y entrenar a los usuarios en el conocimiento disponible, en el acceso al conocimiento y en el uso de herramientas de acceso al conocimiento.	3

			92,00	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			95	95		Cumplida
			90	90	F	Cumplida
			92	92	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
BAI08.05 Evaluar y retirar la información. Medir el uso y evaluar la actualización y relevancia de la información. Retirar la información obsoleta.			Resultados de la evaluación de uso del conocimiento	Interno
			Reglas para la retirada de conocimiento	Interno

Actividades	Nivel de capacidad
1. Medir el uso y evaluar la utilidad, relevancia y valor de los elementos de conocimiento. Identificar información relacionada que ya no es relevante para cubrir las necesidades de conocimiento de la organización.	3
2. Definir las reglas para la retirada de conocimiento y retirar el mismo de forma acorde.	3

			91,00
N	**P**	**L**	**F**
			90
			92

Nivel de cumplimiento
Valor
90
92

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida

Tabla 28. BAI09 Gestionar los Activos

BAI09 Gestionar los Activos	**Área: Administración** **Dominio: Construir, Adquirir e Implantar**
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 le 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.	
El proceso apoya la consecución de un conjunto de objetivos primarios relacionados con las TI:	
Metas 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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Las licencias cumplen y están alineadas con las necesidades del negocio.	• Porcentaje de licencias usadas respecto a licencias pagadas
2. Los activos se mantienen en condiciones óptimas.	• Número de activos no utilizados • Comparativa de costes • Número de activos obsoletos

Matriz RACI BAI09

Prácticas Clave de Gestión	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
BAI09.01 Identificar y registrar activos actuales.			C			C												I	C	C	A	R	C			
BAI09.02 Gestionar activos críticos			C		I	C										C	C		R	R	A	R	C	C	C	
BAI09.03 Gestionar el ciclo de vida de los activos.						C													C	C	A	R	R			
BAI09.04 Optimizar el coste de los activos.			R		I	C												A	R	R	R	R	R			
BAI09.05 Administrar licencias.					I	C										C	R	A		R	R	R	C			

BAI09 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
BAI09.01 Identificar y registrar los 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.	BAI03.04	Actualizaciones al inventario de activos	Registro de activos	APO06.01 BAI10.03
	BAI10.02	Repositorio de configuración	Resultados de comprobaciones físicas de inventario	BAI10.03 BAI10.04 DSS05.03
			Resultados de revisiones de adecuación al objetivo	APO02.02

Actividades	Nivel de capacidad	N	P	L	F
					91,20
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				88
2. Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.	3				95
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				90
4. Comprobar que los activos se adecuan a sus objetivos (p.ej., están en condiciones útiles).	4				92
5. Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.	3				91
6. Asegurar la contabilización de todos los activos.	3				95

Nivel de cumplimiento
Valor
88
95
90
92
91
95

Nivel de capacidad objetivo	
3	
Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI09.02 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.			Comunicación de tiempo de inactividad planificado para mantenimiento	APO08.04
			Contratos de mantenimiento	Interno

Actividades	Nivel de capacidad
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
2. Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes y, en caso necesario, tomar medidas para reparar o reemplazar.	3
3. De forma regular, considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico.	3
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
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.	4
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
7. Comunicar a los clientes y los usuarios afectados el impacto esperado (p. ej., las restricciones de rendimiento) de las actividades de mantenimiento.	3
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.	2
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

			91,00
N	P	L	F
			95
			90
			90
			90
			90
			90
			92
			90
			87
			90

Nivel de cumplimiento
Valor
95
90
90
90
90
90
92
90
87
90

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

BAI09 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
BAI09.03 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.			Solicitudes de adquisición de activos aprobadas.	Interno
			Registro de activos actualizado.	BAI10.03
			Retirada autorizada de activos.	BAI10.03

Actividades	Nivel de capacidad
1. Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa.	4
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. Aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por contrato.	3
4. Desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación.	3
5. Asignar activos a los usuarios, con aceptación y firma de responsabilidades, según corresponda.	3
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
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.	4
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
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

			90,20	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90		Cumplida
			95	95	F	Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida
			86	86	F	Cumplida
			90	90	F	Cumplida
			90	90		Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
BAI09.04 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.			Resultados de las revisiones de optimización de costes	APO02.02
			Oportunidades para reducir el coste de activos o aumentar su valor	APO02.02

Actividades	Nivel de capacidad					Nivel de cumplimiento	Nivel de cumplimiento objetivo	
					92,40			
		N	P	L	F	Valor	Meta	Observación
1. Revisar la base general de activos de forma regular, teniendo en cuenta si está alineada con los requerimientos del negocio.	3				95	95	F	Cumplida
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				90	90	F	Cumplida
3. Revisar las garantías y considerar la relación calidad-precio y estrategias de reemplazo para determinar opciones de menor coste.	4				95	95		Cumplida
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				90	90	F	Cumplida
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				92	92	F	Cumplida
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				90	90	F	Cumplida

BAI09 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
BAI09.05 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.			Registro de licencias de software	BAI10.02
			Resultado de auditorías de licencias instaladas	MEA03.03
			Plan de acción para ajustar el número de licencias y su asignación	APO02.05

Actividades	Nivel de capacidad
1. Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.	4
2. De forma regular, llevar a cabo una auditoría para identificar a todos las copias de software instalado con licencia.	3
3. Comparar el número de copias de software instalado con el número de licencias en propiedad.	3
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
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
6. De forma regular, considerar si se puede obtenerse un mejor valor mediante la actualización de productos y licencias asociadas.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			93,00			
N	P	L	F	Valor	Meta	Observación
			95	95		Cumplida
			92	92	F	Cumplida
			90	90	F	Cumplida
			98	98	F	Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida

Tabla 29. DSS01 Gestionar Operaciones

DSS01 Gestionar Operaciones	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
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.	
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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Las actividades operativas se realizan según lo requerido y programado.	• Número de procedimientos operativos no estándar ejecutados • Número de incidentes causados por problemas operativos
2. Las operaciones son monitorizadas, medidas, reportadas y remediadas.	• Tasa de eventos comparada con el número de incidentes • Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática

DSS01 Cuadro RACI

Prácticas Clave de Gestión	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS01.01 Ejecutar procedimientos operativos																					A		C	C	C	
DSS01.02 Gestionar servicios externalizados de TI											I							A			R					
DSS01.03 Supervisar la infraestructura de TI				I		C					I						C	I		C	A		C	C		
DSS01.04 Gestionar el entorno						I					C	A				C	C	C	I	C	R		I	R	I	
DSS01.05 Gestionar las instalaciones						I					C	A				C	C	C	I	C	R		I	R	I	

DSS01 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
DSS01.01 Ejecutar procedimientos operativos. Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	BAI05.05	Plan de operación y uso	Programación operativa	Interno
			Registro de copia de respaldo	Interno

Actividades	**Nivel de capacidad**
1. Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	3
2. Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento de las actividades programadas.	3
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
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.	4
5. Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.	5

Nivel de capacidad objetivo

3

			89,20
N	**P**	**L**	**F**
		85	
			86
			90
			95
			90

Nivel de cumplimiento
Valor
85
86
90
95
90

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	No se cumple
F	Cumplida
F	Cumplida
	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS01.02 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.	APO09.03	• OLAs • ANSs	Planes de aseguramiento independientes	MEA02.06
	BAI05.05	Plan de operación y uso		

Nivel de capacidad objetivo: 3

Actividades	Nivel de capacidad
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
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
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 problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos.	3
4. Planificar la realización de auditorías y aseguramientos independiente de los entornos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.	3

			89,75	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			88	88	F	Cumplida
			86	86	F	Cumplida
			95	95	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS01.03 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.	BAI03.11	Definiciones de servicio	Reglas de monitorización de activos y condiciones de eventos	DSS02.01 DSS02.02
			Registro de eventos	Interno
			Tiques (*tickets*) de incidentes	DSS02.02

Actividades	Nivel de capacidad
1. Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.	3
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.	4
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
4. Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.	3
5. Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	3
6. Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.	3

Nivel de capacidad objetivo

3

			89,50	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			90	90		Cumplida
			88	88	F	Cumplida
			92	92	F	Cumplida
			88	88	F	Cumplida
			89	89	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS01.04 Gestionar el entorno. Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.			Políticas de entorno	APO01.08
			Informes de pólizas de seguro	MEA03.03

DSS01 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

Actividades	Nivel de capacidad	N	P	L	F
					91,50
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.	4				90
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				90
3. Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.	3				92
4. Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad).	4				90
5. Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas y el contacto con las autoridades locales de respuesta ante emergencias y entrenar al personal en estos procedimientos.	3				89
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				90
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).	5				96
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				95

Nivel de cumplimiento	Nivel de cumplimiento objetivo	
Valor	Meta	Observación
90		Cumplida
90	F	Cumplida
92	F	Cumplida
90		Cumplida
89	F	Cumplida
90	F	Cumplida
96		Cumplida
95	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
DSS01.05 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.	**De**	**Descripción**	**Descripción**	**A**
			Informes de evaluación de instalaciones	MEA01.03
			Concienciación en salud y seguridad en el trabajo	Interno

Actividades	Nivel de capacidad
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.	4
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. 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
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
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).	4
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
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
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
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
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
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

Nivel de capacidad objetivo: 3

			90,09	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90		Cumplida
			86	86	F	Cumplida
			92	92	F	Cumplida
			90	90	F	Cumplida
			90	90		Cumplida
			95	95	F	Cumplida
			88	88	F	Cumplida
			88	88	F	Cumplida
			87	87	F	Cumplida
			90	90	F	Cumplida
			95	95	F	Cumplida

MARCA	DESCRIPCION
	En la actividad de la metodología COBIT Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados. Se obtuvo un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, por consiguiente no hay un responsable para dar apoyo a los servicios extras que da la empresa. HH (7)

Tabla 30. DSS02 Gestionar Peticiones e Incidentes de Servicio

DSS02 Gestionar Peticiones e Incidentes de Servicio	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
Descripción del Proceso Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	
Declaración del Propósito del Proceso Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	
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
Objetivos y Métricas del Proceso	
Objetivos del Proceso	**Métricas Relacionadas**
1. Los servicios relacionados con TI están disponibles para ser utilizados.	• Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio • Tiempo promedio entre incidentes de acuerdo con el servicio facilitado por TI
2. Los incidentes son resueltos según los niveles de servicio acordados.	• Porcentaje de incidentes resueltos dentro de un periodo acordado/ aceptable
3. Las peticiones de servicio son resueltas según los niveles de servicio acordados y la satisfacción del usuario.	• Nivel de satisfacción del usuario con la resolución de las peticiones de servicio • Tiempo promedio transcurrido para el tratamiento de cada tipo de petición de servicio

Matriz RACI DSS02

Prácticas Clave de Gestión	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02 Registrar, clasificar y priorizar peticiones e						I					I	I									A		R			I
DSS02.03 Verificar, aprobar y resolver peticiones de servicio.						R												I		R	R		A			
DSS02.04 Investigar, diagnosticar y localizar incidentes.						R					I	I				I	I	I		C	R		A	C		
DSS02.05 Resolver y recuperarse de incidentes.						I					I	I				C	C	I		R	R		A	R		C
DSS02.06 Cerrar peticiones de servicio e incidentes.						I					I	I				I	I	I		I	A		I	R		I
DSS02.07 Seguir el estado y emitir informes.						I					I	I				I	I	I		I	A		R	I		

DSS02 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.	APO09.03	ANSs	Esquemas y modelos de clasificación de incidentes y peticiones de servicio	Interno
	BAI10.02	Repositorio de configuración	Reglas para escalado de incidentes	Interno
	BAI10.03	Repositorio actualizado con elementos de configuración	Criterios para registro de problemas	DSS03.01
	BAI10.04	Informes de estado de configuración		
	DSS01.03	Reglas de monitorización de activos y condiciones de eventos		
	DSS03.01	Esquema de clasificación de problemas		
	DSS04.03	Acciones y comunicaciones de respuesta a incidentes		

Actividades	**Nivel de capacidad**
1. Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas, para asegurar enfoques consistentes en el tratamiento, informando a los usuarios y realizando análisis de tendencias.	4
2. Definir modelos de incidentes para errores conocidos con el fin de facilitar su resolución eficiente y efectiva.	3
3. Definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar.	3
4. Definir reglas y procedimientos de escalaco de incidentes, especialmente para incidentes importantes e incidentes de seguridad.	5
5. Definir fuentes de conocimiento de incidentes y peticiones y su uso.	4

Nivel de capacidad objetivo: 3

			93,40
N	**P**	**L**	**F**
			90
			95
			92
			100
			90

Nivel de cumplimiento
Valor
90
95
92
100
90

Nivel de cumplimiento objetivo	
Meta	**Observación**
	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes. Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.	APO09.03	ANSs	Registro de incidentes y peticiones de servicio	Interno
	BAI04.05	Procedimiento de emergencia y escalado	Incidentes y peticiones de servicio clasificados y priorizados	APO08.03 APO09.04 APO13.03
	DSS01.03	• Tiques de incidentes • Reglas de supervisión de activos y condiciones de eventos		
	DSS05.07	Tiques de incidentes de seguridad		

Actividades	Nivel de capacidad
1. Registrar todos los incidentes y peticiones de servicio, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo.	4
2. Para posibilitar análisis de tendencias, clasificar incidentes y peticiones de servicio identificando tipo y categoría.	3
3. Priorizar peticiones de servicio e incidentes según la definición de impacto en el negocio del ANS y la urgencia.	3

			93,00
N	P	L	F
			95
			92
			92

Nivel de cumplimiento
Valor
95
92
92

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.03 Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.	APO12.06	Causas raíz relacionadas con riesgos	Peticiones de servicio aprobadas	BAI06.01
			Peticiones de servicio completas	Interno

Actividades	Nivel de capacidad
1. Verificar los derechos para realizar peticiones de servicio usando, cuando sea posible, un flujo de proceso predefinido y cambios estándar.	3
2. Obtener aprobación financiera y funcional o firmada, si se requiere, o aprobaciones predefinidas para cambios estándar acordados.	4
3. Completar las peticiones siguiendo el procedimiento de petición seleccionado, utilizando, cuando sea posible, menús automáticos de autoayuda y modelos de petición predefinidos para los elementos solicitados frecuentemente.	4

			89,00
N	P	L	F
			87
			90
			90

Nivel de cumplimiento
Valor
87
90
90

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.04 Investigar, diagnosticar y localizar incidentes. Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.	BAI07.07	Plan de soporte adicional	Síntomas de incidentes	Interno
			Registro de problemas	DSS03.01

Actividades	Nivel de capacidad
1. Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Hacer referencia a los recursos de conocimiento disponibles (incluyendo errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes).	3
2. Registrar un nuevo problema si un problema relacionado o error conocido no existe aún y si el incidente satisface los criterios acordados para registro de problemas.	3
3. Asignar incidentes a funciones especialistas si se necesita de un conocimiento más profundo, e implicar al nivel de gestión apropiado, cuando sea necesario.	3

			95,33
N	P	L	F
			90
			98
			98

Nivel de cumplimiento
Valor
90
98
98

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.05 Resolver y recuperarse ante incidentes. Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.	APO12.06	Planes de respuesta a incidentes relacionados con riesgos	Resoluciones de incidentes	DSS03.04
	DSS03.03	Registros de errores conocidos		
	DSS03.04	Comunicación de conocimiento aprendido		

Actividades	Nivel de capacidad
1, Seleccionar y aplicar las resoluciones de incidentes más apropiadas (soluciones provisionales y/o soluciones permanentes)	4
2. Registrar si se usaron soluciones temporales para resolver los incidentes.	3
3. Ejecutar acciones de recuperación, si se requieren.	4
4. Documentar la resolución del incidente y evaluar si puede usarse como una fuente de conocimiento en el futuro.	4

			92,00
N	P	L	F
			98
			88
			90
			92

Nivel de cumplimiento
Valor
98
88
90
92

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
F	Cumplida
	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.06 Cerrar peticiones de servicio e incidentes. Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.	DSS03.04	Registros de problemas cerrados	Peticiones de servicio e incidentes cerrados	APO08.03 APO09.04 DSS03.04
			Confirmación del usuario de resolución o cumplimiento satisfactorios	APO08.03

Actividades	Nivel de capacidad
1. Verificar con los usuarios afectados (si lo han acordado) que la petición de servicio ha sido completada o el incidente ha sido resuelto de manera satisfactoria.	3
2. Cerrar peticiones de servicio e incidentes.	3

			92,50
N	P	L	F
			90
			95

Nivel de cumplimiento
Valor
90
95

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.07 Seguir el estado y emitir de informes. Hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.	APO09.03	OLAs	Informe de estado y tendencias de incidentes	APO08.03 APO09.04 APO11.04 APO12.01 MEA01.03
	DSS03.01	Informes de estado de problemas		
	DSS03.02	Informes de resolución de problemas		
	DSS03.05	Informes de monitorización de resolución de problemas	Informes de estado de cumplimiento de peticiones y tendencias	APO08.03 APO09.04 APO11.04 MEA01.03

Actividades	Nivel de capacidad
1. Supervisar y hacer seguimiento del escalado de incidentes y de resoluciones y de los procedimientos de gestión de resoluciones para progresar hacia la resolución o cumplimentación.	4
2. Identificar la información para las partes interesadas y sus necesidades de datos o informes. Identificar la frecuencia y el medio para informarles.	3
3. Analizar incidentes y peticiones de servicio por categoría y tipo para establecer tendencias e identificar patrones de asuntos recurrentes, infracciones de ANSs o ineficiencias. Utilizar la información como entrada a la planificación de la mejora continua.	3
4. Producir y distribuir informes en tiempo o proporcionar acceso controlado a datos online.	3

			90,00
N	P	L	F
			90
			86
			94
			90

Nivel de cumplimiento
Valor
90
86
94
90

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Tabla 31. DSS03 Gestionar Problemas

DSS03 Gestionar Problemas	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
Descripción del Proceso Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.	
Declaración del Propósito del Proceso Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.	
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 y 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
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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Garantizar que los problemas relativos a TI son resueltos de forma que no vuelven a suceder.	• Descenso del número de incidentes recurrentes causados por problemas no resueltos • Porcentaje de incidentes graves para los que se han registrado problemas • Porcentaje de soluciones temporales definidos para problemas abiertos • Porcentaje de problemas registrados como parte de una gestión de problemas proactiva • Número de problemas para los que se ha encontrado una solución satisfactoria que apunta a causas raíz

Matriz RACI DSS03

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Privacy Officer
DSS03.01 Identificar y clasificar problemas.					I	C					I	I				I	I	R	C	R	R		A	C		
DSS03.02 Investigar y diagnosticar problemas.											I	I							C	C	A		R	R		
DSS03.03 Levantar errores conocidos.																					A		R	R		
DSS03.04 Resolver y cerrar problemas.					I	C					I	I				C	C	I	C	C	R		A			
DSS03.05 Realizar una gestión de problemas proactiva.						C													C	C	R		A			

DSS03 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
DSS03.01 Identificar y clasificar problemas. Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.	APO12.06	Causas raíz relacionadas con riesgos	Esquema de clasificación de problemas	DSS02.01
	DSS02.01	Criterios para el registro de problemas	Informes de estado de problemas	DSS02.07
	DSS02.04	Registro de problemas	Registro de problemas	Interno

Actividades	**Nivel de capacidad**
1. Identificar problemas a través de la correlación de informes de incidentes, registros de error y otros recursos de identificación de problemas. Determinar niveles de prioridad y categorización para dedicarse a la resolución de problemas en tiempo basándose en los riesgos de negocio y en la definición del servicio.	3
2. Manejar formalmente todos los problemas con acceso a todos los datos relevantes, incluyendo información sobre el sistema de gestión de cambios y los detalles de incidentes sobre configuración/activos TI.	4
3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, en el análisis de la causa raíz, y en la determinación de la solución, para respaldar la gestión de problemas. Determinar grupos de soporte basados en categorías predefinidas, tales como hardware, redes, software, aplicaciones y software de soporte.	3
4. Definir niveles de prioridad mediante consultas con el negocio para asegurar que la identificación de problemas y el análisis de la causa raíz se llevan a cabo a tiempo de acuerdo con los ANSs acordados. Basar los niveles de prioridad en el impacto en el negocio y en la urgencia.	3
5. Informar del estado de problemas identificados al centro de servicios de forma que los clientes y la gestión de TI pueden mantenerse informados.	4
6. Mantener un catálogo de gestión de problemas único para registrar e informar sobre problemas identificados y para establecer pistas de auditoría sobre los procesos de gestión de problemas, incluyendo el estado de cada problema (p. ej., abierto, reabierto, en progreso o cerrado).	3

			92,00	**Nivel de cumplimiento**	**Nivel de capacidad objetivo**	
					3	
N	**P**	**L**	**F**	**Valor**	**Nivel de cumplimiento objetivo**	
					Meta	**Observación**
			95	95	F	Cumplida
			86	86		Cumplida
			99	99	F	Cumplida
			90	90	F	Cumplida
			90	90		Cumplida
			90	90	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS03.02 Investigar y diagnosticar problemas. Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.	APO12.06	Causas raíz relacionadas con riesgos	Causas raíz de los problemas	Interno
			Informes de resolución de problemas	DSS02.07

Actividades	Nivel de capacidad
1. Identificar problemas que pueden ser errores conocidos comparando datos de incidentes con la base de datos de errores conocidos y posibles (p. ej., los comunicados por los proveedores externo) y clasificar problemas como errores conocidos.	4
2. Asociar los elementos de configuración afectados con el error conocido/establecido.	3
3. Producir informes para comunicar el progreso de la resolución de problemas y para supervisar el impacto continuado de los problemas no resueltos. Supervisar el estado del proceso de gestión de problemas a través de su ciclo de vida, incluyendo aportaciones de la gestión de cambios y de configuración.	3

			88,67
N	P	L	F
			90
			90
			86

Nivel de cumplimiento
Valor
90
90
86

Nivel de cumplimiento objetivo	
Meta	Observación
	Cumplida
F	Cumplida
F	Cumplida

DSS03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
DSS03.03 Levantar errores conocidos. Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.			Registros de errores conocidos	DSS02.05
			Soluciones propuestas para errores conocidos	BAI06.01

Actividades	Nivel de capacidad
1. Tan pronto como las causas raíz de los problemas se han identificado, crear registros de errores conocidos y desarrollar una solución temporal adecuada.	3
2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambios) soluciones a los errores conocidos basándose en un caso de negocio coste- beneficio y en el impacto de negocio y la urgencia.	3

			88,00
N	P	L	F
			88
			88

Nivel de cumplimiento
Valor
88
88

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS03.04 Resolver y cerrar problemas. Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.	DSS02.05	Resoluciones de incidentes	Registros de problemas cerrados	DSS02.06
	DSS02.06	Incidentes y peticiones de servicio cerrados	Comunicación del conocimiento aprendido	APO08.04 DSS02.05

Actividades	Nivel de capacidad
1. Cerrar registros de problemas, bien después de la confirmación de la eliminación satisfactoria del error conocido, bien tras acordar con el negocio cómo gestionar el problema de una manera alternativa.	3
2. Informar al centro de servicio del calendario de cierre del problema, p. ej., del calendario para solucionar los errores conocidos, la posible solución alternativa o el hecho de que el problema permanecerá hasta que el cambio se haya implementado, y las consecuencias de la solución escogida. Mantener adecuadamente informados a los usuarios y a los clientes afectados.	3
3. A través del proceso de resolución, obtener informes periódicos de gestión de cambios acerca del progreso en la resolución de problemas y errores.	3
4. Supervisar el continuo impacto de los problemas y errores conocidos en los servicios.	4
5. Revisar y confirmar la resolución satisfactoria de problemas graves.	3
6. Asegurar que el conocimiento aprendido de esta revisión se incorpora en una reunión de revisión del servicio con el cliente de negocio.	3

			90,80	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			87	87	F	Cumplida
			90	90	F	Cumplida
			92	92		Cumplida
			95	95	F	Cumplida
			92	92	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS03.05 Realizar una gestión de problemas proactiva. Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.			Registros de monitorización de resolución de problemas	DSS02.07
			Identificar soluciones sostenibles	BAI06.01

Actividades	Nivel de capacidad
1.Capturar información de problemas relacionada con cambios e incidentes TI y comunicarla a las partes interesadas clave. Esta comunicación podría tomar la forma de informes y reuniones periódicas entre los responsables de los procesos de gestión de incidentes, problemas, cambios y configuración para considerar problemas recientes y acciones correctivas potenciales.	3
2. Asegurar que los responsables de los procesos y los responsables de gestión de incidentes, problemas, cambios y configuración se reúnen regularmente para discutir problemas conocidos y cambios futuros planificados.	4
3. Permitir a la empresa supervisar los costes totales de problemas, capturar esfuerzos de cambio resultantes de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar de ellos.	3
4. Producir informes para supervisar la resolución de problemas respecto a los requisitos de negocio y ANSs. Asegurar el adecuado escalado de problemas, p. ej., escalado a un nivel de gestión superior de acuerdo con los criterios acordados, contactando proveedores externos, o enviando al comité de gestión de cambios para incrementar la prioridad de una petición de cambio urgente para implementar una solución temporal.	3
5. Optimizar el uso de recursos y reducir las soluciones temporales y hacer seguimiento de las tendencias de problemas.	3
6. Identificar e iniciar soluciones sostenibles (soluciones permanentes) identificando la causa raíz, y levantar peticiones de cambio a través de los procesos de gestión de cambios establecidos.	3

			90,40
N	P	L	F
			90
			90
			92
			90
			90
			88

Nivel de cumplimiento
Valor
90
90
92
90
90
88

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Tabla 32. DSS05 Gestionar Servicios de Seguridad

DSS05 Gestionar Servicios de Seguridad	Área: Gestión Dominio: Entrega, Servicio y Soporte
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	
Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	
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
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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	• Número de vulnerabilidades descubiertas
	• Número de rupturas (*breaches*) de cortafuegos
2. La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final
	• Número de incidentes que impliquen dispositivos de usuario final
	• Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	• Promedio de tiempo entre los cambios y actualizaciones de cuentas
	• Número de cuentas (con respecto al número de usuarios/empleados autorizados)
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno
	• Clasificación media para las evaluaciones de seguridad física
	• Número de incidentes relacionados con seguridad física
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	• Número de incidentes relacionados con accesos no autorizados a la información

Matriz RACI DSS05

Práctica Clave de Gobierno	Consejo de Administ	Director General Ejecutivo	Director General Financiero	Director de Operaciones	Ejecutivos de negocio	Propietarios de los Procesos de	Comité Ejecutivo Estrat	Comité Estratégico (Desarrollo/Pr	Oficina de Gestión de Pro	Oficina de Gestión del	Director de Riesgos	Director de Seguridad de la Informa	Consejo de Arquitectura de la E	Comité de Riesgos Corpo	Jefe de Recursos Hun	Cumplimiento Normativo (Comp	Auditoría	Director de Informática/Sistema	Jefe de Arquitectura del Ne	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración	Gestor de Servicio (Service M	Gestor de Seguridad de la Info	Gestor de Continuidad de N	Gestor de Privacidad de la info
DSS05.01 Proteger contra software malicioso (*malware*).						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Gestionar la seguridad de la red y las conexiones.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Gestionar la seguridad de los puestos de usuario final.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Gestionar el acceso físico a los activos de TI.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.											I					C	C	A			R					
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.01 Proteger contra software malicioso (malware).	**De**	**Descripción**	**Descripción**	**A**
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).			Política de prevención de software malicioso	APO01.04
			Evaluaciones de amenazas potenciales	APO12.02
				APO12.03

Actividades	Nivel de capacidad
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	3
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
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
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	3
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
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.	4

			90,33
N	**P**	**L**	**F**
			90
		85	
			92
			90
			90
			95

Nivel de cumplimiento
Valor
90
85
92
90
90
95

Nivel de capacidad objetivo

3

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	No se cumple
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.02 Gestionar la seguridad de la red y las conexiones.	**De**	**Descripción**	**Descripción**	**A**
Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	APO01.06	Guías de clasificación de la información	Política de seguridad en la conectividad	APO01.04
	APO09.03	ANSs	Resultados de las pruebas de intrusión	MEA02.08

Actividades	**Nivel de capacidad**
1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	3
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.	4
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.	4
4. Cifrar la información en tránsito de acuerdo con su clasificación.	3
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.	3
6. Configurar los equipamientos de red de forma segura.	4
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	3
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	3
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	3

3

			91,22
N	**P**	**L**	**F**
			90
			88
			92
			90
			87
			95
			96
			95
			88

Nivel de cumplimiento
Valor
90
88
92
90
87
95
96
95
88

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
	Cumplida
F	Cumplida
F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
DSS05.03 Gestionar la seguridad de los puestos de usuario final.	**De**	**Descripción**	**Descripción**	**A**
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.	APO03.02	Modelo de arquitectura de la información	Políticas de seguridad para dispositivos de usuario final	APO01.04
	APO09.03	• Acuerdos de Nivel de Servicio (ANSs)		
		• Acuerdos de Nivel		
		Operativo (OLAs)		
	BAI09.01	Resultados de pruebas de inventarios físicos		
	DSS06.06	Informes de violaciones		

Actividades	Nivel de capacidad
1. Configurar los sistemas operativos de forma segura.	3
2. Implementar mecanismos de bloqueo de los dispositivos.	3
3. Cifrar la información almacenada de acuerdo a su clasificación.	3
4. Gestionar el acceso y control remoto.	3
5. Gestionar la configuración de la red de forma segura.	3
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	4
7. Proteger la integridad del sistema.	4
8. Proveer de protección física a los dispositivos de usuario final.	4
9. Deshacerse de los dispositivos de usuario final de forma segura.	3

3

			91,33	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			86	86		Cumplida
			92	92	F	Cumplida
			89	89	F	Cumplida
			94	94	F	Cumplida
			95	95		Cumplida
			94	94		Cumplida
			90	90		Cumplida
			92	92	F	Cumplida

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	**De**	**Descripción**	**Descripción**	**A**
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.				
	APO01.02	Definición de roles y responsabilidades relacionadas con TI	Derechos de acceso de los usuarios aprobados	Interno
	APO03.02	Modelo de arquitectura de la información	Resultados de las revisiones de cuentas y privilegios de los usuarios	Interno

Actividades	Nivel de capacidad
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. 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
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.	2
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
5. Segregar y gestionar cuentas de usuario privilegiadas.	3
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	4
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.	2
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.	3

			91,88	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			90	90	F	Cumplida
			92	92	F	Cumplida
			90	90	F	Cumplida
			87	87	F	Cumplida
			95	95		Cumplida
			96	96	F	Cumplida
			95	95	F	Cumplida

3

Prácticas de Gestión	Entradas		Salidas	
DSS05.05 Gestionar el acceso físico a los activos de TI.	**De**	**Descripción**	**Descripción**	**A**
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.			Peticiones de acceso aprobadas	Interno
			Registros de acceso	DSS06.03

Actividades	Nivel de capacidad
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. 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
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
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
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
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 alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	4
7. Realizar regularmente formación de concienciación de seguridad física.	3

3

			92,57	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90	F	Cumplida
			88	88		Cumplida
			92	92	F	Cumplida
			90	90	F	Cumplida
			97	97	F	Cumplida
			95	95		Cumplida
			96	96	F	Cumplida

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	**De**	**Descripción**	**Descripción**	**A**
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.	APO03.02	Modelo de arquitectura de la información	Inventario de documentos y dispositivos sensibles	Interno
			Privilegios de acceso	Interno

Actividades	Nivel de capacidad
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
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
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	3
4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	3
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

3

			89,60	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90	F	Cumplida
			88	88		Cumplida
			92	92	F	Cumplida
			90	90	F	Cumplida
			88	88	F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
DSS05.07 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.			Registros de incidentes de seguridad	Interno
			Características de incidentes de seguridad	Interno
			Tiques de incidentes de seguridad	DSS02.02

Actividades	Nivel de capacidad
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
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.	4
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.	3
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.	4
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			89,40		3	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			90	90	F	Cumplida
			88	88		Cumplida
			92	92	F	Cumplida
			90	90		Cumplida
			87	87	F	Cumplida

MARCA	DESCRIPCIÓN
	La metodología COBIT tiene como actividad Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios. Además, tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, es por ello que la empresa posee un antivirus para combatir a cualquier programa o virus malisioso pero el respaldo de información no se realiza frecuentemente. **HH (8)**

Tabla 33. DSS06 Gestionar Controles de Proceso de Negocio

DSS06 Gestionar Controles de Proceso de Negocio	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
Descripción de Proceso Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	
Propósito del proceso Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.	
El proceso apoya la obtención de un conjunto de objetivos relacionados con las TI:	
Metas 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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La cobertura y efectividad de los controles clave para cumplir con los requerimientos de negocio para el procesamiento de la información es completa.	• Porcentaje completado de inventario de procesos críticos y controles clave • Porcentaje de controles clave cubiertos con los planes de pruebas • Número de incidentes y evidencias del informe de auditoría indicando fallos de los controles clave
2. El inventario de roles, responsabilidades y derechos de acceso está alineado con las necesidades autorizadas de negocio.	• Porcentaje de roles de proceso de negocio con derechos de acceso y niveles de autorización asignados • Porcentaje de roles de proceso de negocio con una separación clara de tareas • Número de incidentes y evidencias de auditoría debido a acceso o violación de segregación de funciones.
3. Las transacciones de negocio son retenidas completamente y según se requiera en registros	• Porcentaje de completitud de registros de transacciones rastreables • Número de incidentes donde el historial de transacciones no pueda ser recuperado

Matriz RACI DSS06

Prácticas de Gestión Clave	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.		C	C	C	A	R					I	I				C	C	C			C		C	C		C
DSS06.02 Controlar el procesamiento de la información.		R	R	R	A	R					I	I				C	C	C			C		C	C		
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.			R		A	R						I			I	C	C	C			C		C	R		C
DSS06.04 Gestionar errores y excepciones.				I	I	A										C	C	I			C		R			
DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.					C	A						I				C	C	C			C		C	C		
DSS06.06 Asegurar los activos de información.			C	C	C	A					I	I				C	C	C			C			C	C	C

DSS06 Prácticas, Entradas/Salidas y Actividades del Proceso				
Prácticas de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos. Evaluar y supervisar continuamente la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.	APO01.06	•Procedimientos de integridad de datos • Directrices de clasificación de datos	Resultados de las revisiones de efectividad de procesamiento	MEA02.04
			Recomendaciones y análisis de las causas raíces	BAI06.01 MEA02.04 MEA02.07 MEA02.08

Actividades	Nivel de capacidad
1. Identificar y documentar las actividades de control de los procesos de negocio claves para satisfacer los requerimientos de control para los objetivos estratégicos, operacionales, de informes y cumplimiento.	3
2. Priorizar las actividades de control basadas en el riesgo inherente del negocio e identificar controles clave.	3
3. Asegurar la propiedad de las actividades de control claves.	3
4. Supervisar continuamente las actividades de control de extremo a extremo para identificar oportunidades de mejora.	4
5. Mejorar continuamente el diseño y operación de los controles de procesos de negocio.	4

3

			91,00
N	**P**	**L**	**F**
			90
			88
			95
			94
			88

Nivel de cumplimiento
Valor
90
88
95
94
88

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.02 Controlar el procesamiento de la información. Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).	BAI05.05	Plan de operación y uso	Informes de control de procesamiento	Interno
	BAI07.02	Plan de migración		

Actividades	Nivel de capacidad
1. Crear transacciones por individuos autorizados siguiendo los procedimientos establecidos, incluyendo, cuando sea apropiado, la adecuada segregación de tareas en relación al origen y aprobación de esas transacciones.	4
2. Autenticar la fuente de las transacciones y verificar que él o ella tiene la autoridad para originar las transacciones.	3
3. Introducir transacciones en el momento oportuno. Verificar que las transacciones son precisas, completas y válidas. Validar los datos de entrada y la edición o, cuando sea aplicable, la devolución para su corrección tan cerca al punto de origen como sea posible.	4
4. Corregir y reenviar datos cuya entrada fue erróneamente aceptada, sin comprometer los niveles de autorización de la transacción original. Cuando sea apropiado para la reconstrucción, conservar los documentos fuentes originales durante tiempo apropiado.	3
5. Mantener la integridad y validez de los datos a través del ciclo de procesamiento. Asegurar que la detección de transacciones erróneas no interrumpe el procesamiento de las transacciones válidas.	4
6. Mantener la integridad de los datos durante interrupciones no esperadas en el procesamiento de negocio y confirmar la integridad de los datos después de los fallos de procesamiento.	3
7. Manejar la salida de una forma autorizada, entregarla al beneficiario apropiado y proteger la información durante la transmisión. Verificar la precisión y completitud de la salida.	3
8. Antes de pasar datos de la transacción entre las aplicaciones internas y las funciones operacionales o de negocio (dentro o fuera de la organización), comprobar el correcto direccionamiento, autenticidad de origen e integridad del contenido. Mantener la autenticidad e integridad durante la transmisión o la generación del informe.	3

			89,63	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			89	89		Cumplida
			90	90	F	Cumplida
			90	90		Cumplida
			86	86	F	Cumplida
			91	91		Cumplida
			98	98	F	Cumplida
			86	86	F	Cumplida
			87	87	F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización. Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe donde están los datos y quien los está manejando en su nombre.	EDM04.02	Responsabilidades asignadas para la gestión de recursos	Responsabilidades y roles asignados	APO01.02
	APO11.01	Roles, responsabilidades y derechos de decisión del SGC	Niveles de autoridad asignados	APO01.02
	APO13.01	Declaración de alcance del SGSI	Derechos de acceso asignados	APO07.04
	DSS05.05	Registros de acceso		

Actividades	Nivel de capacidad
1. Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas.	4
2. Asignar niveles de autoridad para la aprobación de transacciones, límites y cualquier otra decisión relativa a los procesos de negocio, basadas en los roles de trabajo aprobados.	3
3. Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto pre- definidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso es adecuado para las actuales amenazas, riesgos, tecnología y necesidades del negocio.	3
4. Asignar roles para las actividades sensibles de manera que haya una segregación clara de funciones.	4
5. Proporcionar concienciación y formación en relación a los roles y responsabilidades de forma regular para que todo el mundo entienda sus responsabilidades; la importancia de los controles; y la integridad, confidencialidad y privacidad de la información de la empresa en todas sus formas.	3
6. Revisar periódicamente las definiciones de control de acceso, registros e informes de excepciones para asegurar que todos los privilegios de acceso son válidos y están alineados con el personal actual y sus roles asignados.	3

			92,00	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90		Cumplida
			90	90	F	Cumplida
			92	92	F	Cumplida
			100	100		Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida

.

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.04 Gestionar errores y excepciones. Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.			Evidencia de corrección y remediación de errores	MEA02.04
			Informes de errores y análisis de las causas raíces	Interno

Actividades	Nivel de capacidad
1. Definir y mantener procedimientos para asignar propiedad, corregir errores, remplazar errores y manejar las condiciones fuera de equilibrio.	4
2. Revisar errores, excepciones y desviaciones.	4
3. Hacer seguimiento, corregir, aprobar y reenviar documentos fuente y transacciones.	4
4. Mantener evidencia de las medidas correctivas.	3
5. Informar acerca de errores de proceso de información relevantes de manera oportuna para realizar el análisis de tendencias y causas raíces.	3

			90,80	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			89	89		Cumplida
			87	87		Cumplida
			98	98		Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información. Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.			Requerimientos de retención	Interno
			Registro de transacciones	Interno

Actividades	Nivel de capacidad
1. Definir requerimientos de retención, basados en los requerimientos de negocio, para conocer las necesidades operativas, de reporte financiero y cumplimiento.	4
2. Capturar la fuente de información, evidencia que la soporta y el registro de las transacciones.	3
3. Eliminar la fuente de información, la evidencia que la soporta y el registro de transacciones de acuerdo con la política de retención.	3

			93,33	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			98	98		Cumplida
			90	90	F	Cumplida
			92	92	F	Cumplida

Prácticas de Gestión	Entradas		Salidas	
DSS06.06 Asegurar los activos de información. Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin.	**De**	**Descripción**	**Descripción**	**A**
			Informes de violación	DSS05.03

Actividades	Nivel de capacidad
1. Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.	3
2. Proporcionar concienciación y formación de un uso aceptable.	3
3. Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación.	3
4. Identificar e implementar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento.	3
5. Informar al negocio y otros grupos de interés acerca de violaciones y desviaciones.	3

			88,40	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	**P**	**L**	**F**	**Valor**	**Meta**	**Observación**
			89	89	F	Cumplida
			87	87	F	Cumplida
			92	92	F	Cumplida
			88	88	F	Cumplida
			86	86	F	Cumplida

Tabla 34. MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad

MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	**Área: Gestión** **Dominio: Supervisar, Evaluar y Valorar**
Descripción de 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.	
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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Objetivos y métricas aprobadas por las partes interesadas.	•Porcentaje de informes de rendimiento entregados en plazo •Porcentaje de objetivos y métricas aprobadas por las partes interesadas
2. Procesos medidos acorde a las métricas y objetivos acordados.	• Porcentaje de procesos con objetivos y métricas definidas.
3. La monitorización, evaluación y generación de información es efectiva y operativa.	• Porcentaje de procesos con efectividad de objetivos y métricas revisadas y mejoradas • Porcentaje de procesos críticos supervisados
4. Objetivos y métricas integradas dentro de los sistemas de supervisión de la empresa.	• Porcentaje de objetivos y métricas alineadas al sistema de supervisión de la empresa
5. Los informes acerca del rendimiento y conformidad de los procesos es útil y a tiempo.	• Porcentaje de informes de rendimiento entregados en plazo

Matriz RACI MEA01																										
Práctica Clave de Gobierno	Consejo de Administración	**Director General Ejecutivo (CEO)**	**Director General Financiero (CFO)**	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	**Comité Estratégico**	**Oficina de Gestión de Proyectos**	**Oficina de Gestión del Valor**	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	**Director de Informática/Sistemas (CIO)**	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	**Gestor de Servicio (Service Manager)**	**Gestor de Seguridad de la Información**	**Gestor de Continuidad de Negocio**	**Gestor de Privacidad de la información**
MEA01.01 Establecer un enfoque de la supervisión.		A	R	R	R	I	C		I						C	C	C	R	I	C	C	I	C	I	I	I
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.		I	I	I	A	R			I						C			C	C	R	R	I	R	I	I	I
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.					C	R			I						C			A		R	R	I	R	I	I	I
MEA01.04 Analizar e informar sobre el rendimiento.					A	R			C						C	C	C	C	C	R	R	C	R	C	C	C
MEA01.05 Asegurar la implantación de medidas correctivas.	I	I	I	I	C	R			C						C	C	C	A	C	R	R	C	R	C	C	C

MEA01 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
MEA01.01 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.	EDM05.01	•Principios de comunicación e informes •Evaluación de los requisitos de información de la organización	Requisitos de supervisión	Interno
	EDM05.02	Reglas de validación y aprobación de los informes preceptivos	Métricas y objetivos de supervisión aprobado.	Interno
	EDM05.03	Evaluación de la efectividad de los informes		

Actividades	**Nivel de capacidad**
1. Identificar las partes interesadas (p. ej. dirección, propietarios de procesos o usuarios).	4
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).	4
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
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
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
6. Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).	3
7. Validar periódicamente el enfoque utilizado e identificar los nuevos o cambiantes grupos de interés, requisitos y recursos.	3

			90,14
N	**P**	**L**	**F**
			94
			93
			91
			89
			86
			88
			90

Nivel de cumplimiento
Valor
94
93
91
89
86
88
90

Nivel de cumplimiento objetivo	
Meta	**Observación**
	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA01.02 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.	APO01.07	Métricas y objetivos de rendimiento y métricas para el seguimiento de la mejora de los procesos	Objetos de supervisión	Todo APO Todo BAI Todo DSS Todo MEA

Actividades	Nivel de capacidad
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.	4
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. Hacer público a los usuarios de la información los cambios en metas y tolerancias.	3
4. Evaluar si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			90,25			
N	P	L	F	Valor	Meta	Observación
			94	94		Cumplida
			90	90	F	Cumplida
			87	87	F	Cumplida
			90	90	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento. Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.	APO01.07	Evaluación de la capacidad de los procesos	Datos de supervisión procesados	Interno
	APO05.04	Informes de rendimiento del portafolio de inversiones		
	APO09.04	Informes de desempeño del nivel de servicio		
	APO10.05	Resultados de las revisiones de supervisión del cumplimiento de los proveedores		
	BAI01.06	Resultados de las revisiones de rendimiento de los programas		
	BAI04.04	Informes de revisión de supervisión de la capacidad, rendimiento y disponibilidad		
	BAI05.05	Medidas y resultados exitosos		
	DSS01.05	Informes de evaluación de instalaciones		
	DSS02.07	• Informe de tendencia y estado de completitud de las peticiones • Informe de tendencia y estado de incidentes		

Actividades	Nivel de capacidad
1. Recopilar datos de los procesos definidos, de forma automatizada, cuando sea posible.	4
2. Evaluar la eficiencia (esfuerzo en relación con la comprensión detallada proporcionada) y oportunidad (utilidad y significado) y validar la integridad (precisión y completitud) de los datos recopilados.	3
3. Consolidar los datos para soportar el cálculo de las métricas acordadas.	4
4. Alinear los datos consolidados a los enfoques y objetivos de presentación de información de la compañía.	3
5. Utilizar herramientas y sistemas apropiados para el procesamiento y formateo de datos para análisis.	3

				Nivel de cumplimiento	Nivel de cumplimiento objetivo	
			90,60			
N	P	L	F	Valor	Meta	Observación
			89	89		Cumplida
			90	90	F	Cumplida
			94	94		Cumplida
			90	90	F	Cumplida
			90	90	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA01.04 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.			Informes de desempeño.	EDM01.03 Todo APO Todo BAI Todo DSS Todo MEA

Actividades	Nivel de capacidad
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. 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
3. Recomendar cambios a los objetivos y métricas, cuando sea procedente.	4
4. Distribuir los informes a las partes interesadas relevantes.	3
6. 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
6. Cuando sea factible, enlazar el cumplimiento de objetivos de desempeño con el sistema de compensación y gratificación de la organización.	3

			88,67	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			87	87	F	Cumplida
			92	92		Cumplida
			90	90	F	Cumplida
			87	87	F	Cumplida
			86	86	F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA01.05 Asegurar la implantación de medidas correctivas. Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.	EDM05.02	Directrices de escalado	Acciones y asignaciones correctivas	Todo APO Todo BAI Todo DSS Todo MEA
	APO01.08	Acciones correctivas de incumplimientos	Estado y resultado de las acciones	EDM01.03

Actividades	Nivel de capacidad
1. Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores.	3
2. Asegurar que se mantiene la asignación de responsabilidades en las acciones correctivas.	3
3. Hacer seguimiento de los resultados de las acciones comprometidas.	3
4. Informar de los resultados a las partes interesadas.	4

			91,75	Nivel de cumplimiento	Nivel de cumplimiento objetivo	
N	P	L	F	Valor	Meta	Observación
			90	90	F	Cumplida
			90	90	F	Cumplida
			92	92	F	Cumplida
			95	95		Cumplida

Tabla 35. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	**Área: Dirección** **Dominio: Supervisar, Evaluar y Valorar**
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.	
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
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la empresa.	• Porcentaje de procesos con la seguridad de que las salidas cumplen el objetivo dentro de los márgenes de tolerancia • Porcentaje de procesos con la seguridad de que son conformes con las metas de control interno
2. Todas las iniciativas de aseguramiento se planean y ejecutan de forma efectiva.	• Porcentaje de iniciativas de aseguramiento que siguen a programas de aseguramiento aprobados y los estándares de planificación
3. Se proporciona aseguramiento independiente de que el sistema de control interno es operativo y efectivo.	• Porcentaje de procesos bajo revisión independiente
4. El control interno está establecido y las deficiencias son identificadas y comunicadas.	• Número de debilidades identificadas en los informes externos de certificación y cualificación • Número de brechas mayores en el control interno • Tiempo transcurrido entre la ocurrencia de la deficiencia del control interno y su comunicación

Matriz RACI MEA02

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática / Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
MEA02.01 Supervisar el control interno.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.	I	I	R	I	A	R	I				I	I				R	R	C			C		C	C	C	
MEA02.03 Realizar autoevaluaciones de control.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.04 Identificar y comunicar las deficiencias de control.		I	C	I	C	R			R		I	I				R	R	A	I	R	R	R	R	R	R	R
MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.						R										A	A	R								
MEA02.06 Planificar iniciativas de aseguramiento.		A			C	R			C							C	C	R	C	C	C	C	C	C	C	C
MEA02.07 Estudiar las iniciativas de aseguramiento.				R	R	R			C							C	A	R	C	C	C	C	C	C	C	C
MEA02.08 Ejecutar las iniciativas de aseguramiento.	I	I			C	R			C		I	I				C	A	R	C	C	C	C	C	C	C	C

MEA02 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
MEA02.01 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.	APO12.04	Resultados de las evaluaciones de riegos realizadas por terceros	Resultados de las revisiones y supervisión del control interno	EDM01.03 Todo APO Todo BAI Todo DSS Todo MEA
	APO13.03	Informes de auditoría del SGSI	Resultados de estudios comparativos y otras evaluaciones	EDM01.03 Todo APO Todo BAI Todo DSS Todo MEA
	Fuera del Ámbito de COBIT	Estándares y buenas prácticas de la industria		

Actividades	**Nivel de capacidad**
1. Realizar actividades de evaluación y supervisión del control interno basadas en los estándares de gobierno organizativos y los marcos y prácticas aceptadas en la industria. Incluir el seguimiento y evaluación de la eficiencia y efectividad de las revisiones de supervisión de la Dirección.	3
2. Considerar las evaluaciones independientes del sistema de control interno (p. ej. por auditoría interna o iguales - *peers*).	4
3. Identificar los límites del sistema de control interno de TI (p. ej., considerar cómo los controles internos organizativos de TI toman en consideración las actividades de producción o desarrollo externalizadas y/o deslocalizadas).	3
4. Asegurar que las actividades de control están operativas y que las excepciones son comunicadas puntualmente, seguidas y analizadas, y que se priorizan e implementan las acciones correctivas oportunas de acuerdo con el perfil de gestión del riesgo (p. ej., clasificar ciertas excepciones como riesgos clave y otras como riesgos no-clave).	3
5. Mantener el sistema de control interno de TI, considerando los cambios en curso en el negocio y el riesgo de TI, el entorno de control organizativo, los procesos de negocio y de TI relevantes y el riesgo de TI. Si existen lagunas, evaluar y recomendar cambios.	4
6. Evaluar regularmente el rendimiento del marco de control de TI, realizando estudios comparativos con los estándares y buenas prácticas aceptadas por la industria. Considerar la adopción formal de un enfoque de mejora continua en la supervisión de control interno.	3
7. Evaluar el estado de los controles internos de los proveedores externos de servicios y confirmar que dichos proveedores cumplen con los requisitos legales y regulatorios, así como las obligaciones contractuales.	3

Nivel de capacidad objetivo

3

			90,43
N	**P**	**L**	**F**
			90
			91
			90
			91
			92
			90
			89

Nivel de cumplimiento
Valor
90
91
90
91
92
90
89

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
MEA02.02 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.	BAI05.06	Resultados de la auditoría de cumplimiento	Evidencia de la efectividad del control	Interno
	BAI05.07	Revisiones del uso operativo		

Actividades	Nivel de capacidad
1. Entender y priorizar el riesgo de acuerdo con los objetivos organizativos.	3
2. Identificar los controles clave y desarrollar una estrategia adecuada para la validación de controles.	3
3. Identificar la información que indica de forma convincente si el entorno de control interno está operando de forma efectiva.	3
4. Desarrollar e implementar procedimientos eficientes para determinar si la información convincente está basada en los criterios de información.	3
5. Mantener evidencia de la efectividad del control.	4

			89,40
N	**P**	**L**	**F**
			92
			86
			92
			90
			87

Nivel de cumplimiento
Valor
92
86
92
90
87

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
MEA02.03 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.			Planes y criterios de autoevaluación	Todo APO Todo BAI Todo DSS Todo MEA
			Resultados de las autoevaluaciones	Interno
			Resultados de las revisiones de las autoevaluaciones	EDM01.03 Todo APO Todo BAI Todo DSS Todo MEA

Actividades	Nivel de capacidad
1. Mantener planes y alcances e identificar los criterios de evaluación para la realización de las autoevaluaciones. Planificar la comunicación de resultados del proceso de autoevaluación al negocio, TI y Dirección General y al Consejo. Considerar estándares de auditoría interna en el diseño de las autoevaluaciones.	3
2. Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua.	4
3. Asignar la responsabilidad de la autoevaluación a las personas oportunas con el fin de asegurar la objetividad y la competencia.	3
4. Proporcionar revisiones independientes para asegurar la objetividad de la autoevaluación y hacer posible compartir las buenas prácticas de control interno con otras compañías.	4
5. Comparar los resultados de las autoevaluaciones con estándares y buenas prácticas de la industria.	3
6. Resumir y comunicar los resultados de las autoevaluaciones y los estudios comparativos para considerar acciones correctivas.	3
7. Definir un enfoque consistente y consensuado para la realización de autoevaluaciones de control y para la coordinación con auditores internos y externos.	3

			91,29
N	**P**	**L**	**F**
			92
			87
			92
			95
			88
			95
			90

Nivel de cumplimiento
Valor
92
87
92
95
88
95
90

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

MEA02 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
MEA02.04 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.	APO11.05	Causas raíz de los fallos en la calidad de la entrega	Deficiencias de control	Todo APO Todo BAI Todo DSS Todo MEA
	APO12.06	Causas raíz relacionadas con el riesgo		
	DSS06.01	• Análisis de las causas raíz y recomendaciones • Resultados de las revisiones de efectividad del procesamiento	Acciones correctivas	Todo APO Todo BAI Todo DSS Todo MEA
	DSS06.04	Evidencia de la corrección y remediación de errores		

Actividades	Nivel de capacidad
1. Identificar, comunicar y registrar las excepciones de los controles y asignar responsabilidad de su resolución y comunicación de los resultados.	3
2. Considerar el riesgo para la empresa al establecer umbrales para el escalado de las excepciones y desajustes de los controles.	3
3. Comunicar los procedimientos de escalado de las excepciones de control, análisis de causas raíz e información a los propietarios del proceso y grupos de interés de TI.	3
4. Decidir qué excepciones de control deberían ser comunicadas a la persona responsable de la función y qué excepciones deberían ser escaladas. Informar a las partes interesadas y propietarios de los procesos afectados.	3
5. Hacer seguimiento de todas las excepciones para asegurar que se han contemplado las acciones acordadas.	3
6. Identificar, iniciar, rastrear e implementar acciones correctivas que surjan de la evaluación de control e informes.	3

			90,67
N	**P**	**L**	**F**
			90
			92
			90
			89
			89
			94

Nivel de cumplimiento
Valor
90
92
90
89
89
94

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA02.05 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.			Resultados de las evaluaciones del proveedor de aseguramiento	Interno

Actividades	Nivel de capacidad
1. Establecer la adhesión a los códigos de ética y estándares aplicables (p. ej., el Código de Ética Profesional de ISACA) y estándares de aseguramiento (relativos a la industria o ámbito geográfico), p. ej. Estándares de aseguramiento y auditoría de TI de ISACA y Marco Internacional para el Aseguramiento del Comité Internacional para los Estándares de Auditoría y Aseguramiento (IAASB).	3
2. Establecer la independencia de los proveedores de aseguramiento.	3
3. Establecer la competencia y cualificación de los proveedores de aseguramiento.	3

			89,33
N	P	L	F
			92
			90
			86

Nivel de cumplimiento
Valor
92
90
86

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA02.06 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.	BAI01.05	Planes de auditoría de programas	Evaluaciones de alto nivel	Interno
	DSS01.02	Planes de aseguramiento independiente	Planes de aseguramiento	EDM01.03 Todo APO Todo BAI Todo DSS Todo MEA
			Criterios de evaluación	Interno

Actividades	Nivel de capacidad
1. Determinar los destinatarios de las salidas de la iniciativa de aseguramiento y el objeto de la revisión.	3
2. Realizar una evaluación del riesgo a alto nivel y/o evaluar la capacidad del proceso para diagnosticar el riesgo e identificar los procesos críticos de TI.	3
3. Seleccionar, adaptar y llegar a un acuerdo sobre los objetivos de control para los procesos críticos que serán la base para la evaluación de control.	3

			88,67
N	P	L	F
			86
			90
			90

Nivel de cumplimiento
Valor
86
90
90

Nivel de cumplimiento objetivo	
Meta	Observación
F	Cumplida
F	Cumplida
F	Cumplida

MEA02 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
MEA02.07 Estudiar las iniciativas de aseguramiento. Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.	APO11.05	Causas raíz de los fallos en la calidad de la entrega	Alcance de la revisión del aseguramiento	Interno
	APO12.06	Causas raíz relacionadas con el riesgo	Plan de participación	Interno
	DSS06.01	Análisis de las causas raíz y recomendaciones	Prácticas de revisión del aseguramiento	Interno
	MEA03.04	Informes de incidentes de incumplimiento y causas raíz.		

Actividades	**Nivel de capacidad**
1. Definir el alcance actual mediante la identificación de los objetivos empresariales y de TI para el entorno bajo estudio, el conjunto de procesos y recursos de TI y todas las entidades auditables relevantes dentro de la compañía y externas a la compañía (p. ej. proveedores de servicios), si aplica.	3
2. Definir el plan de participación y los recursos necesarios.	4
3. Definir las prácticas de recolección y evaluación de la información de los procesos bajo revisión para identificar los controles a ser validados y los hallazgos reales (tanto aseguramiento positivo como cualquier deficiencia) para la evaluación del riesgo.	3
4. Definir prácticas para validar el diseño de controles y resultados y determinar si el nivel de efectividad es compatible con el riesgo aceptable (requerido por la evaluación de riesgos organizativos o de los procesos).	3
5. Donde la efectividad del control no es aceptable, definir prácticas para identificar el riesgo residual (en preparación para los informes).	3

			90,80
N	**P**	**L**	**F**
			92
			90
			95
			90
			87

Nivel de cumplimiento
Valor
92
90
95
90
87

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Práctica de Gestión	Entradas		Salidas	
	De	**Descripción**	**Descripción**	**A**
MEA02.08 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.	APO11.05	Causas raíz de los fallos en la calidad de la entrega	Alcance refinado	Todo APO Todo BAI Todo DSS Todo MEA
	APO12.04	Análisis de riesgo e informes de perfil de riesgo para las partes interesadas	Resultados de la revisión de aseguramiento	EDM05.01 EDM05.03 Todo APO Todo BAI Todo DSS Todo MEA
	APO12.06	Causas raíz relacionadas con el riesgo		
	DSS05.02	Resultados de las pruebas de intrusión		
	DSS06.01	Análisis de las causas raíces y recomendaciones	Informe de la revisión de aseguramiento	EDM05.03 Todo APO Todo BAI Todo DSS Todo MEA
	MEA03.03	Deficiencias de cumplimiento detectadas		

Actividades	Nivel de capacidad
1. Refinar la comprensión en materia de aseguramiento de TI.	3
2. Refinar el alcance de los objetivos de control clave en materia de aseguramiento de TI.	3
3. Probar la efectividad del diseño de control de los objetivos clave de control.	4
4. Alternativamente/adicionalmente probar los resultados de los objetivos clave de control.	3
5. Documentar el impacto de las debilidades de control.	3
6. Comunicarse con la Dirección durante la ejecución de la iniciativa para que haya un entendimiento claro del trabajo realizado, así como conformidad y aceptación de los hallazgos preliminares y recomendaciones.	3
7. Supervisar las actividades de aseguramiento y asegurar que el trabajo realizado está completo, cumple con sus objetivos y tiene una calidad aceptable.	3
8. Proveer a la Dirección de un informe (alineado con los términos de referencia, alcance y estándares de comunicación acordados) que respalde los resultados de la iniciativa y haga hincapié en las cuestiones clave y las acciones importantes.	3

			90,75
N	**P**	**L**	**F**
			92
			90
			95
			94
			86
			87
			90
			92

Nivel de cumplimiento
Valor
92
90
95
94
86
87
90
92

Nivel de cumplimiento objetivo	
Meta	**Observación**
F	Cumplida
F	Cumplida
	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida
F	Cumplida

Tabla 36. Hoja de hallazgos de la Empresa “La Bahía”

REF P/T	N° HALLAZGO	CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIONES
E.D.M. 5/20	**1**	En la aplicación de la metodología COBIT en la actividad Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno, se obtuvo un nivel de capacidad de 4 y su nivel de cumplimiento alcanzable del 85%, que no está dentro de los parámetros establecidos, es decir existe un desconocimiento de la legislación que regula las TI por parte de la empresa.	La norma **ISO 15504** es aquella norma que tiene como objetivo principal evaluar la utilización que tiene la empresa para analizar que el sistema sea de calidad respecto a los procesos importantes para la empresa en el desarrollo de productos, es decir los procesos de producción de software, la gestión de operaciones, el mantenimiento de productos o soportes técnicos. Es por ello que en el inciso 4.1 En el modelo de evaluación de la noma se plantean diferentes aspectos a considerar para obtener la certificación que permite a la organización identificar el nivel de cumplimiento con el nivel de calidad de un total de 5 niveles. La norma **ISO / IEC 38500** es de alto nivel que aborda el Gobierno corporativo de las TI., la misma que es basada en principios estándar de asesoramiento. Además, se puede mencionar que aparte de proporcionar una orientación general sobre el papel de un órgano rector, también fomenta a las organizaciones a utilizar las normas necesarias para gestionar su gobierno de las TI. Finalmente, el objetivo de este estándar es proporcionar una serie de principios que pueda usar la Dirección al evaluar, dirigir y supervisar el uso de las TI en sus organizaciones.	El personal desconoce la legislación que normaliza las TI, porque la empresa no posee un plan de capacitación constante sobre las normativas y manuales que sistematizan los procesos informáticos. Además, no cuentan con una gestión eficiente sobre los riesgos que pueden ocurrir en la empresa.	La Gerencia no tome decisiones asertivas en cuanto al mejoramiento y regulación de las TI.	**Dirigido al Gerente:** Diseñar un plan de capacitación para los trabajadores sobre la normativa legal de las TI.
E.D.M. 10/20	**2**	En la metodología COBIT en la actividad Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa, la misma que tiene un nivel de capacidad 3 y nivel de cumplimiento alcanzable del 85%, dando como resultado que no dispone de una guía en donde se establezcan los parámetros de las TI.		La Gerencia desconoce la importancia de las TI en la empresa porque no tiene una capacitación constante sobre los beneficios que dan las TI, es por ello que la empresa no mejora en la parte tecnológica.	La empresa tenga una desventaja que con lleva a un manejo incorrecto de las responsabilidades que poseen las TI.	**Dirigido al Gerente:** Capacitarse constantemente en cuanto al manejo y responsabilidades de las TI.
E.D.M 15/20	**3**	En la actividad de la metodología COBIT Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes se tiene un nivel de capacidad 4 y su nivel de cumplimiento alcanzable del 85%, por lo cual se le dificulta el reconocimiento al rendimiento de los recursos informáticos.		Por parte de la Gerencia existe una falta de control al rendimiento de los recursos informáticos que debe tener una empresa, por lo tanto, no se está cumpliendo los objetivos planteados correctamente.	La empresa no ocupa un 100% sus recursos informáticos, por lo cual puede existir un inadecuado manejo de estos.	**Dirigido al Gerente:** Auditar el estado de todos los recursos informáticos de la empresa periódicamente.

A.P.O. 10/30	**4**	En la aplicación de la metodología COBIT en la actividad Tener en cuenta los requisitos desde la empresa y la continuidad del servicio de TI a la hora de definir los roles, incluyendo el respaldo por parte de la plantilla y los requisitos de formación interdisciplinar, se menciona que tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, es decir que los empleados no poseen un conocimiento amplio acerca de las TI.		La administración no tiene un conocimiento claro acerca de la importancia de las TI en la empresa, teniendo en cuenta que desempeñan un papel importante, para que de esta manera puedan cumplir correctamente los objetivos.	Los empleados no ocupen adecuadamente las TI y a la vez poseen un desconocimiento de las normas y manuales que acogen a los activos informáticos.	**Dirigido al Gerente:** Coordinar incentivos a los empleados que usen y cuiden correctamente las TI.
A.P.O. 10/30	**5**	La metodología COBIT analiza la actividad Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. Además, el nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas, por lo cual está actividad tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 80%, es por ello que la empresa no dispone de un supervisor de recursos y responsabilidades de los activos informáticos.	La norma **ISO 15504** es una norma de evaluación utilizada por las empresas para evaluar su sistema de calidad respecto a los procesos relevantes para la compañía en el desarrollo de productos, como son los procesos de producción de software, gestión de operaciones, mantenimiento de productos o soporte técnico. De esta manera, permite que la organización que utiliza esta norma de evaluación identifica que un nivel de cumplimiento con la calidad de un total de 5 niveles. Además, la norma **ISO 15504**, es una norma de mejora continua, puesto que, una vez identificado el nivel de la empresa, se proporciona directrices para poder alcanzar el siguiente nivel.	Todos los empleados pueden utilizar el mismo activo informático, es por ello que no existe un responsable de cada uno de ellos. Además, no se ocupa las actas de entrega de los activos informáticos que va a utilizar en el puesto de trabajo.	La Gerencia empiece a sentir complicaciones al momento de solucionar un problema ante las TI.	**Dirigido al Gerente:** Establecer como política que el empleado que tenga un activo informático deberá firmar un acta de entrega, la misma que facilitará a la persona encargada de supervisar y monitorear las TI.
B.A.I 5/23	**6**	En la metodología COBIT en la actividad analizada dice Obtener revisiones de calidad completas y de cada fase clave del proyecto, iteración o versión comparando los resultados obtenidos contra los criterios originales de aceptación, por lo tanto, disponer de la firma del patrocinador y otros interesados en cada revisión de calidad. Dando como resultado que posee un nivel de capacidad 3 y un nivel de cumplimiento alcanzable del 85%, por lo cual la empresa no realiza periódicamente controles de calidad de las TI.		La Gerencia desconoce la importancia de controlar la calidad que nos está brindando las TI en la empresa.	La empresa tendrá un avance tecnológico muy lento y no permitirá proyectar a sus clientes una mejora tecnológica.	**Dirigido al Gerente:** Implementar una guía con los niveles de riesgo y oportunidad que tienen las TI, ayudando a mejorar el control de las mismas.

D.S.S. 7/36	**7**	En la actividad de la metodología COBIT Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados. Se obtuvo un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, por consiguiente, no hay un responsable para dar apoyo a los servicios extras que da la empresa.	Esta norma internacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma **ISO/IEC 27001[10]** o bien como documento guía para organizaciones que implanten controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de la seguridad de la información en industrias y organizaciones específicas, teniendo en cuenta su(s) entorno(s) específico(s) de riesgo de seguridad de la información. * En el apartado 5 menciona las políticas de seguridad de la información, en el ítem 5.1 las directrices de gestión de la seguridad de la información juntamente con las políticas.	Los administradores no identifican, ni conocen el proceso que tienen las TI en cuanto a los inconvenientes que poseen, es por ello que los empleados no reconocen fácilmente las soluciones adecuadas ante los problemas de las TI.	Las TI no tienen una actividad eficiente dentro de la empresa y al momento en que se presente un problema en cuanto a las TI, no podrán operar de manera correcta ante cualquier adversidad.	**Dirigido al Gerente:** Establecer como responsabilidad que todos los empleados deben mantenerse informados sobre los servicios que se entrega a los clientes.
D.S.S. 29/36	**8**	La metodología COBIT tiene como actividad Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios. Además, tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, es por ello que la empresa posee un antivirus para combatir a cualquier programa o virus malicioso pero el respaldo de información no se realiza frecuentemente.	La norma **ISO 15504** es una norma de evaluación utilizada por las empresas para evaluar su sistema de calidad respecto a los procesos relevantes para la compañía en el desarrollo de productos, como son los procesos de producción de software, gestión de operaciones, mantenimiento de productos o soporte técnico. De esta manera, permite que la organización que utiliza esta norma de evaluación identifica que un nivel de cumplimiento con la calidad de un total de 5 niveles. Además, la norma **ISO 15504**, es una norma de mejora continua, puesto que, una vez identificado el nivel de la empresa, se proporciona directrices para poder alcanzar el siguiente nivel.	La tecnología va avanzando día a día es por ello que se debe tener un software que cuide la información de la empresa. Por lo tanto, la Gerencia debe invertir en un software que realice respaldos de información frecuentemente, es decir automáticamente.	La información estaría resguardada tecnológicamente y a la vez obtendríamos un respaldo instantáneo.	**Dirigido al Gerente:** Invertir en un software tecnológico avanzado que proporcione seguridad total efectiva de las TI.

Auditoría Líder
¡Te ayudamos a conocer la realidad de tu empresa!

INFORME DE RESULTADOS

Empresa “La Bahía”

APLICACIÓN DE LA METODOLOGÍA COBIT 5 EN LOS PROCESOS INFORMÁTICOS EN LA EMPRESA LA BAHÍA

SIGLAS Y/O ABREVIATURAS UTILIZADAS

SIGLAS Y/O ABREVIATURAS	SIGNIFICADO
SGSI	Sistema de Gestión de Seguridad de la Información
COBIT	Control Objectives for Information and related Technology
SI	Sistemas de Información
TI	Tecnologías de Información
ISO	Internacional Organization for Standardization
CGE	Contraloría General del Estado

Auditoría Líder
¡Te ayudamos a conocer la realidad de tu empresa!

Ambato, 23 de marzo de 2022

Sra.
Rosa Benigna Torres Rodríguez
Gerente General
Presente. -
De mi consideración:

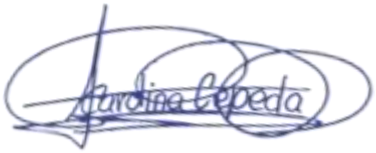
Hemos efectuado la evaluación de elementos importantes en la evaluación del control interno mediante la metodología COBIT en la Empresa “La Bahía”.

El examen se efectuó de acuerdo con los Estándares de normas ISO y marcos de referencia. Además, se ha considerado diversos factores informáticos que pueden estar influyendo en las operaciones de la empresa, igualmente que las actividades a las cuales corresponden se hayan ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables, a fin de brindar recomendaciones a las posibles soluciones que garanticen un óptimo resultado en cuanto al gobierno y gestión de las TI, así como al cumplimiento de controles y procedimientos adecuados.

El objetivo de la evaluación de control interno se enmarca al correcto funcionamiento del SGSI, considerando como alcance la evaluación de activos informáticos, el nivel de cumplimiento en cuanto al control interno informático en base a sus catalizadores, identificación y evaluación de niveles de capacidad a los procesos informáticos.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en los criterios, conclusiones y recomendaciones que constan en el presente informe.

Atentamente,



Eliana Carolina Cepeda Cruz
SENIOR DE LA FIRMA DE AUDITORES AUDITORÍA LÍDER

RESULTADOS DEL EXAMEN

1. *En la aplicación de la metodología COBIT en la actividad Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno, se obtuvo un nivel de capacidad de 4 y su nivel de cumplimiento alcanzable del 85%, que no está dentro de los parámetros establecidos, es decir existe un desconocimiento de la legislación que regula las TI por parte de la empresa*.

Comentario

El personal desconoce la legislación que normaliza las TI, porque la empresa no posee un plan de capacitación constante sobre las normativas y manuales que sistematizan los procesos informáticos. Además, no cuentan con una gestión eficiente sobre los riesgos que pueden ocurrir en la empresa. Lo que conlleva a que la Gerencia no tome decisiones asertivas en cuanto al mejoramiento y regulación de las TI.

Conclusión

Según la Norma 500 Información y Comunicación se incumple el parámetro de la 500-02 Canales de comunicación abiertos. Se establecerán canales de comunicación abiertos, que permitan trasladar la información de manera segura, correcta y oportuna a los destinatarios dentro y fuera de la institución. Las entidades que ofrezcan servicios en línea deberán publicar y mantener en su página web los horarios de operación de los sistemas en línea, a fin de facilitar a los usuarios su acceso. Una política de comunicación interna debe permitir las diferentes interacciones entre las servidoras y senadores, cualquiera sea el rol que desempeñen, así como entre las distintas unidades administrativas de la institución. Las entidades dispondrán de canales abiertos de comunicación que faculten a los usuarios aportar información sobre el diseño y la calidad de los productos y servicios brindados, que servirá para considerar la implementación de cambios que permitan un funcionamiento adecuado y permanente, así como su mejora continua. Causando como efecto que no se encuentra la información pertinente de la Cooperativa en páginas web, los socios y demás personas desconocen de información importante que debería ser de su conocimiento, dado a que

es una institución que ofrece servicios a la sociedad.

Recomendaciones

Dirigido a la Gerencia que debe diseñar un plan de capacitación para los trabajadores sobre la normativa legal de las TI.

2. *En la metodología COBIT en la actividad Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa, la misma que tiene un nivel de capacidad 3 y nivel de cumplimiento alcanzable del 85%, dando como resultado que no dispone de una guía en donde se establezcan los parámetros de las TI.*

Comentario

La Gerencia desconoce la importancia de las TI en la empresa porque no tiene una capacitación constante sobre los beneficios que dan las TI, es por ello que la empresa no mejora en la parte tecnológica. Dando como resultado que la empresa tenga una desventaja, que con lleva a un manejo incorrecto de las responsabilidades que poseen las TI.

Conclusión

La norma ISO 15504 es aquella norma que tiene como objetivo principal evaluar la utilización que tiene la empresa para analizar que el sistema sea de calidad respecto a los procesos importantes para la empresa en el desarrollo de productos, es decir los procesos de producción de software, la gestión de operaciones, el mantenimiento de productos o soportes técnicos. Es por ello que en el inciso 4.1 En el modelo de evaluación de la noma se plantean diferentes aspectos a considerar para obtener la certificación que permite a la organización identificar el nivel de cumplimiento con el nivel de calidad de un total de 5 niveles.

La norma ISO / IEC 38500 es de alto nivel que aborda el Gobierno corporativo de las TI., la misma que es basada en principios estándar de asesoramiento. Además, se puede mencionar que aparte de proporcionar una orientación general sobre el papel de un

órgano rector, también fomenta a las organizaciones a utilizar las normas necesarias para gestionar su gobierno de las TI. Finalmente, el objetivo de este estándar es proporcionar una serie de principios que pueda usar la Dirección al evaluar, dirigir y supervisar el uso de las TI en sus organizaciones.

Recomendaciones

Dirigido al Gerente que debe capacitarse constantemente en cuanto al manejo y responsabilidades de las TI.

3. *En la actividad de la metodología COBIT Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes se tiene un nivel de capacidad 4 y su nivel de cumplimiento alcanzable del 85%, por lo cual se le dificulta el reconocimiento al rendimiento de los recursos informáticos.*

Comentario

Por parte de la Gerencia existe una falta de control al rendimiento de los recursos informáticos que debe tener una empresa, por lo tanto, no se está cumpliendo los objetivos planteados correctamente. Así mismo, la empresa no ocupa un 100% sus recursos informáticos, por lo cual puede existir un inadecuado manejo de los mismos.

Conclusión

La norma ISO 15504 es aquella norma que tiene como objetivo principal evaluar la utilización que tiene la empresa para analizar que el sistema sea de calidad respecto a los procesos importantes para la empresa en el desarrollo de productos, es decir los procesos de producción de software, la gestión de operaciones, el mantenimiento de productos o soportes técnicos. Es por ello que en el inciso 4.1 En el modelo de evaluación de la noma se plantean diferentes aspectos a considerar para obtener la certificación que permite a la organización identificar el nivel de cumplimiento con el nivel de calidad de un total de 5 niveles.

La norma ISO / IEC 38500 es de alto nivel que aborda el Gobierno corporativo de las TI., la misma que es basada en principios estándar de asesoramiento. Además, se puede mencionar que aparte de proporcionar una orientación general sobre el papel de un órgano rector, también fomenta a las organizaciones a utilizar las normas necesarias para gestionar su gobierno de las TI. Finalmente, el objetivo de este estándar es proporcionar una serie de principios que pueda usar la Dirección al evaluar, dirigir y supervisar el uso de las TI en sus organizaciones.

Recomendaciones

Dirigido al Gerente en primer lugar auditar el estado de todos los recursos informáticos de la empresa periódicamente.

4. *En la aplicación de la metodología COBIT en la actividad Tener en cuenta los requisitos desde la empresa y la continuidad del servicio de TI a la hora de definir los roles, incluyendo el respaldo por parte de la plantilla y los requisitos de formación interdisciplinar, se menciona que tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, es decir que los empleados no poseen un conocimiento amplio acerca de las TI.*

Comentario

La administración no tiene un conocimiento claro acerca de la importancia de las TI en la empresa, teniendo en cuenta que desempeñan un papel importante, para que de esta manera puedan cumplir correctamente los objetivos. A su vez los empleados no ocupan adecuadamente las TI y al mismo tiempo poseen un desconocimiento de las normas y manuales que acogen a los activos informáticos.

Conclusión

La norma ISO 15504 es aquella norma que tiene como objetivo principal evaluar la utilización que tiene la empresa para analizar que el sistema sea de calidad respecto a los procesos importantes para la empresa en el desarrollo de productos, es decir los procesos de producción de software, la gestión de operaciones, el mantenimiento de productos o soportes técnicos. Es por ello que en el inciso 4.1 En el modelo de

evaluación de la noma se plantean diferentes aspectos a considerar para obtener la certificación que permite a la organización identificar el nivel de cumplimiento con el nivel de calidad de un total de 5 niveles.

La norma ISO / IEC 38500 es de alto nivel que aborda el Gobierno corporativo de las TI., la misma que es basada en principios estándar de asesoramiento. Además, se puede mencionar que aparte de proporcionar una orientación general sobre el papel de un órgano rector, también fomenta a las organizaciones a utilizar las normas necesarias para gestionar su gobierno de las TI. Finalmente, el objetivo de este estándar es proporcionar una serie de principios que pueda usar la Dirección al evaluar, dirigir y supervisar el uso de las TI en sus organizaciones.

Recomendaciones

Dirigido al Gerente que debe coordinar algunos incentivos a los empleados que usen y cuiden correctamente las TI.

5. *La metodología COBIT analiza la actividad Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. Además, el nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas, por lo cual está actividad tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 80%, es por ello que la empresa no dispone de un supervisor de recursos y responsabilidades de los activos informáticos.*

Comentario

Todos los empleados pueden utilizar el mismo activo informático, es por ello que no existe un responsable de cada uno de ellos. Además, no se ocupa las actas de entrega de los activos informáticos que va a utilizar en el puesto de trabajo. De la misma forma la Gerencia, empiece a sentir complicaciones al momento de solucionar un problema

ante las TI.

Conclusión

La norma ISO 15504 es una norma de evaluación utilizada por las empresas para evaluar su sistema de calidad respecto a los procesos relevantes para la compañía en el desarrollo de productos, como son los procesos de producción de software, gestión de operaciones, mantenimiento de productos o soporte técnico. De esta manera, permite que la organización que utiliza esta norma de evaluación, identifica que un nivel de cumplimiento con la calidad de un total de 5 niveles.

Además, la norma ISO 15504, es una norma de mejora continua, puesto que, una vez identificado el nivel de la empresa, se proporciona directrices para poder alcanzar el siguiente nivel.

Recomendaciones

Dirigido al Gerente que debe implementar una guía con los niveles de riesgo y oportunidad que tienen las TI, ayudando a mejorar el control de las mismas.

6. *En la metodología COBIT en la actividad analizada dice Obtener revisiones de calidad completas y de cada fase clave del proyecto, iteración o versión comparando los resultados obtenidos contra los criterios originales de aceptación, por lo tanto, disponer de la firma del patrocinador y otros interesados en cada revisión de calidad. Dando como resultado que posee un nivel de capacidad 3 y un nivel de cumplimiento alcanzable del 85%, por lo cual la empresa no realiza periódicamente controles de calidad de las TI.*

Comentario

La Gerencia desconoce la importancia de controlar la calidad que nos está brindando las TI en la empresa. Posiblemente la empresa tendrá un avance tecnológico muy lento y no permitirá proyectar a sus clientes una mejora tecnológica.

Conclusión

La norma ISO 15504 es una norma de evaluación utilizada por las empresas para evaluar su sistema de calidad respecto a los procesos relevantes para la compañía en el desarrollo de productos, como son los procesos de producción de software, gestión de operaciones, mantenimiento de productos o soporte técnico. De esta manera, permite que la organización que utiliza esta norma de evaluación, identifica que un nivel de cumplimiento con la calidad de un total de 5 niveles.

Además, la norma ISO 15504, es una norma de mejora continua, puesto que, una vez identificado el nivel de la empresa, se proporciona directrices para poder alcanzar el siguiente nivel.

Recomendaciones

Dirigido al Gerente que se debe implementar una guía con los niveles de riesgo y oportunidad que tienen las TI, ayudando a mejorar el control de estas.

7. *En la actividad de la metodología COBIT Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados. Se obtuvo un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, por consiguiente, no hay un responsable para dar apoyo a los servicios extras que da la empresa.*

Comentario

Los administradores no identifican, ni conocen el proceso que tienen las TI en cuanto a los inconvenientes que poseen, es por lo que los empleados no reconocen fácilmente las soluciones adecuadas ante los problemas de las TI. Es necesario recalcar que las TI no tienen una actividad eficiente dentro de la empresa y al momento en que se presente un problema en cuanto a las TI, no podrán operar de manera correcta ante cualquier adversidad.

Conclusión

Esta norma internacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma

ISO/IEC 27001[10] o bien como documento guía para organizaciones que implanten controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de la seguridad de la información en industrias y organizaciones específicas, teniendo en cuenta su(s) entorno(s) específico(s) de riesgo de seguridad de la información.

* En el apartado 5 menciona las políticas de seguridad de la información, en el ítem 5.1 las directrices de gestión de la seguridad de la información conjuntamente con las políticas.

Recomendaciones

Dirigido al Gerente que se debe establecer como responsabilidad que todos los empleados deben mantenerse informados sobre los servicios que se entrega a los clientes.

8. *La metodología COBIT tiene como actividad Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios. Además, tiene un nivel de capacidad 3 y su nivel de cumplimiento alcanzable del 85%, es por ello que la empresa posee un antivirus para combatir a cualquier programa o virus malicioso pero el respaldo de información no se realiza frecuentemente.*

Comentario

La tecnología va avanzando día a día es por ello que se debe tener un software que cuide la información de la empresa. Por lo tanto, la Gerencia debe invertir en un software que realice respaldos de información frecuentemente, es decir automáticamente. Por esta razón la información estaría resguardada tecnológicamente y a la vez obtendríamos un respaldo instantáneo.

Conclusión

La norma ISO 15504 es una norma de evaluación utilizada por las empresas para evaluar su sistema de calidad respecto a los procesos relevantes para la compañía en

el desarrollo de productos, como son los procesos de producción de software, gestión de operaciones, mantenimiento de productos o soporte técnico. De esta manera, permite que la organización que utiliza esta norma de evaluación, identifica que un nivel de cumplimiento con la calidad de un total de 5 niveles.

Además, la norma ISO 15504, es una norma de mejora continua, puesto que, una vez identificado el nivel de la empresa, se proporciona directrices para poder alcanzar el siguiente nivel.

Recomendación

Dirigido al Gerente que se debe invertir en un software tecnológico avanzado que proporcione seguridad total efectiva de las TI.

GUÍA DE POLÍTICAS Y PROCEDIMIENTOS PARA LOS PROCESOS INFORMÁTICOS

3.3 Guía de políticas y procedimientos para los procesos informáticos

Se presenta a continuación la Guía de políticas y procedimientos que será sugerida a la empresa "LA BAHÍA" para que puedan analizar cada uno y ponerlas en práctica para que la empresa siga creciendo de mejor manera.

1. GOBIERNO Y CULTURA

El Gobierno tiene como objetivo principal reforzar la importancia de la gestión del riesgo que tiene la empresa instaurando responsabilidades que ayuden a la supervisión de cada uno de ellos (Instituto de Auditores Internos, 2017).

Se entiende como la cultura todos los valores éticos, comportamientos deseados y a la comprensión que tenga la entidad sobre los riesgos (Instituto de Auditores Internos, 2017).

MISIÓN

Ofrecer a nuestros clientes electrodomésticos de calidad a un precio económico, dándoles la mayor tranquilidad para que puedan solventar sus necesidades (Empresa La Bahía, 2022).

VISIÓN

Ser la empresa líder a nivel nacional en la venta de electrodomésticos, superando las expectativas de nuestros clientes e ir mejorando nuestra propuesta de negocio (Empresa La Bahía, 2022).

VALORES EMPRESARIALES

Los valores más importantes que tienen la empresa son:

- **Respeto:** Tratamos a todos con amabilidad dentro y fuera de la institución.
- **Puntualidad:** Todos respetamos el tiempo programado para cada actividad como también nuestro horario de trabajo.
- **Responsabilidad:** Cumplimos con cada uno de los requerimientos y

obligaciones que se ponga a cada empleado.

- **Eficiencia:** Tenemos la capacidad para hacer o cumplir adecuadamente nuestra función dentro de la empresa.
- **Liderazgo:** Nos comprendemos entre toda la empresa, siendo empáticos en momentos difíciles y también ayudándonos mutuamente para mantener un buen ambiente laboral.
- **Trabajo en equipo:** Cada uno de nosotros los empleados somos quienes nos motivamos a diario y nos organizamos para cumplir todas nuestras obligaciones correctamente.

ENTIDADES DE CONTROL

- Servicio de Rentas Internas
- Ministerio de Industrias y Productividad (MIPRO)
- Asociación de Almacenes de Electrodomésticos del Ecuador (Asadelec)

RECONOCIMIENTO DE LOS RIESGOS EN LOS PROCESOS INFORMÁTICOS

Para la elaboración de la ficha de la identificación de los riesgos se tomará en cuenta únicamente a los procesos informáticos.

Tabla 37. Tabla de reconocimiento de los Riesgos en los procesos informáticos – PROCESO 1 COMPRAS

La Bahía
tradición y economía

RECONOCIMIENTO DE LOS RIESGOS EN LOS PROCESOS INFORMÁTICOS

Este documento ayudará a mejorar los procesos informáticos, es por ello que es necesario que sea llenado con toda la sinceridad y responsabilida, teniendo en cuenta que será anónima.
- Se debe marcar con una X en el porcentaje que usted considere.

PROCESO 1 - COMPRAS

No.	DESCRIPCIÓN	GRAVEDAD DEL RIESGO				OBSERVACIÓN
		0% - 25%	26% - 50%	51% - 75%	76% - 100%	
1	Enviar el pedido de compra de inventario					
2	Ingreso de factura de compra al sistema					
3	Analización de las formas de pago					

Fuente: (Cepeda Carolina, 2022)

Tabla 38. Tabla de reconocimiento de los Riesgos en los procesos informáticos – PROCESO 2 VENTAS

La Bahía tradición y economía

RECONOCIMIENTO DE LOS RIESGOS EN LOS PROCESOS INFORMÁTICOS

Este documento ayudará a mejorar los procesos informáticos, es por ello que es necesario que sea llenado con toda la sinceridad y responsabilida, teniendo en cuenta que será anónima.
- Se debe marcar con una X en el porcentaje que usted considere.

PROCESO 2 - VENTAS

No.	DESCRIPCIÓN	GRAVEDAD DEL RIESGO				OBSERVACIÓN
		0% - 25%	26% - 50%	51% - 75%	76% - 100%	
1	Escoger en la lista de precios a cual corresponde el cliente.					
2	Elegir la forma de pago que pueden ser efectivo, cheque y tarjeta de crédito					
3	Se realiza la facturación electrónica.					

Fuente: (Cepeda Carolina, 2022)

Tabla 39. Tabla de reconocimiento de los Riesgos en los procesos informáticos – PROCESO 3 VENTAS

La Bahía tradición y economía

RECONOCIMIENTO DE LOS RIESGOS EN LOS PROCESOS INFORMÁTICOS

Este documento ayudará a mejorar los procesos informáticos, es por ello que es necesario que sea llenado con toda la sinceridad y responsabilida, teniendo en cuenta que será anónima.
- Se debe marcar con una X en el porcentaje que usted considere.

PROCESO 3 - CONTABILIDAD

No.	DESCRIPCIÓN	GRAVEDAD DEL RIESGO				OBSERVACIÓN
		0% - 25%	26% - 50%	51% - 75%	76% - 100%	
1	Ingresa la factura de venta al sistema					
2	Se verifica la forma de pago					
3	Inicia el proceso de contabilización					

Fuente: (Cepeda Carolina, 2022)

2. ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS

La estrategia y establecimiento de objetivos funcionan siempre juntos en el proceso de la planificación estratégica, en donde se establece la importancia

del riesgo, que continúa con la evaluación de estrategias alternativas y finaliza con la formulación de objetivos correctos para el negocio (Instituto de Auditores Internos, 2017).

IDENTIFICACIÓN DE OBJETIVOS DE LOS PROCESOS INFORMÁTICOS

A continuación, se procede a identificar los objetivos que tienen los procesos informáticos, los mismos que son clasificados en diferentes aspectos.

Tabla 40. Objetivos de los Procesos Informáticos

OBJETIVOS	
CUMPLIMIENTO	Fortalecer el cumplimiento de las normas, reglamentos, leyes, políticas y procedimientos para los procesos informáticos por parte de los empleados de la empresa.
OPERACIÓN	Examinar frecuentemente el correcto funcionamiento de los procesos informáticos.
FINANCIERO	Contabilizar correctamente los activos informáticos que forman parte de los procesos informáticos de manera confiable y oportuna.

Fuente: (Cepeda Carolina, 2022)

ESTRATEGIAS PARA RIESGOS EN LOS PROCESOS INFORMÁTICOS

Todo riesgo debe tener una estrategia para que puedan trabajar de mejor manera, cumpliendo objetivos y siendo eficientes en cada uno de los procesos.

Tabla 41. Estrategias para riesgos en los procesos informáticos

La Bahía
tradición y economía

ESTRATEGIAS PARA RIESGOS EN LOS PROCESOS INFORMÁTICOS

Este documento nos ayudará a mejorar en lo posible los procesos informáticos, es por ello que es necesario que sea llenado con toda la sinceridad y responsabilida, teniendo en cuenta que será anónima.

- Se debe marcar con una X en el porcentaje que usted considere.

PROCESO 1 - COMPRAS

No.	DESCRIPCIÓN	ESTRATEGIA	VALORACION DE LA ESTRATEGIA				OBSERVACIÓN
			0% - 25%	26% - 50%	51% - 75%	76% - 100%	
1	Enviar el pedido de compra de inventario	Tener un archivo de excel en donde se vaya alimentando automáticamente cada uno de los pedidos de compra.					
2	Ingreso de factura de compra al sistema						
3	Analización de las formas de pago	Analizar minuciosamente la forma de pago por la compra del inventario y verificando los beneficios que nos da.					

PROCESO 2 - VENTAS							
No.	DESCRIPCIÓN	ESTRATEGIA	VALORACIÓN DE LA ESTRATEGIA				OBSERVACIÓN
			0% - 25%	26% - 50%	51% - 75%	76% - 100%	
1	Escoger en la lista de precios a cual corresponde el cliente.	Informar al cliente el regalo que tiene por comprar en la empresa y sus ventajas.					
2	Elegir la forma de pago que pueden ser efectivo, cheque y tarjeta de crédito	Explicar cada una de las formas de pago que tiene el cliente y a la vez el descuento que tendrá por la compra en efectivo.					
3	Se realiza la facturación electrónica.	Enviar los comprobantes de venta por medio del sistema contable para que sean autorizados diariamente.					

PROCESO 3 - CONTABILIDAD							
No.	DESCRIPCIÓN	ESTRATEGIA	VALORACIÓN DE LA ESTRATEGIA				OBSERVACIÓN
			0% - 25%	26% - 50%	51% - 75%	76% - 100%	
1	Ingresa la factura de venta al sistema	Realizar auditorias diariamente como un cierre de ventas en donde se verifique que las ventas estén correctamente registradas.					
2	Se verifica la forma de pago	Crear un documento en donde se registre ordenadamente y cronológicamente con la fecha de la factura la forma de pago.					
3	Inicia el proceso de contabilización	Efectuar las concialeciones bancarias diariamente con la finalidad de tener un control de ingresos.					

Fuente: (Cepeda Carolina, 2022)

3. DESEMPEÑO

Es un componente importante, porque identifica y evalúa los riesgos que pueden afectar de una u otra manera a la empresa, por consiguiente, los riesgos son ordenados por prioridad en función a la gravedad, luego la empresa verifica cada uno de los riesgos y se procede a buscar una estrategia que ayude a solucionarlos, además los resultados de este proceso deben ser comunicados a las partes interesadas en el riesgo (Instituto de Auditores Internos, 2017).

INDICADORES PARA CADA RIESGO ENCONTRADO

En la empresa se encuentra algunos riesgos que afectan los procesos informáticos por lo que se sugiere a continuación algunos indicadores que servirán para que cada uno sea medible correctamente.

Tabla 42. Indicadores para medir los riesgos en los procesos informáticos

La Bahía
tradición y economía

INDICADORES PARA MEDIR LOS RIESGOS EN LOS PROCESOS INFORMÁTICOS

OBJETIVO	No.	DESCRIPCIÓN DEL RIESGO	INDICADORES
CUMPLIMIENTO	R1	El personal desconoce la legislación que normaliza las TI, porque la empresa no posee un plan de capacitación constante sobre las normativas y manuales que sistematizan los procesos informáticos. Además, no cuentan con una gestión eficiente sobre los riesgos que pueden ocurrir en la empresa.	$\frac{\text{Personal capacitado}}{\text{Total personal}} \times 100$
	R2	Por parte de la Gerencia existe una falta de control al rendimiento de los recursos informáticos que debe tener una empresa, por lo tanto, no se está cumpliendo los objetivos planteados correctamente.	$\frac{\text{Rendimiento de los recursos informáticos}}{\text{Rendimiento óptimo de los recursos informáticos}} \times 100$
	R3	La tecnología va avanzando día a día es por ello por lo que se debe tener un software que cuide la información de la empresa. Por lo tanto, la Gerencia debe invertir en un software que realice respaldos de información frecuentemente, es decir automáticamente.	$\frac{\text{Software Actualizado}}{\text{Total de Softwares}} \times 100$
	R4	La Gerencia desconoce la importancia de las TI en la empresa porque no tiene una capacitación constante sobre los beneficios que dan las TI, es por ello por lo que la empresa no mejora en la parte tecnológica.	$\frac{\text{Capacitaciones asistidas}}{\text{Capacitaciones sugeridas}} \times 100$

OPERACIÓN	R5	Todos los empleados pueden utilizar el mismo activo informático, es por ello por lo que no existe un responsable de cada uno de ellos. Además, no se ocupa las actas de entrega de los activos informáticos que va a utilizar en el puesto de trabajo.	$\frac{\text{Activos Informáticos con acta entrega}}{\text{Total de Activos Informáticos}} \times 100$
	R6	La Gerencia desconoce la importancia de controlar la calidad que nos está brindando las TI en la empresa.	$\frac{\text{Tiempo utilizado de los Activos Informáticos}}{\text{VIda útil de los Activos Informáticos}} \times 100$
	R7	Los administradores no identifican, ni conocen el proceso que tienen las TI en cuanto a los inconvenientes que poseen, es por ello por lo que los empleados no reconocen fácilmente las soluciones adecuadas ante los problemas de las TI.	$\frac{\text{Soluciones resueltas ante los problemas de las TI}}{\text{Total de problemas de las TI}} \times 100$
FINANCIERO	R8	Exista un mal registro de los activos informáticos por parte del Departamento Contable.	$\frac{\text{Activos Informáticos contabilizados}}{\text{Total de Activos Informáticos}} \times 100$

Fuente: (Cepeda Carolina, 2022)

LISTA DE ACTIVOS INFORMÁTICOS

La lista de activos Informáticos tiene como objetivo que la empresa identifique que cada uno tiene misión de mejorar y ayudar a la empresa a que cada día sea segura.

Tabla 43. Lista de Activos Informáticos

La Bahía
tradición y economía

LISTA DE ACTIVOS INFORMÁTICOS

No.	ACTIVO INFORMÁTICO	ÍCONO	REFERENCIA	APLICACIÓN		PORCENTAJE DE MEJORAMIENTO			
				SI	NO	0% - 25%	26% - 50%	51% - 75%	76% - 100%
1	Software DLP		Son programas de prevención de pérdidas de datos (DLP) los mismos que pueden ser implementados como medida de seguridad en la empresa para supervisar que ningún usuario esté copiando o compartiendo información o datos que no falsifiquen.						
2	Hardware de infraestructura		Incluye los dispositivos de red, los centros de datos, servidores físicos, etc.						
3	Contratos de arrendamiento de instalaciones e infraestructuras		Los contratos para acceder y usar las infraestructuras de terceros sí pueden considerarse activos.						
4	Software desarrollado en la empresa		Todo lo que su personal informático haya escrito o compilado internamente pertenece a su empresa.						
5	Licencias de software		Ocasionalmente denominado software comercialmente disponible, el concepto incluye los programas creados por otra persona por los que usted ha pagado una licencia para usarlos por un periodo de tiempo determinado. Tenga en cuenta que son las licencias las que constituyen los activos y no el software en sí.						
6	Dispositivos de usuario final propiedad de la empresa		Ordenadores de escritorio, monitores, impresoras, teléfonos y otros dispositivos de usuario final suelen considerarse activos informáticos.						
7	Sistema de Alimentación Ininterrumpida (SAI)		Dispositivo que permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.						

Fuente: (Cepeda Carolina, 2022)

Tabla 44. Políticas y procedimientos para los procesos informáticos

POLITICAS Y PROCEDIMIENTOS PARA LOS PROCESOS INFORMÁTICOS

ADQUISICIÓN DE ACTIVOS INFORMÁTICOS

POLÍTICAS ADMINISTRATIVAS

No.	DESCRIPCIÓN
1	Presentar la solicitud de requerimiento de compra de un activo informático.
2	El Gerente debe autorizar la compra del activo informático.
3	El Área Contable debe realizar un mínimo de cuatro cotizaciones de proveedores diferentes y seleccionar el adecuado.
4	Las compras de bienes deben respaldarse con su respectivo comprobante.
5	Los comprobantes de compra deben cumplir como lo menciona el Reglamento de Comprobantes de Venta, Retenciones y documentos complementarios.
6	Contabilidad debe realizar un registro contable sobre las nuevas adquisiciones de la empresa.
7	Archivar correctamente la documentación de las nuevas adquisiciones.
8	Todo activo informático debe tener su respectiva codificación en su etiqueta.

CONTROLES

No.	DESCRIPCIÓN
1	Codificar todos los bienes nuevos.
2	Elaborar actas de recepción de los activos informáticos al personal.
3	Realizar constataciones físicas frecuentemente.
4	Registrar en el sistema de manera correcta y oportuna el bien.
5	Etiquetar todos los bienes nuevos.
6	Elaborar actas de entrega de los activos informáticos al personal.

PROCEDIMIENTOS

No.	DESCRIPCIÓN	RESPONSABLE
1	Realiza la notificación de compra de un activo informático	Empleado
2	Recepta la solicitud del requerimiento.	Contabilidad
3	Cotiza y selecciona al proveedor ideal	Contabilidad
4	Elabora la orden de compra del bien.	Contabilidad
5	Autoriza la orden de compra	Gerente
6	Envía la orden de compra al proveedor	Contabilidad
7	Recibe la factura de la compra	Contabilidad
8	Recibe el bien requerido	Bodega
9	Verifica el correcto funcionamiento del bien	Bodega
10	Se procede a codificar el bien mediante una etiqueta	Bodega
11	Ingresa el bien a la lista de activos informáticos	Contabilidad
12	Entrega el acta de recepción del bien	Contabilidad
13	Recibe y firma el acta de recepción del bien	Empleado

Fuente: (Cepeda Carolina, 2022)

Tabla 45. Políticas y procedimientos para los procesos informáticos

	POLITICAS Y PROCEDIMIENTOS PARA LOS PROCESOS INFORMÁTICOS
MANTENIMIENTO DE ACTIVOS INFORMÁTICOS	
POLÍTICAS ADMINISTRATIVAS	

No.	DESCRIPCIÓN
1	Todo mantenimiento de los activos informáticos deberá ser autorizados por Gerencia.
2	El activo que haya tenido el respectivo mantenimiento deberá tener una etiqueta que lo distinga.
3	El mantenimiento del activo se realizará previa solicitud.
4	Llevar una respectiva lista de los activos que ya fueron dados el mantenimiento.

CONTROLES

No.	DESCRIPCIÓN
1	Codificar todos los activos informáticos que fueron dados el mantenimiento.
2	Elaborar actas de recepción de los activos informáticos al personal en donde conste que su funcionamiento es óptimo.
3	Realizar constataciones físicas frecuentemente.

PROCEDIMIENTOS

No.	DESCRIPCIÓN	RESPONSABLE
1	Presentar una solicitud para el mantenimiento del activo informático.	Empleado
2	Autoriza la solicitud del mantenimiento del activo informático.	Gerencia
3	Realizar el respectivo mantenimiento.	Personal responsable de las TI
4	Llevar una lista de los activos que ya fueron parte de un mantenimiento.	Personal responsable de las TI
5	Ubicar una etiqueta en el bien que se distinga que ya fue dado el mantenimiento.	Personal responsable de las TI
6	Firmar el acta de recepción del correcto funcionamiento del bien.	Empleado

Fuente: (Cepeda Carolina, 2022)

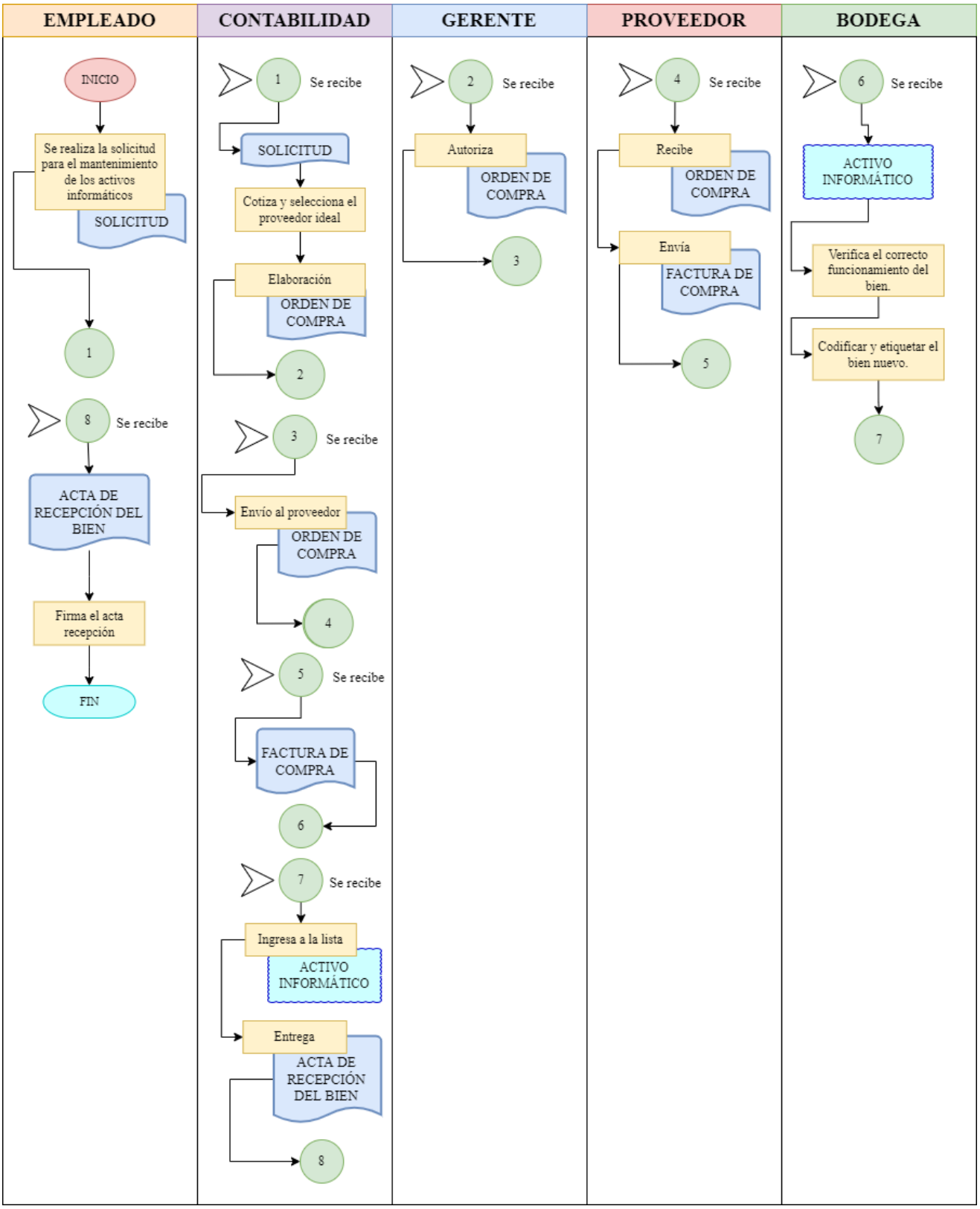


Gráfico 24. Flujograma de Políticas y procedimientos para los procesos informáticos – adquisición

Fuente: (Cepeda Carolina, 2022)

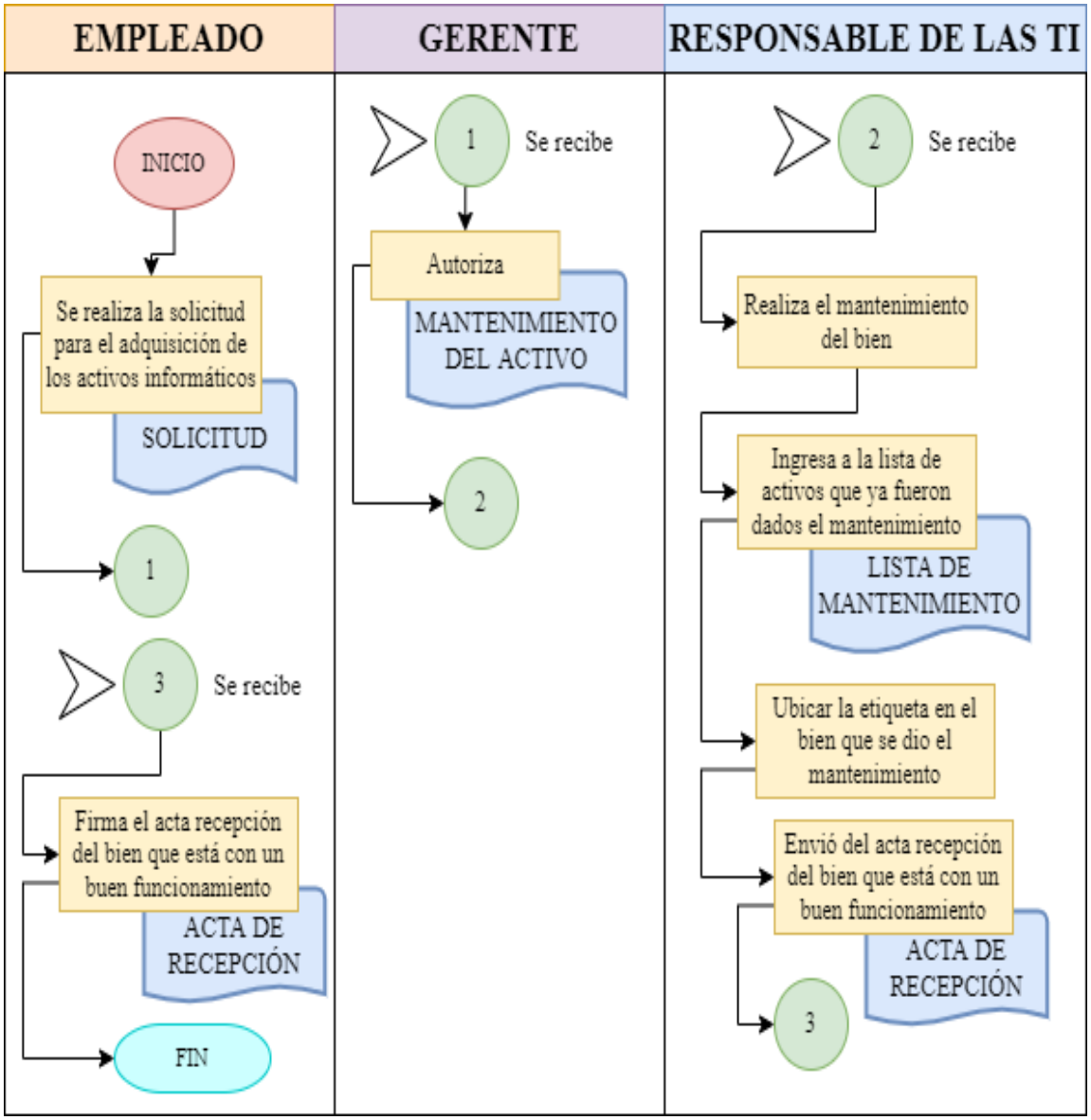


Gráfico 25. Flujograma de Políticas y procedimientos para los procesos informáticos - mantenimiento

Fuente: (Cepeda Carolina, 2022)

4. REVISIÓN

Aquí se debe examinar el rendimiento de la entidad conjuntamente con los cambios significativos, luego se procede a revisar el riesgo y el desempeño, y finalmente se analiza minuciosamente la mejora de la gestión del riesgo empresarial (Instituto de Auditores Internos, 2017).

Tabla 46. Check List de Control Interno de los procesos informáticos – Adquisición

La Bahía

CHECK LIST DE CONTROL INTERNO DE LOS PROCESOS INFORMÁTICOS

No.	DESCRIPCIÓN	RESPUESTA		OBSERVACIONES
		SI	NO	
ADQUISICIÓN DE LOS ACTIVOS INFORMÁTICOS				
1	¿Existen políticas para la compra de activos informáticos?			
2	¿Se realiza acta de entrega de los bienes a la persona encargada del mismo?			
3	¿Los bienes adquiridos son etiquetados y a la vez codificados?			
4	¿Toda adquisición de bienes es sustentada con un comprobante de venta?			
5	¿Se tiene un correcto orden de toda la documentación de las compras de los activos?			
6	¿Se realiza actas de recepción de los bienes?			
7	¿Poseen un archivo digital en donde se cargue todas las compras realizadas?			
8	¿Las compras se realizan previa autorización de Gerencia?			
9	¿Se emite una solicitud de compra del activo?			
10	¿Para la selección de proveedor de los bienes se cotiza un mínimo de cuatro proveedores?			
11	¿Se registra los comprobantes que sustente la compra del bien inmediatamente?			
12	¿Cada vez que se realiza una nueva adquisición se actualiza el listado de activos informáticos?			
13	¿Existe un responsable que coloque las etiquetas y codificaciones en el bien?			

G.P.P.
14/14

Fuente: (Cepeda Carolina, 2022)

Tabla 47. Check List de Control Interno de los procesos informáticos - Mantenimiento

La Bahía

CHECK LIST DE CONTROL INTERNO DE LOS PROCESOS INFORMÁTICOS

No.	DESCRIPCIÓN	RESPUESTA		OBSERVACIONES
		SI	NO	
MANTENIMIENTO DE LOS ACTIVOS INFORMÁTICOS				
1	¿Se realiza una solicitud para pedir el mantenimiento de un bien?			
2	¿Existe una persona responsable del mantenimiento de los activos informáticos?			
3	¿El mantenimiento es autorizado por el Gerente General?			
4	¿Cada activo que haya tenido el respectivo mantenimiento posee una etiqueta que lo distinga?			
5	¿Se realiza una lista de los activos que ya fueron dados el mantenimiento?			
6	¿Se constata físicamente los activos informáticos?			
7	¿La constatación física de los activos se realiza frecuentemente?			
8	¿Se realiza un acta de recepción del activo en buen funcionamiento?			
9	¿Se efectúa mantenimientos de activos por terceras personas?			
10	¿Los activos informáticos ya hechos el mantenimiento tienen otra codificación?			
11	¿El responsable de las TI lo realiza efectivamente el mantenimiento?			
12	¿El mantenimiento del bien es rápido?			

Fuente: (Cepeda Carolina, 2022)

5. INFORMACIÓN, COMUNICACIÓN Y REPORTE

Se realiza un proceso de intercambio de información en donde se analiza las fuentes internas como externas, las mismas que pueden fluir a lo largo de todos los niveles de la organización (Instituto de Auditores Internos, 2017).

G.I.P.
15/14

CARTA DE PRESENTACIÓN DEL DISEÑOS DEL SISTEMA DE CONTROL INTERNO A LOS PROCESOS INFORMÁTICOS

Ambato, 25 de abril del 2022

Sra.

Rosa Benigna Torres Rodríguez

Gerente Propietaria de la Empresa “La Bahía”

Presente

De mi consideración:

Como es de su conocimiento, se ha efectuado un respectivo diagnóstico a los procesos informáticos por medio del control interno de la empresa“La Bahía” para el año terminado en diciembre del 2021.

Mi responsabilidad consiste en presentar el “Diseño del Sistema de Control Interno a los procesos informáticos”. Teniendo en cuenta que la administración podrá considerar la propuesta con el fin de implementarla y mantener una estructura adecuada del control interno para los procesos informáticos alcanzando los objetivos establecidos por la empresa.

El diagnóstico y diseño del sistema de control interno se elaboró en base a los cinco componentes del COBIT 5. La indicada evaluación contribuyó de manera significativa a la obtención de fortalezas y debilidades en su manejo, de esta manera se valoró el riesgo de que existan debilidades importantes, a la vez evaluar la efectividad del diseño y la operación del control interno en base al riesgo valorado.

El diseño del sistema de control interno a los procesos informáticos tiene como objetivo principal salvaguardar los activos informáticos que posee la empresa. Además, se incluye políticas, controles y procedimientos que deberán ser consideradas por el responsable en el manejo de dichos bienes. La finalidad del sistema de control interno es proveer la seguridad e integridad de la información.

1.- GOBIERNO Y CULTURA	
Planificación Estratégica	Reconocimiento de los riesgos en los procesos informáticos

2.- ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS	
Identificación de objetivos de los procesos	Estrategias para riesgos en los procesos

por cada uno de los cinco componentes.

Gráfico 26. Dominios del COBIT 5
Fuente: (Cepeda Carolina, 2022)

En el caso de que la empresa decida efectuar la propuesta dada, se le recomienda a la Gerente capacitar al personal sobre el correcto manejo del sistema de control interno propuesto, con ello podrán cumplir eficientemente todos sus objetivos.

Atentamente,

Eliana Carolina Cepeda Cruz
1804392882
carolinacepe1999@gmail.com

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- **En base al objetivo 1:** Se puede concluir que en base al diagnóstico previo que se realizó en la empresa a la Gerente y contadora, se constató que el personal desconocía el valor que tienen los activos informáticos ante la empresa, teniendo en cuenta que los mismos no poseen ningún tipo de control.
- **En el objetivo 2:** En donde se aplicó la metodología COBIT 5 con sus cinco componentes y principios, se evaluó cada proceso informático que tiene la empresa, teniendo como riesgo alto el desconocimiento total sobre los procesos informáticos, en base a la metodología también se pudo encontrar que no existe una capacitación adecuada sobre las TI.
- **Finalmente, en el objetivo 3:** Con el diseño del Sistema de Control Interno a los procesos informáticos, la empresa contará con un manejo adecuado de los activos informáticos en base a los cinco componentes de la metodología COBIT.

4.2 Recomendaciones

- Se recomienda implementar el Sistema de Control Interno para los procesos informáticos, en vista de que está hecho de acuerdo con las situaciones presentadas en la empresa, por lo cual se deberá planificar un cronograma de capacitación que sea dirigido a todo el personal y de manera obligatoria al personal involucrado.
- Se sugiere revisar periódicamente las políticas y procedimientos de los procesos informáticos que fueron establecidas en el Sistema de Control Interno, con el propósito de ejecutar el trabajo de forma eficiente.
- Invertir en un fireware que ayude a resguardar la información confidencial de toda la empresa, el mismo que tiene como función principal crear una barrera entre el internet y la empresa, teniendo en cuenta que en la actualidad se puede fugar información por medio del internet.

BIBLIOGRAFÍA

Alarcón, A., González, J., & Rodríguez, S. (2011). Guía para pymes desarrolladoras de software, basada en la norma ISO / IEC 15504. *Revista Virtual Universidad Católica Del Norte*, *34*(0124–5821), 1–29. Guía para pymes desarrolladoras ISO / IEC 15504

Almanza - Gomez, A. I. (2012). *La Aplicación de COBIT en las organizaciones ¿Vale la pena el esfuerzo?*

Alvarado, P. (2021). *El comercio electrónico va por otro año de crecimiento*. El Comercio. https://www.elcomercio.com/actualidad/negocios/comercio-electronico-ofertas-mercados-ventas.html

Arévalo, M. C. (2020). *Así puedes documentar un activo de información*. Pirani Blog. https://www.piranirisk.com/es/blog/como-documentar-un-activo-de-informacion#:~:text=Los activos de información son,propuestos desde la alta dirección

Avilés, D. (2020). *Las Estrategias de Marketing en la Venta de Electrodomésticos en la Ciudad de Guayaquil*. Universidad Católica de Santiago de Guayaquil.

Bertolin Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información* (Edición Pa).

Blanco Encinosa, L. J. (2008). *Auditoría y sistemas informáticos* (Editorial).

Cabrera, C., & Ortega, A. (2013). La efectividad del control interno de las empresas de transporte urbano. *Dictamen LIbre*, *12*(13), 96–104. file:///C:/Users/User/Desktop/tesishecha/Dialnet-LaEfectividadDelControlInternoDeLasEmpresasDeTrans-6578964.pdf

Cajiao, M. E., García, M. A., & Jimbo, M. (2016). *Auditoría Administrativa y de gestión*.

Centro de Investigaciones Económicas y de la Micro, P. y M. E. (2011). Flacso -

MIPRO. *Centro de Investigaciones Económicas y de La Micro, Pequeña y Mediana Empresa*, *17*, 1–26.

Comité Directivo de COBIT, & IT Governance Institute. (2000). *Cobit Marco Referencial* (Tercera). www.itgovernance.org

Conejos Merita, P. (2018). Marco de apetito y tolerancia al riesgo. In *Icade Bussiness School*. Universidad Pontificia ICAI ICADE Comillas Madrid.

Coopers & Lybrand. (1997). *Los nuevos conceptos del control interno (INFORME COSO)* (Diaz de Sa).

Daltabuit, E., Hernández, L., Mallén, G., & Vázquez, J. de J. (2007). *La seguridad de la información* (Limusa S.A).

Diogo Reis, L. C. (2015). Fundamentos de COBIT 5. *Escola Superior de Redes CEDIA*, 1–129. https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI5.pdf

El Universo. (2020). *Industria de línea blanca empieza a recuperarse en ventas tras confinamiento por la pandemia*. El Universo. https://www.eluniverso.com/noticias/2020/07/13/nota/7905210/industria-linea-blanca-ventas-reactivacion-economica-pandemia/

Espino, M. (2014). *Fundamentos de auditoría* (Grupo Edit).

Estupiñan Rodrigo. (2015). Control interno y fraudes. In *Control interno y fraudes* (Ecoe Edici, pp. 1–20). https://www.ecoeediciones.com/wp-content/uploads/2015/07/Control-interno-y-fraudes-3ra-Edición.pdf

Gamboa, J., Puente, S., & Vera, P. (2016). Importancia del control interno en el sector público. *Revista Publicando*, *3*(8), 487–502.

Gómez, R., Pérez, D., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, *31*, 109–118. http://www.redalyc.org/articulo.oa?id=121015012006

Grimaldo, L. carina. (2017). La importancia de las auditorias internas y externas dentro de las organizaciones. In *Conatbilidad y negocios* (Vol. 1, Issue 25). www.pearsoneducacion.net/arens%250Ahttps://skarlethcruzgaitan.files.wordpress.com/2016/04/auditoria-un-enfoque-integral-11ma-ed-alvin-a-arens-randal-j-elder-mark-s-beasley-libro-de-maestrc3ada.pdf%250Ahttp://www.unilibre.edu.co/bogota/pdfs/2016/4sin/B20.p

Hernández Trasobares, A. (2003). Los sistemas de información: evolución y desarrollo. *Proyecto Social: Revista de Relaciones Laborales*, *10*, 149–165.

IBM. (2010). *Adición de sistemas de punto final a la red de Management Central*. https://www.ibm.com/docs/es/i/7.1?topic=system-adding-endpoint-systems-your-management-central-network

Industria y Comercio Superintendencia. (2018). Metodología para la idenficación, clasificación y valoración de activos de información. *Angewandte Chemie International Edition*, *6*(11), 1–16.

Instituto de Auditores Internos. (2017). Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño - Resumen Ejecutivo. *Auditores Internos de España PwC*, *0*, 16. https://auditoresinternos.es/uploads/media_items/coso-2018-esp.original.pdf

ISACA. (2012a). COBIT 5 Un Marco de negocio para el Gobierno y la Gestión de las TI de la Empresa. In *Guía de inspiración para la implementación de PRME: Segunda Edición: Aprender para Avanzar* (Vol. 147, Issue 17). https://doi.org/10.9774/gleaf.9781783537846_16

ISACA. (2012b). *Procesos Catalizadores*.

Jiménez, M. (2011). *Guía didáctica Auditoría de Control Interno I Módulo : I Segundo Semestre*. https://www.utpl.edu.ec/

Laudon, K. C., & Laudon, J. P. (2012). Sistemas de informacion gerencial. In *Pearson Educación*.

Lind, D. A., Marchal, W. G., & Wathen, S. A. (2012). Estadística aplicada a los negocios y la economía. In *The Mc Graw-Hill* (Decimoquin). https://eduvirtual.cuc.edu.co/moodle/mod/resource/view.php?id=386224

Lopez, A. A., & Cañizares, M. (2018). El control interno en el sector público ecuatoriano. Caso de Estudio: gobiernos autónomos descentralizados cantonales de Morona Santiago Internal. *Cofin Habana*, *2*, 124–146.

Mantilla, S. (2013). *Auditoría del control interno* (Eco Edicio).

Mantilla, S. (2018). *Auditoría del Control Interno* (A. García Reyes (ed.); Cuarta Edi). Ecoe Ediciones.

Mendoza-Walter, Delgado-María, Ponce-Tania, C.-I. (2018). El control interno y su influencia en la gestión administrativa del sector público Internal. *Revista Científica Dominio de Las Ciencias*, *4*(4), 206–240. http://dx.doi.org/10.23857/dom.cien.pocaipURL:http://dominiodelasciencias.com/ojs/index.php/es/indexNúmeroPublicadoel28deoctubrede2018

Ministerio de Industrias y Productividad. (2015). *Línea Blanca* (pp. 1–25). Bain & Company.

Mora, J., León, J., Huilcapi, M., & Escobar, D. (2017). El modelo COBIT 5 para auditoría y el control de los sistemas de información. *Universidad Técnica de Babahoyo*, 1–16. https://doi.org/2550-679X

Muñoz-Razo, C. (2011). *Cómo elaborar y asesorar una investigación de tesis* (L. Gaona - Figueroa & F. Hernández - Carrasco (eds.); Segunda Ed). Pearson Educación de México, S.A. de C.V.

Nación, L. (2020). *El Sector Comercial prevee mejores ventas*. La Nación. https://lanacion.com.ec/el-sector-comercial-preve-mejores-ventas/

Panchi Arias, M. P. (2021). La auditoría interna como herramienta de control y seguimiento de la gestión en las universidades. *Universidad y Sociedad*, *13*(3), 333–341.

Pérez-Mergarejo, E., Pérez-Vergara, I., & Rodríguez-Ruíz, Y. (2014). Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. *Ingeniería Industrial*, *35*(2), 1–13. http://ezproxy.uniandes.edu.co:8080/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=108922111&lang=es&site=eds-live&scope=site

Pérez-Rojas, A., Medina-Marin, J., Corona-Armenta, J. R., & Montaño-Arango, O. (2010). Modelo que identifica la madurez de los procesos. *Organización y Dirección de Empresas*, *85*(2003), 392–400.

Picón, D., & Melian, Y. (2014). La unidad de análisis en la problemática enseñanza-aprendizaje. *Universidad Nacional de La Patagonia Austral*, *2*, 101–117. https://dialnet.unirioja.es/descarga/articulo/5123550.pdf

Purificación Aguilera López. (2010). *Seguridad Informatica* (Editorial).

Quinaluisa Morán, N. V., Ponce Álava, V. A., Muñoz Macías, S. C., Ortega Haro, X. F., & Pérez Salazar, J. A. (2018). El control interno y sus herramientas de aplicación entre COSO y COCO. *Cofin Habana*, *12*(1), 268–283.

Robledano, A. (2019). *Qué es MySQL: Características y ventajas*. https://openwebinars.net/blog/que-es-mysql/

Santacruz Espinoza, J. J., Vega Abad, C. R., Pinos Castillo, L. F., & Cárdenas Villavicencio, O. E. (2017). Sistema cobit en los procesos de auditorías de los de sistemas informáticos. *Revista Ciencia e Investigación*, *2*(8), 65–68. https://doi.org/10.26910/issn.2528-8083vol2iss8.2017pp65-68

Serrano Carrión, P. A., Señalin Morales, L. O., Vega Jaramillo, F. Y., & Herrera Peña, J. N. (2018). El control interno como herramienta indispensable para una gestión financiera y contable eficiente en las empresas bananeras del cantón Machala (Ecuador). *Espacios*, *39*(3).

Velásquez Pérez, T., Puentes Velásquez, A. M., & Pérez Pérez, Y. M. (2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. *Tecnura*, 159–169.

https://doi.org/10.14483/udistrital.jour.tecnu-ra.2015.SE1.a14

Villa, C., Samaniego, F. del R., & Vargas, D. (2017). Sistema de Control Interno para determinar el riesgo empresarial en la provincia de Chimborazo: Caso GAD Cantón Guano. *Revista de Investigación Talentos*, *4*(1), 31–38. http://www.ueb.edu.ec/app/talentos/images/PDF/REVISTA-TALENTOS/VOLUMEN-IV-N1/SISTEMA DE CONTROL INTERNO PARA DETERMINAR EL RIESGO.pdf

Villardefrancos Alvarez, M., & Rivera, Z. (2006). La auditoría como proceso de control: Concepto y tipología. *Ciencias de La Información*, *37*(2–3), 53–59.

Vivar Gualsaquí, C. J. (2013). *Desarrollo del Marco de referencia Cobit 5.0 para la Gestión del Área de TI de la empresa Blue Card*.

Yustas, J. C. (2015). ¿ Qué es un Cortafuegos (Firewall) para Internet ? *Autores Científico-Técnicos y Académicos*, 1–9. https://www.acta.es/medios/articulos/internet/010095.pdf